aws

Benutzerhandbuch

Amazon Macie

Amazon Macie: Benutzerhandbuch

Table of Contents

Was ist Amazon Macie? 1
Funktionen von Amazon Macie 2
Zugriff auf Amazon Macie 5
Preise für Amazon Macie 6
Zugehörige Services 7
Erste Schritte 9
Bevor Sie beginnen 9
Schritt 1: Amazon Macie aktivieren 9
Schritt 2: Konfigurieren Sie ein Repository für die Ergebnisse der Erkennung sensibler Daten 10
Schritt 3: Erkunden Sie die Ergebnisse der Beispiele 11
Schritt 4: Erstellen Sie einen Job, um sensible Daten zu ermitteln 12
Schritt 5: Überprüfen Sie Ihre Ergebnisse 14
Konzepte und Terminologie 16
Konto 16
Administratorkonto 16
Zulassungsliste 17
automatisierte Erkennung sensibler Daten 17
AWS Security Finding Format (ASFF) 18
klassifizierbare Byte oder Größe 18
klassifizierbares Objekt 18
benutzerdefinierte Daten-ID 19
Filterregel 19
Ergebnis 19
Ereignis finden 20
Auftrag 20
ID für verwaltete Daten 20
Mitgliedskonto 21
Organisation 21
Festlegung von Richtlinien 21
Befund einer Stichprobe 22
Feststellung sensibler Daten 22
Job zur Entdeckung sensibler Daten 22
Ergebnis der Entdeckung sensibler Daten 23
eigenständiges Konto 23

unterdrückter Befund ... 23
Unterdrückungsregel ... 24
nicht klassifizierbare Byte oder Größe ... 24
nicht klassifizierbares Objekt ... 24
Überwachung von Datensicherheit und Datenschutz ... 26
So überwacht Macie die Amazon S3 S3-Datensicherheit ... 27
Zentrale Komponenten ... 28
Datenaktualisierungen ... 31
Weitere Überlegungen ... 32
Bewertung Ihrer Amazon S3-Sicherheitslage ... 34
Anzeigen des Dashboards ... 35
Grundlegendes zu Dashboard-Komponenten ... 36
Grundlegendes zu Datensicherheitsstatistiken im Dashboard ... 41
Amazon S3 ... 45
Überprüfen Ihres S3-Bucket-Bestands ... 46
Filtern Ihres S3-Bucket-Inventars ... 58
Macie den Zugriff von S3-Buckets und -Objekten erlauben ... 72
Erkennen vertraulicher Daten ... 77
Verwenden von verwalteten Datenbezeichnern ... 80
Anforderungen an Schlüsselwörter ... 81
Kurzreferenz nach sensiblem Datentyp ... 82
Detaillierte Referenz nach Kategorien sensibler Daten ... 96
Erstellen von benutzerdefinierten Datenbezeichnern ... 138
Definition von Erkennungskriterien ... 139
Einstellungen für den Schweregrad definieren ... 141
Erstellen benutzerdefinierter Datenkennungen ... 143
Regex-Unterstützung ... 146
Definition von Ausnahmen für sensible Daten mit Zulassungslisten ... 147
Optionen und Anforderungen für Zulassungslisten ... 148
Erlaubnislisten erstellen und verwalten ... 161
Durchführung automatisierter Erkennung vertraulicher Daten ... 181
So funktioniert die automatische Erkennung ... 182
Konfiguration der automatischen Erkennung für Ihr Konto ... 190
Verwaltung der automatisierten Erkennung für einzelne S3-Buckets ... 201
Bewertung des Umfangs automatisierter Entdeckungen ... 204
Überprüfung der Statistiken und Ergebnisse der automatisierten Erkennung ... 218

Empfindlichkeitsbewertung für S3-Buckets ... 247
Standardeinstellungen für die automatische Erkennung ... 255
Ausführen von Erkennungsaufgaben für vertrauliche Daten ... 266
Bereichsoptionen für Aufgaben ... 268
Erstellen eines-Auftrags ... 282
Überprüfung der Jobstatistiken und Ergebnisse ... 295
Überwachen von Aufträgen ... 300
Verwalten von Aufträgen ... 319
Prognose und Überwachung der Arbeitskosten ... 330
Für Jobs empfohlene Identifikatoren verwalteter Daten ... 334
Analysieren verschlüsselter S3-Objekte ... 337
Verschlüsselungsoptionen für S3-Objekte ... 338
Macie erlauben, einen vom Kunden verwalteten zu verwenden AWS KMS key ... 341
Speicherung und Beibehaltung der Erkennungsergebnisse von vertraulichen Daten ... 347
Übersicht ... 349
Schritt 1: Überprüfen Sie Ihre Berechtigungen ... 351
Schritt 2: Konfigurieren Sie ein AWS KMS key ... 352
Schritt 3: Wählen Sie einen S3-Bucket ... 356
Unterstützte Speicherklassen und -formate ... 365
Unterstützte Speicherklassen ... 366
Unterstützte Datei- und Speicherformate ... 367
Analyse der Ergebnisse ... 370
Arten von Ergebnissen ... 372
Arten von Richtlinienergebnissen ... 373
Arten von Erkenntnissen zu sensiblen Daten ... 376
Arbeiten mit Stichprobenergebnissen ... 377
Beispielergebnisse erstellen ... 378
Überprüfung der Stichprobenergebnisse ... 380
Unterdrücken von Stichprobenergebnissen ... 382
Überprüfung der Ergebnisse ... 383
Filtern von Ergebnissen ... 387
Grundlagen des Filters ... 388
Filter erstellen und anwenden ... 397
Filterregeln erstellen und verwalten ... 407
Felder zum Filtern von Ergebnissen ... 416
Untersuchung sensibler Daten anhand von Ergebnissen ... 454

Erkennen sensibler Daten ... 455
Stichproben sensibler Daten werden abgerufen ... 459
Schema für Speicherorte sensibler Daten ... 504
Unterdrücken von Ergebnissen ... 515
Unterdrückungsregeln erstellen ... 517
Überprüfung unterdrückter Ergebnisse ... 520
Unterdrückungsregeln ändern ... 521
Löschen von Unterdrückungsregeln ... 523
Bewertung des Schweregrads der Ergebnisse ... 525
Bewertung des Schweregrads von politischen Ergebnissen ... 526
Bewertung des Schweregrads von Ergebnissen sensibler Daten ... 527
Überwachung und Verarbeitung von Ergebnissen ... 535
Konfigurieren von Veröffentlichungseinstellungen für Ergebnisse ... 536
Auswählen von Veröffentlichungszielen ... 537
Bestimmung der Veröffentlichungshäufigkeit ... 538
Ändern der Veröffentlichungshäufigkeit ... 539
EventBridge-Integration ... 540
Arbeiten mit EventBridge ... 541
EventBridgeRegeln für Ergebnisse erstellen ... 542
Integration in Security Hub ... 546
Wie Macie Ergebnisse in Security Hub veröffentlicht ... 547
Beispiele für Macie-Erkenntnisse in Security Hub ... 552
Aktivieren und Konfigurieren der Security Hub-Integration ... 558
Einstellung der Veröffentlichung von Erkenntnissen in Security Hub ... 559
Integration von Benutzerbenachrichtigungen ... 559
Arbeiten mit AWS-Benutzerbenachrichtigungen arbeiten arbeiten ... 560
Aktivieren und Konfigurieren von Benachrichtigungen für Ergebnisse aktivieren und konfigurieren ... 561
Zuordnen von Benachrichtigungsfeldern zu Suchfeldern ... 563
Änderung der Benachrichtigungseinstellungen für Ergebnisse ... 567
Benachrichtigungen für Ergebnisse deaktivieren ... 567
EventBridge Ereignisschema für Ergebnisse ... 568
Schema des Ereignisses ... 569
Beispiel für ein Ereignis für ein Richtlinienergebnis ... 569
Beispiel für ein Ereignis, bei dem sensible Daten gefunden wurden ... 574
Prognose und Überwachung der Kosten ... 580

Verstehen, wie die geschätzten Nutzungskosten berechnet werden 580
Überprüfung der geschätzten Nutzungskosten 584
Überprüfung der geschätzten Nutzungskosten auf der Konsole 585
Abfrage der geschätzten Nutzungskosten mit der API 586
Teilnahme an der kostenlosen Testversion 591
Verwalten mehrerer Konten 595
Beziehungen zwischen Administrator- und Mitgliedskonten 596
Verwaltung von Konten mit AWS Organizations 601
Überlegungen und Empfehlungen 602
Integration und Konfiguration einer Organisation 606
Überprüfung der Unternehmenskonten 616
Verwaltung von Mitgliedskonten 620
Benennen eines anderen Administratorkontos 628
Deaktivierung der Integration mit AWS Organizations 631
Mitgliedskonten nach Einladung verwalten 633
Überlegungen und Empfehlungen 634
Erstellen und Verwalten einer Organisation 638
Überprüfung der Organisationskonten 651
Benennen eines anderen Administratorkontos 656
Verwaltung Ihrer Mitgliedschaft in einer Organisation 657
Sicherheit 663
Datenschutz 664
Verschlüsselung im Ruhezustand 665
Verschlüsselung während der Übertragung 665
Identity and Access Management 665
Zielgruppe 666
Authentifizierung mit Identitäten 666
Verwalten des Zugriffs mit Richtlinien 670
Wie arbeitet Macie mit IAM 673
Beispiele für identitätsbasierte Richtlinien 683
Service-verknüpfte Rollen 693
Von AWS verwaltete Richtlinien 697
Fehlerbehebung 703
Protokollierung und Überwachung 705
Compliance-Validierung 705
Ausfallsicherheit 706

Sicherheit der Infrastruktur 707
VPC-Endpunkte (AWS PrivateLink) 707
Überlegungen zu Macie VPC-Endpunkten 708
Erstellen eines Schnittstellen-VPC-Endpunkts für Macie 708
Protokollieren von API-Aufrufen 710
Macie-Informationen in CloudTrail 710
Macie-Protokolldateieinträge verstehen 711
Markieren von Ressourcen 717
Grundlagen des Taggens 717
Verwendung von Tags in IAM-Richtlinien 719
Hinzufügen von Tags zu Ressourcen 720
Stichwörter für Ressourcen überprüfen 724
Tags für Ressourcen bearbeiten 727
Entfernen von Tags von Ressourcen 730
Ressourcen erstellen mit AWS CloudFormation 733
Macie und Vorlagen AWS CloudFormation 733
Weitere Informationen zu AWS CloudFormation 734
Macie suspendieren oder deaktivieren 735
Macie suspendieren 735
Macie deaktivieren 736
Macie-Kontingente 739
Dokumentverlauf 743
..... dcclxix

Was ist Amazon Macie?

Amazon Macie ist ein Datensicherheitsservice, der sensible Daten mithilfe von Machine Learning und Musterabgleich entdeckt, Einblicke in Datensicherheitsrisiken bietet und automatischen Schutz vor diesen Risiken ermöglicht.

Um Sie bei der Verwaltung des Sicherheitsstatus des Amazon Simple Storage Service (Amazon S3) -Datenbestands Ihres Unternehmens zu unterstützen, stellt Macie Ihnen eine Bestandsaufnahme Ihrer S3-Buckets zur Verfügung und bewertet und überwacht die Buckets automatisch im Hinblick auf Sicherheit und Zugriffskontrolle. Wenn Macie ein potenzielles Problem mit der Sicherheit oder dem Datenschutz erkennt, wie einen Bucket, der öffentlich zugänglich wird, generiert Macie eine Erkenntnis, die Sie überprüfen und bei Bedarf korrigieren können.

Macie automatisiert auch die Erkennung und Berichterstattung vertraulicher Daten, um Ihnen ein besseres Verständnis der Daten zu vermitteln, die Ihr Unternehmen in Amazon S3 speichert. Um sensible Daten zu erkennen, können Sie die von Macie bereitgestellten integrierten Kriterien und Techniken, benutzerdefinierte Kriterien, die Sie definieren, oder eine Kombination aus beiden verwenden. Wenn Macie sensible Daten in einem S3-Objekt erkennt, generiert Macie einen Befund, um Sie über die vertraulichen Daten zu informieren, die Macie gefunden hat.

Zusätzlich zu den Ergebnissen stellt Macie Statistiken und andere Daten bereit, die Aufschluss über den Sicherheitsstatus Ihrer Amazon S3-Daten geben und darüber, wo sich sensible Daten in Ihrem Datenbestand befinden könnten. Die Statistiken und Daten können als Grundlage für Ihre Entscheidungen dienen, um eingehendere Untersuchungen bestimmter S3-Buckets und -Objekte durchzuführen. Sie können Ergebnisse, Statistiken und andere Daten mithilfe der Amazon Macie-Konsole oder der Amazon Macie-API überprüfen und analysieren. Sie können auch die Macie-Integration mit Amazon nutzenEventBridgeundAWS Security Hubum Ergebnisse mithilfe anderer Dienste, Anwendungen und Systeme zu überwachen, zu verarbeiten und zu korrigieren.

Themen

- Funktionen von Amazon Macie
- Zugriff auf Amazon Macie
- Preise für Amazon Macie
- Zugehörige Services

Funktionen von Amazon Macie

Hier sind einige der wichtigsten Möglichkeiten, mit denen Amazon Macie Ihnen helfen kann, Ihre vertraulichen Daten in Amazon S3 zu erkennen, zu überwachen und zu schützen.

Automatisieren Sie die Erkennung sensibler Daten

Mit Macie können Sie die Erkennung und Berichterstattung vertraulicher Daten auf zwei Arten automatisieren: indem Sie Macie so konfigurieren, dassautomatische Erkennung vertraulicher Daten durchführen, und vonAufgaben zur Erkennung vertraulicher Daten erstellen und ausführen. Wenn Macie vertrauliche Daten in einem S3-Objekt erkennt, erstellt es eine Suche nach vertraulichen Daten für Sie. Das Ergebnis enthält einen detaillierten Bericht über die sensiblen Daten, die Macie gefunden hat.

Die automatische Erkennung vertraulicher Daten bietet einen umfassenden Überblick darüber, wo sich sensible Daten in Ihrem Amazon S3-Datenbestand befinden könnten. Mit dieser Option wertet Macie kontinuierlich Ihr S3-Bucket-Inventar aus und verwendet Stichprobenverfahren, um repräsentative S3-Objekte aus Ihren Buckets zu identifizieren und auszuwählen. Macie ruft dann die ausgewählten Objekte ab, analysiert sie und untersucht sie auf sensible Daten.

Aufgaben zur Erkennung vertraulicher Daten ermöglichen tiefere, zielgerichtetere Analysen. Mit dieser Option definieren Sie die Breite und Tiefe der Analyse — die zu analysierenden S3-Buckets, die Stichprobentiefe und benutzerdefinierte Kriterien, die sich aus Eigenschaften von S3-Objekten ableiten. Sie können einen Job auch so konfigurieren, dass er nur einmal für Analysen und Bewertungen auf Abruf oder wiederholt für regelmäßige Analysen, Bewertungen und Überwachungen ausgeführt wird.

Beide Optionen können Ihnen helfen, einen umfassenden Überblick über die Daten, die Ihr Unternehmen in Amazon S3 speichert, sowie über alle Sicherheits- oder Compliance-Risiken für diese Daten zu erstellen und zu verwalten.

Entdecken Sie eine Vielzahl sensibler Datentypen

Um mit Macie sensible Daten zu ermitteln, können Sie integrierte Kriterien und Techniken wie maschinelles Lernen und Musterabgleich verwenden, um Objekte in S3-Buckets zu analysieren. Diese Kriterien und Techniken, bezeichnet alsIdentifikatoren für verwaltete Daten, kann für viele Länder und Regionen eine große und wachsende Liste vertraulicher Datentypen erkennen, darunter mehrere Arten von personenbezogenen Daten (PII), Finanzinformationen und Anmeldeinformationen.

Sie können auch verwendenbenutzerdefinierte Datenkennungen. Ein benutzerdefinierter Datenbezeichner ist eine Reihe von Kriterien, die Sie definieren, um vertrauliche Daten zu erkennen — ein regulärer Ausdruck (Regex), das ein übereinstimmendes Textmuster und optional Zeichenfolgen und eine Näherungsregel definiert, die die Ergebnisse verfeinern. Mit diesem Identifizierungstyp können Sie sensible Daten erkennen, die Ihre speziellen Szenarien, Ihr geistiges Eigentum oder Ihre urheberrechtlich geschützten Daten widerspiegeln. Sie können die von Macie bereitgestellten Identifikatoren für verwaltete Daten ergänzen.

Zur Feinabstimmung der Analysen können Sie auchListen zulassen. Erlauben Sie Listen, um bestimmten Text und Textmuster zu definieren, die Macie in S3-Objekten ignorieren soll. Dies sind in der Regel Ausnahmen für sensible Daten für Ihre speziellen Szenarien oder Umgebungen — zum Beispiel die Namen von Vertretern des öffentlichen Dienstes für Ihr Unternehmen, öffentliche Telefonnummern für Ihr Unternehmen oder Beispieldaten, die Ihre Organisation für Tests verwendet.

Daten für Sicherheit und Zugriffskontrolle auswerten und überwachen

Wenn Sie Macie aktivieren, generiert Macie automatisch ein vollständiges Inventar Ihrer S3-Buckets und beginnt damit, dieses zu verwalten. Macie beginnt auch mit der Bewertung und Überwachung der Buckets im Hinblick auf Sicherheit und Zugriffskontrolle. Wenn Macie ein potenzielles Problem mit der Sicherheit oder dem Datenschutz eines Buckets feststellt, erstellt es einpolitische Findungfür dich.

Neben spezifischen Ergebnissen wurde einDashboardbietet Ihnen eine Momentaufnahme der aggregierten Statistiken für Ihre Amazon S3-Daten. Dazu gehören Statistiken für wichtige Kennzahlen, z. B. wie viele Ihrer Buckets öffentlich zugänglich sind oder mit anderen geteilt werden.AWS-Konten. Sie können jede Statistik aufschlüsseln, um die unterstützenden Daten zu überprüfen.

Macie bietet auch detaillierte Informationen und Statistiken für einzelne S3-Buckets in Ihrem Inventar. Zu den Daten gehören Aufschlüsselungen der öffentlichen Zugriffs- und Verschlüsselungseinstellungen eines Buckets sowie die Größe und Anzahl der Objekte, die Macie analysieren kann, um sensible Daten im Bucket zu erkennen. Du kannststöbern Sie im Inventar, oder sortieren und filtern Sie das Inventar nach bestimmten Feldern. Wenn Sie einen Bucket auswählen, werden in einem Fenster die Details des Buckets angezeigt.

Überprüfen und analysieren Sie die Ergebnisse

In Macie ist ein Ergebnis ein detaillierter Bericht über sensible Daten, die Macie in einem S3-Objekt entdeckt, oder ein potenzielles Problem mit der Sicherheit oder dem Datenschutz eines

S3-Buckets. Jedes Ergebnis enthält einen Schweregrad, Informationen über die betroffene Ressource und zusätzliche Details, z. B. wann und wie Macie das Problem gefunden hat.

ZuErgebnisse überprüfen, analysieren und verwalten, du kannst das benutzenFeststellungenSeiten auf der Amazon Macie-Konsole. Auf diesen Seiten werden Ihre Ergebnisse aufgeführt und die Einzelheiten der einzelnen Ergebnisse aufgeführt. Sie bieten auch mehrere Optionen zum Gruppieren, Filtern, Sortieren und Unterdrücken von Ergebnissen. Sie können auch die Amazon Macie-API verwenden, um Ergebnisse abzufragen, abzurufen und zu unterdrücken. Wenn Sie die API verwenden, können Sie die Daten zur eingehenderen Analyse, Langzeitspeicherung oder Berichterstattung an eine andere Anwendung, einen anderen Dienst oder ein anderes System weitergeben.

Überwachen und verarbeiten Sie Ergebnisse mit anderen Diensten und Systemen

Um die Integration mit anderen Diensten und Systemen zu unterstützen, Macieveröffentlicht Ergebnisse auf AmazonEventBridgewie das Finden von Ereignissen. EventBridgeist ein serverloser Eventbus-Service, der Ergebnisdaten an Ziele weiterleiten kann, wieAWS LambdaFunktionen und Amazon Simple Notification Service (Amazon SNS) -Themen. MitEventBridge, können Sie die Ergebnisse im Rahmen Ihrer bestehenden Sicherheits- und Compliance-Workflows nahezu in Echtzeit überwachen und verarbeiten.

Sie können Macie auch so konfigurierenErgebnisse veröffentlichen unterAWS Security Hub. Security Hub ist ein Service, der einen umfassenden Überblick über Ihre Sicherheitslage in Ihrem gesamten Unternehmen bietetAWSUmgebung und hilft Ihnen dabei, Ihre Umgebung anhand von Sicherheitsstandards und bewährten Verfahren zu überprüfen. Mit Security Hub können Sie Ihre Ergebnisse im Rahmen einer umfassenderen Analyse der Sicherheitslage Ihres Unternehmens einfacher überwachen und verarbeitenAWS. Sie können auch Ergebnisse aus mehreren zusammenfassenAWS-Regionen, und überwachen und verarbeiten Sie dann aggregierte Ergebnisdaten aus einer einzigen Region.

Zentrale Verwaltung mehrerer Macie-Konten

Wenn deinAWSDie Umgebung hat mehrere Konten, Sie könnenMacie zentral verwaltenfür Konten in Ihrer Umgebung. Sie können dies auf zwei Arten tun, indem Sie Macie mit integrierenAWS Organizationsoder indem Sie Einladungen zur Mitgliedschaft in Macie senden und annehmen.

In einer Konfiguration mit mehreren Konten kann ein bestimmter Macie-Administrator bestimmte Aufgaben ausführen und auf bestimmte Macie-Einstellungen, Daten und Ressourcen für Konten zugreifen, die Mitglieder derselben Organisation sind. Zu den Aufgaben gehören die Überprüfung von Informationen über S3-Buckets, die Mitgliedskonten gehören, die Überprüfung

der Richtlinienergebnisse für diese Buckets und die Überprüfung der Buckets auf vertrauliche Daten. Wenn die Konten verknüpft sind überAWS Organizations, kann der Macie-Administrator Macie auch für Mitgliedskonten in der Organisation aktivieren.

Ressourcen programmgesteuert entwickeln und verwalten

Zusätzlich zur Amazon Macie-Konsole können Sie mit Macie interagieren, indem Sie dieAmazon Macie-API. Die Amazon Macie-API bietet Ihnen umfassenden, programmatischen Zugriff auf Ihre Macie-Kontoeinstellungen, Daten und Ressourcen.

Um programmgesteuert mit Macie zu interagieren, können Sie HTTPS-Anfragen direkt an Macie senden oder eine aktuelle Version einesAWSBefehlszeilentool oderAWSSDK.AWSstellt Tools und SDKs bereit, die aus Bibliotheken und Beispielcode für verschiedene Sprachen und Plattformen bestehen, wiePowerShell, Java, Go, Python, C++ und.NET.

Zugriff auf Amazon Macie

Amazon Macie ist in den meistenAWS-Regionen. Eine Liste der Regionen, in denen Macie derzeit verfügbar ist, finden Sie unterAmazon Macie-Endgeräte und Kontingentein derAllgemeine AWS-Referenz. Für Informationen zur VerwaltungAWS-Regionenfür deinAWS-Konto, siheSpezifizieren, welcheAWS-RegionenIhr Konto kannin derAWS Account ManagementReferenzhandbuch.

In jeder Region kannst du auf eine der folgenden Arten mit Macie zusammenarbeiten.

AWS Management Console

DerAWS Management Consoleist eine browserbasierte Oberfläche, mit der Sie erstellen und verwalten könnenAWSRessourcen. Als Teil dieser Konsole bietet die Amazon Macie-Konsole Zugriff auf Ihr Macie-Konto, Ihre Daten und Ressourcen. Mit der Macie-Konsole können Sie jede Macie-Aufgabe ausführen — Statistiken und andere Informationen zu Ihren S3-Buckets überprüfen, sensible Datenermittlungsaufträge erstellen und ausführen, Ergebnisse überprüfen und analysieren und vieles mehr.

AWSBefehlszeilentools

MitAWSBefehlszeilentools, Sie können Befehle an der Befehlszeile Ihres Systems ausführen, um Macie-Aufgaben auszuführen undAWSAufgaben. Die Verwendung der Befehlszeile kann schneller und bequemer sein als die Verwendung der Konsole. Die Befehlszeilen-Tools können auch beim Erstellen von Skripts für -Aufgaben hilfreich sein.

AWS bietet zwei Sätze an Befehlszeilen-Tools: AWS Command Line Interface (AWS CLI) und AWS Tools for PowerShell. Weitere Informationen zum Installieren und Konfigurieren der AWS CLI finden Sie im AWS Command Line InterfaceLeitfaden. Für Informationen zur Installation und Verwendung der Tools fürPowerShell, sieheAWS Tools for PowerShellBenutzerleitfaden.

AWS-SDKs

AWSstellt SDKs bereit, die aus Bibliotheken und Beispielcode für verschiedene Programmiersprachen und Plattformen bestehen — zum Beispiel Java, Go, Python, C++ und.NET. Die SDKs bieten bequemen, programmatischen Zugriff auf Macie und andereAWS-Services. Sie erledigen auch Aufgaben wie das kryptografische Signieren von Anfragen, die Verwaltung von Fehlern und das automatische Wiederholen von Anfragen. Für Informationen zur Installation und Verwendung desAWSSDKs, sieheTools, auf denen man aufbauen kannAWS.

Amazon Macie REST-API

Die Amazon Macie REST-API bietet Ihnen umfassenden, programmatischen Zugriff auf Ihr Macie-Konto, Ihre Daten und Ressourcen. Mit dieser API können Sie HTTPS-Anfragen direkt an Macie senden. Im Gegensatz zuAWSBefehlszeilentools und SDKs. Die Verwendung dieser API erfordert, dass Ihre Anwendung grundlegende Details verarbeitet, z. B. einen Hash generiert, um eine Anfrage zu signieren. Informationen zu dieser API finden Sie in derAmazon Macie API-Referenz.

Preise für Amazon Macie

Wie bei anderenAWSProdukte, es gibt keine Verträge oder Mindestverpflichtungen für die Nutzung von Amazon Macie.

Die Preisgestaltung von Macie basiert auf mehreren Dimensionen: Bewertung und Überwachung von S3-Buckets für Sicherheit und Zugriffskontrolle, Überwachung von S3-Objekten für die automatische Erkennung vertraulicher Daten und Analyse von S3-Objekten, um sensible Daten in den Objekten zu erkennen und zu melden. Weitere Informationen finden Sie unterPreise für Amazon Macie.

Um Ihnen zu helfen, die Kosten für die Nutzung von Macie zu verstehen und zu prognostizieren, stellt Macie die geschätzten Nutzungskosten für Ihr Konto bereit. Du kannstüberprüfe diese Schätzungenauf der Amazon Macie-Konsole und greifen Sie mit der Amazon Macie-API auf sie zu. Je nachdem, wie Sie den Dienst nutzen, können zusätzliche Kosten für die Nutzung anderer Dienste anfallenAWS-Servicesin Kombination mit bestimmten Macie-Funktionen, z. B. dem Abrufen von Bucket-Daten aus Amazon S3 und der Verwendung von kundenverwaltetenAWS KMS keysum Objekte für die Analyse zu entschlüsseln.

Wenn Sie Macie zum ersten Mal aktivieren, wird IhrAWS-Kontowird automatisch für die kostenlose 30-Tage-Testversion von Macie angemeldet. Dazu gehören einzelne Konten, die als Teil einer Organisation in aktiviert sindAWS Organizations. Während der kostenlosen Testphase fallen für die Nutzung von Macie keine Gebühren anAWS-Regionzur Bewertung und Überwachung Ihrer S3-Buckets im Hinblick auf Sicherheit und Zugriffskontrolle. Abhängig von Ihren Kontoeinstellungen kann die kostenlose Testversion auch die automatische Erkennung vertraulicher Daten für Ihre Amazon S3-Daten beinhalten. Die kostenlose Testversion beinhaltet nicht die Ausführung von Aufträgen zur Erkennung vertraulicher Daten zur Erkennung und Meldung vertraulicher Daten in S3-Objekten.

Um Ihnen zu helfen, die Kosten für die Nutzung von Macie nach Ablauf der kostenlosen Testversion zu verstehen und zu prognostizieren, stellt Macie Ihnen geschätzte Nutzungskosten auf der Grundlage Ihrer Nutzung von Macie während der Testphase zur Verfügung. Ihre Nutzungsdaten geben auch an, wie viel Zeit bis zum Ende Ihrer kostenlosen Testversion verbleibt. Du kannstüberprüfe diese Datenauf der Amazon Macie-Konsole und greifen Sie mit der Amazon Macie-API darauf zu.

Zugehörige Services

Um Ihre Daten, Workloads und Anwendungen weiter zu sichern inAWS, erwägen Sie, Folgendes zu verwendenAWS-Servicesin Kombination mit Amazon Macie.

AWS Security Hub

AWS Security Hubgibt Ihnen einen umfassenden Überblick über den Sicherheitsstatus IhresAWSRessourcen und hilft Ihnen bei der Überprüfung IhrerAWSUmwelt im Vergleich zu den Standards und bewährten Verfahren der Sicherheitsbranche. Dies geschieht teilweise, indem es Ihre Sicherheitsergebnisse aus mehreren Quellen verarbeitet, aggregiert, organisiert und priorisiert.AWS-Services(einschließlich Macie) und unterstütztAWSProdukte des Partner Network (APN). Security Hub hilft Ihnen, Ihre Sicherheitstrends zu analysieren und die Sicherheitsprobleme mit der höchsten Priorität in Ihrem Unternehmen zu identifizierenAWSUmwelt.

Weitere Informationen über Security Hub finden Sie auf derAWS Security HubBenutzerleitfaden. Weitere Informationen zur gleichzeitigen Verwendung von Macie und Security Hub finden Sie unterAmazon MacieIntegration mit AWS Security Hub.

Amazon GuardDuty

AmazonasGuardDutyist ein Sicherheitsüberwachungsdienst, der bestimmte Arten von analysiert und verarbeitetAWSProtokolle, wieAWS CloudTrailDatenereignisprotokolle für Amazon S3

undCloudTrailVerwaltungsereignisprotokolle. Es verwendet Feeds mit Bedrohungsinformationen, wie Listen bösartiger IP-Adressen und Domänen, und maschinelles Lernen, um unerwartete und potenziell unbefugte und bösartige Aktivitäten in IhremAWSUmwelt.

Um mehr zu erfahren überGuardDuty, sieheAmazonasGuardDutyBenutzerleitfaden.

Um mehr über weitere zu erfahrenAWSSicherheitsdienste, sieheSicherheit, Identität und Compliance aufAWS.

Erste Schritte mit Amazon Macie

Dieses Tutorial bietet eine Einführung in Amazon Macie. Sie erfahren, wie Sie Macie für Ihr aktivieren. AWS-Konto Außerdem erfahren Sie, wie Sie Ihren Sicherheitsstatus bei Amazon Simple Storage Service (Amazon S3) beurteilen und wichtige Macie-Einstellungen für die Erkennung und Meldung sensibler Daten in Ihren S3-Buckets konfigurieren können.

Aufgaben

- Bevor Sie beginnen
- Schritt 1: Amazon Macie aktivieren
- Schritt 2: Konfigurieren Sie ein Repository für die Ergebnisse der Erkennung sensibler Daten
- Schritt 3: Erkunden Sie die Ergebnisse der Beispiele
- Schritt 4: Erstellen Sie einen Job, um sensible Daten zu ermitteln
- Schritt 5: Überprüfen Sie Ihre Ergebnisse

Bevor Sie beginnen

Wenn Sie sich für Amazon Web Services (AWS) registrieren, wird Ihr Konto automatisch für alle registriertAWS-Services, auch für Amazon Macie. Um Macie zu aktivieren und zu verwenden, müssen Sie jedoch zunächst Berechtigungen einrichten, die Ihnen den Zugriff auf die Amazon Macie Macie-Konsole und API-Operationen ermöglichen. Sie oder Ihr AWS Administrator können dies tun, indem Sie AWS Identity and Access Management (IAM) verwenden, um die AWS verwaltete Richtlinie mit dem Namen `AmazonMacieFullAccess` Ihrer IAM-Identität anzuhängen. Weitere Informationen hierzu finden Sie unter AWSverwaltete Richtlinien für Amazon Macie.

Schritt 1: Amazon Macie aktivieren

Nachdem Sie die erforderlichen Berechtigungen eingerichtet haben, können Sie Amazon Macie für Ihre AWS-Konto aktivieren. Folgen Sie diesen Schritten, um Macie für Ihr Konto zu aktivieren.

Um Macie zu aktivieren

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie Macie aktivieren und verwenden möchten.

3. Wählen Sie auf der Amazon Macie-Seite die Option Erste Schritte aus.
4. (Optional) Wenn Sie Macie aktivieren, erstellt Macie automatisch eine servicebezogene Rolle, die Macie die erforderlichen Berechtigungen erteilt, um andere Personen anzurufen AWS-Services und Ressourcen in Ihrem Namen zu überwachenAWS. Um die Berechtigungsrichtlinie für diese Rolle zu überprüfen, wählen Sie in der Konsole die Option Rollenberechtigungen anzeigen aus. Weitere Informationen zu dieser Rolle finden Sie unterServicebezogene Rollen für Amazon Macie.
5. Wählen Sie Enable Macie (Macie aktivieren) aus.

Innerhalb weniger Minuten generiert Macie automatisch ein vollständiges Inventar Ihrer S3-Buckets in der aktuellen Region und beginnt damit, dieses zu verwalten. Macie beginnt außerdem mit der Bewertung und Überwachung der Buckets im Hinblick auf Sicherheit und Zugriffskontrolle. Weitere Informationen hierzu finden Sie unter So überwacht Macie die Amazon S3 S3-Datensicherheit.

Abhängig von Ihren Kontoeinstellungen beginnt Macie auch mit der automatischen Erkennung sensibler Daten für Ihre S3-Buckets. Macie beginnt, kontinuierlich repräsentative S3-Objekte in Ihren Buckets zu identifizieren, auszuwählen und zu analysieren und die Objekte auf sensible Daten zu untersuchen. Im Laufe der Analysen stellt Macie Statistiken und andere Ergebnisse zur Verfügung, die Sie überprüfen können, in der Regel innerhalb von 48 Stunden, nachdem Macie für Ihr Konto aktiviert wurde. Sie können die Analysen individuell anpassen, indem Sie die Einstellungen für die automatische Erkennung sensibler Daten für Ihr Konto konfigurieren. Weitere Informationen hierzu finden Sie unter So funktioniert die automatische Erkennung vertraulicher Daten.

Um die aggregierten Statistiken zu überprüfen, wählen Sie im Navigationsbereich der Konsole Zusammenfassung aus. Um Details zu einzelnen S3-Buckets in Ihrem Inventar zu überprüfen, wählen Sie im Navigationsbereich S3-Buckets aus. Um anschließend die Details eines Buckets anzuzeigen, wählen Sie den Bucket aus. Im Detailbereich werden Statistiken und andere Informationen angezeigt, die Aufschluss über die Sicherheit, den Datenschutz und die Vertraulichkeit der Daten des Buckets geben. Weitere Informationen zu diesen Details finden Sie unterÜberprüfen Ihres S3-Bucket-Bestands.

Schritt 2: Konfigurieren Sie ein Repository für die Ergebnisse der Erkennung sensibler Daten

Mit Amazon Macie können Sie sensible Daten in Ihren S3-Buckets auf zwei Arten entdecken: indem Sie Macie so konfigurieren, dass es die automatische Erkennung sensibler Daten durchführt, und

indem Sie Discovery-Jobs für sensible Daten ausführen. Ein Discovery-Job für sensible Daten ist ein Job, den Sie erstellen, um Objekte in S3-Buckets zu analysieren, um festzustellen, ob die Objekte vertrauliche Daten enthalten.

Macie erstellt für jedes S3-Objekt einen Datensatz, den es analysiert, wenn Sie Erkennungsaufträge für sensible Daten ausführen oder eine automatische Erkennung sensibler Daten durchführen. Diese Datensätze, die als Erkennungsergebnisse sensibler Daten bezeichnet werden, protokollieren Details zur Analyse einzelner Objekte. Macie erstellt außerdem Erkennungsergebnisse für sensible Daten für Objekte, die aufgrund von Fehlern oder Problemen nicht analysiert werden können. Die Ergebnisse der Entdeckung sensibler Daten liefern Ihnen Analyseaufzeichnungen, die für Prüfungen oder Untersuchungen zum Datenschutz hilfreich sein können.

Macie speichert Ihre Ergebnisse der Entdeckung sensibler Daten nur 90 Tage lang. Um auf die Ergebnisse zuzugreifen und sie langfristig zu speichern und aufzubewahren, konfigurieren Sie Macie so, dass die Ergebnisse in einem S3-Bucket gespeichert werden. Sie sollten dies innerhalb von 30 Tagen nach der Aktivierung von Macie tun. Nachdem Sie dies getan haben, kann der Bucket als definitives, langfristiges Repository für all Ihre Ergebnisse bei der Entdeckung sensibler Daten dienen.

Informationen zur Konfiguration dieses Repositorys finden Sie unterSpeicherung und Beibehaltung der Erkennungsergebnisse von vertraulichen Daten.

Schritt 3: Erkunden Sie die Ergebnisse der Beispiele

In Amazon Macie ist ein Ergebnis ein detaillierter Bericht über einen potenziellen Richtlinienverstoß, den Macie für einen S3-Bucket oder sensible Daten, die Macie in einem S3-Objekt entdeckt, entdeckt. Macie bietet zwei Kategorien von Ergebnissen: politische Erkenntnisse und Ergebnisse sensibler Daten. Macie erstellt eine Richtlinienfeststellung, wenn die Richtlinien oder Einstellungen für einen Bucket so geändert werden, dass die Sicherheit oder der Datenschutz des Buckets und der Objekte des Buckets beeinträchtigt werden. Macie erstellt eine Suche nach sensiblen Daten, wenn sie sensible Daten in einem S3-Objekt entdeckt. Innerhalb jeder Kategorie gibt es mehrere Arten von Ergebnissen.

Um die verschiedenen Kategorien und Arten von Ergebnissen, die Macie zur Verfügung stellt, zu untersuchen und mehr über sie zu erfahren, können Sie optional Stichprobenergebnisse erstellen und überprüfen. In den Stichprobenergebnissen werden Beispieldaten und Platzhalterwerte verwendet, um zu verdeutlichen, welche Art von Informationen Macie in die einzelnen Befunde einbeziehen könnte.

Gehen Sie wie folgt vor, um Stichprobenergebnisse zu erstellen und zu überprüfen.

Um Stichprobenergebnisse zu erstellen und zu überprüfen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie unter Sample findings (Beispielergebnisse) Generate sample findings (Beispielergebnisse generieren). Macie generiert ein Musterergebnis für jeden Befundtyp, den Macie unterstützt.
4. Wählen Sie im Navigationsbereich Findings aus. Auf der Seite mit den Ergebnissen werden die aktuellen Ergebnisse für Ihr Konto angezeigt. AWS-Region Dazu gehören die Beispielergebnisse, die Sie im vorherigen Schritt erstellt haben.
5. Suchen Sie auf der Seite Ergebnisse nach Ergebnissen, deren Typ mit [SAMPLE] beginnt.
6. Um die Details eines bestimmten Stichprobenergebnisses zu überprüfen, wählen Sie das Ergebnis aus. Im Bereich „Details“ werden die Details des Ergebnisses angezeigt.

Weitere Informationen zu den einzelnen Befundtypen finden Sie unterArten von Ergebnissen. Weitere Informationen zum Erstellen und Überprüfen von Stichprobenergebnissen finden Sie unterArbeiten mit Stichprobenergebnissen.

Schritt 4: Erstellen Sie einen Job, um sensible Daten zu ermitteln

Um sensible Daten in S3-Buckets zu entdecken und zu melden, können Sie Discovery-Jobs für sensible Daten ausführen. Ein Discovery-Job für sensible Daten ist ein Job, den Sie erstellen, um Objekte in S3-Buckets zu analysieren, um festzustellen, ob die Objekte vertrauliche Daten enthalten. Im Gegensatz zur automatisierten Erkennung sensibler Daten definieren Sie den Umfang und die Tiefe der Analyse. Sie geben auch an, wie oft ein Job ausgeführt werden soll — einmalig oder regelmäßig nach einem Zeitplan.

Gehen Sie wie folgt vor, um einen Job zu erstellen, der einmal, unmittelbar nach der Erstellung, ausgeführt wird und die Standardeinstellungen verwendet. Informationen zum Erstellen eines Jobs, der regelmäßig ausgeführt wird oder benutzerdefinierte Einstellungen verwendet, finden Sie unterErstellen einer Aufgabe zur Erkennung vertraulicher Daten.

So erstellen Sie einen Discovery-Job für sensible Daten

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.

2. Wählen Sie im Navigationsbereich die Option Jobs (Aufträge) aus.
3. Wählen Sie Job erstellen aus.
4. Wählen Sie für den Schritt S3-Buckets auswählen die Option Bestimmte Buckets auswählen aus. Aktivieren Sie dann in der Tabelle das Kontrollkästchen für jeden S3-Bucket, den der Job analysieren soll.

   Die Tabelle enthält eine vollständige Bestandsaufnahme Ihrer aktuellen AWS-Region S3-Buckets. Um bestimmte Buckets einfacher zu finden, geben Sie Filterkriterien in das Filterfeld über der Tabelle ein. Sie können die Tabelle auch sortieren, indem Sie eine Spaltenüberschrift in der Tabelle auswählen.
5. Wenn Sie mit der Auswahl der Buckets fertig sind, wählen Sie Weiter.
6. Überprüfen und verifizieren Sie für den Schritt S3-Buckets überprüfen Ihre Bucket-Auswahl und wählen Sie dann Weiter aus.
7. Wählen Sie für den Schritt Umfang verfeinern die Option Einmaliger Auftrag und anschließend Weiter aus.
8. Wählen Sie für den Schritt „Verwaltete Datenkennungen auswählen“ die Option Empfohlen aus. Sehen Sie sich optional die Tabelle der verwalteten Datenkennungen an, die wir für Jobs empfehlen, und wählen Sie dann Weiter aus.

   Ein verwalteter Datenbezeichner besteht aus einer Reihe integrierter Kriterien und Techniken, mit denen ein bestimmter Typ vertraulicher Daten erkannt werden kann, z. B. Kreditkartennummern, AWS geheime Zugangsschlüssel oder Passnummern für ein bestimmtes Land oder eine bestimmte Region. Weitere Informationen hierzu finden Sie unter Verwenden von verwalteten Datenbezeichnern.
9. Wählen Sie für den Schritt Benutzerdefinierte Datenkennungen auswählen die Option Weiter aus.

   Ein benutzerdefinierter Datenbezeichner besteht aus einer Reihe von Kriterien, die Sie definieren, um vertrauliche Daten zu erkennen. Dabei handelt es sich um einen regulären Ausdruck (Regex), der ein passendes Textmuster definiert, sowie optional Zeichenfolgen und eine Näherungsregel, die die Ergebnisse verfeinern. Weitere Informationen hierzu finden Sie unter Erstellen von benutzerdefinierten Datenbezeichnern.
10. Wählen Sie für den Schritt „Zulässige Listen auswählen“ die Option Weiter aus.

    In Macie gibt eine Zulassungsliste Text oder ein Textmuster an, das Macie ignorieren soll, wenn es S3-Objekte auf sensible Daten untersucht. Dabei handelt es sich in der Regel um Ausnahmen

für sensible Daten für bestimmte Szenarien oder Umgebungen. Weitere Informationen hierzu finden Sie unter Definition von Ausnahmen für sensible Daten mit Zulassungslisten.

11. Geben Sie für den Schritt Allgemeine Einstellungen eingeben einen Namen und optional eine Beschreibung des Jobs ein. Wählen Sie anschließend Weiter.
12. Überprüfen Sie für den Schritt Überprüfen und erstellen die Konfigurationseinstellungen des Jobs und stellen Sie sicher, dass sie korrekt sind.

    Sie können auch die geschätzten Gesamtkosten (in US-Dollar) für die Ausführung des Jobs überprüfen. Anhand der Schätzung können Sie entscheiden, ob Sie die Einstellungen des Jobs anpassen sollten, bevor Sie den Job speichern. Weitere Informationen hierzu finden Sie unter Prognostizieren der Kosten einer Aufgabe zur Erkennung sensibler Daten.
13. Wenn Sie mit der Überprüfung und Überprüfung der Auftragseinstellungen fertig sind, wählen Sie Absenden.

Macie beginnt sofort mit der Ausführung des Jobs. Informationen zur Überwachung des Jobs finden Sie unter Überprüfen des Status von Aufträgen zur Erkennung vertraulicher Daten.

Schritt 5: Überprüfen Sie Ihre Ergebnisse

Amazon Macie überwacht Ihre S3-Buckets automatisch im Hinblick auf Sicherheit und Zugriffskontrolle und erstellt Richtlinienergebnisse, um potenzielle Probleme mit der Sicherheit oder dem Datenschutz Ihrer Buckets zu melden. Wenn Sie einen Job zur Erkennung vertraulicher Daten erstellen und ausführen oder Macie für die automatische Erkennung sensibler Daten konfigurieren, erstellt Macie auch Ergebnisse für sensible Daten, um sensible Daten zu melden, die es in S3-Objekten erkennt. Weitere Informationen zu den Ergebnissen finden Sie unter. Analyse der Ergebnisse

Gehen Sie wie folgt vor, um Ihre Ergebnisse zu überprüfen.

Um Ihre Ergebnisse zu überprüfen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich Findings aus. Auf der Seite mit den Ergebnissen werden die aktuellen AWS-Region Ergebnisse für Ihr Konto angezeigt.
3. (Optional) Um die Ergebnisse nach bestimmten Kriterien zu filtern, geben Sie die Kriterien in das Filterfeld über der Tabelle ein.

4. Um die Details eines bestimmten Ergebnisses zu überprüfen, wählen Sie das Ergebnis aus. Im Detailbereich werden die Details des Ergebnisses angezeigt.

Weitere Informationen, z. B. zum Gruppieren und Filtern von Ergebnissen, finden Sie unterÜberprüfung der Ergebnisse.

Konzepte und Terminologie von Amazon Macie

In Amazon Macie bauen wir auf gemeinsamen AWS Konzepten und Terminologie auf und verwenden diese zusätzlichen Begriffe.

Konto

Ein StandardAWS-Konto, der Ihre AWS Ressourcen und die Identitäten enthält, die auf diese Ressourcen zugreifen können.

Um Macie zu verwenden, melden Sie sich AWS mit Ihren AWS-Konto Anmeldeinformationen an, wählen das aus, AWS-Region in dem Sie Macie verwenden möchten, und aktivieren dann Macie für Sie AWS-Konto in dieser Region. Weitere Informationen finden Sie unter Erste Schritte mit Amazon Macie.

In Macie gibt es drei Arten von Konten:

- Administratorkonto — Dieser Kontotyp verwaltet Macie-Konten für eine Organisation. Eine Organisation besteht aus einer Reihe von Macie-Konten, die miteinander verknüpft und als Gruppe verwandter Konten in einem bestimmten Bereich zentral verwaltet werden. AWS-Region
- Mitgliedskonto — Dieser Kontotyp ist dem Macie-Administratorkonto einer Organisation zugeordnet und wird von diesem verwaltet.
- Eigenständiges Konto — Bei diesem Kontotyp handelt es sich weder um ein Administrator- noch um ein Mitgliedskonto. Es ist nicht Teil einer Organisation.

Sie können Macie-Konten auf zwei Arten zu einer Organisation hinzufügen: indem Sie Macie in Macie integrieren AWS Organizations oder indem Sie Einladungen zur Macie-Mitgliedschaft senden und annehmen. Weitere Informationen finden Sie unter Verwalten mehrerer Konten.

Administratorkonto

In Macie ein Konto, das Macie-Konten für eine Organisation verwaltet. Eine Organisation ist eine Gruppe von Macie-Konten, die miteinander verknüpft und als Gruppe verwandter Konten in einem bestimmten Bereich zentral verwaltet werden. AWS-Region

Benutzer eines Macie-Administratorkontos haben Zugriff auf Inventardaten, Richtlinienfeststellungen und bestimmte Macie-Einstellungen und Ressourcen für alle Konten in ihrer Organisation von

Amazon Simple Storage Service (Amazon S3). Sie können auch eine automatische Erkennung sensibler Daten durchführen und Aufgaben zur Erkennung sensibler Daten ausführen, um sensible Daten in S3-Buckets zu erkennen, die den Konten gehören. Je nachdem, wie ein Konto als Administratorkonto bezeichnet wird, können sie möglicherweise auch zusätzliche Aufgaben für andere Konten in ihrer Organisation ausführen.

Weitere Informationen finden Sie unter Verwalten mehrerer Konten.

Zulassungsliste

In Macie gibt eine Zulassungsliste Text oder ein Textmuster an, das Macie ignorieren soll, wenn es S3-Objekte auf sensible Daten untersucht.

In Macie können Sie zwei Arten von Zulassungslisten erstellen: eine Klartextdatei, die bestimmte Wörter und andere Arten von Zeichenfolgen auflistet, die ignoriert werden sollen, oder einen regulären Ausdruck (Regex), der ein zu ignorierendes Textmuster definiert. Wenn ein Objekt Text enthält, der einem Eintrag oder Muster in einer Zulassungsliste entspricht, meldet Macie den Text nicht in Ergebnissen sensibler Daten, Statistiken und anderen Arten von Ergebnissen, selbst wenn der Text den Kriterien einer verwalteten Daten-ID oder einer benutzerdefinierten Daten-ID entspricht.

Weitere Informationen finden Sie unter Definition von Ausnahmen für sensible Daten mit Zulassungslisten.

automatisierte Erkennung sensibler Daten

Eine Reihe automatisierter Analyseaktivitäten, die Macie kontinuierlich durchführt, um repräsentative Objekte aus S3-Buckets zu identifizieren und auszuwählen und die ausgewählten Objekte auf sensible Daten zu untersuchen.

Im Laufe der Analysen erstellt Macie Aufzeichnungen über die gefundenen sensiblen Daten (Ergebnisse sensibler Daten) und über die durchgeführten Analysen (Ergebnisse der Entdeckung sensibler Daten). Macie aktualisiert auch Statistiken und andere Informationen, die es zu Amazon S3 S3-Daten bereitstellt.

Weitere Informationen finden Sie unter Durchführung automatisierter Erkennung vertraulicher Daten.

AWS Security Finding Format (ASFF)

Ein standardisiertes JSON-Format für den Inhalt von Ergebnissen, die veröffentlicht oder von AWS Security Hub generiert wurden. Das ASFF enthält Einzelheiten zur Ursache eines Sicherheitsproblems, zu den betroffenen Ressourcen und zum Status eines Befundes.

Informationen zu ASFF finden Sie unter AWSSecurity Finding Format (ASFF) im AWS Security Hub Benutzerhandbuch. Informationen zur Veröffentlichung von Macie-Ergebnissen auf Security Hub finden Sie unterAmazon MacieIntegration mit AWS Security Hub.

klassifizierbare Byte oder Größe

In den von Macie bereitgestellten S3-Bucket-Statistiken die Gesamtspeichergröße aller klassifizierbaren Objekte in einem S3-Bucket.

Wenn die Versionierung für einen Bucket aktiviert ist, basiert dieser Wert auf der Speichergröße der neuesten Version jedes klassifizierbaren Objekts im Bucket. Wenn es sich bei einem Objekt um eine komprimierte Datei handelt, spiegelt dieser Wert nicht die tatsächliche Größe des Dateiinhalts nach der Dekomprimierung wider.

Weitere Informationen finden Sie unter Überprüfen Ihres S3-Bucket-Bestands und Bewertung Ihrer Amazon S3-Sicherheitslage.

klassifizierbares Objekt

Ein S3-Objekt, das Macie analysieren kann, um sensible Daten zu erkennen.

Bei der Berechnung der S3-Bucket-Statistiken stellt Macie fest, dass ein Objekt anhand der Speicherklasse und der Dateinamenerweiterung des Objekts klassifizierbar ist. Ein Objekt ist klassifizierbar, wenn es eine unterstützte Amazon S3 S3-Speicherklasse verwendet und eine Dateinamenerweiterung für ein unterstütztes Datei- oder Speicherformat hat.

Weitere Informationen finden Sie unter Überprüfen Ihres S3-Bucket-Bestands und Bewertung Ihrer Amazon S3-Sicherheitslage.

Bei der Erkennung sensibler Daten bestimmt Macie, dass ein Objekt anhand der Speicherklasse, der Dateinamenerweiterung und des Inhalts des Objekts klassifizierbar ist. Ein Objekt ist klassifizierbar, wenn: es eine unterstützte Amazon S3 S3-Speicherklasse verwendet, eine Dateinamenerweiterung

für ein unterstütztes Datei- oder Speicherformat hat und Macie bestätigt hat, dass es Daten aus dem Objekt extrahieren und analysieren kann.

Weitere Informationen finden Sie unter Erkennen vertraulicher Daten und Prognose und Überwachung der Kosten.

benutzerdefinierte Daten-ID

Eine Reihe von Kriterien, die Sie definieren, um sensible Daten zu erkennen.

Die Kriterien bestehen aus einem regulären Ausdruck (Regex), der ein zu suchendes Textmuster definiert und optional Zeichenfolgen und eine Näherungsregel zur Eingrenzung der Ergebnisse festlegt. Die Zeichenfolgen können Folgendes sein:

- Schlüsselwörter – Wörter oder Ausdrücke, die sich in der Nähe von Text befinden müssen, der dem Regex entspricht
- Zu ignorierende Wörter – Wörter oder Ausdrücke, die aus den Ergebnissen ausgeschlossen werden sollen

Zusätzlich zu den Erkennungskriterien können Sie benutzerdefinierte Schweregradeinstellungen für die Ergebnisse sensibler Daten definieren, die eine benutzerdefinierte Daten-ID hervorruft.

Weitere Informationen finden Sie unter Erstellen von benutzerdefinierten Datenbezeichnern.

Filterregel

Eine Reihe von attributbasierten Filterkriterien, die Sie erstellen und speichern, um Ergebnisse auf der Amazon Macie Macie-Konsole zu analysieren. Mithilfe von Filterregeln können Sie eine konsistente Analyse von Ergebnissen durchführen, die bestimmte Merkmale aufweisen, z. B. alle Ergebnisse mit hohem Schweregrad, die einen bestimmten Typ vertraulicher Daten melden.

Weitere Informationen finden Sie unter Filterregeln für Ergebnisse erstellen und verwalten.

Ergebnis

Ein detaillierter Bericht über sensible Daten, die Macie in einem S3-Objekt gefunden hat, oder über ein potenzielles Problem mit der Sicherheit oder dem Datenschutz eines S3-Buckets. Jedes Ergebnis

enthält Einzelheiten wie einen Schweregrad, Informationen über die betroffene Ressource und den Zeitpunkt, zu dem Macie die Daten oder das Problem gefunden hat.

Macie generiert zwei Kategorien von Ergebnissen: Ergebnisse vertraulicher Daten für sensible Daten, die Macie in S3-Objekten entdeckt, und Richtlinienergebnisse für potenzielle Probleme, die Macie mit den Sicherheits- und Zugriffskontrolleinstellungen für S3-Buckets entdeckt. Innerhalb jeder Kategorie gibt es spezifische Arten von Ergebnissen.

Weitere Informationen finden Sie unter Arten von Amazon Macie-Ergebnissen.

Ereignis finden

Ein EventBridge Amazon-Ereignis, das die Einzelheiten einer Feststellung sensibler Daten oder einer Richtlinienfeststellung enthält.

Macie veröffentlicht automatisch Ergebnisse sensibler Daten und politische Ergebnisse EventBridge als Ereignisse an Amazon. Ein Ereignis ist ein JSON-Objekt, das dem EventBridge Schema für AWS Ereignisse entspricht. Sie können diese Ereignisse verwenden, um Ergebnisse zu überwachen, zu verarbeiten und darauf zu reagieren, indem Sie andere Anwendungen, Dienste und Systeme verwenden.

Weitere Informationen finden Sie unter Integration von Amazon Macie mit Amazon EventBridge und EventBridge Amazon-Ereignisschema für Amazon Macie-Ergebnisse.

Auftrag

Siehe Job zur Erkennung sensibler Daten.

ID für verwaltete Daten

Eine Reihe integrierter Kriterien und Techniken, die darauf ausgelegt sind, einen bestimmten Typ vertraulicher Daten zu erkennen. Zu den sensiblen Daten gehören beispielsweise Kreditkartennummern, AWS geheime Zugangsschlüssel oder Passnummern für ein bestimmtes Land oder eine bestimmte Region. Diese Identifikatoren können eine große und ständig wachsende Liste sensibler Datentypen für viele Länder und Regionen erkennen.

Weitere Informationen finden Sie unter Verwenden von verwalteten Datenbezeichnern.

Mitgliedskonto

Ein Macie-Konto, das vom designierten Macie-Administratorkonto für eine Organisation verwaltet wird. Eine Organisation besteht aus einer Reihe von Macie-Konten, die miteinander verknüpft und als Gruppe verwandter Konten in einem bestimmten Bereich zentral verwaltet werden. AWS-Region

Ein Konto kann auf zwei Arten zu einem Mitgliedskonto werden: durch die Integration von Macie in die Organisation des Kontos AWS Organizations oder durch Annahme einer Einladung zur Macie-Mitgliedschaft.

Wenn Sie ein Mitgliedskonto haben, hat Ihr Macie-Administrator Zugriff auf Amazon S3 S3-Inventardaten, Richtlinienfeststellungen und bestimmte Macie-Einstellungen und Ressourcen für Ihr Konto. Ihr Administrator kann auch eine automatische Erkennung sensibler Daten durchführen und Aufgaben zur Erkennung sensibler Daten ausführen, um sensible Daten in Ihren S3-Buckets zu erkennen. Je nachdem, wie Ihr Konto zu einem Mitgliedskonto wurde, können sie möglicherweise auch zusätzliche Aufgaben für Ihr Konto ausführen.

Weitere Informationen finden Sie unter Verwalten mehrerer Konten.

Organisation

Eine Reihe von Macie-Konten, die miteinander verknüpft sind und als Gruppe verwandter Konten in einem bestimmten AWS-Region Bereich zentral verwaltet werden.

Jede Organisation besteht aus einem bestimmten Macie-Administratorkonto und einem oder mehreren zugehörigen Mitgliedskonten. Das Administratorkonto kann auf bestimmte Macie-Einstellungen, Daten und Ressourcen für Mitgliedskonten zugreifen. Sie können eine Organisation auf zwei Arten erstellen: durch die Integration von Macie in Macie AWS Organizations oder durch das Senden und Annehmen von Mitgliedschaftseinladungen in Macie.

Weitere Informationen finden Sie unter Verwalten mehrerer Konten.

Festlegung von Richtlinien

Ein detaillierter Bericht über einen möglichen Richtlinienverstoß oder ein Problem mit den Sicherheits- und Zugriffskontrolleinstellungen für einen S3-Bucket. Zu den Details gehören eine Bewertung des Schweregrads, Informationen zur betroffenen Ressource und wann Macie das Problem gefunden hat.

Macie generiert Richtlinienergebnisse, wenn die Richtlinien oder Einstellungen für einen S3-Bucket so geändert werden, dass die Sicherheit oder der Datenschutz des Buckets und der Objekte des Buckets beeinträchtigt werden. Macie generiert diese Ergebnisse im Rahmen seiner laufenden Überwachungsaktivitäten für Ihre Amazon S3 S3-Daten. Macie kann verschiedene Arten von politischen Ergebnissen generieren.

Weitere Informationen finden Sie unter Arten von Amazon Macie-Ergebnissen und Überwachung von Datensicherheit und Datenschutz.

Befund einer Stichprobe

Ein Ergebnis, das anhand von Beispieldaten und Platzhalterwerten veranschaulicht, welche Arten von Informationen ein Ergebnis enthalten könnte.

Weitere Informationen finden Sie unter Arbeiten mit Stichprobenergebnissen.

Feststellung sensibler Daten

Ein detaillierter Bericht über sensible Daten, die Macie in einem S3-Objekt gefunden hat. Zu den Einzelheiten gehören ein Schweregrad, Informationen über die betroffene Ressource, Art und Anzahl der Vorkommen der sensiblen Daten, die Macie gefunden hat, und wann Macie die sensiblen Daten gefunden hat.

Macie generiert Ergebnisse zu sensiblen Daten, wenn es sensible Daten in S3-Objekten entdeckt, die es analysiert, wenn Sie Erkennungsaufträge für vertrauliche Daten ausführen, oder wenn es eine automatisierte Erkennung sensibler Daten durchführt. Macie kann verschiedene Arten von Ergebnissen für sensible Daten generieren.

Weitere Informationen finden Sie unter Arten von Amazon Macie-Ergebnissen und Erkennen vertraulicher Daten.

Job zur Entdeckung sensibler Daten

Wird auch als Job bezeichnet und ist eine Reihe automatisierter Verarbeitungs- und Analyseaufgaben, die Macie ausführt, um sensible Daten in S3-Objekten zu erkennen und zu melden. Wenn Sie einen Job erstellen, geben Sie an, wie oft der Job ausgeführt werden soll, und Sie definieren den Umfang und die Art der Analyse des Jobs.

Wenn ein Job ausgeführt wird, erstellt Macie Aufzeichnungen über die gefundenen vertraulichen Daten (Ergebnisse sensibler Daten) und über die durchgeführten Analysen (Ergebnisse der Erkennung sensibler Daten). Macie veröffentlicht auch Protokolldaten in Amazon CloudWatch Logs.

Weitere Informationen finden Sie unter Ausführen von Erkennungsaufgaben für vertrauliche Daten.

Ergebnis der Entdeckung sensibler Daten

Ein Datensatz, der Details zu der Analyse protokolliert, die Macie an einem S3-Objekt durchgeführt hat, um festzustellen, ob das Objekt vertrauliche Daten enthält. Macie generiert und schreibt diese Datensätze in JSON Lines (.jsonl) -Dateien, die es verschlüsselt und in einem von Ihnen angegebenen S3-Bucket speichert. Die Datensätze entsprechen einem standardisierten Schema.

Wenn Sie einen Discovery-Job für sensible Daten ausführen oder Macie eine automatische Erkennung sensibler Daten durchführt, erstellt Macie für jedes Objekt, das in den Umfang der Analyse einbezogen wird, ein Erkennungsergebnis für sensible Daten. Dies umfasst:

- Objekte, in denen Macie sensible Daten findet und die daher auch zu Ergebnissen sensibler Daten führen.
- Objekte, in denen Macie keine sensiblen Daten findet und die daher keine Ergebnisse mit sensiblen Daten liefern.
- Objekte, die Macie aufgrund von Fehlern oder Problemen nicht analysieren kann, z. B. aufgrund von Berechtigungseinstellungen oder der Verwendung eines nicht unterstützten Datei- oder Speicherformats.

Weitere Informationen finden Sie unter Speicherung und Beibehaltung der Erkennungsergebnisse von vertraulichen Daten.

eigenständiges Konto

Ein Macie-Konto, das weder ein Administrator- noch ein Mitgliedskonto in einer Organisation ist. Das Konto ist nicht Teil einer Organisation.

unterdrückter Befund

Ein Ergebnis, das automatisch durch eine Unterdrückungsregel archiviert wurde. Das heißt, Macie hat den Status des Ergebnisses automatisch in archiviert geändert, weil das Ergebnis den Kriterien einer Unterdrückungsregel entsprach, als Macie das Ergebnis generierte.

Weitere Informationen finden Sie unter Unterdrücken von Ergebnissen.

Unterdrückungsregel

Eine Reihe von attributbasierten Filterkriterien, die Sie erstellen und speichern, um Ergebnisse automatisch zu archivieren (zu unterdrücken). Unterdrückungsregeln sind in Situationen hilfreich, in denen Sie eine Gruppe von Ergebnissen überprüft haben und nicht erneut darüber informiert werden möchten.

Wenn Sie Ergebnisse mit einer Unterdrückungsregel unterdrücken, generiert Macie weiterhin Ergebnisse, die den Kriterien der Regel entsprechen. Macie ändert den Status der Ergebnisse jedoch automatisch in archiviert. Das bedeutet, dass die Ergebnisse nicht standardmäßig auf der Amazon Macie Macie-Konsole angezeigt werden und Macie sie nicht auf anderen veröffentlicht. AWS-Services

Weitere Informationen finden Sie unter Unterdrücken von Ergebnissen.

nicht klassifizierbare Byte oder Größe

In den von Macie bereitgestellten S3-Bucket-Statistiken die Gesamtspeichergröße aller nicht klassifizierbaren Objekte in einem S3-Bucket.

Wenn die Versionierung für einen Bucket aktiviert ist, basiert dieser Wert auf der Speichergröße der neuesten Version jedes nicht klassifizierbaren Objekts im Bucket. Wenn es sich bei einem Objekt um eine komprimierte Datei handelt, spiegelt dieser Wert nicht die tatsächliche Größe des Dateiinhalts nach der Dekomprimierung wider.

Weitere Informationen finden Sie unter Überprüfen Ihres S3-Bucket-Bestands und Bewertung Ihrer Amazon S3-Sicherheitslage.

nicht klassifizierbares Objekt

Ein S3-Objekt, das Macie nicht analysieren kann, um sensible Daten zu erkennen.

Bei der Berechnung der S3-Bucket-Statistiken stellt Macie anhand der Speicherklasse und der Dateinamenerweiterung des Objekts fest, dass ein Objekt nicht klassifizierbar ist. Ein Objekt ist nicht klassifizierbar, wenn es keine unterstützte Amazon S3 S3-Speicherklasse verwendet oder keine Dateinamenerweiterung für ein unterstütztes Datei- oder Speicherformat hat.

Weitere Informationen finden Sie unter Überprüfen Ihres S3-Bucket-Bestands und Bewertung Ihrer Amazon S3-Sicherheitslage.

Bei der Erkennung sensibler Daten bestimmt Macie anhand der Speicherklasse, der Dateinamenerweiterung und des Inhalts des Objekts, dass ein Objekt nicht klassifizierbar ist. Ein Objekt ist nicht klassifizierbar, wenn: es keine unterstützte Amazon S3 S3-Speicherklasse verwendet, es keine Dateinamenerweiterung für ein unterstütztes Datei- oder Speicherformat hat oder Macie keine Daten aus dem Objekt extrahieren und analysieren konnte. Beispielsweise handelt es sich bei dem Objekt um eine fehlerhafte Datei.

Weitere Informationen finden Sie unter Erkennen vertraulicher Daten und Prognose und Überwachung der Kosten.

Überwachung der Datensicherheit und des Datenschutzes mit Amazon Macie

Wenn Sie Amazon Macie für Ihre aktivierenAWS-Konto, generiert Macie automatisch ein vollständiges Inventar Ihrer Amazon Simple Storage Service (Amazon S3) -Buckets und beginnt damit, dieses aktuell zu verwalten. AWS-Region Macie beginnt auch mit der Bewertung und Überwachung der Buckets auf Sicherheits- und Zugriffskontrolle. Wenn Macie ein Ereignis erkennt, das die Sicherheit oder den Datenschutz erkennt, werden ein Ergebnis erstellt, das Sie bei Bedarf überprüfen und bei Bedarf korrigieren können.

Um auch S3-Buckets auf das Vorhandensein vertraulicher Daten auszuwerten und zu überwachen, können Sie Aufgaben zur Erkennung vertraulicher Daten erstellen und ausführen. Bei der Erkennung von Daten können tägliche, wöchentliche oder monatliche Analysen von Bucket-Objekten durchgeführt werden. Abhängig von Ihren Kontoeinstellungen können Sie Macie auch so konfigurieren, dass es eine automatische Erkennung vertraulicher Daten für Ihre Buckets durchführt. Die automatische Erkennung vertraulicher Daten verwendet Stichprobenverfahren, um kontinuierlich repräsentative Objekte in Ihren Buckets zu identifizieren, auszuwählen und zu analysieren. Wenn Macie sensible Daten in einem von einem S3-Objekt entdeckt, werden sensible Daten erstellt, um Sie über die sensible Daten zu benachrichtigen, die Macie gefunden hat. Weitere Informationen finden Sie unter Erkennen vertraulicher Daten.

Zusätzlich zu den Ergebnissen bietet Macie einen ständigen Überblick über die Sicherheit und den Datenschutz Ihrer Amazon S3 S3-Daten. Um den Sicherheitsstatus Ihrer Daten zu beurteilen und festzustellen, wo Sie Maßnahmen ergreifen müssen, können Sie das Übersichts-Dashboard auf der Konsole verwenden. Das Dashboard bietet eine Momentaufnahme der aggregierten Statistiken für Ihre Amazon S3 S3-Daten. Die Statistiken beinhalten Daten für wichtige Sicherheitsmetriken wie die Anzahl der Buckets, die öffentlich zugänglich sind oder mit anderen AWS-Konten geteilt werden. Das Dashboard zeigt auch Gruppen aggregierter Ergebnisdaten für Ihr Konto an, z. B. die Namen von 1—5 Buckets mit den meisten Ergebnissen der letzten sieben Tage. Sie können jede Statistik aufschlüsseln, um die zugehörigen Daten zu überprüfen. Wenn Sie es vorziehen, die Statistiken programmgesteuert abzufragen, können Sie die GetBucketStatisticsBedienung der Amazon Macie API verwenden.

Für eine eingehendere Analyse und Bewertung bietet Macie auch detaillierte Informationen und Statistiken für einzelne S3-Buckets in Ihrem Inventar. Dazu gehören Aufschlüsselungen der öffentlichen Zugriffs- und Verschlüsselungseinstellungen der einzelnen Buckets sowie der Größe

und Anzahl der Objekte, die Macie analysieren kann, um sensible Daten im Bucket zu erkennen. Das Inventar gibt auch an, ob Sie sensible Datenermittlungsaufträge für die Analyse von Objekten in einem Bucket konfiguriert haben und, falls ja, wann einer dieser Jobs zuletzt ausgeführt wurde. Sie können das Inventar mithilfe der Amazon Macie-Konsole oder mithilfe der Amazon Macie Macie-API DescribeBucketsdurchsuchen, sortieren und filtern.

Wenn Sie der Macie-Administrator einer Organisation sind, können Sie auf statistische und andere Daten zu S3-Buckets zugreifen, die Ihren Mitgliedskonten gehören. Sie können auch auf die Richtlinienergebnisse zugreifen, die Macie für die Buckets erstellt, und die Buckets auf vertrauliche Daten überprüfen. Als Macie-Administrator können Sie Macie verwenden, um die allgemeine Sicherheitslage des Amazon S3 S3-Datenbestands Ihres Unternehmens zu beurteilen und zu überwachen. Weitere Informationen finden Sie unter Verwalten mehrerer Konten.

Themen

- So überwacht Amazon Macie die Datensicherheit von Amazon S3
- Bewertung Ihres Amazon S3-Sicherheitsstatus mit Amazon Macie
- Analysieren Sie Ihre Amazon S3 S3-Sicherheitslage mit Amazon Macie
- Ermöglichen Sie Amazon Macie den Zugriff auf S3-Buckets und -Objekte

So überwacht Amazon Macie die Datensicherheit von Amazon S3

Wenn Sie Amazon Macie für Ihr Konto aktivierenAWS-Konto, erstellt Macie eine dienstverknüpfte AWS Identity and Access Management (IAM) -Rolle für Ihr Konto in der aktuellen Version. AWS-Region Die Berechtigungsrichtlinie für diese Rolle ermöglicht es Macie, in Ihrem Namen andere AWS-Services Personen anzurufen und AWS Ressourcen zu überwachen. Mithilfe dieser Rolle generiert und verwaltet Macie ein vollständiges Inventar Ihrer Amazon Simple Storage Service (Amazon S3) -Buckets in der Region. Macie überwacht und bewertet die Buckets im Hinblick auf Sicherheit und Zugriffskontrolle.

Wenn Sie der Macie-Administrator für eine Organisation sind, enthält das Inventar statistische und andere Daten über S3-Buckets, die Ihrem Konto und den Mitgliedskonten in Ihrer Organisation gehören. Mit diesen Daten können Sie Macie verwenden, um die Sicherheitslage Ihres Unternehmens in Ihrer Amazon S3 S3-Umgebung zu überwachen und zu bewerten. Weitere Informationen finden Sie unter Verwalten mehrerer Konten.

Themen

- Zentrale Komponenten

- Datenaktualisierungen
- Weitere Überlegungen

Zentrale Komponenten

Amazon-S3-S3-S3-S3-S3-S3-S3-S3-S3-S3-S3-S3-S3-S3-Bckets.

Erfassung von Metadaten und Berechnung von Statistiken

Um Metadaten und Statistiken für Ihr Bucket-Inventar zu generieren und zu verwalten, ruft Macie Bucket- und Objektmetadaten direkt von Amazon S3 ab. Für jeden Bucket beinhalten die Metadaten:

- Allgemeine Informationen zum Bucket, wie der Name des Buckets, der Amazon-Ressourcenname (ARN), das Erstellungsdatum, Verschlüsselungseinstellungen, Tags und die Konto-ID des BucketsAWS-Konto, dem der Bucket gehört.
- Berechtigungseinstellungen auf Kontoebene, die für den Bucket gelten, z. B. die Einstellungen zum Blockieren des öffentlichen Zugriffs für das Konto.
- Berechtigungseinstellungen auf Bucket-Ebene für den Bucket, z. B. die Einstellungen für den blockierten öffentlichen Zugriff für den Bucket und Einstellungen, die aus einer Bucket-Richtlinie oder einer Zugriffskontrollliste (ACL) abgeleitet sind.
- Gemeinsamer Zugriff und Replikationseinstellungen für den Bucket, einschließlich der Frage, ob Bucket-Daten repliziert oder mit AWS-Konten diesen geteilt werden, die nicht Teil Ihrer Organisation sind.
- Objektzahlen und Einstellungen für Objekte im Bucket, z. B. die Anzahl der Objekte im Bucket und Aufschlüsselungen der Objektzahlen nach Verschlüsselungstyp, Dateityp und Speicherklasse.

Macie stellt Ihnen diese Informationen direkt zur Verfügung. Macie verwendet die Informationen auch zur Berechnung von Statistiken und zur Bewertung der Sicherheit und des Datenschutzes Ihres Bucket-Inventars insgesamt und einzelner Buckets in Ihrem Inventar. Sie können beispielsweise die Gesamtspeichergröße und Anzahl der Buckets in Ihrem Inventar, die Gesamtspeichergröße und Anzahl der Objekte in diesen Buckets sowie die Gesamtspeichergröße und Anzahl der Objekte ermitteln, die Macie analysieren kann, um sensible Daten in den Buckets zu erkennen.

Standardmäßig enthalten Metadaten und Statistiken Daten für alle Objektteile, die aufgrund unvollständiger mehrteiliger Uploads existieren. Wenn Sie Objektmetadaten für einen bestimmten

Bucket manuell aktualisieren, berechnet Macie die Statistiken für den Bucket und Ihr Bucket-Inventar insgesamt neu und schließt Daten für Objektteile von den neu berechneten Werten aus. Wenn Macie das nächste Mal im Rahmen des täglichen Aktualisierungszyklus Bucket- und Objektmetadaten von Amazon S3 abruft, aktualisiert Macie Ihre Inventardaten und schließt erneut Daten für die Objektteile ein. Hinweise darüber, wann Macie Bucket- und Objektmetadaten abruft, finden Sie unter. Datenaktualisierungen

Es ist wichtig zu beachten, dass Macie keine Objektteile analysieren kann, um sensible Daten zu erkennen. Amazon S3 muss zuerst die Teile zu einem oder mehreren Objekten zusammenfügen, damit Macie sie analysieren kann. Informationen zu mehrteiligen Uploads und Objektteilen, einschließlich des automatischen Löschens von Teilen mithilfe von Lebenszyklusregeln, finden Sie im Amazon Simple Storage Service-Benutzerhandbuch unter Hochladen und Kopieren von Objekten mithilfe des mehrteiligen Uploads. Um Buckets zu identifizieren, die Objektteile enthalten, können Sie auf unvollständige mehrteilige Upload-Metriken in Amazon S3 Storage Lens zurückgreifen. Weitere Informationen finden Sie unter Bewertung Ihrer Speicheraktivität und -nutzung im Benutzerhandbuch zum Simple Simple Storage.

Überwachung der Sicherheit und des Datenschutzes von Buckets

Um die Richtigkeit der Daten auf Bucketebene in Ihrem Inventar sicherzustellen, überwacht und analysiert Macie bestimmte AWS CloudTrailEreignisse, die für Amazon S3 S3-Daten auftreten können. Tritt ein relevantes Ereignis ein, aktualisiert Macie die entsprechenden Inventardaten.

Wenn Sie beispielsweise die Einstellungen für den öffentlichen Zugriff blockieren für einen Bucket aktivieren, aktualisiert Macie alle Daten über die Einstellungen für den öffentlichen Zugriff des Buckets. In ähnlicher Weise analysiert Macie die Richtlinie und aktualisiert die relevanten Daten in Ihrem Inventar, wenn Sie die Bucket-Richtlinie für einen Bucket hinzufügen oder aktualisieren.

Macie überwacht und analysiert Daten für die folgenden CloudTrail Ereignisse:

- Ereignisse auf Kontoebene — und DeletePublicAccessBlock PutPublicAccessBlock
- Ereignisse auf Bucket-Ebene — CreateBucketDeleteAccountPublicAccessBlock,DeleteBucket,DeleteBucketEncryption,DeleteBucketPo 0, 1, 2, 3 4, und 5 6PutBucketAclPutBucketEncryptionPutBucketPolicyPutBucketPublicAccessBlockPutBucketReplication

Sie können die Überwachung für zusätzliche CloudTrail Ereignisse nicht aktivieren oder die Überwachung für keines der vorherigen Ereignisse deaktivieren. Überarbeitung der Amazon-S3-S3-S3-S3-P3-P3-P3-P3-P3-P3-P3-P3-P3-P3-P3-P3-P

> **Tip**
>
> Um Ereignisse auf Objektebene zu überwachen, empfehlen wir die Amazon-S3-S3-S3-S3-S3-S3-S3-S3-S3-S3-S3-S3-S3-S3-S3-S3 GuardDuty Diese Funktion überwacht Amazon-S3—Datenereignisse und analysiert sie auf bösartige und verdächtige Aktivitäten. Weitere Informationen finden Sie GuardDuty unter GuardDutyAmazon S3

Bewertung der Bucket-Sicherheit und Zugriffskontrolle

Um die Sicherheit und Zugriffskontrolle auf Bucketebene zu bewerten, verwendet Macie automatisiertes, logisches Denken, um ressourcenbasierte Richtlinien zu analysieren, die für einen Bucket gelten. Macie analysiert auch die Berechtigungseinstellungen auf Konto- und Bucket-Ebene, die für einen Bucket gelten. Bei dieser Analyse werden Bucket-Richtlinien, ACLs auf Bucketebene und Einstellungen für den blockierten öffentlichen Zugriff für das Konto und den Bucket berücksichtigt.

Für ressourcenbasierte Richtlinien verwendet Macie Zelkova. Zelkova ist eine Maschine zum AWS Identity and Access Management Erfüllbarkeits-Modulo-Theorien (Satisfiability Modulo-Theorien) gegen das Entscheidungsproblem ausführt. Macie wendet Zelkova wiederholt auf eine Richtlinie mit immer spezifischeren Abfragen an, um die Verhaltensklassen zu beschreiben, die die Richtlinie zulässt. Weitere Informationen zur Natur der von Zelkova verwendeten Solver finden Sie unter Satisfiability-Modulo-Theorien.

> **Important**
>
> Um die vorherigen Aufgaben für einen Bucket ausführen zu können, muss Macie Zugriff auf den Bucket haben. Wenn die Berechtigungseinstellungen eines Buckets Macie daran hindern, Metadaten für den Bucket oder die Objekte des Buckets abzurufen, kann Macie nur einen Teil der Informationen über den Bucket bereitstellen, z. B. den Namen und das Erstellungsdatum des Buckets. Macie kann keine zusätzlichen Aufgaben für den Bucket ausführen. Weitere Informationen finden Sie unter Macie den Zugriff von S3-Buckets und -Objekten erlauben.

Datenaktualisierungen

Wenn Sie Amazon Macie für Ihr aktivierenAWS-Konto, ruft Macie Metadaten für Ihre S3-Buckets und Objekte direkt von Amazon S3 ab. Danach ruft Macie im Rahmen eines täglichen Aktualisierungszyklus automatisch täglich sowohl Bucket- als auch Objektmetadaten direkt aus Amazon S3 ab.

Macie ruft Bucket Metadaten ab Amazon S3 wenn einer der folgenden Fälle auftritt:

- Sie aktualisieren Ihre Inventardaten, indem Sie in der Amazon Macie Macie-Konsole auf refresh () klicken. Sie können die Daten bis zu alle fünf Minuten aktualisieren.
- Sie senden programmgesteuert eine DescribeBucketsAnfrage an die Amazon Macie API und haben innerhalb der letzten fünf Minuten keine DescribeBuckets Anfrage gestellt.
- Macie erkennt ein relevantes AWS CloudTrail Ereignis.

Macie kann auch die neuesten Objektmetadaten für einen bestimmten Bucket abrufen, wenn Sie diese Daten manuell aktualisieren. Dies kann hilfreich sein, wenn Sie kürzlich einen Bucket erstellt oder in den letzten 24 Stunden erhebliche Änderungen an den Objekten eines Buckets vorgenommen haben. Um Objektmetadaten für einen Bucket manuell zu aktualisieren, wählen Sie auf der S3-Bucket-Seite der Konsole im Abschnitt Objektstatistiken des Bereichs Bucket-Details die Option refresh ( ) aus. Diese Funktion ist für Buckets verfügbar, die 30.000 oder weniger Objekte enthalten.

Jedes Mal, wenn Macie Bucket- oder Objektmetadaten abruft, aktualisiert Macie automatisch alle relevanten Daten in Ihrem Inventar. Wenn Macie Unterschiede feststellt, die sich auf die Sicherheit oder den Datenschutz eines Buckets auswirken, beginnt Macie sofort mit der Bewertung und Analyse der Änderungen. Wenn die Analyse abgeschlossen ist, aktualisiert Macie die relevanten Daten in Ihrem Inventar. Wenn Unterschiede die Sicherheit oder den Datenschutz beeinträchtigen, erstellt Macie außerdem die entsprechenden Richtlinien, die Sie bei Bedarf überprüfen und beheben können.

Um festzustellen, wann Macie zuletzt Bucket- oder Objektmetadaten für Ihr Konto abgerufen hat, können Sie in der Konsole im Feld Letzte Aktualisierung nachsehen. Dieses Feld wird auf dem Übersichts-Dashboard und auf der Seite S3-Buckets sowie im Bereich mit den Bucket-Details auf der Seite S3-Buckets angezeigt. (Wenn Sie die Amazon Macie Macie-API verwenden, um Inventardaten abzufragen, enthält das `lastUpdated` Feld diese Informationen.) Wenn Sie der Macie-Administrator

für eine Organisation sind, gibt das Feld „Letzte Aktualisierung“ das früheste Datum und die früheste Uhrzeit an, an dem Macie die Daten für ein Konto in Ihrer Organisation abgerufen hat.

In seltenen Fällen können Latenz- und andere Probleme Macie unter bestimmten Bedingungen daran hindern, Bucket- und Objektmetadaten abzurufen. Sie können auch Benachrichtigungen verzögern, die Macie über Änderungen an Ihrem Bucket-Inventar oder den Berechtigungseinstellungen und Richtlinien für einzelne Buckets erhält. Beispielsweise können Lieferprobleme aufgrund von CloudTrail Ereignissen zu Verzögerungen führen. In diesem Fall analysiert Macie bei der nächsten täglichen Aktualisierung, die innerhalb von 24 Stunden stattfindet.

Weitere Überlegungen

Beachten Sie bei der Verwendung von Amazon Macie zur Überwachung und Bewertung des Sicherheitsstatus Ihrer Amazon S3 S3-Daten Folgendes:

- Inventardaten gelten nur für aktuelle AWS-Region S3-Buckets. Um auf die Daten für weitere Regionen zuzugreifen, aktivieren und verwenden Sie Macie in jeder weiteren Region.
- Wenn Sie der Macie-Administrator einer Organisation sind, können Sie nur dann auf Inventardaten für ein Mitgliedskonto zugreifen, wenn Macie für dieses Konto in der aktuellen Region aktiviert ist.
- Wenn die Berechtigungseinstellungen eines Buckets Macie daran hindern, Informationen über den Bucket oder die Objekte des Buckets abzurufen, kann Macie die Sicherheit und den Datenschutz der Bucket-Daten nicht auswerten und überwachen oder detaillierte Informationen über den Bucket bereitstellen.

  Um Ihnen zu helfen, einen Bucket zu identifizieren, in dem dies der Fall ist, geht Macie wie folgt vor:

  - In Ihrem Bucket-Inventar zeigt Macie ein Warnsymbol (⚠) für den Bucket an. Für die Details des Buckets zeigt Macie nur eine Teilmenge der Felder und Daten an: die Konto-ID des BucketsAWS-Konto, den Namen des Buckets, den Amazon-Ressourcennamen (ARN), das Erstellungsdatum und die Region sowie Datum und Uhrzeit, zu denen Macie im Rahmen des täglichen Aktualisierungszyklus zuletzt sowohl Bucket- als auch Objektmetadaten für den Bucket abgerufen hat. Wenn Sie die Amazon Macie Macie-API verwenden, um Inventardaten abzufragen, gibt Macie einen Fehlercode und eine Meldung für den Bucket aus, und der Wert für die meisten Eigenschaften des Buckets ist Null.
  - Im Übersichts-Dashboard hat der Bucket den Wert Unbekannt für die Statistiken „Öffentlicher Zugriff“, „Verschlüsselung“ und „Teilen“. (Wenn Sie die Amazon Macie Macie-API verwenden,

um die Statistiken abzufragen, hat der Bucket einen Wert von unknown für diese Statistiken.) Darüber hinaus schließt Macie den Bucket aus, wenn er Daten für Speicher - und Objektstatistiken berechnet.

Um das Problem zu untersuchen, überprüfen Sie die Richtlinien- und Berechtigungseinstellungen des Buckets in Amazon S3. Beispielsweise könnte der Bucket eine restriktive Bucket-Richtlinie haben. Weitere Informationen finden Sie unter Macie den Zugriff von S3-Buckets und -Objekten erlauben.

- Daten über Zugriff und Berechtigungen sind auf Einstellungen auf Konto- und Bucket-Ebene beschränkt. Es spiegelt nicht die Einstellungen auf Objektebene wider, die den Zugriff auf bestimmte Objekte in einem Bucket bestimmen. Wenn beispielsweise der öffentliche Zugriff für ein bestimmtes Objekt in einem Bucket aktiviert ist, meldet Macie nicht, dass der Bucket oder die Objekte des Buckets öffentlich zugänglich sind.

  Um den Betrieb auf Objektebene zu überwachen und potenzielle Sicherheitsrisiken zu identifizieren, empfehlen wir Ihnen, die Amazon S3 S3-Schutzfunktion von Amazon zu verwenden. GuardDuty Diese Funktion überwacht Amazon-S3—Datenereignisse und analysiert sie auf bösartige und verdächtige Aktivitäten. Weitere Informationen finden Sie GuardDuty unter GuardDutyAmazon S3
- Wenn Sie Objektmetadaten für einen bestimmten Bucket manuell aktualisieren, meldet Macie vorübergehend Unbekannt für Verschlüsselungsstatistiken, die für die Objekte gelten. Wenn Macie das nächste Mal die tägliche Datenaktualisierung durchführt (innerhalb von 24 Stunden), wertet Macie die Verschlüsselungsmetadaten für die Objekte erneut aus und meldet erneut quantitative Daten für die Statistik.
- Wenn Sie Objektmetadaten für einen bestimmten Bucket manuell aktualisieren, schließt Macie aufgrund unvollständiger mehrteiliger Uploads vorübergehend Daten für alle Objektteile aus, die der Bucket enthält. Wenn Macie das nächste Mal die tägliche Datenaktualisierung durchführt (innerhalb von 24 Stunden), berechnet Macie die Anzahl und die Speichergrößenwerte für die Objekte des Buckets neu und bezieht Daten für die Teile in diese Berechnungen ein.
- In seltenen Fällen kann Macie möglicherweise nicht feststellen, ob ein Bucket öffentlich zugänglich oder gemeinsam genutzt wird oder ob eine serverseitige Verschlüsselung neuer Objekte erforderlich ist. Ein vorübergehendes Problem könnte Macie beispielsweise daran hindern, die erforderlichen Daten abzurufen und zu analysieren. Oder Macie kann möglicherweise nicht vollständig feststellen, ob eine oder mehrere Grundsatzerklärungen einer externen Stelle Zugriff gewähren. In diesen Fällen meldet Macie Unbekannt für die relevanten Statistiken

und Felder im Inventar. Um diese Fälle zu untersuchen, überprüfen Sie die Richtlinien- und Berechtigungseinstellungen des Buckets in Amazon S3.

Beachten Sie außerdem, dass Macie nur dann Richtlinienergebnisse generiert, wenn die Sicherheit oder der Datenschutz eines Buckets eingeschränkt werden, nachdem Sie Macie für Ihr Konto aktiviert haben. Wenn Sie beispielsweise die Einstellungen für den öffentlichen Zugriff blockieren für einen Bucket deaktivieren, nachdem Sie Macie aktiviert haben, generiert Macie eine BlockPublicAccessDisabledPolicy:iamuser/s3-Suche für den Bucket. Wenn jedoch die Einstellungen zum Blockieren des öffentlichen Zugriffs für einen Bucket deaktiviert waren, als Sie Macie aktiviert haben, und sie weiterhin deaktiviert sind, generiert Macie keinen BlockPublicAccessDisabledPolicy:iamuser/S3-Finding für den Bucket.

Wenn Macie die Sicherheit und den Datenschutz eines Buckets bewertet, untersucht es außerdem weder die Zugriffsprotokolle noch analysiert es Benutzer, Rollen und andere relevante Konfigurationen für Konten. Stattdessen analysiert und meldet Macie Daten für wichtige Einstellungen, die auf potenzielle Sicherheitsrisiken hinweisen. Wenn ein Richtlinienbefund beispielsweise darauf hindeutet, dass ein Bucket öffentlich zugänglich ist, bedeutet dies nicht unbedingt, dass eine externe Entität auf den Bucket zugegriffen hat. Ebenso versucht Macie nicht herauszufinden, ob dieser Zugriff beabsichtigt und sicher ist, wenn ein Richtlinienbefund darauf hindeutet, dass ein Bucket mit einer AWS-Konto externen Person innerhalb Ihres Unternehmens geteilt wird. Stattdessen deuten diese Ergebnisse darauf hin, dass eine externe Entität möglicherweise auf die Daten des Buckets zugreifen kann, was ein unbeabsichtigtes Sicherheitsrisiko darstellen kann.

Bewertung Ihres Amazon S3-Sicherheitsstatus mit Amazon Macie

Um den allgemeinen Sicherheitsstatus Ihrer Amazon Simple Storage Service (Amazon S3)-Daten zu bewerten und zu bestimmen, wo Maßnahmen ergriffen werden sollen, können Sie das Übersichts-Dashboard in der Amazon Macie-Konsole verwenden.

Das Übersichts-Dashboard bietet einen Snapshot aggregierter Statistiken für Ihre Amazon S3-Daten in der aktuellen AWS-Region. Die Statistiken enthalten Daten für wichtige Sicherheitsmetriken wie die Anzahl der Buckets, die öffentlich zugänglich sind oder mit anderen geteilt werdenAWS-Konten. Das Dashboard zeigt auch Gruppen aggregierter Erkenntnisdaten für Ihr Konto an, z. B. die Arten von Erkenntnissen, die in den letzten sieben Tagen am häufigsten aufgetreten sind. Wenn Sie der Macie-Administrator für eine Organisation sind, stellt das Dashboard aggregierte Statistiken und Daten für alle Konten in Ihrer Organisation bereit. Sie können die Daten optional nach Konto filtern.

Um eine tiefere Analyse durchzuführen, können Sie die unterstützenden Daten für einzelne Elemente im Dashboard aufschlüsseln und überprüfen. Sie können Ihren S3-Bucket-Bestand auch mithilfe der Amazon-Macie-Konsole überprüfen und analysieren oder Bestandsdaten programmgesteuert mithilfe der -DescribeBucketsOperation der Amazon Macie-Macie-API abfragen und analysieren. Amazon Macie

Themen

- Anzeigen des Übersichts-Dashboards
- Grundlegendes zu den Komponenten des Übersichts-Dashboards
- Grundlegendes zu Datensicherheitsstatistiken im Übersichts-Dashboard

Anzeigen des Übersichts-Dashboards

In der Amazon Macie-Konsole bietet das Übersichts-Dashboard einen Snapshot aggregierter Statistiken und Ergebnisdaten für Ihre Amazon S3-Daten in der aktuellen AWS-Region. Wenn Sie die Statistiken lieber programmgesteuert abfragen möchten, können Sie die -GetBucketStatisticsOperation der Amazon Macie-API verwenden.

So zeigen Sie das Übersichts-Dashboard an

1. Öffnen Sie die Amazon Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich Zusammenfassung aus. Macie zeigt das Übersichts-Dashboard an.
3. Um festzustellen, wann Macie zuletzt Bucket- oder Objektmetadaten von Amazon S3 für Ihr Konto abgerufen hat, lesen Sie das Feld Letzte Aktualisierung oben im Dashboard. Weitere Informationen finden Sie unter Datenaktualisierungen.
4. Um die unterstützenden Daten für ein Element im Dashboard aufzuschlüsseln und zu überprüfen, wählen Sie das Element aus.

Wenn Sie der Macie-Administrator für eine Organisation sind, zeigt das Dashboard aggregierte Statistiken und Daten für Ihre Konto- und Mitgliedskonten in Ihrer Organisation an. Um das Dashboard zu filtern und Daten nur für ein bestimmtes Konto anzuzeigen, geben Sie die ID des Kontos in das Feld Konto über dem Dashboard ein.

Grundlegendes zu den Komponenten des Übersichts-Dashboards

Im Übersichts-Dashboard sind Statistiken und Daten in mehrere Abschnitte unterteilt. Oben im Dashboard finden Sie aggregierte Statistiken, die angeben, wie viele Daten Sie in Amazon S3 speichern und wie viele dieser Daten Amazon Macie analysieren kann, um sensible Daten zu erkennen. Sie können auch im Feld Letzte Aktualisierung nachsehen, wann Macie zuletzt Bucket- oder Objektmetadaten von Amazon S3 für Ihr Konto abgerufen hat. Zusätzliche Abschnitte enthalten Statistiken und Daten zu aktuellen Erkenntnissen, mit denen Sie die Sicherheit, den Datenschutz und die Vertraulichkeit Ihrer Amazon S3-Daten in der aktuellen bewerten könnenAWS-Region.

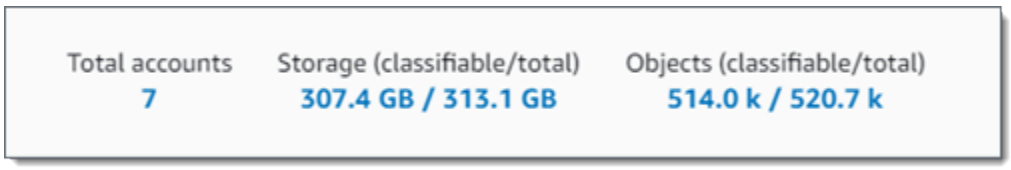
Statistiken und Daten sind in den folgenden Abschnitten unterteilt:

Erkennung von Speicher und sensiblen Daten | Automatisierte Erkennungs- und Abdeckungsprobleme | Datensicherheit | Top-S3-Buckets | Top-Erkenntnistypen | Richtlinienergebnisse

Wählen Sie bei der Überprüfung der einzelnen Abschnitte optional ein Element aus, das Sie aufschlüsseln und die unterstützenden Daten überprüfen möchten.

Erkennung von Speicher- und sensiblen Daten

Die Statistiken oben im Dashboard geben an, wie viele Daten Sie in Amazon S3 speichern und wie viel von diesen Daten Macie analysieren kann, um sensible Daten zu erkennen. Beispielsweise:



In diesem Abschnitt:

- Konten insgesamt – Dieses Feld wird angezeigt, wenn Sie der Macie-Administrator für eine Organisation sind oder ein eigenständiges Macie-Konto haben. Sie gibt die Gesamtzahl der AWS-Konten eigenen Buckets in Ihrem S3-Bucket-Bestand an. Wenn Sie ein Macie-Administrator sind, ist dies die Gesamtzahl der Macie-Konten, die Sie für Ihre Organisation verwalten. Wenn Sie über ein eigenständiges Macie-Konto verfügen, ist dieser Wert 1.

  Gesamtzahl der S3-Buckets – Dieses Feld wird angezeigt, wenn Ihr Macie-Konto Mitglied einer Organisation ist. Sie gibt die Gesamtzahl der Buckets in Ihrem Bestand an, einschließlich Buckets, die keine Objekte enthalten.

- Speicher – Diese Metriken liefern Informationen über die Speichergröße von Objekten in Ihrem Bucket-Bestand:
  - Klassifizierbar – Die Gesamtspeichergröße aller Objekte, die Macie in den Buckets analysieren kann.
  - Gesamt – Die Gesamtspeichergröße aller Objekte in den Buckets, einschließlich Objekte, die Macie nicht analysieren kann.

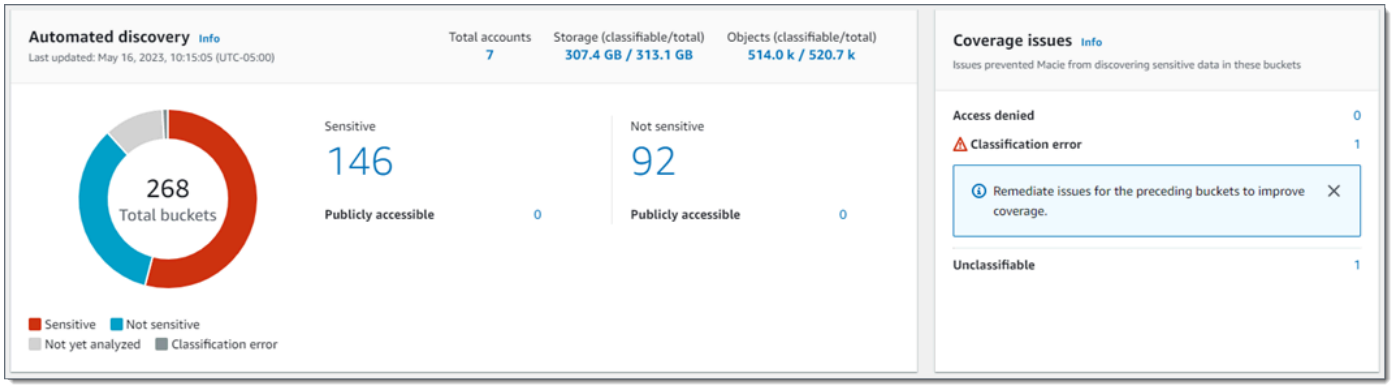
  Wenn es sich bei einem der Objekte um komprimierte Dateien handelt, geben diese Werte nicht die tatsächliche Größe dieser Dateien nach der Dekomprimierung wieder. Wenn Versioning für einen der Buckets aktiviert ist, basieren diese Werte auf der Speichergröße der neuesten Version jedes Objekts in diesen Buckets.
- Objekte – Diese Metriken liefern Informationen über die Anzahl der Objekte in Ihrem Bucket-Bestand:
  - Klassifizierbar – Die Gesamtzahl der Objekte, die Macie in den Buckets analysieren kann.
  - Gesamt – Die Gesamtzahl der Objekte in den Buckets, einschließlich der Objekte, die Macie nicht analysieren kann.

In den vorherigen Statistiken sind Daten und Objekte klassifizierbar, wenn sie eine unterstützte Amazon S3-Speicherklasse verwenden und eine Dateinamenerweiterung für ein unterstütztes Datei- oder Speicherformat haben. Sie können sensible Daten in den Objekten mithilfe von Macie erkennen. Weitere Informationen finden Sie unter Unterstützte Speicherklassen und -formate.

Beachten Sie, dass Speicher- und Objektstatistiken keine Daten zu Objekten in Buckets enthalten, auf die Macie nicht zugreifen darf. Zum Beispiel Objekte in Buckets mit restriktiven Bucket-Richtlinien. Um Buckets zu identifizieren, in denen dies der Fall ist, können Sie Ihren Bucket-Bestand mithilfe der S3-Bucket-Tabelle überprüfen. S3 Wenn das Warnsymbol (⚠) neben dem Namen eines Buckets angezeigt wird, darf Macie nicht auf den Bucket zugreifen.

Probleme bei der automatisierten Erkennung und Abdeckung

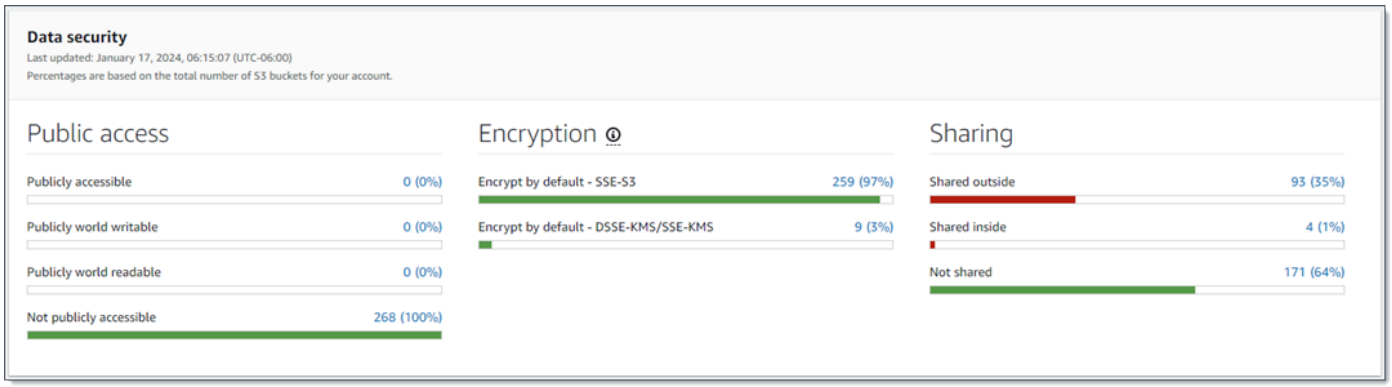
Wenn die automatische Erkennung sensibler Daten für Ihr Konto aktiviert ist, werden diese Abschnitte im Dashboard angezeigt. Die Statistiken in diesen Abschnitten erfassen den Status und die Ergebnisse automatisierter Aktivitäten zur Erkennung sensibler Daten, die Macie bisher für Ihre Amazon S3-Daten ausgeführt hat. Beispielsweise:



Einzelheiten zu diesen Statistiken finden Sie unter Überprüfung der aggregierten Statistiken zur Datensensitivität im Übersichts-Dashboard.

Datensicherheit

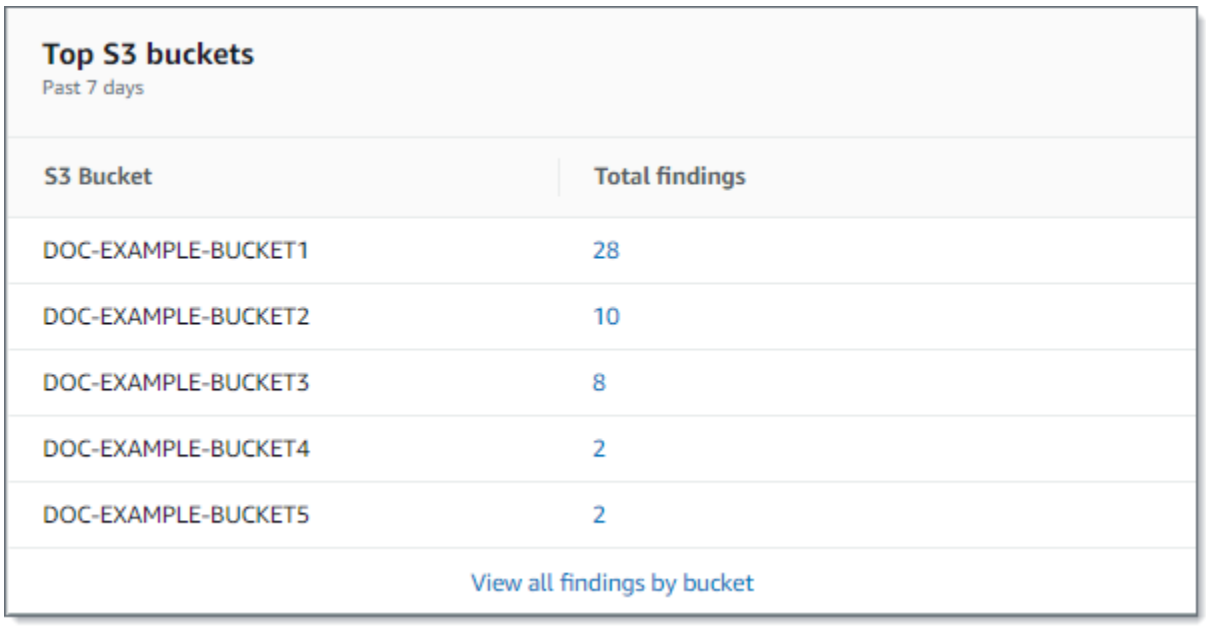
Dieser Abschnitt enthält Statistiken, die auf potenzielle Sicherheits- und Datenschutzrisiken für Ihre Amazon S3-Daten hinweisen. Beispielsweise:



Einzelheiten zu diesen Statistiken finden Sie unter Grundlegendes zu Datensicherheitsstatistiken im Übersichts-Dashboard.

Top-S3-Buckets

In diesem Abschnitt werden die S3-Buckets aufgeführt, die in den letzten sieben Tagen für bis zu fünf Buckets die meisten Erkenntnisse eines beliebigen Typs generiert haben. Sie gibt auch die Anzahl der Erkenntnisse an, die Macie für jeden Bucket erstellt hat. Beispielsweise:

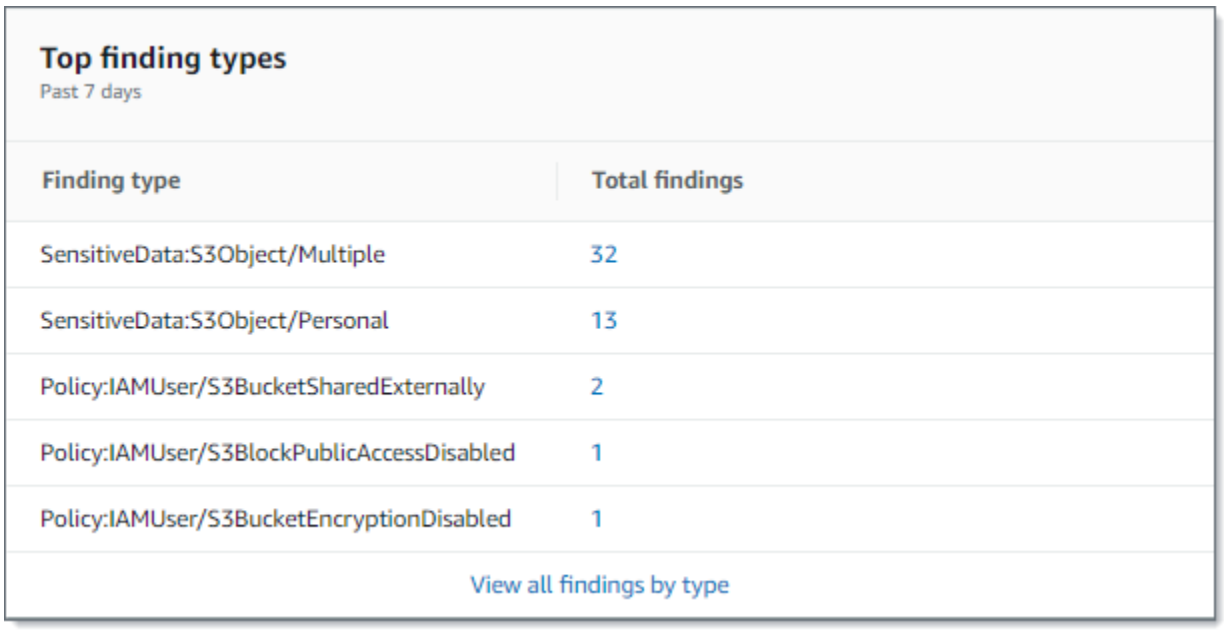


Um alle Ergebnisse für einen Bucket in den letzten sieben Tagen anzuzeigen und optional aufzuschlüsseln, wählen Sie den Wert im Feld Gesamte Ergebnisse aus. Um alle aktuellen Ergebnisse für alle Ihre Buckets anzuzeigen, gruppiert nach Bucket, wählen Sie Alle Ergebnisse nach Bucket anzeigen.

Dieser Abschnitt ist leer, wenn Macie in den letzten sieben Tagen keine Ergebnisse erstellt hat. Oder alle Erkenntnisse, die in den letzten sieben Tagen erstellt wurden, wurden durch eine Unterdrückungsregel unterdrückt.

Top-Erkenntnistypen

In diesem Abschnitt werden die Arten von Erkenntnissen aufgeführt, die in den letzten sieben Tagen am häufigsten aufgetreten sind, und zwar für bis zu fünf Arten von Erkenntnissen. Sie gibt auch die Anzahl der Erkenntnisse an, die Macie für jeden Typ erstellt hat. Beispielsweise:



Um alle Erkenntnisse eines bestimmten Typs in den letzten sieben Tagen anzuzeigen und optional aufzuschlüsseln, wählen Sie den Wert im Feld Gesamte Erkenntnisse aus. Um alle aktuellen Ergebnisse anzuzeigen, gruppiert nach Erkenntnistyp, wählen Sie Alle Ergebnisse nach Typ anzeigen aus.

Dieser Abschnitt ist leer, wenn Macie in den letzten sieben Tagen keine Ergebnisse erstellt hat. Oder alle Erkenntnisse, die in den letzten sieben Tagen erstellt wurden, wurden durch eine Unterdrückungsregel unterdrückt.

Richtlinienergebnisse

In diesem Abschnitt werden die Richtlinienergebnisse aufgeführt, die Macie zuletzt erstellt oder aktualisiert hat, und zwar für bis zu zehn Ergebnisse. Beispielsweise:

Um die Details einer bestimmten Erkenntnis anzuzeigen, wählen Sie die Erkenntnis aus.

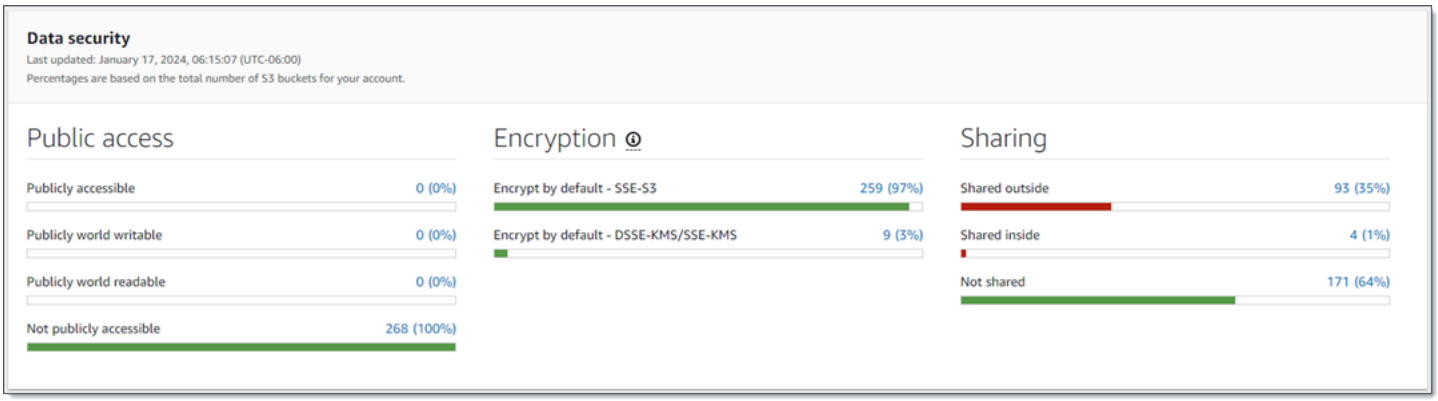
Dieser Abschnitt ist leer, wenn Macie in den letzten sieben Tagen keine Richtlinienergebnisse erstellt oder aktualisiert hat. Oder alle Richtlinienergebnisse, die in den letzten sieben Tagen erstellt oder aktualisiert wurden, wurden durch eine Unterdrückungsregel unterdrückt.

Grundlegendes zu Datensicherheitsstatistiken im Übersichts-Dashboard

Der Abschnitt Datensicherheit des Übersichts-Dashboards enthält Statistiken, mit denen Sie potenzielle Sicherheits- und Datenschutzrisiken für Ihre Amazon S3-Daten in der aktuellen identifizieren und untersuchen könnenAWS-Region. Sie können diese Daten beispielsweise verwenden, um S3-Buckets zu identifizieren, die öffentlich zugänglich sind oder mit anderen geteilt werdenAWS-Konten.

Wenn Ihr Macie-Konto Mitglied einer Organisation ist, geben Speicher- und Erkennungsstatistiken für sensible Daten oben in diesem Abschnitt an, wie viele Daten Sie in Amazon S3 speichern und wie viel von diesen Daten Macie analysieren kann, um sensible Daten zu erkennen.

Für jede Art von Macie-Konto sind zusätzliche Statistiken in drei Bereiche unterteilt, wie in der folgenden Abbildung gezeigt.



Einzelne Statistiken in jedem Bereich lauten wie folgt.

Öffentlicher Zugriff

Diese Statistiken geben an, wie viele S3-Buckets öffentlich zugänglich sind oder nicht:

- Öffentlich zugänglich – Die Anzahl und der Prozentsatz der Buckets, die es der allgemeinen Öffentlichkeit ermöglichen, Lese- oder Schreibzugriff auf den Bucket zu haben.
- Öffentlich beschreibbar – Die Anzahl und der Prozentsatz der Buckets, die es der allgemeinen Öffentlichkeit ermöglichen, Schreibzugriff auf den Bucket zu haben.

- Öffentlich weltweit lesbar – Die Anzahl und der Prozentsatz der Buckets, die es der allgemeinen Öffentlichkeit ermöglichen, Lesezugriff auf den Bucket zu haben.
- Nicht öffentlich zugänglich – Die Anzahl und der Prozentsatz der Buckets, die es der allgemeinen Öffentlichkeit nicht erlauben, Lese- oder Schreibzugriff auf den Bucket zu haben.

Um jeden Prozentsatz zu berechnen, dividiert Macie die Anzahl der anwendbaren Buckets durch die Gesamtzahl der Buckets in Ihrem Bucket-Bestand.

Um die Werte in diesem Abschnitt zu ermitteln, analysiert Macie eine Kombination von Einstellungen auf Konto- und Bucket-Ebene für jeden Bucket: die Block Public Access-Einstellungen für das Konto, die Block Public Access-Einstellungen für den Bucket, die Bucket-Richtlinie für den Bucket und die Zugriffskontrollliste (ACL) für den Bucket. Informationen zu diesen Einstellungen finden Sie unter Identity and Access Management in Amazon S3 und Blockieren des öffentlichen Zugriffs auf Ihren Amazon S3-Speicher im Benutzerhandbuch für Amazon Simple Storage Service.

In bestimmten Fällen zeigt der Abschnitt Öffentlicher Zugriff auch Werte für Unbekannt an. Wenn diese Werte angezeigt werden, konnte Macie die Einstellungen für den öffentlichen Zugriff für die angegebene Anzahl und den Prozentsatz der Buckets nicht auswerten. Beispielsweise verhinderte ein temporäres Problem oder die Berechtigungseinstellungen der Buckets, dass Macie die erforderlichen Daten abrufte. Oder Macie konnte nicht vollständig bestimmen, ob eine oder mehrere Richtlinienanweisungen einer externen Entität den Zugriff auf die Buckets erlauben.

Verschlüsselung

Diese Statistiken geben an, wie viele S3-Buckets so konfiguriert sind, dass bestimmte Arten der serverseitigen Verschlüsselung auf Objekte angewendet werden, die den Buckets hinzugefügt werden:

- Standardmäßig verschlüsseln – SSE-S3 – Die Anzahl und der Prozentsatz der Buckets, deren Standardverschlüsselungseinstellungen für die Verschlüsselung neuer Objekte mit einem von Amazon S3 verwalteten Schlüssel konfiguriert sind. Für diese Buckets werden neue Objekte automatisch mit SSE-S3-Verschlüsselung verschlüsselt.
- Standardmäßig verschlüsseln – DSSE-KMS/SSE-KMS – Die Anzahl und der Prozentsatz der Buckets, deren Standardverschlüsselungseinstellungen so konfiguriert sind, dass neue Objekte mit einem AWS KMS key, entweder einem Von AWS verwalteter Schlüssel oder einem vom Kunden verwalteten Schlüssel, verschlüsselt werden. Für diese Buckets werden neue Objekte automatisch mit DSSE-KMS- oder SSE-KMS-Verschlüsselung verschlüsselt.

Um jeden Prozentsatz zu berechnen, dividiert Macie die Anzahl der anwendbaren Buckets durch die Gesamtzahl der Buckets in Ihrem Bucket-Bestand.

Um die Werte in diesem Abschnitt zu ermitteln, analysiert Macie die Standardverschlüsselungseinstellungen für jeden Bucket. Ab dem 5. Januar 2023 wendet Amazon S3 automatisch serverseitige Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3) als Basisverschlüsselungsstufe für Objekte an, die Buckets hinzugefügt werden. Sie können optional die Standardverschlüsselungseinstellungen eines Buckets so konfigurieren, dass stattdessen die serverseitige Verschlüsselung mit einem -AWS KMSSchlüssel (SSE-KMS) oder die serverseitige Dual-Layer-Verschlüsselung mit einem -AWS KMSSchlüssel (DSSE-KMS) verwendet wird. Informationen zu den Standardverschlüsselungseinstellungen und -optionen finden Sie unter Festlegen des serverseitigen Standardverschlüsselungsverhaltens für S3-Buckets im Benutzerhandbuch für Amazon Simple Storage Service.

In bestimmten Fällen zeigt der Abschnitt Verschlüsselung auch Werte für Unbekannt an. Wenn diese Werte angezeigt werden, konnte Macie die Standardverschlüsselungseinstellungen für die angegebene Anzahl und den Prozentsatz der Buckets nicht auswerten. Beispielsweise verhinderte ein temporäres Problem oder die Berechtigungseinstellungen der Buckets, dass Macie die erforderlichen Daten abrufte.

Freigabe

Diese Statistiken geben an, wie viele S3-Buckets mit anderen AWS-Konten, Amazon- CloudFront Ursprungszugriffsidentitäten (OAIs) oder CloudFront Ursprungszugriffskontrollen (OACs) geteilt werden oder nicht:

- Freigegeben außerhalb – Die Anzahl und der Prozentsatz der Buckets, die für eine oder mehrere der folgenden oder eine beliebige Kombination der folgenden freigegeben werden: eine CloudFront OAI, eine CloudFront OAC oder ein Konto, das sich nicht in derselben Organisation befindet.
- In freigegeben – Die Anzahl und der Prozentsatz der Buckets, die für ein oder mehrere Konten in derselben Organisation freigegeben werden. Diese Buckets werden nicht mit CloudFront OAIs oder OACs geteilt.
- Nicht freigegeben – Die Anzahl und der Prozentsatz der Buckets, die nicht mit anderen Konten, CloudFront OAIs oder CloudFront OACs geteilt werden.

Um jeden Prozentsatz zu berechnen, dividiert Macie die Anzahl der anwendbaren Buckets durch die Gesamtzahl der Buckets in Ihrem Bucket-Bestand.

Um festzustellen, ob Buckets für andere freigegeben sindAWS-Konten, analysiert Macie die Bucket-Richtlinie und ACL für jeden Bucket. Darüber hinaus ist eine Organisation als eine Reihe von Macie-Konten definiert, die zentral als Gruppe verwandter Konten über AWS Organizations oder durch Macie-Einladung verwaltet werden. Informationen zu Amazon S3-Optionen für die Freigabe von Buckets finden Sie unter Identity and Access Management in Amazon S3 im Benutzerhandbuch für Amazon Simple Storage Service.

> **Note**
>
> In bestimmten Fällen meldet Macie möglicherweise fälschlicherweise, dass ein Bucket mit einem geteilt wirdAWS-Konto, der sich nicht in derselben Organisation befindet. Dies kann vorkommen, wenn Macie die Beziehung zwischen dem `Principal` Element in der Richtlinie eines Buckets und bestimmten AWS globalen Bedingungskontextschlüsseln oder Amazon S3-Bedingungsschlüsseln im `Condition` Element der Richtlinie nicht vollständig auswerten kann. Die entsprechenden Bedingungsschlüssel sind: `aws:PrincipalAccount`, `aws:PrincipalArn`, `aws:PrincipalOrgID`, `aws:PrincipalOrgPathsaws:PrincipalTag`, `aws:PrincipalType`, `aws:SourceAccount`, `aws:SourceArn`, , `aws:userid`, `s3:DataAccessPointAccount`, und `s3:DataAccessPointArn`.
> Um festzustellen, ob dies für einzelne Buckets der Fall ist, wählen Sie im Dashboard die Statistik Freigegeben außerhalb von aus. Notieren Sie sich in der angezeigten Tabelle den Namen der einzelnen Buckets. Verwenden Sie dann Amazon S3, um die Richtlinie jedes Buckets zu überprüfen und festzustellen, ob die Einstellungen für den gemeinsamen Zugriff beabsichtigt und sicher sind.

Um festzustellen, ob Buckets mit CloudFront OAIs oder OACs geteilt werden, analysiert Macie die Bucket-Richtlinie für jeden Bucket. Eine CloudFront OAI oder OAC ermöglicht es Benutzern, über eine oder mehrere angegebene CloudFront Verteilungen auf die Objekte eines Buckets zuzugreifen. Informationen zu CloudFront OAIs und OACs finden Sie unter Beschränken des Zugriffs auf einen Amazon S3-Ursprung im Amazon- CloudFront Entwicklerhandbuch.

In bestimmten Fällen zeigt der Abschnitt Freigabe auch Werte für Unbekannt an. Wenn diese Werte erscheinen, konnte Macie nicht feststellen, ob die angegebene Anzahl und der Prozentsatz der Buckets mit anderen Konten, CloudFront OAIs oder CloudFront OACs geteilt werden. Beispielsweise verhinderte ein temporäres Problem oder die Berechtigungseinstellungen der

Buckets, dass Macie die erforderlichen Daten abrufte. Oder Macie konnte die Richtlinien oder ACLs der Buckets nicht vollständig auswerten.

Analysieren Sie Ihre Amazon S3 S3-Sicherheitslage mit Amazon Macie

Um Sie bei der Durchführung eingehender Analysen und der Bewertung des Sicherheitsstatus Ihrer Amazon Simple Storage Service (Amazon S3) -Daten zu unterstützen, führt Amazon Macie an jedem AWS-Region Ort, an dem Sie Macie verwenden, ein vollständiges Inventar Ihrer S3-Buckets. Informationen darüber, wie Macie dieses Inventar für Sie verwaltet, finden Sie unterSo überwacht Macie die Amazon S3 S3-Datensicherheit. Wenn Sie der Macie-Administrator einer Organisation S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 S3 die

Mithilfe dieses Inventars können Sie Ihren Amazon S3 S3-Datenbestand überprüfen und Details und Statistiken zu wichtigen Sicherheitseinstellungen und Metriken überprüfen, die für einzelne S3-Buckets gelten. Sie können beispielsweise auf Aufschlüsselungen der öffentlichen Zugriffs- und Verschlüsselungseinstellungen der einzelnen Buckets sowie auf die Größe und Anzahl der Objekte zugreifen, die Macie analysieren kann, um sensible Daten in jedem Bucket zu erkennen. Sie können auch ermitteln, ob Sie sensible Datenermittlungsaufträge für die Analyse von Objekten in einem Bucket konfiguriert haben und, falls ja, wann einer dieser Jobs zuletzt ausgeführt wurde. Wenn die automatische Erkennung vertraulicher Daten für Ihr Konto aktiviert ist, können Sie das Inventar auch verwenden, um die Ergebnisse automatisierter Aktivitäten zur Erkennung vertraulicher Daten zu überprüfen, die Macie bisher für Ihr Konto oder Ihr Unternehmen durchgeführt hat. Weitere Informationen finden Sie unter Erkennen vertraulicher Daten.

Sie können Inventardaten mithilfe der S3-Buckets-Seite auf der Amazon Macie Macie-Konsole durchsuchen und filtern. Sie können auch programmgesteuert auf Ihre Inventardaten zugreifen, indem Sie die DescribeBucketsAmazon Macie Macie-API verwenden.

Themen

- Überprüfen Ihres S3-Bucket-Bestands mit Amazon Macie
- Filtern Ihres S3-Bucket-Inventars mit Amazon Macie

Überprüfen Ihres S3-Bucket-Bestands mit Amazon Macie

Auf der Amazon Macie-Konsole bietet die Seite S3-Buckets einen detaillierten Einblick in die Sicherheit und den Datenschutz Ihrer Amazon Simple Storage Service (Amazon S3)-Daten in der aktuellen AWS-Region. Auf dieser Seite können Sie ein vollständiges Inventar Ihrer S3-Buckets in der aktuellen Region überprüfen und analysieren sowie detaillierte Informationen und Statistiken für einzelne Buckets überprüfen. Wenn Sie der Macie-Administrator für eine Organisation sind, enthält Ihr Bestand Details und Statistiken für S3-Buckets, die Mitgliedskonten in Ihrer Organisation gehören.

Auf der Seite S3-Buckets wird auch angegeben, wann Macie zuletzt Bucket- oder Objektmetadaten von Amazon S3 für Ihr Konto abgerufen hat. Diese Informationen finden Sie im Feld Letzte Aktualisierung oben auf der Seite. Wenn Sie der Macie-Administrator für eine Organisation sind, gibt dieses Feld das früheste Datum und die früheste Uhrzeit an, zu der Macie die Daten für ein Konto in Ihrer Organisation abgerufen hat. Weitere Informationen finden Sie unter Datenaktualisierungen.

Beachten Sie, dass die meisten Bestandsdaten auf Buckets beschränkt sind, auf die Macie für Ihr Konto zugreifen darf. Wenn die Berechtigungseinstellungen eines Buckets verhindern, dass Macie Informationen über den Bucket oder die Objekte des Buckets abruft, kann Macie nur eine Teilmenge von Informationen über den Bucket bereitstellen. Wenn dies für einen bestimmten Bucket der Fall ist, zeigt Macie ein Warnsymbol (⚠) und eine Meldung für den Bucket in Ihrem Bucket-Bestand an. Für die Details des Buckets zeigt Macie nur eine Teilmenge von Feldern und Daten an: die Konto-ID für das AWS-Konto, das den Bucket besitzt, den Namen des Buckets, den Amazon-Ressourcennamen (ARN), das Erstellungsdatum und die Region und, als Macie im Rahmen des täglichen Aktualisierungszyklus zuletzt sowohl Bucket- als auch Objektmetadaten für den Bucket abgerufen hat. Um das Problem zu untersuchen, überprüfen Sie die Richtlinien- und Berechtigungseinstellungen des Buckets in Amazon S3. Beispielsweise könnte der Bucket eine restriktive Bucket-Richtlinie haben. Weitere Informationen finden Sie unter Macie den Zugriff von S3-Buckets und -Objekten erlauben.

Wenn Sie es vorziehen, programmgesteuert auf Ihre Bestandsdaten zuzugreifen und diese abzufragen, können Sie die -DescribeBucketsOperation der Amazon Macie-API verwenden.

Themen

- Überprüfen Ihres S3-Bucket-Bestands
- Überprüfen der Details von S3-Buckets

Überprüfen Ihres S3-Bucket-Bestands

Die Seite S3-Buckets in der Amazon Macie-Konsole enthält Informationen zu Ihren S3-Buckets in der aktuellen AWS-Region. Auf dieser Seite zeigt eine Tabelle zusammenfassende Informationen für jeden Bucket in Ihrem Bestand an. Um Ihre Ansicht anzupassen, können Sie die Tabelle sortieren und filtern. Wenn Sie einen Bucket in der Tabelle auswählen, werden im Detailbereich zusätzliche Informationen über den Bucket angezeigt. Dazu gehören Details und Statistiken für Einstellungen und Metriken, die einen Einblick in die Sicherheit und den Datenschutz der Daten des Buckets geben. Optional können Sie Daten aus der Tabelle in eine CSV-Datei (durch Kommas getrennte Werte) exportieren.

Wenn die automatische Erkennung sensibler Daten für Ihr Konto aktiviert ist, haben Sie auch die Möglichkeit, Ihren Bestand mithilfe einer interaktiven Heatmap zu überprüfen. Die Karte bietet eine visuelle Darstellung der Datensensibilität in Ihrem Amazon S3-Datenbestand. Es erfasst die Ergebnisse automatisierter Aktivitäten zur Erkennung sensibler Daten, die Macie für Ihr Konto oder Ihre Organisation durchgeführt hat. Weitere Informationen zu dieser Karte finden Sie unter Visualisierung der Datensensitivität mit der S3-Buckets-Map.

So überprüfen Sie Ihren S3-Bucket-Bestand

1. Öffnen Sie die Amazon Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich S3-Buckets aus. Auf der Seite S3-Buckets wird Ihr Bucket-Bestand angezeigt.

   Wenn die Seite eine interaktive Karte Ihres Bucket-Bestands anzeigt, wählen Sie oben auf der Seite Tabelle
   ().
   Macie zeigt dann die Anzahl der Buckets in Ihrem Bestand und eine Tabelle der Buckets an.
3. Wählen Sie oben auf der Seite optional Aktualisieren
   (),
   um die neuesten Bucket-Metadaten von Amazon S3 abzurufen.

   Wenn das Informationssymbol
   ()
   neben Bucket-Namen angezeigt wird, empfehlen wir Ihnen, dies zu tun. Dieses Symbol zeigt an, dass in den letzten 24 Stunden ein Bucket erstellt wurde, möglicherweise nachdem Macie im Rahmen des täglichen Aktualisierungszyklus Bucket- und Objektmetadaten von Amazon S3 abgerufen hat.

4. Verwenden Sie auf der Seite S3-Buckets die Tabelle, um eine Teilmenge der Informationen zu jedem Bucket in Ihrem Bestand zu überprüfen:

   - Sensitivität – Der aktuelle Sensitivitätswert des Buckets. Diese Spalte wird nur angezeigt, wenn die automatische Erkennung sensibler Daten für Ihr Konto aktiviert ist. Informationen zum Bereich der von Macie definierten Empfindlichkeitswerte finden Sie unter Empfindlichkeitsbewertung für S3-Buckets.
   - Bucket – Der Name des Buckets.
   - Konto – Die Konto-ID für das AWS-Konto, dem der Bucket gehört.
   - Klassifizierbare Objekte – Die Gesamtzahl der Objekte, die Macie analysieren kann, um sensible Daten im Bucket zu erkennen.
   - Klassifizierbare Größe – Die Gesamtspeichergröße aller Objekte, die Macie analysieren kann, um sensible Daten im Bucket zu erkennen.

     Beachten Sie, dass dieser Wert nicht die tatsächliche Größe komprimierter Objekte nach der Dekomprimierung widerspiegelt. Wenn Versioning für den Bucket aktiviert ist, basiert dieser Wert auch auf der Speichergröße der neuesten Version jedes Objekts im Bucket.
   - Überwacht nach Auftrag – Ob Aufträge zur Erkennung sensibler Daten so konfiguriert sind, dass Objekte im Bucket täglich, wöchentlich oder monatlich analysiert werden.

     Wenn der Wert für dieses Feld Ja lautet, wird der Bucket explizit in einen periodischen Auftrag aufgenommen oder der Bucket hat die Kriterien für einen periodischen Auftrag innerhalb der letzten 24 Stunden erfüllt. Darüber hinaus lautet der Status mindestens eines dieser Aufträge nicht Storniert. Macie aktualisiert diese Daten täglich.
   - Letzte Auftragsausführung – Wenn einmalige oder regelmäßige Aufträge zur Erkennung sensibler Daten für die Analyse von Objekten im Bucket konfiguriert sind, gibt der Wert für dieses Feld das letzte Datum und die Uhrzeit an, zu der eine dieser Aufträge ausgeführt wurde. Andernfalls ist dieses Feld leer.

   In den vorherigen Daten sind Objekte klassifizierbar, wenn sie eine unterstützte Amazon S3-Speicherklasse verwenden und eine Dateinamenerweiterung für ein unterstütztes Datei- oder Speicherformat haben. Sie können sensible Daten in den Objekten mithilfe von Macie erkennen. Weitere Informationen finden Sie unter Unterstützte Speicherklassen und -formate.
5. Führen Sie einen der folgenden Schritte aus, um Ihren Bestand mithilfe der Tabelle zu analysieren:

- Um die Tabelle nach einem bestimmten Feld zu sortieren, klicken Sie auf die Spaltenüberschrift für das Feld. Um die Sortierreihenfolge zu ändern, klicken Sie erneut auf die Spaltenüberschrift.
- Um die Tabelle zu filtern und nur die Buckets anzuzeigen, die einen bestimmten Wert für ein Feld haben, platzieren Sie den Cursor in das Filterfeld und fügen Sie dann eine Filterbedingung für das Feld hinzu. Um die Ergebnisse weiter zu verfeinern, fügen Sie Filterbedingungen für zusätzliche Felder hinzu. Weitere Informationen finden Sie unter Filtern Ihres S3-Bucket-Inventars.

6. Um Details und Statistiken für einen bestimmten Bucket zu überprüfen, wählen Sie den Namen des Buckets in der Tabelle aus und verweisen Sie dann auf den Detailbereich.

> **Tip**
>
> Sie können viele der Felder im Bucket-Detailbereich pivotieren und aufschlüsseln. Um Buckets anzuzeigen, die denselben Wert für ein Feld haben, wählen Sie
>
> im Feld aus. Um Buckets anzuzeigen, die andere Werte für ein Feld haben, wählen Sie
>
> im Feld aus.

7. Um Daten aus der Tabelle in eine CSV-Datei zu exportieren, aktivieren Sie das Kontrollkästchen für jede Zeile, die Sie exportieren möchten, oder aktivieren Sie das Kontrollkästchen in der Überschrift der Auswahlspalte, um alle Zeilen auszuwählen. Wählen Sie dann oben auf der Seite In CSV exportieren aus. Sie können bis zu 50.000 Zeilen aus der Tabelle exportieren.

Überprüfen der Details von S3-Buckets

In der Amazon Macie-Konsole können Sie den Detailbereich auf der Seite S3-Buckets verwenden, um Statistiken und andere Informationen zu einzelnen S3-Buckets in Ihrem Bucket-Bestand zu überprüfen. Dazu gehören Details und Statistiken für Einstellungen und Metriken, die einen Einblick in die Sicherheit und den Datenschutz der Daten eines Buckets geben.

Sie können beispielsweise Aufschlüsselungen der Einstellungen für den öffentlichen Zugriff eines S3-Buckets überprüfen und feststellen, ob ein Bucket so konfiguriert ist, dass Objekte repliziert werden oder für andere freigegeben wirdAWS-Konten. Sie können auch feststellen, ob Aufträge zur Erkennung sensibler Daten so konfiguriert sind, dass der Bucket auf sensible Daten überprüft

wird. Wenn dies der Fall ist, können Sie auf Details zu dem Auftrag zugreifen, der zuletzt ausgeführt wurde, und optional alle Ergebnisse anzeigen, die der Auftrag erstellt hat.

Wenn die automatische Erkennung sensibler Daten für Ihr Konto aktiviert ist, können Sie auch den Detailbereich verwenden, um Statistiken zur Erkennung sensibler Daten und andere Informationen zu einzelnen S3-Buckets zu überprüfen. Das Panel erfasst die Ergebnisse automatisierter Aktivitäten zur Erkennung sensibler Daten, die Macie bisher für einen Bucket ausgeführt hat. Weitere Informationen zu diesen Details finden Sie unter Überprüfung der Details zur Datensensitivität für einzelne S3-Buckets.

So überprüfen Sie die Details eines S3-Buckets

1. Öffnen Sie die Amazon Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich S3-Buckets aus. Auf der Seite S3-Buckets wird Ihr Bucket-Bestand angezeigt.
3. Wählen Sie oben auf der Seite optional Aktualisieren
   (),
   um die neuesten Bucket-Metadaten von Amazon S3 abzurufen.
4. Wählen Sie in der Tabelle oder Zuordnung der S3-Buckets den Bucket aus, dessen Details Sie überprüfen möchten. Im Detailbereich werden Statistiken und andere Informationen zum Bucket angezeigt.

Im Detailbereich sind Bucket-Statistiken und -Informationen in den folgenden primären Abschnitten unterteilt:

Übersicht | Objektstatistiken | Serverseitige Verschlüsselung | Erkennung sensibler Daten | Öffentlicher Zugriff | Replikation | Tags

Wenn Sie die Informationen in jedem Abschnitt überprüfen, können Sie optional bestimmte Felder pivotieren und aufschlüsseln. Um Buckets anzuzeigen, die denselben Wert für ein Feld haben, wählen Sie

im Feld aus. Um Buckets anzuzeigen, die andere Werte für ein Feld haben, wählen Sie

im Feld aus.

Übersicht

Dieser Abschnitt enthält allgemeine Informationen über den Bucket, z. B. den Namen des Buckets, wann der Bucket erstellt wurde und die Konto-ID für das AWS-Konto, dem der Bucket gehört. Beachten Sie, dass das Feld Letzte Aktualisierung angibt, wann Macie zuletzt Metadaten für den Bucket oder die Objekte des Buckets von Amazon S3 abgerufen hat.

Das Feld Freigegebener Zugriff gibt an, ob der Bucket mit einem anderen AWS-Konto, einer Amazon- CloudFront Ursprungszugriffsidentität (Origin Access Identity, OAI) oder einer CloudFront Ursprungszugriffssteuerung (Origin Access Control, OAC) geteilt wird:

- Extern – Der Bucket wird mit einer oder mehreren der folgenden oder einer beliebigen Kombination der folgenden geteilt: einer CloudFront OAI, einer CloudFront OAC oder einem Konto, das außerhalb (nicht Teil) Ihrer Organisation ist.
- Intern – Der Bucket wird für ein oder mehrere Konten freigegeben, die intern in Ihrer Organisation (Teil davon) sind. Sie wird nicht mit einer CloudFront OAI oder OAC geteilt.
- Nicht freigegeben – Der Bucket wird nicht mit einem anderen Konto, einer CloudFront OAI oder einer CloudFront OAC geteilt.
- Unbekannt – Macie konnte die Einstellungen für den gemeinsamen Zugriff für den Bucket nicht auswerten.

Um festzustellen, ob ein Bucket mit einem anderen geteilt wirdAWS-Konto, analysiert Macie die Bucket-Richtlinie und die Zugriffskontrollliste (ACL) für den Bucket. Die Analyse ist auf Einstellungen auf Bucket-Ebene beschränkt. Sie spiegelt keine Einstellungen auf Objektebene für die Freigabe bestimmter Objekte im Bucket wider. Darüber hinaus ist eine Organisation als eine Reihe von Macie-Konten definiert, die zentral als Gruppe verwandter Konten über AWS Organizations oder durch Macie-Einladung verwaltet werden. Weitere Informationen zu Amazon S3-Optionen für die Freigabe von Buckets finden Sie unter Identity and Access Management in Amazon S3 im Benutzerhandbuch für Amazon Simple Storage Service.

> **Note**
>
> In bestimmten Fällen weist Macie möglicherweise fälschlicherweise darauf hin, dass ein Bucket mit einem geteilt wirdAWS-Konto, der außerhalb (nicht Teil) Ihrer Organisation ist. Dies kann passieren, wenn Macie die Beziehung zwischen dem -`Principal`Element in der Richtlinie des Buckets und bestimmten AWS globalen Bedingungskontextschlüsseln oder Amazon S3-Bedingungsschlüsseln im -`Condition`Element der Richtlinie

nicht vollständig auswerten kann. Die entsprechenden Bedingungsschlüssel sind: `aws:PrincipalAccount`, `aws:PrincipalArn`, `aws:PrincipalOrgID`, `aws:PrincipalOrgPathsaws:PrincipalTag`, `aws:PrincipalType`, `aws:SourceAccount`, `aws:SourceArn`, , `aws:userid`, `s3:DataAccessPointAccount`, und `s3:DataAccessPointArn`. Wir empfehlen Ihnen, die Richtlinie des Buckets zu überprüfen, um festzustellen, ob dieser Zugriff beabsichtigt und sicher ist.

Um festzustellen, ob ein Bucket mit einer CloudFront OAI oder OAC geteilt wird, analysiert Macie die Bucket-Richtlinie für den Bucket. Eine CloudFront OAI oder OAC ermöglicht es Benutzern, über eine oder mehrere angegebene CloudFront Verteilungen auf die Objekte eines Buckets zuzugreifen. Weitere Informationen zu CloudFront OAIs und OACs finden Sie unter Beschränken des Zugriffs auf einen Amazon S3-Ursprung im Amazon- CloudFront Entwicklerhandbuch.

Der Abschnitt Übersicht des Panels enthält auch das Feld Letzte automatisierte Erkennungsausführung. Wenn die automatische Erkennung sensibler Daten für Ihr Konto aktiviert ist, gibt dieses Feld an, wann Macie zuletzt Objekte im Bucket analysiert hat, während die automatische Erkennung für Ihr Konto durchgeführt wird. Wenn die automatische Erkennung sensibler Daten für Ihr Konto deaktiviert ist, wird in diesem Feld ein Bindestrich (–) angezeigt.

Objektstatistiken

Dieser Abschnitt enthält Informationen zu den Objekten im Bucket, beginnend mit der Gesamtzahl der Objekte im Bucket (Gesamtzahl), der Gesamtspeichergröße all dieser Objekte (Gesamtspeichergröße) und der Gesamtspeichergröße aller komprimierten Objekte (.gz, .gzip oder .zip) (Gesamtgröße komprimiert). Zusätzliche Statistiken in diesem Abschnitt können Ihnen bei der Bewertung helfen, wie viele Daten Macie analysieren kann, um sensible Daten im Bucket zu erkennen.

Wenn Sie kürzlich den Bucket erstellt oder in den letzten 24 Stunden signifikante Änderungen an den Objekten des Buckets vorgenommen haben, wählen Sie optional Aktualisieren (), um die neuesten Metadaten für die Objekte des Buckets abzurufen. Macie zeigt das Informationssymbol () an, um festzustellen, ob dies der Fall sein könnte. Die Aktualisierungsoption ist verfügbar, wenn ein Bucket 30.000 oder weniger Objekte enthält.

Beachten Sie bei der Überprüfung der Statistiken in diesem Abschnitt Folgendes:

- Wenn das Versioning für den Bucket aktiviert ist, basieren die Größenwerte auf der Speichergröße der neuesten Version jedes Objekts im Bucket.
- Wenn der Bucket komprimierte Objekte enthält, geben die Größenwerte nicht die tatsächliche Größe dieser Objekte nach der Dekomprimierung wieder.
- Wenn Sie Objektmetadaten für einen Bucket aktualisieren, meldet Macie vorübergehend Unbekannt für Verschlüsselungsstatistiken, die für die Objekte gelten. Macie bewertet und aktualisiert die Daten für diese Statistiken erneut, wenn es die nächste tägliche Aktualisierung der Bucket- und Objektmetadaten durchführt, die innerhalb von 24 Stunden erfolgt.
- Standardmäßig enthalten Objektanzahl und Größenwerte Daten für alle Objektteile, die der Bucket aufgrund unvollständiger mehrteiliger Uploads enthält. Wenn Sie Objektmetadaten für einen Bucket aktualisieren, schließt Macie Daten für Objektteile aus den neu berechneten Werten aus. Wenn Macie die nächste tägliche Aktualisierung der Bucket- und Objektmetadaten (innerhalb von 24 Stunden) durchführt, berechnet und aktualisiert Macie die Werte für diese Statistiken neu und schließt Daten für Objektteile erneut in die Werte ein.

  Beachten Sie, dass Macie keine Objektteile analysieren kann, um sensible Daten zu erkennen. Amazon S3 muss zuerst die Zusammenstellung der Teile in einem oder mehreren Objekten abschließen, damit Macie sie analysieren kann. Informationen zu mehrteiligen Uploads und Objektteilen, einschließlich zum automatischen Löschen von Teilen mit Lebenszyklusregeln, finden Sie unter Hochladen und Kopieren von Objekten mit mehrteiligen Uploads im Benutzerhandbuch für Amazon Simple Storage Service. Um Buckets zu identifizieren, die Objektteile enthalten, können Sie in Amazon S3 Storage Lens auf unvollständige mehrteilige Upload-Metriken verweisen. Weitere Informationen finden Sie unter Bewerten Ihrer Speicheraktivität und -nutzung im Benutzerhandbuch für Amazon Simple Storage Service.

Objektstatistiken sind wie folgt organisiert.

Klassifizierbare Objekte

Dieser Abschnitt gibt die Gesamtzahl der Objekte an, die Macie analysieren kann, um sensible Daten zu erkennen, sowie die Gesamtspeichergröße dieser Objekte. Diese Objekte verwenden eine unterstützte Amazon S3-Speicherklasse und haben eine Dateinamenerweiterung für ein unterstütztes Datei- oder Speicherformat. Sie können sensible Daten in den Objekten mithilfe von Macie erkennen. Weitere Informationen finden Sie unter Unterstützte Speicherklassen und -formate.

Nicht klassifizierbare Objekte

Dieser Abschnitt gibt die Gesamtzahl der Objekte an, die Macie nicht analysieren kann, um sensible Daten zu erkennen, und die Gesamtspeichergröße dieser Objekte. Diese Objekte verwenden keine unterstützte Amazon S3-Speicherklasse oder sie haben keine Dateinamenerweiterung für ein unterstütztes Datei- oder Speicherformat.

Nicht klassifizierbare Objekte: Speicherklasse

Dieser Abschnitt enthält eine Aufschlüsselung der Anzahl und Speichergröße der Objekte, die Macie nicht analysieren kann, da die Objekte keine unterstützte Amazon S3-Speicherklasse verwenden.

Nicht klassifizierbare Objekte: Dateityp

Dieser Abschnitt enthält eine Aufschlüsselung der Anzahl und Speichergröße der Objekte, die Macie nicht analysieren kann, da die Objekte keine Dateinamenerweiterung für ein unterstütztes Datei- oder Speicherformat haben.

Objekte nach Verschlüsselungstyp

Dieser Abschnitt enthält eine Aufschlüsselung der Anzahl der Objekte, die die einzelnen Verschlüsselungstypen verwenden, die Amazon S3 unterstützt:

- Vom Kunden bereitgestellt – Die Anzahl der Objekte, die mit einem vom Kunden bereitgestellten Schlüssel verschlüsselt sind. Diese Objekte verwenden die SSE-C-Verschlüsselung.
- AWS KMS Von verwaltet – Die Anzahl der Objekte, die mit einem AWS KMS key, entweder einem Von AWS verwalteter Schlüssel oder einem vom Kunden verwalteten Schlüssel, verschlüsselt sind. Diese Objekte verwenden DSSE-KMS- oder SSE-KMS-Verschlüsselung.
- Von Amazon S3 verwaltet – Die Anzahl der Objekte, die mit einem von Amazon S3 verwalteten Schlüssel verschlüsselt sind. Diese Objekte verwenden die SSE-S3-Verschlüsselung.
- Keine Verschlüsselung – Die Anzahl der Objekte, die nicht verschlüsselt sind oder die clientseitige Verschlüsselung verwenden. (Wenn ein Objekt mit clientseitiger Verschlüsselung verschlüsselt ist, kann Macie nicht auf Verschlüsselungsdaten für das Objekt zugreifen und diese melden.)
- Unbekannt – Die Anzahl der Objekte, für die Macie keine aktuellen Verschlüsselungsmetadaten hat. Dies tritt in der Regel auf, wenn Sie sich kürzlich dafür entschieden haben, die Metadaten für die Objekte des Buckets manuell zu aktualisieren. Macie aktualisiert die Verschlüsselungsstatistiken, wenn es die nächste tägliche Aktualisierung der Bucket- und Objektmetadaten durchführt, die innerhalb von 24 Stunden erfolgt.

Informationen zu den einzelnen unterstützten Verschlüsselungstypen finden Sie unter Schützen von Daten durch Verschlüsselung im Benutzerhandbuch für Amazon Simple Storage Service.

Server-side encryption

Dieser Abschnitt bietet einen Einblick in die serverseitigen Verschlüsselungseinstellungen für den Bucket.

Das Feld Für Bucket-Richtlinie erforderliche Verschlüsselung gibt an, ob die Bucket-Richtlinie eine serverseitige Verschlüsselung von Objekten erfordert, wenn Objekte zum Bucket hinzugefügt werden:

- Nein – Der Bucket hat keine Bucket-Richtlinie oder die Bucket-Richtlinie erfordert keine serverseitige Verschlüsselung neuer Objekte. Wenn eine Bucket-Richtlinie vorhanden ist, müssen PutObject Anforderungen keinen gültigen serverseitigen Verschlüsselungs-Header enthalten.
- Ja – Die Bucket-Richtlinie erfordert die serverseitige Verschlüsselung neuer Objekte. -PutObjectAnforderungen für den Bucket müssen einen gültigen serverseitigen Verschlüsselungs-Header enthalten. Andernfalls lehnt Amazon S3 die Anforderung ab.
- Unbekannt – Macie konnte die Richtlinie des Buckets nicht auswerten, um festzustellen, ob eine serverseitige Verschlüsselung neuer Objekte erforderlich ist.

Für diese Bewertung sind gültige serverseitige Verschlüsselungsheader: `x-amz-server-side-encryption` mit einem Wert von `AES256` oder `aws:kms`und `x-amz-server-side-encryption-customer-algorithm` mit einem Wert von `AES256`. Informationen zur Verwendung von Bucket-Richtlinien, um die serverseitige Verschlüsselung neuer Objekte zu verlangen, finden Sie unter Schützen von Daten mit serverseitiger Verschlüsselung im Benutzerhandbuch für Amazon Simple Storage Service.

Das Feld Standardverschlüsselung gibt an, welcher serverseitige Verschlüsselungsalgorithmus für den Bucket so konfiguriert ist, dass er standardmäßig auf Objekte angewendet wird, die dem Bucket hinzugefügt werden:

- AES256 – Die Standardverschlüsselungseinstellungen des Buckets sind so konfiguriert, dass neue Objekte mit einem von Amazon S3 verwalteten Schlüssel verschlüsselt werden. Neue Objekte werden automatisch mit SSE-S3-Verschlüsselung verschlüsselt.
- aws:kms – Die Standardverschlüsselungseinstellungen des Buckets sind so konfiguriert, dass neue Objekte mit einem , entweder einem Von AWS verwalteter Schlüssel oder einem vom Kunden verwalteten SchlüsselAWS KMS key, verschlüsselt werden. Neue Objekte werden automatisch

mit SSE-KMS-Verschlüsselung verschlüsselt. Das AWS KMS key Feld zeigt den Amazon-Ressourcennamen (ARN) oder die eindeutige Kennung (Schlüssel-ID) für den verwendeten Schlüssel an.

- aws:kms:dsse – Die Standardverschlüsselungseinstellungen des Buckets sind so konfiguriert, dass neue Objekte mit einem , entweder einem Von AWS verwalteter Schlüssel oder einem vom Kunden verwalteten SchlüsselAWS KMS key, verschlüsselt werden. Neue Objekte werden automatisch mit DSSE-KMS-Verschlüsselung verschlüsselt. Das AWS KMS key Feld zeigt den ARN oder die Schlüssel-ID für den verwendeten Schlüssel an.
- Keine – Die Standardverschlüsselungseinstellungen des Buckets geben kein serverseitiges Verschlüsselungsverhalten für neue Objekte an.

Ab dem 5. Januar 2023 wendet Amazon S3 automatisch serverseitige Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3) als Basisverschlüsselungsstufe für Objekte an, die Buckets hinzugefügt werden. Sie können optional die Standardverschlüsselungseinstellungen eines Buckets so konfigurieren, dass stattdessen die serverseitige Verschlüsselung mit einem -AWS KMSSchlüssel (SSE-KMS) oder die serverseitige Dual-Layer-Verschlüsselung mit einem -AWS KMSSchlüssel (DSSE-KMS) verwendet wird. Informationen zu den Standardverschlüsselungseinstellungen und -optionen finden Sie unter Festlegen des serverseitigen Standardverschlüsselungsverhaltens für S3-Buckets im Benutzerhandbuch für Amazon Simple Storage Service.

Erkennung sensibler Daten

In diesem Abschnitt wird angegeben, ob Aufträge zur Erkennung sensibler Daten so konfiguriert sind, dass Objekte im Bucket täglich, wöchentlich oder monatlich regelmäßig analysiert werden. Wenn der Wert für das Feld Aktiv überwacht durch Auftrag Ja lautet, wird der Bucket explizit in einen periodischen Auftrag aufgenommen oder der Bucket hat die Kriterien für einen periodischen Auftrag innerhalb der letzten 24 Stunden erfüllt. Darüber hinaus lautet der Status mindestens eines dieser Aufträge nicht Storniert. Macie aktualisiert diese Daten täglich.

Wenn eine Art von Aufgabe zur Erkennung sensibler Daten (entweder ein regelmäßiger Auftrag oder ein einmaliger Auftrag) für die Überprüfung des Buckets konfiguriert ist, enthält das Feld Letzter Auftrag die eindeutige Kennung für den Auftrag, der zuletzt mit der Ausführung begonnen hat. Das Feld Letzte Auftragsausführung gibt an, wann dieser Auftrag gestartet wurde.

> **Tip**
>
> Um alle Ergebnisse zu sensiblen Daten anzuzeigen, die der Auftrag erstellt hat, wählen Sie den Link im Feld Letzter Auftrag aus. Wählen Sie im angezeigten Bereich mit den Auftragsdetails oben im Bereich die Option Ergebnisse anzeigen und dann Ergebnisse anzeigen aus.

Öffentlicher Zugriff

In diesem Abschnitt wird angegeben, ob der Bucket öffentlich zugänglich ist. Es bietet auch eine Aufschlüsselung der verschiedenen Einstellungen auf Konto- und Bucket-Ebene, die bestimmen, ob dies der Fall ist. Das Feld Effektive Berechtigung gibt das kumulative Ergebnis dieser Einstellungen an:

- Nicht öffentlich – Der Bucket ist nicht öffentlich zugänglich.
- Öffentlich – Der Bucket ist öffentlich zugänglich.
- Unbekannt – Macie konnte nicht alle Einstellungen für den öffentlichen Zugriff für den Bucket auswerten.

Beachten Sie, dass diese Daten auf Einstellungen auf Konto- und Bucket-Ebene beschränkt sind. Sie spiegelt keine Einstellungen auf Objektebene wider, die den öffentlichen Zugriff auf bestimmte Objekte in einem Bucket ermöglichen.

Weitere Informationen zu Amazon S3-Einstellungen für die Verwaltung des öffentlichen Zugriffs auf Buckets und Bucket-Daten finden Sie unter Identity and Access Management in Amazon S3 und Blocking Public Access to your Amazon S3 Storage im Benutzerhandbuch für Amazon Simple Storage Service.

Replikation

In diesem Abschnitt gibt das Feld Repliziert an, ob der Bucket so konfiguriert ist, dass Objekte in andere Buckets repliziert werden. Wenn der Wert für dieses Feld Ja lautet, werden eine oder mehrere Replikationsregeln für den Bucket konfiguriert und aktiviert. In diesem Abschnitt wird dann auch die Konto-ID für jedes aufgeführtAWS-Konto, das einen Ziel-Bucket besitzt.

Das Feld Extern repliziert gibt an, ob der Bucket so konfiguriert ist, dass Objekte in Buckets für repliziert werdenAWS-Konten, die außerhalb (nicht Teil) Ihrer Organisation liegen. Eine Organisation

besteht aus einer Reihe von Macie-Konten, die zentral als Gruppe verwandter Konten über AWS Organizations oder durch Macie-Einladung verwaltet werden. Wenn der Wert für dieses Feld Ja lautet, wird eine Replikationsregel für den Bucket konfiguriert und aktiviert, und die Regel ist so konfiguriert, dass Objekte in einen Bucket repliziert werden, der einem externen gehörtAWS-Konto.

> **Note**
>
> Unter bestimmten Bedingungen kann Macie fälschlicherweise angeben, dass ein Bucket so konfiguriert ist, dass Objekte in einen Bucket repliziert werden, der einem externen gehörtAWS-Konto. Dies kann der Fall sein, wenn der Ziel-Bucket AWS-Region in den letzten 24 Stunden in einer anderen erstellt wurde, nachdem Macie im Rahmen des täglichen Aktualisierungszyklus Bucket- und Objektmetadaten von Amazon S3 abgerufen hat. Um das Problem mithilfe von Macie zu untersuchen, wählen Sie Aktualisieren (), um die neuesten Bucket-Metadaten von Amazon S3 abzurufen. Überprüfen Sie dann die Liste der Konto-IDs in diesem Abschnitt. Verwenden Sie Amazon S3 für eine eingehendere Untersuchung, um die Replikationsregeln für den Bucket zu überprüfen.

Weitere Informationen zu Amazon S3-Optionen und -Einstellungen für die Replikation von Bucket-Objekten finden Sie unter Replizieren von Objekten im Benutzerhandbuch für Amazon Simple Storage Service.

Tags

Wenn dem Bucket Tags zugeordnet sind, wird dieser Abschnitt im Bereich angezeigt und listet diese Tags auf. Tags sind Bezeichnungen, die Sie definieren und bestimmten Arten von AWS Ressourcen zuweisen können, einschließlich S3-Buckets. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert.

Weitere Informationen zum Markieren von Buckets finden Sie unter Verwenden von Kostenzuordnungs-S3-Bucket-Tags im Benutzerhandbuch für Amazon Simple Storage Service.

Filtern Ihres S3-Bucket-Inventars mit Amazon Macie

Um Buckets mit bestimmten Merkmalen zu identifizieren und sich darauf zu konzentrieren, können Sie Ihr S3-Bucket-Inventar in der Amazon Macie Macie-Konsole und in Abfragen filtern, die Sie programmgesteuert über die Amazon Macie Macie-API einreichen. Wenn Sie einen Filter erstellen, verwenden Sie bestimmte Bucket-Attribute, um Kriterien für das Ein- oder Ausschließen von Buckets

in einer Ansicht oder in Abfrageergebnissen zu definieren. Ein Bucket-Attribut ist ein Feld, das spezifische Metadaten für einen Bucket speichert.

In Macie besteht ein Filter aus einer oder mehreren Bedingungen. Jede Bedingung, auch als Kriterium bezeichnet, besteht aus drei Teilen:

- Ein auf Attributen basierendes Feld, z. B. Bucket-Name, Tag-Schlüssel oder Definiert im Job.
- Ein Operator, z. B. ist gleich oder ungleich.
- Ein oder mehrere Werte. Der Typ und die Anzahl der Werte hängen vom ausgewählten Feld und Operator ab.

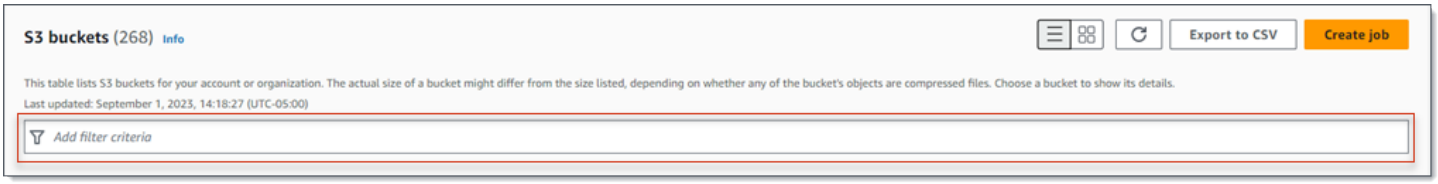
Wie Sie Filterbedingungen definieren und anwenden, hängt davon ab, ob Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden.

Themen

- Ihr Inventar auf der Amazon Macie Macie-Konsole filtern
- Programmgesteuertes Filtern Ihres Inventars mit der Amazon Macie API

Ihr Inventar auf der Amazon Macie Macie-Konsole filtern

Wenn Sie die Amazon Macie Macie-Konsole verwenden, um Ihr S3-Bucket-Inventar zu filtern, bietet Macie Optionen, mit denen Sie Felder, Operatoren und Werte für einzelne Bedingungen auswählen können. Sie greifen auf diese Optionen zu, indem Sie das Filterfeld auf der S3-Buckets-Seite verwenden, wie in der folgenden Abbildung gezeigt.

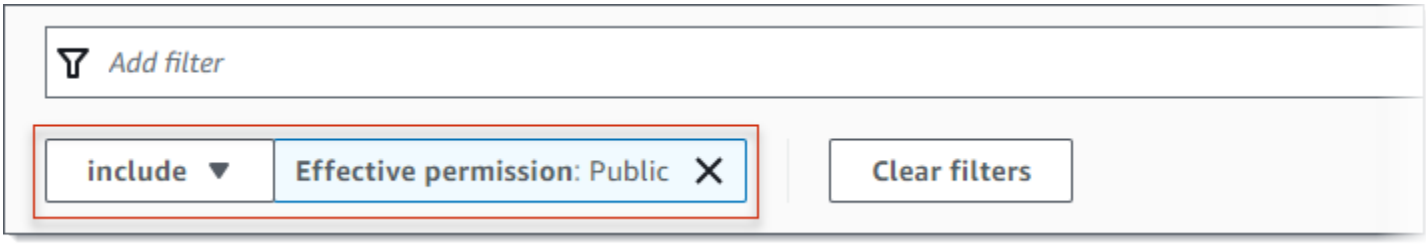


Wenn Sie den Cursor in das Filterfeld setzen, zeigt Macie eine Liste von Feldern an, die Sie für Filterbedingungen verwenden können. Die Felder sind nach logischen Kategorien geordnet. Die Kategorie Allgemeine Felder umfasst beispielsweise Felder, in denen allgemeine Informationen zu einem S3-Bucket gespeichert werden. Zu den Kategorien für den öffentlichen Zugriff gehören Felder, in denen Daten über die verschiedenen Arten von Einstellungen für den öffentlichen Zugriff gespeichert werden, die für einen Bucket gelten können. Die Felder sind innerhalb jeder Kategorie alphabetisch sortiert.

Um eine Bedingung hinzuzufügen, wählen Sie zunächst ein Feld aus der Liste aus. Um ein Feld zu finden, durchsuchen Sie die gesamte Liste oder geben Sie einen Teil des Feldnamens ein, um die Liste der Felder einzugrenzen.

Je nachdem, welches Feld Sie auswählen, zeigt Macie verschiedene Optionen an. Die Optionen spiegeln den Typ und die Art des von Ihnen ausgewählten Feldes wider. Wenn Sie beispielsweise das Feld Gemeinsamer Zugriff auswählen, zeigt Macie eine Liste mit Werten an, aus denen Sie wählen können. Wenn Sie das Feld Bucket-Name auswählen, zeigt Macie ein Textfeld an, in das Sie den Namen eines S3-Buckets eingeben können. Welches Feld Sie auch wählen, Macie führt Sie durch die Schritte zum Hinzufügen einer Bedingung, die die erforderlichen Einstellungen für das Feld enthält.

Nachdem Sie eine Bedingung hinzugefügt haben, wendet Macie die Kriterien für die Bedingung an und zeigt die Bedingung in einem Filtertoken unter dem Filterfeld an, wie in der folgenden Abbildung dargestellt.



In diesem Beispiel ist die Bedingung so konfiguriert, dass sie alle öffentlich zugänglichen Buckets einschließt und alle anderen Buckets ausschließt. Sie gibt Buckets zurück, bei denen der Wert für das Feld Effektive Berechtigung gleich Öffentlich ist.

Wenn Sie weitere Bedingungen hinzufügen, wendet Macie deren Kriterien an und zeigt sie unter dem Filterfeld an. Wenn Sie mehrere Bedingungen hinzufügen, verwendet Macie die UND-Logik, um die Bedingungen zu verknüpfen und die Filterkriterien auszuwerten. Das bedeutet, dass ein S3-Bucket die Filterkriterien nur erfüllt, wenn er allen Bedingungen im Filter entspricht. Sie können jederzeit im Bereich unter dem Filterfeld nachsehen, welche Kriterien Sie angewendet haben.

So filtern Sie Ihr Inventar mithilfe der Konsole

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich S3-Buckets aus. Auf der Seite S3-Buckets wird Ihr Bucket-Inventar angezeigt.

3. Wählen Sie oben auf der Seite optional refresh
   (),
   um die neuesten Bucket-Metadaten von Amazon S3 abzurufen.
4. Platzieren Sie den Cursor in dem Filterfeld und wählen Sie dann das Feld aus, das für die Bedingung verwendet werden soll.
5. Wählen Sie den entsprechenden Wertetyp für das Feld aus, oder geben Sie ihn ein. Beachten Sie dabei die folgenden Tipps.

   Datumsangaben, Uhrzeiten und Zeitbereiche

   Verwenden Sie für Datums- und Uhrzeitangaben die Felder Von und Bis, um einen inklusiven Zeitraum zu definieren:

   - Um einen festen Zeitraum zu definieren, verwenden Sie die Felder Von und Bis, um das erste Datum und die erste Uhrzeit bzw. das letzte Datum und die letzte Uhrzeit im Bereich anzugeben.
   - Um einen relativen Zeitraum zu definieren, der an einem bestimmten Datum und einer bestimmten Uhrzeit beginnt und zur aktuellen Uhrzeit endet, geben Sie das Startdatum und die Startzeit in die Felder Von ein und löschen Sie den gesamten Text in den Feldern Bis.
   - Um einen relativen Zeitraum zu definieren, der an einem bestimmten Datum und einer bestimmten Uhrzeit endet, geben Sie das Enddatum und die Endzeit in die Felder Bis ein und löschen Sie den gesamten Text in den Feldern Von.

   Beachten Sie, dass für Zeitwerte die 24-Stunden-Notation verwendet wird. Wenn Sie die Datumsauswahl verwenden, um Daten auszuwählen, können Sie die Werte verfeinern, indem Sie Text direkt in die Felder Von und Bis eingeben.

   Zahlen und numerische Bereiche

   Verwenden Sie für numerische Werte die Felder Von und Bis, um ganze Zahlen einzugeben, die einen inklusiven numerischen Bereich definieren:

   - Um einen festen numerischen Bereich zu definieren, geben Sie in den Feldern Von und Bis jeweils die niedrigsten und höchsten Zahlen im Bereich an.
   - Um einen festen numerischen Bereich zu definieren, der auf einen bestimmten Wert begrenzt ist, geben Sie den Wert sowohl in die Felder Von als auch in die Felder Bis ein. Um beispielsweise nur die S3-Buckets einzubeziehen, die genau 15 Objekte enthalten, geben Sie **15** in die Felder Von und Bis ein.

- Um einen relativen numerischen Bereich zu definieren, der bei einer bestimmten Zahl beginnt, geben Sie die Zahl in das Feld Von ein und geben Sie keinen Text in das Feld Bis ein.
- Um einen relativen numerischen Bereich zu definieren, der mit einer bestimmten Zahl endet, geben Sie die Zahl in das Feld Bis ein und geben Sie keinen Text in das Feld Von ein.

Textwerte (Zeichenfolge)

Geben Sie für diesen Wertetyp einen vollständigen, gültigen Wert für das Feld ein. Bei Werten wird zwischen Groß- und Kleinschreibung unterschieden.

Beachten Sie, dass Sie in diesem Wertetyp weder einen Teilwert noch Platzhalterzeichen verwenden können. Die einzige Ausnahme ist das Feld Bucket-Name. Für dieses Feld können Sie anstelle eines vollständigen Bucket-Namens ein Präfix angeben. Um beispielsweise alle S3-Buckets zu finden, deren Namen mit my-S3 beginnen, geben Sie **`my-S3`** als Filterwert für das Feld Bucket-Name ein. Wenn Sie einen anderen Wert eingeben, z. B. **`My-s3`** oder**`my*`**, gibt Macie die Buckets nicht zurück.

6. Wenn Sie mit dem Hinzufügen eines Werts für das Feld fertig sind, wählen Sie Anwenden. Macie wendet die Filterkriterien an und zeigt die Bedingung in einem Filtertoken unter dem Filterfeld an.
7. Wiederholen Sie die Schritte 4 bis 6 für jede weitere Bedingung, die Sie hinzufügen möchten.
8. Um eine Bedingung zu entfernen, wählen Sie das X im Filtertoken für die Bedingung aus.
9. Um eine Bedingung zu ändern, entfernen Sie die Bedingung, indem Sie das X im Filtertoken für die Bedingung auswählen. Wiederholen Sie dann die Schritte 4 bis 6, um eine Bedingung mit den richtigen Einstellungen hinzuzufügen.

Programmgesteuertes Filtern Ihres Inventars mit der Amazon Macie API

Um Ihr S3-Bucket-Inventar programmgesteuert zu filtern, geben Sie Filterkriterien in Abfragen an, die Sie mithilfe der Amazon DescribeBucketsMacie Macie-API einreichen. Dieser Vorgang gibt ein Array von Objekten zurück. Jedes Objekt enthält statistische Daten und andere Informationen über einen Bucket, der den Filterkriterien entspricht.

Um Filterkriterien in einer Abfrage anzugeben, fügen Sie Ihrer Anfrage eine Übersicht mit Filterbedingungen hinzu. Geben Sie für jede Bedingung ein Feld, einen Operator und einen oder mehrere Werte für das Feld an. Der Typ und die Anzahl der Werte hängen vom ausgewählten Feld und Operator ab. Informationen zu den Feldern, Operatoren und Wertetypen, die Sie in einer

Bedingung verwenden können, finden Sie unter Amazon S3 S3-Datenquellen in der Amazon Macie API-Referenz.

Die folgenden Beispiele zeigen Ihnen, wie Sie Filterkriterien in Abfragen angeben, die Sie mit AWS Command Line Interface(AWS CLI) einreichen. Sie können dazu auch eine aktuelle Version eines anderen AWS Befehlszeilentools oder eines AWS SDK verwenden oder HTTPS-Anfragen direkt an Macie senden. Informationen zu AWS Tools und SDKs finden Sie unter Tools, auf denen Sie aufbauen können. AWS

Beispiele

- Beispiel 1: Suchen Sie Buckets anhand des Bucket-Namens
- Beispiel 2: Suchen Sie nach Buckets, auf die öffentlich zugegriffen werden kann
- Beispiel 3: Suchen Sie nach Buckets, die unverschlüsselte Objekte enthalten
- Beispiel 4: Suchen Sie nach Buckets, die nicht von einem Job überwacht werden
- Beispiel 5: Suchen Sie nach Buckets, die Daten auf externe Konten replizieren
- Beispiel 6: Finden Sie Buckets auf der Grundlage mehrerer Kriterien

In den Beispielen wird der Befehl describe-buckets verwendet. Wenn ein Beispiel erfolgreich ausgeführt wird, gibt Macie ein Array zurück. `buckets` Das Array enthält ein Objekt für jeden Bucket, der sich im aktuellen Bucket befindet AWS-Region und den Filterkriterien entspricht. Ein Beispiel für diese Ausgabe finden Sie im folgenden Abschnitt.

Beispiel für ein **`buckets`** Array

In diesem Beispiel enthält das `buckets` Array Details zu zwei Buckets, die den in einer Abfrage angegebenen Filterkriterien entsprechen.

```
{
    "buckets": [
        {
            "accountId": "123456789012",
            "allowsUnencryptedObjectUploads": "FALSE",
            "bucketArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
            "bucketCreatedAt": "2020-05-18T19:54:00+00:00",
            "bucketName": "DOC-EXAMPLE-BUCKET1",
            "classifiableObjectCount": 13,
            "classifiableSizeInBytes": 1592088,
            "jobDetails": {
                "isDefinedInJob": "TRUE",
```

```
            "isMonitoredByJob": "TRUE",
            "lastJobId": "08c81dc4a2f3377fae45c9ddaexample",
            "lastJobRunTime": "2021-04-26T14:55:30.270000+00:00"
        },
        "lastAutomatedDiscoveryTime": "2022-12-10T19:11:25.364000+00:00",
        "lastUpdated": "2022-12-13T07:33:06.337000+00:00",
        "objectCount": 13,
        "objectCountByEncryptionType": {
            "customerManaged": 0,
            "kmsManaged": 2,
            "s3Managed": 7,
            "unencrypted": 4,
            "unknown": 0
        },
        "publicAccess": {
            "effectivePermission": "NOT_PUBLIC",
            "permissionConfiguration": {
                "accountLevelPermissions": {
                    "blockPublicAccess": {
                        "blockPublicAcls": true,
                        "blockPublicPolicy": true,
                        "ignorePublicAcls": true,
                        "restrictPublicBuckets": true
                    }
                },
                "bucketLevelPermissions": {
                    "accessControlList": {
                        "allowsPublicReadAccess": false,
                        "allowsPublicWriteAccess": false
                    },
                    "blockPublicAccess": {
                        "blockPublicAcls": true,
                        "blockPublicPolicy": true,
                        "ignorePublicAcls": true,
                        "restrictPublicBuckets": true
                    },
                    "bucketPolicy": {
                        "allowsPublicReadAccess": false,
                        "allowsPublicWriteAccess": false
                    }
                }
            }
        },
        "region": "us-east-1",
```

```
            "replicationDetails": {
                "replicated": false,
                "replicatedExternally": false,
                "replicationAccounts": []
            },
            "sensitivityScore": 78,
            "serverSideEncryption": {
                "kmsMasterKeyId": null,
                "type": "NONE"
            },
            "sharedAccess": "NOT_SHARED",
            "sizeInBytes": 4549746,
            "sizeInBytesCompressed": 0,
            "tags": [
                {
                    "key": "Division",
                    "value": "HR"
                },
                {
                    "key": "Team",
                    "value": "Recruiting"
                }
            ],
            "unclassifiableObjectCount": {
                "fileType": 0,
                "storageClass": 0,
                "total": 0
            },
            "unclassifiableObjectSizeInBytes": {
                "fileType": 0,
                "storageClass": 0,
                "total": 0
            },
            "versioning": true
        },
        {
            "accountId": "123456789012",
            "allowsUnencryptedObjectUploads": "TRUE",
            "bucketArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
            "bucketCreatedAt": "2020-11-25T18:24:38+00:00",
            "bucketName": "DOC-EXAMPLE-BUCKET2",
            "classifiableObjectCount": 8,
            "classifiableSizeInBytes": 133810,
            "jobDetails": {
```

```
            "isDefinedInJob": "TRUE",
            "isMonitoredByJob": "FALSE",
            "lastJobId": "188d4f6044d621771ef7d65f2example",
            "lastJobRunTime": "2021-04-09T19:37:11.511000+00:00"
        },
        "lastAutomatedDiscoveryTime": "2022-12-12T19:11:25.364000+00:00",
        "lastUpdated": "2022-12-13T07:33:06.337000+00:00",
        "objectCount": 8,
        "objectCountByEncryptionType": {
            "customerManaged": 0,
            "kmsManaged": 0,
            "s3Managed": 8,
            "unencrypted": 0,
            "unknown": 0
        },
        "publicAccess": {
            "effectivePermission": "NOT_PUBLIC",
            "permissionConfiguration": {
                "accountLevelPermissions": {
                    "blockPublicAccess": {
                        "blockPublicAcls": true,
                        "blockPublicPolicy": true,
                        "ignorePublicAcls": true,
                        "restrictPublicBuckets": true
                    }
                },
                "bucketLevelPermissions": {
                    "accessControlList": {
                        "allowsPublicReadAccess": false,
                        "allowsPublicWriteAccess": false
                    },
                    "blockPublicAccess": {
                        "blockPublicAcls": true,
                        "blockPublicPolicy": true,
                        "ignorePublicAcls": true,
                        "restrictPublicBuckets": true
                    },
                    "bucketPolicy": {
                        "allowsPublicReadAccess": false,
                        "allowsPublicWriteAccess": false
                    }
                }
            }
        },
```

```
            "region": "us-east-1",
            "replicationDetails": {
                "replicated": false,
                "replicatedExternally": false,
                "replicationAccounts": []
            },
            "sensitivityScore": 95,
            "serverSideEncryption": {
                "kmsMasterKeyId": null,
                "type": "AES256"
            },
            "sharedAccess": "EXTERNAL",
            "sizeInBytes": 175978,
            "sizeInBytesCompressed": 0,
            "tags": [
                {
                    "key": "Division",
                    "value": "HR"
                },
                {
                    "key": "Team",
                    "value": "Recruiting"
                }
            ],
            "unclassifiableObjectCount": {
                "fileType": 3,
                "storageClass": 0,
                "total": 3
            },
            "unclassifiableObjectSizeInBytes": {
                "fileType": 2999826,
                "storageClass": 0,
                "total": 2999826
            },
            "versioning": true
        }
    ]
}
```


Wenn keine Buckets den Filterkriterien entsprechen, gibt Macie ein leeres Array zurück. `buckets`


```
{
    "buckets": []
```

```
}
```

Beispiel 1: Suchen Sie Buckets anhand des Bucket-Namens

In diesem Beispiel wird der Befehl describe-buckets verwendet, um Metadaten für alle Buckets abzufragen, deren Namen mit my-S3 beginnen und sich in der aktuellen Liste befinden. AWS-Region

Für Linux, macOS oder Unix:

```
$ aws macie2 describe-buckets --criteria '{"bucketName":{"prefix":"my-S3"}}'
```

Für Microsoft Windows:

```
C:\> aws macie2 describe-buckets --criteria={\"bucketName\":{\"prefix\":\"my-S3\"}}
```

Wobei gilt:

- *BucketName* gibt den JSON-Namen des Felds bucketName an.
- *Präfix gibt den Präfix-Operator* an.
- *my-S3* ist der Wert für das Feld Bucket-Name.

Beispiel 2: Suchen Sie nach Buckets, auf die öffentlich zugegriffen werden kann

In diesem Beispiel wird der Befehl describe-buckets verwendet, um Metadaten für Buckets abzufragen, die sich in der aktuellen Version befinden AWS-Region und, basierend auf einer Kombination von Berechtigungseinstellungen, öffentlich zugänglich sind.

Für Linux, macOS oder Unix:

```
$ aws macie2 describe-buckets --criteria '{"publicAccess.effectivePermission":{"eq":
["PUBLIC"]}}'
```

Für Microsoft Windows:

```
C:\> aws macie2 describe-buckets --criteria={\"publicAccess.effectivePermission\":
{\"eq\":[\"PUBLIC\"]}}
```

Wobei gilt:

- *publicAccess.EffectivePermission* gibt den JSON-Namen des Felds Effective Permission an.
- *eq* gibt den Gleichheitsoperator an.
- *PUBLIC* ist ein Aufzählungswert für das Feld Effektive Berechtigung.

Beispiel 3: Suchen Sie nach Buckets, die unverschlüsselte Objekte enthalten

In diesem Beispiel wird der Befehl describe-buckets verwendet, um Metadaten für Buckets abzufragen, die sich in der aktuellen Version befinden und unverschlüsselte Objekte enthalten. AWS-Region

Für Linux, macOS oder Unix:

```
$ aws macie2 describe-buckets --criteria '{"objectCountByEncryptionType.unencrypted":
{"gte":1}}'
```

Für Microsoft Windows:

```
C:\> aws macie2 describe-buckets --
criteria={\"objectCountByEncryptionType.unencrypted\":{\"gte\":1}}
```

Wobei gilt:

- *objectCountByEncryptionType.unencrypted* gibt den JSON-Namen des Felds Keine Verschlüsselung an.
- *gte* gibt den Operator „Größer als“ oder „gleich“ an.
- *1* ist der niedrigste Wert in einem inklusiven, relativen numerischen Bereich für das Feld Keine Verschlüsselung.

Beispiel 4: Suchen Sie nach Buckets, die nicht von einem Job überwacht werden

In diesem Beispiel wird der Befehl describe-buckets verwendet, um Metadaten für Buckets abzufragen, die sich in der aktuellen Version befinden AWS-Region und nicht mit periodischen Discovery-Jobs für sensible Daten verknüpft sind.

Für Linux, macOS oder Unix:

```
$ aws macie2 describe-buckets --criteria '{"jobDetails.isMonitoredByJob":{"eq":
["FALSE"]}}'
```

Für Microsoft Windows:

```
C:\> aws macie2 describe-buckets --criteria={\"jobDetails.isMonitoredByJob\":{\"eq\":
[\"FALSE\"]}}
```

Wobei gilt:

- *Einzelheiten zum Job. isMonitoredBy*Job gibt den JSON-Namen des Jobfeldes Aktiv überwacht von an.
- *eq* gibt den Gleichheitsoperator an.
- *FALSE* ist ein Aufzählungswert für das Feld Aktiv überwacht von Job.

Beispiel 5: Suchen Sie nach Buckets, die Daten auf externe Konten replizieren

In diesem Beispiel wird der Befehl describe-buckets verwendet, um Metadaten für Buckets abzufragen, die sich in der aktuellen Version befinden AWS-Region und so konfiguriert sind, dass Objekte in einen Bereich repliziert werdenAWS-Konto, der nicht Teil Ihrer Organisation ist.

Für Linux, macOS oder Unix:

```
$ aws macie2 describe-buckets --criteria '{"replicationDetails.replicatedExternally":
{"eq":["true"]}}'
```

Für Microsoft Windows:

```
C:\> aws macie2 describe-buckets --
criteria={\"replicationDetails.replicatedExternally\":{\"eq\":[\"true\"]}}
```

Wobei gilt:

- *ReplicationDetails.ReplicatedExternally* gibt den JSON-Namen des Felds Replicated external an.
- *eq gibt den* Gleichheitsoperator an.
- *true* gibt einen booleschen Wert für das Feld Extern repliziert an.

Beispiel 6: Finden Sie Buckets auf der Grundlage mehrerer Kriterien

In diesem Beispiel wird der Befehl describe-buckets verwendet, um Metadaten nach Buckets abzufragen, die sich in der aktuellen Version befinden AWS-Region und die folgenden Kriterien erfüllen: Sie sind aufgrund einer Kombination von Berechtigungseinstellungen öffentlich zugänglich, enthalten unverschlüsselte Objekte und sind nicht mit regelmäßigen Discovery-Aufträgen für sensible Daten verknüpft.

Verwenden Sie für Linux, macOS oder Unix den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit:

```
$ aws macie2 describe-buckets \
--criteria '{"publicAccess.effectivePermission":{"eq":
["PUBLIC"]},"objectCountByEncryptionType.unencrypted":
{"gte":1},"jobDetails.isMonitoredByJob":{"eq":["FALSE"]}}'
```

Verwenden Sie für Microsoft Windows das Zeilenfortsetzungszeichen Caret (^), um die Lesbarkeit zu verbessern:

```
C:\> aws macie2 describe-buckets ^
--criteria={\"publicAccess.effectivePermission\":{\"eq\":
[\"PUBLIC\"]},\"objectCountByEncryptionType.unencrypted\":{\"gte\":1},
\"jobDetails.isMonitoredByJob\":{\"eq\":[\"FALSE\"]}}
```

Wobei gilt:

- *publicAccess.EffectivePermission* gibt den JSON-Namen des Felds Effective Permission an und:
  - *eq* gibt den Gleichheitsoperator an.
  - *PUBLIC* ist ein Aufzählungswert für das Feld Effektive Berechtigung.
- *objectCountByEncryptionType.unencrypted* gibt den JSON-Namen des Felds Keine Verschlüsselung an und:
  - *gte* gibt den Operator „größer als“ oder „gleich“ an.
  - *1* ist der niedrigste Wert in einem inklusiven, relativen numerischen Bereich für das Feld Keine Verschlüsselung.
- *Einzelheiten des Auftrags. isMonitoredBy*Job gibt den JSON-Namen des Jobfeldes Aktiv überwacht von an und:

- `eq` gibt den Gleichheitsoperator an.
- `FALSE` ist ein Aufzählungswert für das Feld Aktiv überwacht von Job.

Ermöglichen Sie Amazon Macie den Zugriff auf S3-Buckets und -Objekte

Wenn Sie Amazon Macie für Sie aktivierenAWS-Konto, erstellt Macie eine serviceverknüpfte Rolle, die Macie die erforderlichen Berechtigungen gewährt, um Amazon Simple Storage Service (Amazon S3) und andere AWS-Services in Ihrem Namen aufzurufen. Eine dienstverknüpfte Rolle vereinfacht die Einrichtung einer, AWS-Service da Sie nicht manuell Berechtigungen hinzufügen müssen, damit der Service Aktionen in Ihrem Namen durchführen kann. Weitere Informationen zu diesem Rollentyp finden Sie unter Verwenden von dienstverknüpften Rollen im AWS Identity and Access ManagementBenutzerhandbuch.

Die Berechtigungsrichtlinie für die dienstverknüpfte Macie-Rolle (`AWSServiceRoleForAmazonMacie`) ermöglicht es Macie, Aktionen auszuführen, zu denen das Abrufen von Informationen über Ihre S3-Buckets und -Objekte sowie das Abrufen von Objekten aus Ihren Buckets gehören. Wenn Sie der Macie-Administrator einer Organisation sind, erlaubt die Richtlinie Macie außerdem, diese Aktionen in Ihrem Namen für Mitgliedskonten in Ihrer Organisation durchzuführen.

Macie verwendet diese Berechtigungen, um Aufgaben wie die folgenden auszuführen:

- Generieren und verwalten Sie ein Inventar Ihrer S3-Buckets
- Stellen Sie statistische und andere Daten zu den Buckets und Objekten in den Buckets bereit
- Überwachen und bewerten Sie die Buckets im Hinblick auf Sicherheit und Zugriffskontrolle
- Analysieren Sie Objekte in den Buckets, um sensible Daten zu erkennen

In den meisten Fällen verfügt Macie über die Berechtigungen, die sie zur Ausführung dieser Aufgaben benötigt. Wenn ein S3-Bucket jedoch über eine restriktive Bucket-Richtlinie verfügt, kann die Richtlinie Macie daran hindern, einige oder alle dieser Aufgaben auszuführen.

Eine Bucket-Richtlinie ist eine ressourcenbasierte AWS Identity and Access Management (IAM) -Richtlinie, die festlegt, welche Aktionen ein Principal (Benutzer, Konto, Dienst oder andere Entität) in einem S3-Bucket ausführen kann und unter welchen Bedingungen ein Principal diese Aktionen ausführen kann. Die Aktionen und Bedingungen können für Operationen auf Bucketebene gelten, z.

B. das Abrufen von Informationen über einen Bucket, und für Operationen auf Objektebene, wie das Abrufen von Objekten aus einem Bucket.

Bucket-Richtlinien gewähren oder beschränken in der Regel den Zugriff, indem sie explizite `Deny` Anweisungen `Allow` oder Anweisungen und Bedingungen verwenden. Eine Bucket-Richtlinie kann beispielsweise eine `Deny` ODER-Anweisung enthalten, die den Zugriff auf den Bucket verweigert, sofern nicht bestimmte Quell-IP-Adressen, Amazon Virtual Private Cloud (Amazon VPC) -Endpunkte oder VPCs für den Zugriff auf den Bucket verwendet werden. `Allow` Informationen zur Verwendung von Bucket-Richtlinien, um den Zugriff auf Buckets zu gewähren oder einzuschränken, finden Sie unter Bucket-Richtlinien und Benutzerrichtlinien und Wie Amazon S3 eine Anfrage autorisiert im Amazon Simple Storage Service-Benutzerhandbuch.

Wenn eine Bucket-Richtlinie eine explizite `Allow` Anweisung verwendet, hindert die Richtlinie Macie nicht daran, Informationen über den Bucket und die Objekte des Buckets abzurufen oder Objekte aus dem Bucket abzurufen. Dies liegt daran, dass die `Allow` Anweisungen in der Berechtigungsrichtlinie für die dienstverknüpfte Macie-Rolle diese Berechtigungen gewähren.

Wenn eine Bucket-Richtlinie jedoch eine explizite `Deny` Anweisung mit einer oder mehreren Bedingungen verwendet, darf Macie möglicherweise keine Informationen über den Bucket oder die Objekte des Buckets oder die Objekte des Buckets abrufen. Wenn eine Bucket-Richtlinie beispielsweise ausdrücklich den Zugriff von allen Quellen außer einer bestimmten IP-Adresse verweigert, darf Macie die Objekte des Buckets nicht analysieren, wenn Sie einen Job zur Erkennung vertraulicher Daten ausführen. Dies liegt daran, dass restriktive Bucket-Richtlinien Vorrang vor den `Allow` Anweisungen in der Berechtigungsrichtlinie für die dienstverknüpfte Macie-Rolle haben.

Um Macie den Zugriff auf einen S3-Bucket zu ermöglichen, für den eine restriktive Bucket-Richtlinie gilt, können Sie der Bucket-Richtlinie eine Bedingung für die dienstverknüpfte Macie-Rolle (`AWSServiceRoleForAmazonMacie`) hinzufügen. Diese Bedingung kann verhindern, dass die dienstverknüpfte Macie-Rolle der `Deny` Einschränkung in der Richtlinie entspricht. Dies kann geschehen, indem der `aws:PrincipalArn` globale Bedingungskontextschlüssel und der Amazon-Ressourcenname (ARN) der dienstverknüpften Macie-Rolle verwendet werden.

Das folgende Verfahren führt Sie durch diesen Prozess und stellt ein Beispiel zur Verfügung.

So fügen Sie die dienstverknüpfte Macie-Rolle zu einer Bucket-Richtlinie hinzu

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie im Navigationsbereich die Option Buckets aus.

3. Wählen Sie den S3-Bucket aus, auf den Sie Macie zugreifen möchten.
4. Wählen Sie auf der Registerkarte Berechtigungen unter Bucket-Richtlinie die Option Bearbeiten aus.
5. Identifizieren Sie im Bucket-Richtlinien-Editor jede `Deny` Anweisung, die den Zugriff einschränkt und Macie daran hindert, auf den Bucket oder die Objekte des Buckets zuzugreifen.
6. Fügen Sie in jeder `Deny` Anweisung eine Bedingung hinzu, die den `aws:PrincipalArn` globalen Bedingungskontextschlüssel verwendet und den ARN der dienstverknüpften Macie-Rolle für Ihre Anweisung angibt. AWS-Konto

   Der Wert für den Bedingungsschlüssel sollte lauten`arn:aws:iam::`*`123456789012`*`:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`, wobei *`123456789012 die Konto-ID für Ihr`* Konto ist. AWS-Konto

Wo Sie dies zu einer Bucket-Richtlinie hinzufügen, hängt von der Struktur, den Elementen und Bedingungen ab, die die Richtlinie derzeit enthält. Informationen zu unterstützten Strukturen und Elementen finden Sie unter Richtlinien und Berechtigungen in Amazon S3 im Amazon Simple Storage Service-Benutzerhandbuch.

Im Folgenden finden Sie ein Beispiel für eine Bucket-Richtlinie, die eine explizite `Deny` Anweisung verwendet, um den Zugriff auf einen S3-Bucket mit dem Namen DOC-EXAMPLE-BUCKET einzuschränken. Mit der aktuellen Richtlinie kann auf den Bucket nur von dem VPC-Endpunkt aus zugegriffen werden, dessen ID lautet`vpce-1a2b3c4d`. Der Zugriff von allen anderen VPC-Endpunkten aus wird verweigert, einschließlich des Zugriffs von AWS Management Console und Macie.

```
{
   "Version": "2012-10-17",
   "Id": "Policy1415115example",
   "Statement": [
      {
         "Sid": "Access from specific VPCE only",
         "Effect": "Deny",
         "Principal": "*",
         "Action": "s3:*",
         "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
         ],
         "Condition": {
```

```
            "StringNotEquals": {
               "aws:SourceVpce": "vpce-1a2b3c4d"
            }
         }
      }
   ]
}
```

Um diese Richtlinie zu ändern und Macie den Zugriff auf den S3-Bucket und die Objekte des Buckets zu ermöglichen, können wir eine Bedingung hinzufügen, die `StringNotLike` den Bedingungsoperator und den `aws:PrincipalArn` globalen Bedingungskontextschlüssel verwendet. Diese zusätzliche Bedingung schließt aus, dass die dienstverknüpfte Macie-Rolle der Einschränkung nicht entspricht. `Deny`

```
{
   "Version": "2012-10-17",
   "Id":" Policy1415115example ",
   "Statement": [
      {
         "Sid": "Access from specific VPCE and Macie only",
         "Effect": "Deny",
         "Principal": "*",
         "Action": "s3:*",
         "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
         ],
         "Condition": {
            "StringNotEquals": {
               "aws:SourceVpce": "vpce-1a2b3c4d"
            },
            "StringNotLike": {
               "aws:PrincipalArn": "arn:aws:iam::123456789012:role/aws-service-role/
macie.amazonaws.com/AWSServiceRoleForAmazonMacie"
            }
         }
      }
   ]
}
```

Im vorherigen Beispiel verwendet der Bedingungsoperator den `aws:PrincipalArn` Bedingungskontextschlüssel, um den ARN der dienstverknüpften Macie-Rolle anzugeben, wobei: `StringNotLike`

- `123456789012`ist die Konto-ID des BenutzersAWS-Konto, der Macie verwenden darf, um Informationen über den Bucket und die Objekte des Buckets abzurufen und Objekte aus dem Bucket abzurufen.
- `macie.amazonaws.com`ist die Kennung des Macie-Serviceprinzips.
- `AWSServiceRoleForAmazonMacie`ist der Name der dienstverknüpften Macie-Rolle.

Wir haben den `StringNotLike` Operator verwendet, weil die Richtlinie bereits einen `StringNotEquals` Operator verwendet. Eine Police kann den `StringNotEquals` Operator nur einmal verwenden.

Weitere Richtlinienbeispiele und detaillierte Informationen zur Verwaltung des Zugriffs auf Amazon S3-Ressourcen finden Sie unter Identity and Access Management in Amazon S3 im Amazon-Simple-Storage-Service-Benutzerhandbuch.

Entdecken vertraulicher Daten mit Amazon Macie

Mit Amazon Macie können Sie die Erkennung, Protokollierung und Berichterstattung vertraulicher Daten in Ihrem Amazon Simple Storage Service (Amazon S3) -Datenbestand automatisieren. Sie können dies auf zwei Arten tun: indem Sie Macie so konfigurieren, dass es die automatische Erkennung vertraulicher Daten für Ihr Konto oder Ihre Organisation durchführt, und indem Sie Aufträge zur Erkennung vertraulicher Daten für Ihr Konto oder Ihre Organisation erstellen und ausführen.

Automatisierte Erkennung vertraulicher Daten

> Die automatische Erkennung vertraulicher Daten bietet einen umfassenden Überblick darüber, wo sich sensible Daten in Ihrem Amazon S3-Datenbestand befinden könnten. Mit dieser Option wertet Macie Ihr S3-Bucket-Inventar täglich aus und verwendet Stichprobenverfahren, um repräsentative S3-Objekte aus Ihren Buckets zu identifizieren und auszuwählen. Macie ruft dann die ausgewählten Objekte ab, analysiert sie und untersucht sie auf sensible Daten. Weitere Informationen finden Sie unter Durchführung automatisierter Erkennung vertraulicher Daten.

Aufgaben zur Erkennung vertraulicher Daten

> Aufgaben zur Erkennung vertraulicher Daten ermöglichen tiefere, zielgerichtetere Analysen. Mit dieser Option definieren Sie die Breite und Tiefe der Analyse — spezifische S3-Buckets, die Sie auswählen, oder Buckets, die bestimmten Kriterien entsprechen. Sie können den Umfang der Analyse auch verfeinern, indem Sie Optionen wie benutzerdefinierte Kriterien auswählen, die sich aus Eigenschaften von S3-Objekten ableiten. Darüber hinaus können Sie einen Job so konfigurieren, dass er nur einmal für Analysen und Bewertungen auf Abruf oder wiederholt für regelmäßige Analysen, Bewertungen und Überwachungen ausgeführt wird. Weitere Informationen finden Sie unter Ausführen von Erkennungsaufgaben für vertrauliche Daten.

Mit beiden Optionen, der automatisierten Erkennung vertraulicher Daten oder der Erkennung vertraulicher Daten, können Sie S3-Objekte analysieren, indem Sie von Macie bereitgestellte verwaltete Datenkennungen, benutzerdefinierte Datenkennungen, die Sie definieren, oder eine Kombination aus beiden verwenden. Sie können die Analyse auch mithilfe von Zulassungslisten optimieren.

Identifikatoren für verwaltete Daten

Bei verwalteten Datenkennungen handelt es sich um integrierte Kriterien und Techniken, mit denen bestimmte Arten vertraulicher Daten erkannt werden können, z. B. Kreditkartennummern,AWSgeheime Zugangsschlüssel oder Passnummern für bestimmte Länder oder Regionen. Sie können eine große und wachsende Liste sensibler Datentypen für viele Länder und Regionen erkennen, darunter mehrere Arten von Anmeldeinformationen, Finanzinformationen und persönlich identifizierbaren Informationen (PII). Weitere Informationen finden Sie unter Verwenden von verwalteten Datenbezeichnern.

Benutzerdefinierte Datenkennungen

Benutzerdefinierte Datenkennungen definieren benutzerdefinierte Kriterien für die Erkennung vertraulicher Daten. Jeder benutzerdefinierte Datenbezeichner gibt einen regulären Ausdruck an (Regex), das ein übereinstimmendes Textmuster und optional Zeichenfolgen und eine Näherungsregel definiert, die die Ergebnisse verfeinern. Sie können sie verwenden, um sensible Daten zu erkennen, die Ihre speziellen Szenarien, Ihr geistiges Eigentum oder Ihre firmeneigenen Daten widerspiegeln, z. B. Mitarbeiter-IDs, Kundenkontonummern oder interne Datenklassifizierungen. Weitere Informationen finden Sie unter Erstellen von benutzerdefinierten Datenbezeichnern.

Listen zulassen

In Macie geben Listen Text und Textmuster an, die in S3-Objekten ignoriert werden sollen. Dabei handelt es sich in der Regel um Ausnahmen für sensible Daten für Ihre speziellen Szenarien oder Umgebungen, z. B. öffentliche Namen oder Telefonnummern für Ihr Unternehmen oder Beispieldaten, die Ihre Organisation für Tests verwendet. Wenn Macie Text findet, der einem Eintrag oder Muster in einer Zulassungsliste entspricht, meldet Macie dieses Vorkommen von Text nicht, selbst wenn der Text den Kriterien einer verwalteten Daten-ID oder einer benutzerdefinierten Daten-ID entspricht. Weitere Informationen finden Sie unter Definition von Ausnahmen für sensible Daten mit Zulassungslisten.

Wenn Macie ein S3-Objekt analysiert, ruft Macie die neueste Version des Objekts von Amazon S3 ab und überprüft dann den Inhalt des Objekts auf vertrauliche Daten. Macie kann ein Objekt analysieren, wenn Folgendes zutrifft:

- Das Objekt verwendet ein unterstütztes Datei- oder Speicherformat und wird mithilfe einer unterstützten Speicherklasse direkt in Amazon S3 gespeichert. Weitere Informationen finden Sie unter Unterstützte Speicherklassen und -formate.

- Wenn das Objekt verschlüsselt ist, wird es mit einem Schlüssel verschlüsselt, auf den Macie zugreifen kann und den er verwenden darf. Weitere Informationen finden Sie unter Analysieren verschlüsselter S3-Objekte.
- Wenn das Objekt in einem Bucket gespeichert ist, für den eine restriktive Bucket-Richtlinie gilt, ermöglicht die Richtlinie Macie den Zugriff auf Objekte im Bucket. Weitere Informationen finden Sie unter Macie den Zugriff von S3-Buckets und -Objekten erlauben.

Um Ihnen dabei zu helfen, Ihre Anforderungen an Datensicherheit und Datenschutz zu erfüllen und einzuhalten, erstellt Macie Aufzeichnungen über die sensiblen Daten, die sie findet, und die Analysen, die sie durchführt —Erkenntnisse aus sensiblen DatenundErgebnisse der Erkennung vertraulicher Daten. EINAuffinden sensibler Datenist ein detaillierter Bericht über sensible Daten, die Macie in einem S3-Objekt gefunden hat. Ein Erkennungsergebnis für vertrauliche Daten ist ein Datensatz, der Details zur Analyse eines Objekts protokolliert. Jeder Datensatztyp entspricht einem standardisierten Schema, mit dem Sie sie abfragen, überwachen und verarbeiten können, indem Sie bei Bedarf andere Anwendungen, Dienste und Systeme verwenden.

> **Tip**
>
> Macie ist zwar für Amazon S3 optimiert, Sie können es jedoch verwenden, um vertrauliche Daten in Ressourcen zu finden, die Sie derzeit an anderer Stelle speichern. Sie können dies tun, indem Sie die Daten vorübergehend oder dauerhaft nach Amazon S3 verschieben. Exportieren Sie beispielsweise Amazon Relational Database Service- oder Amazon Aurora-Snapshots im Apache Parquet-Format nach Amazon S3. Oder exportieren Sie eine Amazon DynamoDB-Tabelle nach Amazon S3. Anschließend können Sie einen Job erstellen, um die Daten in Amazon S3 zu analysieren.

Themen

- Verwenden verwalteter Datenkennungen in Amazon Macie
- Erstellen benutzerdefinierter Datenkennungen in Amazon Macie
- Definition von Ausnahmen für sensible Daten mit Amazon Macie Allow Lists
- Durchführung automatisierter Erkennung vertraulicher Daten mit Amazon Macie
- Ausführen von Aufträgen zur Erkennung vertraulicher Daten in Amazon Macie
- Analysieren verschlüsselter Amazon S3-Objekte mit Amazon Macie
- Speichern und Aufbewahren von Erkennungsergebnissen sensibler Daten mit Amazon Macie

- Von Amazon Macie unterstützte Speicherklassen und -formate

Verwenden verwalteter Datenkennungen in Amazon Macie

Amazon Macie verwendet eine Kombination von Kriterien und Techniken, einschließlich maschinellem Lernen und Musterabgleich, um vertrauliche Daten in Amazon Simple Storage Service (Amazon S3) -Objekten zu erkennen. Diese Kriterien und Techniken, zusammenfassend bezeichnet alsIdentifikatoren für verwaltete Daten, kann für viele Länder und Regionen eine große und wachsende Liste vertraulicher Datentypen erkennen, darunter mehrere Arten von Anmeldeinformationen, Finanzinformationen, persönlichen Gesundheitsinformationen (PHI) und persönlich identifizierbaren Informationen (PII). Jeder verwaltete Datenbezeichner ist so konzipiert, dass er einen bestimmten Typ sensibler Daten erkennt, z. B.AWSgeheime Zugangsschlüssel, Kreditkartennummern oder Passnummern für ein bestimmtes Land oder eine bestimmte Region.

Macie kann mithilfe verwalteter Datenkennungen die folgenden Kategorien vertraulicher Daten erkennen:

- Anmeldeinformationen, für Anmeldeinformationsdaten wie private Schlüssel undAWSgeheime Zugangsschlüssel.
- Finanzinformationen, für Finanzdaten wie Kreditkartennummern und Bankkontonummern.
- Personenbezogene Daten für persönliche Daten wie Krankenversicherungs- und medizinische Identifikationsnummern und personenbezogene Daten wie Führerscheinnummern und Reisepassnummern.

Innerhalb jeder Kategorie kann Macie mehrere Arten sensibler Daten erkennen. In den Themen in diesem Abschnitt werden die einzelnen Arten und alle relevanten Anforderungen für deren Erkennung aufgeführt und beschrieben. Für jede Art geben sie auch die eindeutige Kennung (ID) für die verwaltete Datenkennung an, die für die Erkennung der Daten konzipiert ist. Wenn duein Job zur Erkennung vertraulicher Daten erstellenoderEinstellungen für die automatische Erkennung vertraulicher Daten konfigurieren, Sie können diese IDs verwenden, um anzugeben, welche verwalteten Datenkennungen Macie bei der Analyse von S3-Objekten verwenden soll.

Eine Liste der verwalteten Datenkennungen, die wir für Jobs empfehlen, finden Sie unterVerwaltete Datenkennungen, die für die Erkennung vertraulicher Daten empfohlen werden. Eine Liste der verwalteten Datenkennungen, die wir empfehlen und die standardmäßig für die automatische Erkennung vertraulicher Daten verwendet werden, finden Sie unterStandardeinstellungen für die automatische Erkennung vertraulicher Daten.

Themen

- Schlüsselwortanforderungen für von Amazon Macie verwaltete Datenkennungen
- Kurzreferenz: Von Amazon Macie verwaltete Datenkennungen
- Ausführliche Referenz: Von Amazon Macie verwaltete Datenkennungen

Schlüsselwortanforderungen für von Amazon Macie verwaltete Datenkennungen

Um bestimmte Arten vertraulicher Daten mithilfe verwalteter Datenkennungen zu erkennen, benötigt Amazon Macie ein Schlüsselwort, das sich in der Nähe der Daten befindet. Wenn dies bei einem bestimmten Datentyp der Fall ist, geben die nachfolgenden Themen in diesem Abschnitt die Schlüsselwortanforderungen für diese Daten an.

Wenn ein Schlüsselwort in der Nähe eines bestimmten Datentyps stehen muss, muss das Schlüsselwort in der Regel innerhalb von 30 Zeichen (einschließlich) von den Daten entfernt sein. Zusätzliche Näherungsanforderungen variieren je nach Dateityp oder Speicherformat eines Amazon Simple Storage Service (Amazon S3) -Objekts.

Strukturierte, spaltenförmige Daten

Bei spaltenförmigen Daten muss ein Schlüsselwort Teil desselben Werts oder im Namen der Spalte oder des Felds sein, in der ein Wert gespeichert ist. Dies gilt für Microsoft Excel-Arbeitsmappen, CSV-Dateien und TSV-Dateien.

Zum Beispiel, wenn der Wert für ein Feld beide enthältSSNund einer neunstelligen Zahl, die die Syntax einer US-Sozialversicherungsnummer (SSN) verwendet, kann Macie die SSN im Feld erkennen. Ähnlich, wenn der Name einer Spalte enthältSSN, Macie kann jede SSN in der Spalte erkennen. Macie behandelt die Werte in dieser Spalte so, als ob sie sich in der Nähe des Schlüsselworts befinden.SSN.

Strukturierte, datensatzbasierte Daten

Bei datensatzbasierten Daten muss ein Schlüsselwort Teil desselben Werts oder im Namen eines Elements im Pfad zu dem Feld oder Array sein, das einen Wert speichert. Dies gilt für Apache Avro-Objektcontainer, Apache Parquet-Dateien, JSON-Dateien und JSON Lines-Dateien.

Zum Beispiel, wenn der Wert für ein Feld beide enthältReferenzenund eine Zeichenfolge, die die Syntax einerAWSgeheimer Zugangsschlüssel, Macie kann den Schlüssel im Feld erkennen. Ähnlich, wenn der Pfad zu einem Feld ist`$.credentials.aws.key`, Macie kann einen

erkennenAWSgeheimer Zugangsschlüssel im Feld. Macie behandelt den Wert im Feld so, als ob er sich in der Nähe des Schlüsselworts befindet.Referenzen.

Unstrukturierte Daten

Für Dateien im Adobe Portable Document Format, Microsoft Word-Dokumente, E-Mail-Nachrichten und nichtbinäre Textdateien außer CSV-, JSON-, JSON-Lines- und TSV-Dateien gelten keine zusätzlichen Näherungsanforderungen. Ein Schlüsselwort muss in der Regel innerhalb von 30 Zeichen (einschließlich) von den Daten entfernt sein. Dazu gehören alle strukturierten Daten, wie z. B. Tabellen, in diesen Dateitypen.

Bei Schlüsselwörtern muss die Groß- und Kleinschreibung nicht beachtet werden. Wenn ein Schlüsselwort ein Leerzeichen enthält, sucht Macie außerdem automatisch nach Keyword-Varianten, die das Leerzeichen nicht enthalten oder einen Unterstrich (_) oder einen Bindestrich (-) anstelle des Leerzeichens enthalten. In bestimmten Fällen erweitert oder kürzt Macie ein Keyword auch, um gängige Varianten des Keywords zu berücksichtigen.

Sehen Sie sich das folgende Video an, um zu demonstrieren, wie Stichwörter Kontext bieten und Macie dabei helfen, bestimmte Arten vertraulicher Daten zu erkennen:Wie Amazon Macie Schlüsselwörter verwendet, um sensible Daten zu entdecken.

Kurzreferenz: Von Amazon Macie verwaltete Datenkennungen

In Amazon Macie besteht eine verwaltete Daten-ID aus einer Reihe integrierter Kriterien und Techniken, die darauf ausgelegt sind, eine bestimmte Art vertraulicher Daten zu erkennen, z. B. Kreditkartennummern, AWS geheime Zugangsschlüssel oder Passnummern für ein bestimmtes Land oder eine bestimmte Region. Diese Identifikatoren können eine große und wachsende Liste sensibler Datentypen für viele Länder und Regionen erkennen, darunter mehrere Arten von Anmeldedaten, Finanzinformationen, persönlichen Gesundheitsinformationen (PHI) und persönlich identifizierbaren Informationen (PII).

In der folgenden Tabelle sind alle verwalteten Datenkennungen aufgeführt, die Macie derzeit bereitstellt, geordnet nach sensiblen Datentypen. Für jeden Typ werden die folgenden Informationen bereitgestellt:

- Kategorie sensibler Daten — Gibt die allgemeine Kategorie sensibler Daten an, zu der folgende Typen gehören: Anmeldeinformationen für Anmeldeinformationen wie private Schlüssel; Finanzinformationen für Finanzdaten wie Kreditkartennummern und

Bankkontonummern; Persönliche Informationen: PHI für persönliche Gesundheitsinformationen wie Krankenversicherungs- und medizinische Identifikationsnummern; und, Persönliche Informationen: PII für persönlich identifizierbare Informationen wie Führerschein-Identifikationsnummern und Reisepassnummern.

- ID für verwaltete Daten — Gibt die eindeutige Kennung (ID) für eine oder mehrere verwaltete Datenkennungen an, mit denen die Daten erkannt werden sollen. Wenn Sie einen Auftrag zur Erkennung vertraulicher Daten erstellen oder Einstellungen für die automatische Erkennung vertraulicher Daten konfigurieren, können Sie anhand dieser IDs angeben, welche verwalteten Datenkennungen Macie bei der Datenanalyse verwenden soll. Eine Liste der verwalteten Datenbezeichner, die wir für Jobs empfehlen, finden Sie unter. Verwaltete Datenkennungen, die für die Erkennung vertraulicher Daten empfohlen werden Eine Liste der verwalteten Datenbezeichner, die wir für die automatische Erkennung sensibler Daten empfehlen, finden Sie unter. Standardeinstellungen für die automatische Erkennung vertraulicher Daten
- Schlüsselwort erforderlich — Gibt an, ob die Erkennung erfordert, dass sich ein Schlüsselwort in der Nähe der Daten befindet. Hinweise dazu, wie Macie bei der Datenanalyse Schlüsselwörter verwendet, finden Sie unterAnforderungen an Schlüsselwörter.
- Länder und Regionen — Gibt an, für welche Länder oder Regionen die entsprechenden Identifikatoren für verwaltete Daten konzipiert sind. Wenn die verwalteten Datenkennungen nicht für bestimmte Länder oder Regionen konzipiert sind, ist dieser Wert „Beliebig“.

Um zusätzliche Details zu den verwalteten Datenkennungen für einen bestimmten Typ vertraulicher Daten zu überprüfen, wählen Sie den Typ aus.

Vertraulicher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüsselwort erforderlich	Länder und Regionen
Geheimer AWS-Zugriffsschlüssel	Anmeldeinformationen	AWS_CREDENTIALS	Ja	Any
Bankkontonummer	Finanzinformationen	BANK_ACCOUNT_NUMBER(sowohl für Kanada als auch für die USA)	Ja	Kanada, USA

Vertrauli cher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüssel wort erforderlich	Länder und Regionen
Grundlege nde Bankkonto nummer (BBAN)	Finanzinf ormationen	Je nach Land oder Region: FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOU NT_NUMBER, ITALY_BAN K_ACCOUNT_NUMBER, SPAIN_BAN K_ACCOUNT_NUMBER, UK_BANK_A CCOUNT_NUMBER	Ja	Frankreich, Deutschla nd, Italien, Spanien, Vereinigtes Königreich
Geburtsda tum	Persönlic he Informati onen: PII	DATE_OF_BIRTH	Ja	Any
Ablaufdat um der Kreditkarte	Finanzinf ormationen	CREDIT_CARD_EXPIRATION	Ja	Any
Magnetstr eifendate n der Kreditkarte	Finanzinf ormationen	CREDIT_CARD_MAGNETIC_STRIPE	Ja	Any
Kreditkar tennummer	Finanzinf ormationen	CREDIT_CARD_NUMBER(für Kreditkartennummern in der Nähe eines Schlüsselworts), CREDIT_CA RD_NUMBER_(NO_KEYWORD) (für Kreditkartennummern, die sich nicht in der Nähe eines Schlüsselworts befinden)	Variiert	Any

Vertrauli cher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüssel wort erforderlich	Länder und Regionen
Bestätigu ngscode für die Kreditkarte	Finanzinf ormationen	CREDIT_CARD_SECURITY_CODE	Ja	Any

Vertrauli cher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüssel wort erforderlich	Länder und Regionen
Identifik ationsnum mer des Führersch eins	Persönlic he Informati onen: PII	Je nach Land oder Region: AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICE	Ja	Australien, Österreich, Belgien, Bulgarien, Kanada, Kroatien, Zypern, Tschechische Republik, Dänemark, Estland, Finnland, Frankreich, Deutschland, Griechenland, Ungarn, Indien, Irland, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Polen, Portugal, Rumänien, Slowakei, Slowenien

Vertrauli cher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüssel wort erforderlich	Länder und Regionen
		NSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE		, Spanien, Schweden, Großbrita nnien, USA
Registrie rungsnumm er der Drug Enforceme nt Agency (DEA)	Persönlic he Informati onen: PHI	US_DRUG_ENFORCEMEN T_AGENCY_NUMBER	Ja	US
Nummer der Wählerliste	Persönlic he Informati onen: PII	UK_ELECTORAL_ROLL_NUMBER	Ja	UK
Vollständ iger Name	Persönlic he Informati onen: PII	NAME	Nein	Beliebig, wenn der Name einen lateinisc hen Zeichensa tz verwendet

Vertraulicher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüsselwort erforderlich	Länder und Regionen
Koordinaten des Global Positioning Systems (GPS)	Persönliche Informationen: PII	LATITUDE_LONGITUDE	Ja	Beliebig, wenn sich die Koordinaten in der Nähe eines englischen Schlüsselworts befinden
Google-Cloud-API-Schlüssel	Anmeldeinformationen	GCP_API_KEY	Ja	Any
Krankenversicherungsantragsnummer (HICN)	Persönliche Informationen: PHI	USA_HEALTH_INSURANCE_CLAIM_NUMBER	Ja	US
Krankenversicherungs- oder medizinische Identifizierungsnummer	Persönliche Informationen: PHI	Je nach Land oder Region: CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER	Ja	Kanada, EU, Finnland, Frankreich, Großbritannien, USA

Vertrauli cher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüssel wort erforderlich	Länder und Regionen
Code des HCPCS (Common Procedure Coding System) für das Gesundhei tswesen	Persönlic he Informati onen: PHI	USA_HEALTHCARE_PRO CEDURE_CODE	Ja	US
HTTP Basic Authoriza tion-Head er	Anmeldein formation en	HTTP_BASIC_AUTH_HEADER	Nein	Any
HTTP-Cookie	Persönlic he Informati onen: PII	HTTP_COOKIE	Nein	Any

Vertrauli cher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüssel wort erforderlich	Länder und Regionen
Internati onale Bankkonto nummer (IBAN)	Finanzinf ormationen	Je nach Land oder Region: ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER	Nein	Albanien, Andorra, Bosnien-Herzegowina, Brasilien, Bulgarien, Costa Rica, Dänemark, Dominikanische Republik, Ägypten, Estland, Faröer-Inseln, Finnland, Frankreich, Georgien, Deutschland, Griechenland, Grönland, Kroatien, Ungarn, Irland, Island, Italien, Jordanien, Kosovo, Liechtens

Vertrauli cher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüssel wort erforderlich	Länder und Regionen
		, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER		tein, Litauen, Malta, Mauretanien, Mauretanien, Mauretanien, Mauritius, Monaco, Montenegro, Niederlande, Nordmazedonien, Polen, Portugal, San Marino, Senegal, Serbien, Slowakei, Slowenien, Spanien, Schweden, Schweiz, Timor-Leste, Tunesien, Türkiye, Großbrita

Vertrauli cher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüssel wort erforderlich	Länder und Regionen
		, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER , UNITED_ARAB_EMIRATES_BANK_A CCOUNT_NUMBER, VIRGIN_IS LANDS_BANK_ACCOUNT_NUMBER(f ür die Britischen Jungferninseln)		nnien, Ukraine, Vereinigte Arabische Emirate, Britische Jungferni nseln
JSON-Web-Token (JWT)	Anmeldein formation en	JSON_WEB_TOKEN	Nein	Any
Postansch rift	Persönlic he Informati onen: PII	ADDRESS, BRAZIL_CEP_CODE (für den brasilianischen Code de Endereçamento Postal)	Variiert	Australie n, Brasilien , Kanada, Frankreich, Deutschla nd, Italien, Spanien, Großbrita nnien, USA
Nationaler Drogenkod ex (NDC)	Persönlic he Informati onen: PHI	USA_NATIONAL_DRUG_CODE	Ja	US

Vertrauli cher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüssel wort erforderlich	Länder und Regionen
Nationale Identifik ationsnum mern	Persönlic he Informati onen: PII	Je nach Land oder Region: BRAZIL_RG_NUMBER, FRANCE_NA TIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICA TION_NUMBER, INDIA_AAD HAAR_NUMBER, ITALY_NAT IONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER	Ja	Brasilien, Frankreich, Deutschla nd, Indien, Italien, Spanien
Nationale Versicher ungsnumme r (NINO)	Persönlic he Informati onen: PII	UK_NATIONAL_INSURANCE_NUMBE R	Ja	UK
Nationale Anbieterk ennzeichn ung (NPI)	Persönlic he Informati onen: PHI	USA_NATIONAL_PROVIDER_IDENT IFIER	Ja	US
Privater OpenSSH-Schlüssel	Anmeldein formation en	OPENSSH_PRIVATE_KEY	Nein	Any
Passnumme r	Persönlic he Informati onen: PII	Je nach Land oder Region: CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER	Ja	Kanada, Frankreich, Deutschla nd, Italien, Spanien, Vereinigtes Königreich, USA

Vertrauli cher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüssel wort erforderlich	Länder und Regionen
Ständige Wohnsitzn ummer	Persönlic he Informati onen: PII	CANADA_NATIONAL_IDENTIFICAT ION_NUMBER	Ja	Kanada
Privater PGP-Schlü ssel	Anmeldein formation en	PGP_PRIVATE_KEY	Nein	Any
Phone number (Telefonn ummer)	Persönlic he Informati onen: PII	Je nach Land oder Region: BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMB ER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER	Variiert	Brasilien , Kanada, Frankreich, Deutschla nd, Italien, Spanien, Vereinigtes Königreich, USA
Privater Schlüssel des Public Key Cryptogra phy Standard (PKCS)	Anmeldein formation en	PKCS	Nein	Any
Privater PuTTY-Schlüssel	Anmeldein formation en	PUTTY_PRIVATE_KEY	Nein	Any

Vertrauli cher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüssel wort erforderlich	Länder und Regionen
Sozialver sicherung snummer (SIN)	Persönlic he Informati onen: PII	CANADA_SOCIAL_INSURANCE_NUM BER	Ja	Kanada
Sozialver sicherung snummer (SSN)	Persönlic he Informati onen: PII	Je nach Land oder Region:SP AIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER	Ja	Spanien, USA
the section called “Stripe-A PI-Schlüs sel”	Anmeldein formation en	STRIPE_CREDENTIALS	Nein	Any
Steuerpfl ichtigen-Identifik ationsnum mer oder Referenzn ummer	Persönlic he Informati onen: PII	Je nach Land oder Region: AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CP F_NUMBER, FRANCE_TAX_IDENTIF ICATION_NUMBER, GERMANY_T AX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUM BER, ITALY_NATIONAL_IDENTIFICATI ON_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX _IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBE R, USA_INDIVIDUAL_TAX_IDENTIFI CATION_NUMBER	Ja	Australien, Brasilien, Frankreich, Deutschla nd, Indien, Italien, Spanien, Großbrita nnien, USA

Vertraulicher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüsselwort erforderlich	Länder und Regionen
Eindeutige Gerätekennung (UDI)	Persönliche Informationen: PHI	MEDICAL_DEVICE_UDI	Ja	US
Fahrzeug-Identifikationsnummer (VIN)	Persönliche Informationen: PII	VEHICLE_IDENTIFICATION_NUMBER	Ja	Beliebig, wenn sich die VIN in der Nähe eines Schlüsselworts in einer der folgenden Sprachen befindet: Englisch, Französisch, Deutsch, Litauisch, Polnisch, Portugiesisch, Rumänisch oder Spanisch

Ausführliche Referenz: Von Amazon Macie verwaltete Datenkennungen

Bei Amazon Macie handelt es sich bei verwalteten Datenkennungen um integrierte Kriterien und Techniken, mit denen bestimmte Arten vertraulicher Daten erkannt werden sollen. Sie können eine

große und wachsende Liste sensibler Datentypen für viele Länder und Regionen erkennen, darunter mehrere Arten von Anmeldeinformationen, Finanzinformationen und persönlichen Informationen. Jeder verwaltete Datenbezeichner ist darauf ausgelegt, eine bestimmte Art sensibler Daten zu erkennen, z. B. AWS geheime Zugangsschlüssel, Kreditkartennummern oder Passnummern für ein bestimmtes Land oder eine bestimmte Region.

Macie kann mithilfe verwalteter Datenkennungen mehrere Kategorien sensibler Daten erkennen. Innerhalb jeder Kategorie kann Macie mehrere Arten sensibler Daten erkennen. In den Themen in diesem Abschnitt werden die einzelnen Typen sowie alle relevanten Anforderungen für die Erkennung der Daten aufgeführt und beschrieben. Einzelheiten zu den verwalteten Datenkennungen für bestimmte Arten vertraulicher Daten finden Sie in den Themen nach Kategorien:

- Anmeldeinformationen — Für Anmeldedaten wie private Schlüssel und AWS geheime Zugriffsschlüssel.
- Finanzinformationen — Für Finanzdaten wie Kreditkartennummern und Bankkontonummern.
- Persönliche Daten: PHI — Für persönliche Gesundheitsinformationen (PHI) wie Krankenversicherungs- und medizinische Identifikationsnummern.
- Persönliche Daten: PII — Für persönlich identifizierbare Informationen (PII) wie Führerschein-Identifikationsnummern und Passnummern.

Oder Sie können einen bestimmten Typ sensibler Daten aus der folgenden Tabelle auswählen. In der Tabelle sind alle verwalteten Datenkennungen aufgeführt, die Macie derzeit bereitstellt, geordnet nach vertraulichen Datentypen. In der Tabelle sind auch die relevanten Anforderungen für die Erkennung der einzelnen Typen zusammengefasst.

Vertraulicher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüsselwort erforderlich	Länder und Regionen
Geheimer AWS-Zugriffsschlüssel	Anmeldeinformationen	AWS_CREDENTIALS	Ja	Any
Bankkontonummer	Finanzinformationen	BANK_ACCOUNT_NUMBER(sowohl für Kanada als auch für die USA)	Ja	Kanada, USA

Vertraulicher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüsselwort erforderlich	Länder und Regionen
Grundlegende Bankkontonummer (BBAN)	Finanzinformationen	Je nach Land oder Region: FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER	Ja	Frankreich, Deutschland, Italien, Spanien, Vereinigtes Königreich
Geburtsdatum	Persönliche Informationen: PII	DATE_OF_BIRTH	Ja	Any
Ablaufdatum der Kreditkarte	Finanzinformationen	CREDIT_CARD_EXPIRATION	Ja	Any
Magnetstreifendaten der Kreditkarte	Finanzinformationen	CREDIT_CARD_MAGNETIC_STRIPE	Ja	Any
Kreditkartennummer	Finanzinformationen	CREDIT_CARD_NUMBER(für Kreditkartennummern in der Nähe eines Schlüsselworts), CREDIT_CARD_NUMBER_(NO_KEYWORD) (für Kreditkartennummern, die sich nicht in der Nähe eines Schlüsselworts befinden)	Variiert	Any

Vertrauli cher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüssel wort erforderlich	Länder und Regionen
Bestätigu ngscode für die Kreditkarte	Finanzinf ormationen	CREDIT_CARD_SECURITY_CODE	Ja	Any

Vertraulicher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüsselwort erforderlich	Länder und Regionen
Identifikationsnummer des Führerscheins	Persönliche Informationen: PII	Je nach Land oder Region: AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICE	Ja	Australien, Österreich, Belgien, Bulgarien, Kanada, Kroatien, Zypern, Tschechische Republik, Dänemark, Estland, Finnland, Frankreich, Deutschland, Griechenland, Ungarn, Indien, Irland, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Polen, Portugal, Rumänien, Slowakei, Slowenien

Vertrauli cher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüssel wort erforderlich	Länder und Regionen
		NSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE		, Spanien, Schweden, Großbrita nnien, USA
Registrie rungsnumm er der Drug Enforceme nt Agency (DEA)	Persönlic he Informati onen: PHI	US_DRUG_ENFORCEMEN T_AGENCY_NUMBER	Ja	US
Nummer der Wählerliste	Persönlic he Informati onen: PII	UK_ELECTORAL_ROLL_NUMBER	Ja	UK
Vollständ iger Name	Persönlic he Informati onen: PII	NAME	Nein	Beliebig, wenn der Name einen lateinisc hen Zeichensa tz verwendet

Vertraulicher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüsselwort erforderlich	Länder und Regionen
Koordinaten des Global Positioning Systems (GPS)	Persönliche Informationen: PII	LATITUDE_LONGITUDE	Ja	Beliebig, wenn sich die Koordinaten in der Nähe eines englischen Schlüsselworts befinden
Google-Cloud-API-Schlüssel	Anmeldeinformationen	GCP_API_KEY	Ja	Any
Krankenversicherungsantragsnummer (HICN)	Persönliche Informationen: PHI	USA_HEALTH_INSURANCE_CLAIM_NUMBER	Ja	US
Krankenversicherungs- oder medizinische Identifizierungsnummer	Persönliche Informationen: PHI	Je nach Land oder Region: CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER	Ja	Kanada, EU, Finnland, Frankreich, Großbritannien, USA

Vertrauli cher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüssel wort erforderlich	Länder und Regionen
Code des HCPCS (Common Procedure Coding System) für das Gesundhei tswesen	Persönlic he Informati onen: PHI	USA_HEALTHCARE_PRO CEDURE_CODE	Ja	US
HTTP Basic Authoriza tion-Head er	Anmeldein formation en	HTTP_BASIC_AUTH_HEADER	Nein	Any
HTTP-Cookie	Persönlic he Informati onen: PII	HTTP_COOKIE	Nein	Any

Vertrauli cher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüssel wort erforderlich	Länder und Regionen
Internati onale Bankkonto nummer (IBAN)	Finanzinf ormationen	Je nach Land oder Region: ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER	Nein	Albanien, Andorra, Bosnien-Herzegowina, Brasilien, Bulgarien, Costa Rica, Dänemark, Dominikanische Republik, Ägypten, Estland, Faröer-Inseln, Finnland, Frankreich, Georgien, Deutschland, Griechenland, Grönland, Kroatien, Ungarn, Irland, Island, Italien, Jordanien, Kosovo, Liechtens

Vertrauli cher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüssel wort erforderlich	Länder und Regionen
		, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER		tein, Litauen, Malta, Mauretanien, Mauretanien, Mauretanien, Mauritius, Monaco, Montenegro, Niederlande, Nordmazedonien, Polen, Portugal, San Marino, Senegal, Serbien, Slowakei, Slowenien, Spanien, Schweden, Schweiz, Timor-Leste, Tunesien, Türkiye, Großbrita

Vertrauli cher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüssel wort erforderlich	Länder und Regionen
		, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER , UNITED_ARAB_EMIRATES_BANK_A CCOUNT_NUMBER, VIRGIN_IS LANDS_BANK_ACCOUNT_NUMBER(f ür die Britischen Jungferninseln)		nnien, Ukraine, Vereinigte Arabische Emirate, Britische Jungferni nseln
JSON-Web-Token (JWT)	Anmeldein formation en	JSON_WEB_TOKEN	Nein	Any
Postansch rift	Persönlic he Informati onen: PII	ADDRESS, BRAZIL_CEP_CODE (für den brasilianischen Code de Endereçamento Postal)	Variiert	Australie n, Brasilien , Kanada, Frankreich, Deutschla nd, Italien, Spanien, Großbrita nnien, USA
Nationaler Drogenkod ex (NDC)	Persönlic he Informati onen: PHI	USA_NATIONAL_DRUG_CODE	Ja	US

Vertraulicher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüsselwort erforderlich	Länder und Regionen
Nationale Identifikationsnummern	Persönliche Informationen: PII	Je nach Land oder Region: BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER	Ja	Brasilien, Frankreich, Deutschland, Indien, Italien, Spanien
Nationale Versicherungsnummer (NINO)	Persönliche Informationen: PII	UK_NATIONAL_INSURANCE_NUMBER	Ja	UK
Nationale Anbieterkennzeichnung (NPI)	Persönliche Informationen: PHI	USA_NATIONAL_PROVIDER_IDENTIFIER	Ja	US
Privater OpenSSH-Schlüssel	Anmeldeinformationen	OPENSSH_PRIVATE_KEY	Nein	Any
Passnummer	Persönliche Informationen: PII	Je nach Land oder Region: CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER	Ja	Kanada, Frankreich, Deutschland, Italien, Spanien, Vereinigtes Königreich, USA

Vertrauli cher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüssel wort erforderlich	Länder und Regionen
Ständige Wohnsitzn ummer	Persönlic he Informati onen: PII	CANADA_NATIONAL_IDENTIFICAT ION_NUMBER	Ja	Kanada
Privater PGP-Schlü ssel	Anmeldein formation en	PGP_PRIVATE_KEY	Nein	Any
Phone number (Telefonn ummer)	Persönlic he Informati onen: PII	Je nach Land oder Region: BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMB ER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER	Variiert	Brasilien , Kanada, Frankreich, Deutschla nd, Italien, Spanien, Vereinigtes Königreich, USA
Privater Schlüssel des Public Key Cryptogra phy Standard (PKCS)	Anmeldein formation en	PKCS	Nein	Any
Privater PuTTY-Schlüssel	Anmeldein formation en	PUTTY_PRIVATE_KEY	Nein	Any

Vertrauli cher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüssel wort erforderlich	Länder und Regionen
Sozialver sicherung snummer (SIN)	Persönlic he Informati onen: PII	CANADA_SOCIAL_INSURANCE_NUM BER	Ja	Kanada
Sozialver sicherung snummer (SSN)	Persönlic he Informati onen: PII	Je nach Land oder Region:SP AIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER	Ja	Spanien, USA
the section called “Stripe-A PI-Schlüs sel”	Anmeldein formation en	STRIPE_CREDENTIALS	Nein	Any
Steuerpfl ichtigen-Identifik ationsnum mer oder Referenzn ummer	Persönlic he Informati onen: PII	Je nach Land oder Region: AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CP F_NUMBER, FRANCE_TAX_IDENTIF ICATION_NUMBER, GERMANY_T AX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUM BER, ITALY_NATIONAL_IDENTIFICATI ON_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX _IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBE R, USA_INDIVIDUAL_TAX_IDENTIFI CATION_NUMBER	Ja	Australien, Brasilien, Frankreich, Deutschla nd, Indien, Italien, Spanien, Großbrita nnien, USA

Vertrauli cher Datentyp	Kategorie sensibler Daten	ID der verwalteten Datenkennung	Schlüssel wort erforderlich	Länder und Regionen
Eindeutige Geräteken nung (UDI)	Persönlic he Informati onen: PHI	MEDICAL_DEVICE_UDI	Ja	US
Fahrzeug-Identifik ationsnum mer (VIN)	Persönlic he Informati onen: PII	VEHICLE_IDENTIFICATION_NUMBER	Ja	Beliebig, wenn sich die VIN in der Nähe eines Schlüssel worts in einer der folgenden Sprachen befindet: Englisch, Französis ch, Deutsch, Litauisch, Polnisch, Portugies isch, Rumänisch oder Spanisch

Verwaltete Datenkennungen für Anmeldeinformationen

Amazon Macie kann mithilfe verwalteter Datenkennungen mehrere Arten sensibler Anmeldeinformationen erkennen. Die Themen auf dieser Seite geben jeden Typ an und enthalten

Informationen über die verwaltete Datenkennung, die zur Erkennung der Daten entwickelt wurde. Jedes Thema enthält die folgenden Informationen:

- ID der verwalteten Datenkennung – Gibt die eindeutige Kennung (ID) für die verwaltete Datenkennung an, die zur Erkennung der Daten entwickelt wurde. Wenn Sie einen Auftrag zur Erkennung vertraulicher Daten erstellen oder Einstellungen für die automatische Erkennung vertraulicher Daten konfigurieren, können Sie diese ID verwenden, um anzugeben, ob Macie bei der Analyse von Daten die verwaltete Datenkennung verwenden soll.
- Unterstützte Länder und Regionen – Gibt an, für welche Länder oder Regionen die entsprechende verwaltete Datenkennung bestimmt ist. Wenn die verwaltete Datenkennung nicht für ein bestimmtes Land oder eine bestimmte Region konzipiert ist, lautet dieser Wert Beliebig.
- Schlüsselwort erforderlich – Gibt an, ob sich ein Schlüsselwort in der Nähe der Daten befinden muss. Wenn ein Schlüsselwort erforderlich ist, enthält das Thema auch Beispiele für erforderliche Schlüsselwörter. Informationen darüber, wie Macie Schlüsselwörter bei der Analyse von Daten verwendet, finden Sie unter Anforderungen an Schlüsselwörter.
- Kommentare – Stellt alle relevanten Details bereit, die sich auf Ihre Auswahl der verwalteten Datenkennung oder Ihre Untersuchung gemeldeter Vorkommen der sensiblen Daten auswirken könnten. Zu den Details gehören Informationen wie unterstützte Standards, Syntaxanforderungen und Ausnahmen.

Die Themen werden in alphabetischer Reihenfolge nach sensiblem Datentyp aufgelistet.

Sensible Datentypen

- Geheimer AWS-Zugriffsschlüssel
- Google-Cloud-API-Schlüssel
- HTTP Basic Authorization-Header
- JSON-Web-Token (JWT)
- Privater OpenSSH-Schlüssel
- Privater PGP-Schlüssel
- Privater Schlüssel des Public Key Cryptography Standard (PKCS)
- Privater PuTTY-Schlüssel
- Stripe-API-Schlüssel

Geheimer AWS-Zugriffsschlüssel

ID der verwalteten Datenkennung: AWS_CREDENTIALS

Unterstützte Länder und Regionen: Beliebige

Schlüsselwort erforderlich: Ja. Zu den Schlüsselwörtern gehören: aws_secret_access_key, credentials, secret access key, secret key, set-awscredential

Kommentare: Macie meldet keine Vorkommen der folgenden Zeichenfolgen, die häufig als fiktive Beispiele verwendet werden: `je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY` und `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`.

Google-Cloud-API-Schlüssel

ID der verwalteten Datenkennung: GCP_API_KEY

Unterstützte Länder und Regionen: Beliebige

Schlüsselwort erforderlich: Ja. Zu den Schlüsselwörtern gehören: G_PLACES_KEY, GCP api key, GCP key, google cloud key, google-api-key, google-cloud-apikeys, GOOGLEKEY, X-goog-api-key

Kommentare: Macie kann nur die Zeichenfolgenkomponente (`keyString`) eines Google Cloud-API-Schlüssels erkennen. Die Unterstützung beinhaltet nicht die Erkennung der ID oder der Anzeigenamenkomponente eines Google Cloud-API-Schlüssels.

HTTP Basic Authorization-Header

ID der verwalteten Datenkennung: HTTP_BASIC_AUTH_HEADER

Unterstützte Länder und Regionen: Beliebige

Schlüsselwort erforderlich: Nein

Kommentare: Die Erkennung erfordert einen vollständigen Header, einschließlich des Feldnamens und der Authentifizierungsschemarichtlinie, wie in RFC 7617 angegeben. Zum Beispiel `Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==` und `Proxy-Authorization: Basic dGVzdDoxMjPCow==`.

JSON-Web-Token (JWT)

ID der verwalteten Datenkennung: JSON_WEB_TOKEN

Unterstützte Länder und Regionen: Beliebige

Schlüsselwort erforderlich: Nein

Kommentare: Macie kann JSON-Web-Token (JWTs) erkennen, die den Anforderungen von RFC 7519 für JSON Web Signature (JWS)-Strukturen entsprechen. Die Token können signiert oder unsigniert sein.

Privater OpenSSH-Schlüssel

ID der verwalteten Datenkennung: OPENSSH_PRIVATE_KEY

Unterstützte Länder und Regionen: Beliebige

Schlüsselwort erforderlich: Nein

Kommentare: Keine

Privater PGP-Schlüssel

ID der verwalteten Datenkennung: PGP_PRIVATE_KEY

Unterstützte Länder und Regionen: Beliebige

Schlüsselwort erforderlich: Nein

Kommentare: Keine

Privater Schlüssel des Public Key Cryptography Standard (PKCS)

ID der verwalteten Datenkennung: PKCS

Unterstützte Länder und Regionen: Beliebige

Schlüsselwort erforderlich: Nein

Kommentare: Keine

Privater PuTTY-Schlüssel

ID der verwalteten Datenkennung: PUTTY_PRIVATE_KEY

Unterstützte Länder und Regionen: Beliebige

Schlüsselwort erforderlich: Nein

Kommentare: Macie kann private PuTTY-Schlüssel erkennen, die die folgenden Standard-Header und die folgende Header-Sequenz verwenden: `PuTTY-User-Key-File`, `Encryption`, `Comment`, `Public-LinesPrivate-Lines`, und `Private-MAC`. Die Header-Werte können alphanumerische Zeichen, Bindestriche (`-`) und Zeilenumbruchzeichen (`\n` oder) enthalten`\r`. - `Public-Lines` und -`Private-Lines`Werte können auch Schrägstriche (`/`), Pluszeichen (`+`) und Gleichheitszeichen () enthalten=. -`Private-MAC`Werte können auch Pluszeichen () enthalten+. Die Unterstützung beinhaltet nicht die Erkennung privater Schlüssel mit Header-Werten, die andere Zeichen wie Leerzeichen oder Unterstriche () enthalten_. Die Unterstützung beinhaltet auch nicht die Erkennung privater Schlüssel, die benutzerdefinierte Header enthalten.

Stripe-API-Schlüssel

ID der verwalteten Datenkennung: STRIPE_CREDENTIALS

Unterstützte Länder und Regionen: Beliebige

Schlüsselwort erforderlich: Nein

Kommentare: Macie meldet keine Vorkommen der folgenden Zeichenfolgen, die häufig in Stripe-Codebeispielen verwendet werden: `sk_test_4eC39HqLyjWDarjtT1zdp7dc` und `pk_test_TYooMQauvdEDq54NiTphI7jx`.

Verwaltete Datenkennungen für Finanzinformationen

Amazon Macie kann mithilfe verwalteter Datenkennungen mehrere Arten sensibler Finanzinformationen erkennen. In den Themen auf dieser Seite werden die einzelnen Typen aufgeführt und Informationen zu den verwalteten Datenkennungen bereitgestellt, mit denen die Daten erkannt werden sollen. Jedes Thema enthält die folgenden Informationen:

- ID für verwaltete Daten — Gibt den eindeutigen Bezeichner (ID) für einen oder mehrere verwaltete Datenbezeichner an, mit denen die Daten erkannt werden sollen. Wenn Sie einen Auftrag zur Erkennung vertraulicher Daten erstellen oder Einstellungen für die automatische Erkennung vertraulicher Daten konfigurieren, können Sie anhand dieser IDs angeben, welche verwalteten Datenkennungen Macie bei der Datenanalyse verwenden soll.
- Unterstützte Länder und Regionen — Gibt an, für welche Länder oder Regionen die entsprechenden Identifikatoren für verwaltete Daten konzipiert sind. Wenn die verwalteten

Datenkennungen nicht für bestimmte Länder oder Regionen konzipiert sind, ist dieser Wert „Beliebig“.

- Schlüsselwort erforderlich — Gibt an, ob die Erkennung erfordert, dass sich ein Schlüsselwort in der Nähe der Daten befindet. Wenn ein Schlüsselwort erforderlich ist, enthält das Thema auch Beispiele für erforderliche Schlüsselwörter. Informationen darüber, wie Macie bei der Datenanalyse Schlüsselwörter verwendet, finden Sie unterAnforderungen an Schlüsselwörter.
- Kommentare — Enthält alle relevanten Informationen, die sich auf Ihre Wahl der verwalteten Daten-ID oder auf Ihre Untersuchung der gemeldeten Vorkommen vertraulicher Daten auswirken könnten. Zu den Details gehören Informationen wie unterstützte Standards, Syntaxanforderungen und Ausnahmen.

Die Themen sind in alphabetischer Reihenfolge nach sensiblen Datentypen aufgelistet.

Sensible Datentypen

- Bankkontonummer
- Grundlegende Bankkontonummer (BBAN)
- Ablaufdatum der Kreditkarte
- Magnetstreifendaten der Kreditkarte
- Kreditkartennummer
- Bestätigungscode für die Kreditkarte
- Internationale Bankkontonummer (IBAN)

Bankkontonummer

Macie kann kanadische und US-amerikanische Bankkontonummern erkennen, die aus 9- bis 17-stelligen Sequenzen bestehen und keine Leerzeichen enthalten.

ID der verwalteten Daten-ID: BANK_ACCOUNT_NUMBER

Unterstützte Länder und Regionen: Kanada, USA

Schlüsselwort erforderlich: Ja. Zu den Schlüsselwörtern gehören: bank account, bank acct, checking account, checking acct, deposit account, deposit acct, savings account, savings acct, chequing account, chequing acct

Kommentare: Diese verwaltete Daten-ID dient ausdrücklich der Erkennung von Bankkontonummern für Kanada und die USA. Diese Länder verwenden nicht die Formate Basic Bank Account Number

(BBAN) oder International Bank Account Number (IBAN), die im internationalen ISO-Standard für die Nummerierung von Bankkonten definiert sind, wie in ISO 13616 spezifiziert. Um Bankkontonummern für andere Länder und Regionen zu ermitteln, verwenden Sie die verwalteten Datenkennungen, die für diese Formate entwickelt wurden. Weitere Informationen finden Sie unter Grundlegende Bankkontonummer (BBAN) und Internationale Bankkontonummer (IBAN).

Grundlegende Bankkontonummer (BBAN)

Macie kann grundlegende Bankkontonummern (BBANs) erkennen, die der BBAN-Struktur entsprechen, die im internationalen ISO-Standard für die Nummerierung von Bankkonten definiert ist, wie in ISO 13616 festgelegt. Dazu gehören BBANs, die keine Leerzeichen enthalten oder Leerzeichen oder Bindestriche als Trennzeichen verwenden, z. B., und. `NWBK60161331926819` `NWBK 6016 1331 9268 19` `NWBK-6016-1331-9268-19`

ID des verwalteten Datenbezeichners: Je nach Land oder Region FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER

Unterstützte Länder und Regionen: Frankreich, Deutschland, Italien, Spanien, Großbritannien

Schlüsselwort erforderlich: Ja. In der folgenden Tabelle sind die Schlüsselwörter aufgeführt, die Macie für bestimmte Länder und Regionen erkennt.

Land oder Region	Schlüsselwörter
Frankreich	account code, account number, accountno#, accountnumber#, bban, code bancaire, compte bancaire, customer account id, customer account number, customer bank account id, iban, numéro de compte
Deutschland	account code, account number, accountno #, accountnumber#, bankleitzahl, bban, customer account id, customer account number, customer bank account id, geheimzah l, iban, kartennummer, kontonummer, kreditkar tennummer, sepa

Land oder Region	Schlüsselwörter
Italien	account code, account number, accountno #, accountnumber#, bban, codice bancario, conto bancario, customer account id, customer account number, customer bank account id, iban, numero di conto
Spanien	account code, account number, accountno #, accountnumber#, bban, código cuenta, código cuenta bancaria, cuenta cliente id, customer account ID, customer account number, customer bank account id, iban, número cuenta bancaria cliente, número cuenta cliente
UK	account code, account number, accountno #, accountnumber#, bban, customer account id, customer account number, customer bank account id, iban, sepa

Kommentare: Diese verwalteten Datenkennungen können auch internationale Bankkontonummern (IBANs) erkennen, die dem ISO-13616-Standard entsprechen. Weitere Informationen finden Sie unter Internationale Bankkontonummer (IBAN). Die verwaltete Daten-ID für das Vereinigte Königreich (UK_BANK_ACCOUNT_NUMBER) kann auch inländische Bankkontonummern für das Vereinigte Königreich erkennen, zum Beispiel. `60-16-13 31926819`

Ablaufdatum der Kreditkarte

ID für verwaltete Daten: CREDIT_CARD_EXPIRATION

Unterstützte Länder und Regionen: Alle

Schlüsselwort erforderlich: Ja. Zu den Schlüsselwörtern gehören: exp d, exp m, exp y, expiration, expiry

Kommentare: Die Support umfasst die meisten Datumsformate, z. B. alle Ziffern und Kombinationen von Ziffern und Monatsnamen. Datumskomponenten können durch Schrägstriche (/), Bindestriche (-)

oder entsprechende Schlüsselwörter getrennt werden. Macie kann beispielsweise Datumsangaben wie`02/26`,`,02/2026`, `Feb 2026` und erkennen. `26-Feb` `expY=2026, expM=02`

Magnetstreifendaten der Kreditkarte

ID der verwalteten Daten: CREDIT_CARD_MAGNETIC_STRIPE

Unterstützte Länder und Regionen: Alle

Schlüsselwort erforderlich: Ja. Zu den Schlüsselwörtern gehören: card data, iso7813, mag, magstripe, stripe, swipe

Kommentare: Die Support umfasst die Titel 1 und 2.

Kreditkartennummer

ID für verwaltete Daten: CREDIT_CARD_NUMBER für Kreditkartennummern, die sich in der Nähe eines Schlüsselworts befinden, CREDIT_CARD_NUMBER_(NO_KEYWORD) für Kreditkartennummern, die sich nicht in der Nähe eines Schlüsselworts befinden

Unterstützte Länder und Regionen: Alle

Erforderliches Schlüsselwort: Variiert. Für den Identifier der CREDIT_CARD_NUMBER verwalteten Daten sind Schlüsselwörter erforderlich. Zu den Schlüsselwörtern gehören: account number, american express, amex, bank card, card, card num, card number, cc #, ccn, check card, credit, credit card#, dankort, debit, debit card, diners club, discover, electron, japanese card bureau, jcb, mastercard, mc, pan, payment account number, payment card number, pcn, union pay, visa. Schlüsselwörter sind für den CREDIT_CARD_NUMBER_(NO_KEYWORD) verwalteten Datenbezeichner nicht erforderlich.

Kommentare: Für die Erkennung müssen die Daten eine 13- bis 19-stellige Sequenz sein, die der Luhn-Checkformel entspricht und ein Standardpräfix für Kartennummern verwendet, die für jede der folgenden Arten von Kreditkarten verwendet werden: American Express, Dankort, Diner's Club, Discover, Electron, Japanese Card Bureau (JCB), Mastercard und Visa. UnionPay

Macie meldet keine Vorkommen der folgenden Sequenzen, die Kreditkartenaussteller für öffentliche Tests reserviert haben:`122000000000003`,`,,,2222405343248877`,`2222990905257051`,`2223007648726984`,`22235771252047400099000 14`,`5420923878724339`,`5454545454545454`,`5455330760000018`,`5506900490000463049506000000000` `6331101999990016675964982643845 3`, `679999010000000019` und. `76009244561`

Bestätigungscode für die Kreditkarte

ID der verwalteten Daten-ID: CREDIT_CARD_SECURITY_CODE

Unterstützte Länder und Regionen: Alle

Schlüsselwort erforderlich: Ja. Zu den Schlüsselwörtern gehören: card id, card identification code, card identification number, card security code, card validation code, card validation number, card verification data, card verification value, cvc, cvc2, cvv, cvv2, elo verification code

Kommentare: Keine

Internationale Bankkontonummer (IBAN)

Macie kann internationale Bankkontonummern (IBANs) erkennen, die aus bis zu 34 alphanumerischen Zeichen bestehen, einschließlich Elementen wie der Landesvorwahl. Insbesondere kann Macie IBANs erkennen, die dem internationalen ISO-Standard für die Nummerierung von Bankkonten entsprechen, wie er in ISO 13616 festgelegt ist. Dazu gehören IBANs, die keine Leerzeichen enthalten oder Leerzeichen oder Bindestriche verwenden, z. B., und. `GB29NWBK60161331926819` `GB29 NWBK 6016 1331 9268 19` `GB29-NWBK-6016-1331-9268-19` Die Erkennung umfasst Validierungsprüfungen, die auf dem Modulus 97-Schema basieren.

ID der verwalteten Daten-ID: Je nach Land oder Region ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER,

MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER (für die Britischen Jungferninseln)

Unterstützte Länder und Regionen: Albanien, Andorra, Bosnien-Herzegowina, Brasilien, Bulgarien, Costa Rica, Kroatien, Zypern, Tschechische Republik, Dänemark, Dominikanische Republik, Ägypten, Estland, Faröer-Inseln, Finnland, Frankreich, Georgien, Deutschland, Griechenland, Grönland, Ungarn, Island, Irland, Italien, Jordanien, Kosovo, Liechtenstein, Litauen, Malta, Mauretanien, Mauretanien, Mauritius, Monaco, Montenegro, Niederlande, Nordmazedonien, Polen, Portugal, San Marino, Senegal, Serbien, Slowakei, Slowenien, Spanien, Schweden, Schweiz, Timor-Leste, Tunesien, Türkei, Großbritannien, Ukraine, Vereinigte Arabische Emirate Emirates, Britische Jungferninseln

Schlüsselwort erforderlich: Nein

Kommentare: Die verwalteten Datenkennungen für Frankreich, Deutschland, Italien, Spanien und das Vereinigte Königreich können auch grundlegende Bankkontonummern (BBANs) erkennen, die der durch den ISO-13616-Standard definierten BBAN-Struktur entsprechen, wenn sich die Zeichenfolge in der Nähe eines Schlüsselworts befindet. Weitere Informationen finden Sie unter Grundlegende Bankkontonummer (BBAN).

Verwaltete Datenkennungen für persönliche Gesundheitsinformationen (PHI)

Amazon Macie kann mithilfe verwalteter Datenkennungen mehrere Arten sensibler, persönlicher Gesundheitsinformationen (PHI) erkennen. In den Themen auf dieser Seite werden die einzelnen Typen spezifiziert und Informationen zur verwalteten Daten-ID bereitgestellt, mit der die Daten erkannt werden sollen. Jedes Thema enthält die folgenden Informationen:

- ID des verwalteten Datenbezeichners — Gibt den eindeutigen Bezeichner (ID) für den verwalteten Datenbezeichner an, mit dem die Daten erkannt werden sollen. Wenn Sie einen Auftrag zur

Erkennung vertraulicher Daten erstellen oder Einstellungen für die automatische Erkennung vertraulicher Daten konfigurieren, können Sie mit dieser ID angeben, ob Macie die ID für verwaltete Daten verwenden soll, wenn es Daten analysiert.

- Unterstützte Länder und Regionen — Gibt an, für welche Länder oder Regionen der entsprechende Identifier für verwaltete Daten konzipiert ist. Wenn der verwaltete Datenbezeichner nicht für ein bestimmtes Land oder eine bestimmte Region konzipiert ist, ist dieser Wert „Beliebig“.
- Schlüsselwort erforderlich — Gibt an, ob die Erkennung erfordert, dass sich ein Schlüsselwort in der Nähe der Daten befindet. Wenn ein Schlüsselwort erforderlich ist, enthält das Thema auch Beispiele für erforderliche Schlüsselwörter. Informationen darüber, wie Macie bei der Datenanalyse Schlüsselwörter verwendet, finden Sie unterAnforderungen an Schlüsselwörter.
- Kommentare — Enthält alle relevanten Informationen, die sich auf Ihre Wahl der verwalteten Daten-ID oder auf Ihre Untersuchung der gemeldeten Vorkommen vertraulicher Daten auswirken könnten. Zu den Details gehören Informationen wie unterstützte Standards, Syntaxanforderungen und Ausnahmen.

Die Themen sind in alphabetischer Reihenfolge nach sensiblen Datentypen aufgelistet.

Sensible Datentypen

- Registrierungsnummer der Drug Enforcement Agency (DEA)
- Krankenversicherungsantragsnummer (HICN)
- Krankenversicherungs- oder medizinische Identifizierungsnummer
- Code des HCPCS (Common Procedure Coding System) für das Gesundheitswesen
- Nationaler Drogenkodex (NDC)
- Nationale Anbieterkennzeichnung (NPI)
- Eindeutige Gerätekennung (UDI)

Registrierungsnummer der Drug Enforcement Agency (DEA)

ID der verwalteten Daten-ID: US_DRUG_ENFORCEMENT_AGENCY_NUMBER

Unterstützte Länder und Regionen: USA

Schlüsselwort erforderlich: Ja. Zu den Schlüsselwörtern gehören: dea number, dea registration

Kommentare: Keine

Krankenversicherungsantragsnummer (HICN)

ID der verwalteten Daten-ID: USA_HEALTH_INSURANCE_CLAIM_NUMBER

Unterstützte Länder und Regionen: USA

Schlüsselwort erforderlich: Ja. Zu den Schlüsselwörtern gehören: health insurance claim number, hic no, hic no., hic number, hic#, hicn, hicn#., hicno#

Kommentare: Keine

Krankenversicherungs- oder medizinische Identifizierungsnummer

Der Support umfasst europäische Krankenversicherungskartennummern für die EU und Finnland, Krankenversicherungsnummern für Frankreich, Medicare-Begünstigte für die USA, NHS-Nummern für Großbritannien und persönliche Gesundheitsnummern für Kanada.

ID der verwalteten Daten-ID: Je nach Land oder Region CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER

Unterstützte Länder und Regionen: Kanada, EU, Finnland, Frankreich, Großbritannien, USA

Schlüsselwort erforderlich: Ja. In der folgenden Tabelle sind die Schlüsselwörter aufgeführt, die Macie für bestimmte Länder und Regionen erkennt.

Land oder Region	Schlüsselwörter
Kanada	canada healthcare number, msp number, personal healthcare number, phn, soins de santé
EU	assicurazione sanitaria numero, carta assicurazione numero, carte d’assurance maladie, carte européenne d'assurance maladie, ceam, ehic, ehic#, finlandehicnumber#, gesundheitskarte, hälsokort, health card, health card number, health insurance card, health insurance number, insurance card

Land oder Region	Schlüsselwörter
	number, krankenversicherungskarte, krankenversicherungsnummer, medical account number, numero conto medico, numéro d'assurance maladie, numéro de carte d'assurance, numéro de compte medical, número de cuenta médica, número de seguro de salud, número de tarjeta de seguro, sairaanhoitokortin, sairausva kuutuskortti, sairausvakuutusnumero, sjukförsäkring nummer, sjukförsäkringskort, suomi ehic-numero, tarjeta de salud, terveyskortti, tessera sanitaria assicurazione numero, versicherungsnummer
Finnland	ehic, ehic#, finland health insurance card, finlandehicnumber#, finska sjukförsäkringskort, hälsokort, health card, health card number, health insurance card, health insurance number, sairaanhoitokortin, sairaanhoitokortin, sairausvakuutuskortti, sairausvakuutusnumero, sjukförsäkring nummer, sjukförsäkringskort, suomen sairausvakuutuskortti, suomi ehic-numero, terveyskortti
Frankreich	carte d'assuré social, carte vitale, insurance card
Vereinigtes Königreich	national health service, NHS
US	mbi, medicare beneficiary

Kommentare: Keine

Code des HCPCS (Common Procedure Coding System) für das Gesundheitswesen

ID der verwalteten Daten-ID: USA_HEALTHCARE_PROCEDURE_CODE

Unterstützte Länder und Regionen: USA

Schlüsselwort erforderlich: Ja. Zu den Schlüsselwörtern gehören: current procedural terminology, hcpcs, healthcare common procedure coding system

Kommentare: Keine

Nationaler Drogenkodex (NDC)

ID der verwalteten Daten-ID: USA_NATIONAL_DRUG_CODE

Unterstützte Länder und Regionen: USA

Schlüsselwort erforderlich: Ja. Zu den Schlüsselwörtern gehören: national drug code, ndc

Kommentare: Keine

Nationale Anbieterkennzeichnung (NPI)

ID der verwalteten Daten-ID: USA_NATIONAL_PROVIDER_IDENTIFIER

Unterstützte Länder und Regionen: USA

Schlüsselwort erforderlich: Ja. Zu den Schlüsselwörtern gehören: hipaa, n.p.i, national provider, npi

Kommentare: Keine

Eindeutige Gerätekennung (UDI)

ID der verwalteten Daten-ID: MEDICAL_DEVICE_UDI

Unterstützte Länder und Regionen: USA

Schlüsselwort erforderlich: Ja. Zu den Schlüsselwörtern gehören: blood, blood bag, dev id, device id, device identifier, gs1, hibcc, iccbba, med, udi, unique device id, unique device identifier

Kommentare: Macie kann eindeutige Gerätekennungen (UDIs) erkennen, die den von der US-amerikanischen Food and Drug Administration zugelassenen Formaten entsprechen. Dazu gehören Standardformate, die von GS1, HIBCC und ICCBBA definiert wurden. Die ICCBA-Unterstützung bezieht sich auf den ISBT-Standard.

Verwaltete Datenkennungen für persönlich identifizierbare Informationen (PII)

Amazon Macie kann mithilfe verwalteter Datenkennungen mehrere Arten sensibler, persönlich identifizierbarer Informationen (PII) erkennen. In den Themen auf dieser Seite werden die einzelnen Typen aufgeführt und Informationen zu den verwalteten Datenkennungen bereitgestellt, mit denen die Daten erkannt werden sollen. Jedes Thema enthält die folgenden Informationen:

- ID für verwaltete Daten — Gibt den eindeutigen Bezeichner (ID) für einen oder mehrere verwaltete Datenbezeichner an, mit denen die Daten erkannt werden sollen. Wenn Sie einen Auftrag zur Erkennung vertraulicher Daten erstellen oder Einstellungen für die automatische Erkennung vertraulicher Daten konfigurieren, können Sie anhand dieser IDs angeben, welche verwalteten Datenkennungen Macie bei der Datenanalyse verwenden soll.
- Unterstützte Länder und Regionen — Gibt an, für welche Länder oder Regionen die entsprechenden Identifikatoren für verwaltete Daten konzipiert sind. Wenn die verwalteten Datenkennungen nicht für bestimmte Länder oder Regionen konzipiert sind, ist dieser Wert „Beliebig“.
- Schlüsselwort erforderlich — Gibt an, ob die Erkennung erfordert, dass sich ein Schlüsselwort in der Nähe der Daten befindet. Wenn ein Schlüsselwort erforderlich ist, enthält das Thema auch Beispiele für erforderliche Schlüsselwörter. Informationen darüber, wie Macie bei der Datenanalyse Schlüsselwörter verwendet, finden Sie unterAnforderungen an Schlüsselwörter.
- Kommentare — Enthält alle relevanten Informationen, die sich auf Ihre Wahl der verwalteten Daten-ID oder auf Ihre Untersuchung der gemeldeten Vorkommen vertraulicher Daten auswirken könnten. Zu den Details gehören Informationen wie unterstützte Standards, Syntaxanforderungen und Ausnahmen.

Die Themen sind in alphabetischer Reihenfolge nach sensiblen Datentypen aufgelistet.

Sensible Datentypen

- Geburtsdatum
- Identifikationsnummer des Führerscheins
- Nummer der Wählerliste
- Vollständiger Name
- Koordinaten des Global Positioning Systems (GPS)
- HTTP-Cookie
- Postanschrift
- Nationale Identifikationsnummern
- Nationale Versicherungsnummer (NINO)
- Passnummer
- Ständige Wohnsitznummer
- Phone number (Telefonnummer)

- Sozialversicherungsnummer (SIN)
- Sozialversicherungsnummer (SSN)
- Steuerpflichtigen-Identifikationsnummer oder Referenznummer
- Fahrzeug-Identifikationsnummer (VIN)

Geburtsdatum

ID der verwalteten Daten: DATE_OF_BIRTH

Unterstützte Länder und Regionen: Alle

Schlüsselwort erforderlich: Ja. Zu den Schlüsselwörtern gehören: bday, b-day, birth date, birthday, date of birth, dob

Kommentare: Die Support umfasst die meisten Datumsformate, z. B. alle Ziffern und Kombinationen von Ziffern und Monatsnamen. Datumskomponenten können durch Leerzeichen, Schrägstriche (/) oder Bindestriche (-) getrennt werden.

Identifikationsnummer des Führerscheins

ID für verwaltete Datenbezeichner: Je nach Land oder Region AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE

Unterstützte Länder und Regionen: Australien, Österreich, Belgien, Bulgarien, Kanada, Kroatien, Zypern, Tschechische Republik, Dänemark, Estland, Finnland, Frankreich, Deutschland, Griechenland, Ungarn, Indien, Irland, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Polen, Portugal, Rumänien, Slowakei, Slowenien, Spanien, Schweden, Großbritannien, USA

Schlüsselwort erforderlich: Ja. In der folgenden Tabelle sind die Schlüsselwörter aufgeführt, die Macie für bestimmte Länder und Regionen erkennt.

Land oder Region	Schlüsselwörter
Australien	dl#, dl:, dlno#, driver licence, driver license, driver permit, drivers lic., drivers licence, driver's licence, drivers license, driver's license, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit
Österreich	führerschein, fuhrerschein, führerschein republik österreich, fuhrerschein republik osterreich
Belgien	fuehrerschein, fuehrerschein- nr, fuehrersc heinnummer, fuhrerschein, führerschein, fuhrerschein- nr, führerschein- nr, fuhrersch einnummer, führerscheinnummer, numéro permis conduire, permis de conduire, rijbewijs, rijbewijsnummer
Bulgarien	превозно средство, свидетелство за управление на моторно, свидетелство за управление на мпс, сумпс, шофьорска книжка
Kanada	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit, permis de conduire
Kroatien	vozačka dozvola

Land oder Region	Schlüsselwörter
Zypern	άδεια οδήγησης
Tschechische Republik	číslo licence, číslo licence řidiče, číslo řidičskéh o průkazu, ovladače lic., povolení k jízdě, povolení řidiče, řidiči povolení, řidičský prúkaz, řidičský průkaz
Dänemark	kørekort, kørekortnummer
Estland	juhi litsentsi number, juhiloa number, juhiluba, juhiluba number
Finnland	ajokortin numero, ajokortti, förare lic., körkort, körkort nummer, kuljettaja lic., permis de conduire
Frankreich	permis de conduire
Deutschland	fuehrerschein, fuehrerschein- nr, fuehrersc heinnummer, fuhrerschein, führerschein, fuhrerschein- nr, führerschein- nr, fuhrersch einnummer, führerscheinnummer
Griechenland	δεια οδήγησης, adeia odigisis
Ungarn	illesztőprogramok lic, jogosítvány, jogsi, licencszám, vezető engedély, vezetői engedély
Indien	driver licence, driver licences, driver license, driver licenses, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, driving licence, driving license
Irland	ceadúnas tiomána

Land oder Region	Schlüsselwörter
Italien	patente di guida, patente di guida numero, patente guida, patente guida numero
Lettland	autovadītāja apliecība, licences numurs, vadītāja apliecība, vadītāja apliecības numurs, vadītāja atļauja, vadītāja licences numurs, vadītāji lic.
Litauen	vairuotojo pažymėjimas
Luxemburg	fahrerlaubnis, führerschäin
Malta	liċenzja tas-sewqan
Niederlande	permis de conduire, rijbewijs, rijbewijsnummer
Polen	numer licencyjny, prawo jazdy, zezwolenie na prowadzenie
Portugal	carta de condução, carteira de habilitação, carteira de motorist, carteira habilitação, carteira motorist, licença condução, licença de condução, número de licença, número licença, permissão condução, permissão de condução
Rumänien	numărul permisului de conducere, permis de conducere
Slowakei	číslo licencie, číslo vodičského preukazu, ovládače lic., povolenia vodičov, povolenie jazdu, povolenie na jazdu, povolenie vodiča, vodičský preukaz
Slowenien	vozniško dovoljenje

Land oder Region	Schlüsselwörter
Spanien	carnet conducer, el carnet de conducer, licencia conducer, licencia de manejo, número carnet conducer, número de carnet de conducer, número de permiso conducer, número de permiso de conducer, número licencia conducer, número permiso conducer, permiso conducción, permiso conducer, permiso de conducción
Schweden	ajokortin numero, dlno# ajokortti, drivere lic., förare lic., körkort, körkort nummer, körkortsn ummer, kuljettajat lic.
UK	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit
US	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit

Kommentare: Keine

Nummer der Wählerliste

ID der verwalteten Daten-ID: UK_ELECTORAL_ROLL_NUMBER

Unterstützte Länder und Regionen: Großbritannien

Schlüsselwort erforderlich: Ja. Zu den Schlüsselwörtern gehören: electoral #, electoral number, electoral roll #, electoral roll no., electoral roll number, electoralrollno

Kommentare: Keine

Vollständiger Name

ID der verwalteten Daten-ID: NAME

Unterstützte Länder und Regionen: Alle

Schlüsselwort erforderlich: Nein

Kommentare: Macie kann nur vollständige Namen erkennen. Unterstützt werden nur lateinische Zeichensätze.

Koordinaten des Global Positioning Systems (GPS)

ID der verwalteten Daten-ID: LATITUDE_LONGITUDE

Unterstützte Länder und Regionen: Alle, wenn sich die Koordinaten in der Nähe eines englischen Schlüsselworts befinden.

Schlüsselwort erforderlich: Ja. Zu den Schlüsselwörtern gehören: coordinate, coordinates, lat long, latitude longitude, position

Kommentare: Macie kann GPS-Koordinaten erkennen, wenn die Breiten- und Längengradkoordinaten paarweise gespeichert werden und sie beispielsweise `41.948614,-87.655311` im Format Dezimal Degrees (DD) vorliegen. Die Support umfasst nicht die Erkennung von Koordinaten im Format Degrees Decimal Minutes (DDM) oder beispielsweise `41°56.9168'N 87°39.3187'W` im Format Degrees, Minutes, Seconds (DMS). `41°56'55.0104"N 87°39'19.1196"W`

HTTP-Cookie

ID der verwalteten Daten-ID: HTTP_COOKIE

Unterstützte Länder und Regionen: Alle

Schlüsselwort erforderlich: Nein

Kommentare: Für die Erkennung ist eine vollständige `Set-Cookie` Kopfzeile `Cookie` oder ein Header erforderlich. Der Header kann ein oder mehrere Name-Wert-Paare enthalten, zum Beispiel: `Set-Cookie: id=TWlrZQ` und. `Cookie: session=3948; lang=en`

Postanschrift

ID des verwalteten Datenbezeichners: ADDRESS (für Australien, Kanada, Frankreich, Deutschland, Italien, Spanien, Großbritannien und die USA), BRAZIL_CEP_CODE (für das brasilianische Unternehmen, das auch für das brasilianische Unternehmen, das folgende Unternehmen hat)

Unterstützte Länder und Regionen: Australien, Brasilien, Kanada, Frankreich, Deutschland, Italien, Spanien, Großbritannien, USA

Erforderliches Schlüsselwort: Variiert. Für die ADDRESS verwaltete Daten-ID sind keine Schlüsselwörter erforderlich. Für den Identifier für BRAZIL_CEP_CODE verwaltete Daten sind Schlüsselwörter erforderlich. Zu den Schlüsselwörtern gehören: cep, código de endereçamento postal, codigo de endereçamento postal, código postal, codigo postal

Kommentare: Obwohl für die ADDRESS verwaltete Daten-ID kein Schlüsselwort erforderlich ist, erfordert die Erkennung, dass eine Adresse den Namen einer Stadt oder eines Ortes und eine entsprechende Postleitzahl oder Postleitzahl in einem unterstützten Land oder einer unterstützten Region enthält. Der BRAZIL_CEP_CODE verwaltete Datenbezeichner kann nur den Teil mit dem Code Code de Endereçamento Postal (CEP) einer Adresse erkennen.

Nationale Identifikationsnummern

Die Support umfasst Aadhaar-Nummern für Indien, Codice Fiscale-Nummern für Italien, Documento Nacional de Identidad (DNI) -Identifikatoren für Spanien, Codes des französischen Nationalen Instituts für Statistik und Wirtschaftsstudien (INSEE), deutsche Personalausweisnummern und Registro Geral (RG) -Nummern für Brasilien.

ID für verwaltete Datenbezeichner: Je nach Land oder Region BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER

Unterstützte Länder und Regionen: Brasilien, Frankreich, Deutschland, Indien, Italien, Spanien

Schlüsselwort erforderlich: Ja. In der folgenden Tabelle sind die Schlüsselwörter aufgeführt, die Macie für bestimmte Länder und Regionen erkennt.

Land oder Region	Schlüsselwörter
Brasilien	registro geral, rg
Frankreich	assurance sociale, carte nationale d’identit é, cni, code sécurité sociale, French social security number, fssn#, insee, insurance number, national id number, nationalid#, numéro d'assurance, sécurité sociale, sécurité sociale non., sécurité sociale numéro, social, social security, social security number, socialsecuritynumber, ss#, ssn, ssn#
Deutschland	ausweisnummer, id number, identification number, identity number, insurance number, personal id, personalausweis
Indien	aadhaar, aadhar, adhaar, uidai
Italien	codice fiscal, dati anagrafici, ehic, health card, health insurance card, p. iva, partita i.v.a., personal data, tax code, tessera sanitaria
Spanien	dni, dni#, dninúmero#, documento nacional de identidad, identidad único, identidadúnico#, insurance number, national identification number, national identity, nationalid#, nationali dno#, número nacional identidad, personal identification number, personal identity no, unique identity number, uniqueid#

Kommentare: Keine

Nationale Versicherungsnummer (NINO)

ID der verwalteten Daten-ID: UK_NATIONAL_INSURANCE_NUMBER

Unterstützte Länder und Regionen: Großbritannien

Schlüsselwort erforderlich: Ja. Zu den Schlüsselwörtern gehören: insurance no., insurance number, insurance#, national insurance number, nationalinsurance#, nationalinsurancenumber, nin, nino

Kommentare: Keine

Passnummer

ID der verwalteten Daten-ID: Je nach Land oder Region CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER

Unterstützte Länder und Regionen: Kanada, Frankreich, Deutschland, Italien, Spanien, Großbritannien, USA

Schlüsselwort erforderlich: Ja. In der folgenden Tabelle sind die Schlüsselwörter aufgeführt, die Macie für bestimmte Länder und Regionen erkennt.

Land oder Region	Schlüsselwörter
Kanada	passeport, passeport#, passport, passport#, passportno, passportno#
Frankreich	numéro de passeport, passeport, passeport #, passeport n °, passeport non
Deutschland	ausstellungsdatum, ausstellungsort, geburtsdatum, passport, passports, reisepass, reisepass–nr, reisepassnummer
Italien	italian passport number, numéro passeport , numéro passeport italien, passaporto, passaporto italiana, passaporto numero, passport number, repubblica italiana passaporto
Spanien	españa pasaporte, libreta pasaporte, número pasaporte, pasaporte, passport, passport book, passport no, passport number, spain passport

Land oder Region	Schlüsselwörter
UK	passeport #, passeport n °, passeport non, passeportn °, passport #, passport no, passport number, passport#, passportid
US	passport, travel document

Kommentare: Keine

Ständige Wohnsitznummer

ID der verwalteten Daten-ID: CANADA_NATIONAL_IDENTIFICATION_NUMBER

Unterstützte Länder und Regionen: Kanada

Schlüsselwort erforderlich: Ja. Zu den Schlüsselwörtern gehören: carte résident permanent, numéro carte résident permanent, numéro résident permanent, permanent resident card, permanent resident card number, permanent resident no, permanent resident no., permanent resident number, pr no, pr no., pr non, pr number, résident permanent no., résident permanent non

Kommentare: Keine

Phone number (Telefonnummer)

ID der verwalteten Daten-ID: Je nach Land oder Region BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER

Unterstützte Länder und Regionen: Brasilien, Kanada, Frankreich, Deutschland, Italien, Spanien, Großbritannien, USA

Erforderliches Schlüsselwort: Variiert. Wenn sich ein Schlüsselwort in der Nähe der Daten befindet, muss die Nummer keine Landesvorwahl enthalten. Zu den Schlüsselwörtern gehören: cell, contact, fax, fax number, mobile, phone, phone number, tel, telephone, telephone number. Für Brasilien gehören zu den Schlüsselwörtern auch: cel, celular, fone, móvel, número residencial, numero residencial, telefone. Wenn sich ein Schlüsselwort nicht in der Nähe der Daten befindet, muss die Nummer eine Landesvorwahl enthalten.

Kommentare: Für die USA umfasst der Support gebührenfreie Nummern.

Sozialversicherungsnummer (SIN)

ID der verwalteten Daten-ID: CANADA_SOCIAL_INSURANCE_NUMBER

Unterstützte Länder und Regionen: Kanada

Schlüsselwort erforderlich: Ja. Zu den Schlüsselwörtern gehören: canadian id, numéro d'assurance sociale, sin, social insurance number

Kommentare: Keine

Sozialversicherungsnummer (SSN)

ID der verwalteten Daten-ID: Je nach Land oder Region, SPAIN_SOCIAL_SECURITY_NUMBER USA_SOCIAL_SECURITY_NUMBER

Unterstützte Länder und Regionen: Spanien, USA

Schlüsselwort erforderlich: Ja. Für Spanien gehören zu den Schlüsselwörtern: número de la seguridad social, social security no., social security number, socialsecurityno#, ssn, ssn#. Für die USA gehören zu den Schlüsselwörtern: social security, ss#, ssn.

Kommentare: Keine

Steuerpflichtigen-Identifikationsnummer oder Referenznummer

Die Support umfasst: CIF-, NIE- und NIF-Nummern für Spanien; CNPJ- und CPF-Nummern für Brasilien; Codice Fiscale-Nummern für Italien; ITINs für die USA; PANs für Indien; Steueridentifikationsnummern für Deutschland; TFNs für Australien; TINs für Frankreich sowie TRN- und UTR-Nummern für Großbritannien.

ID der verwalteten Daten-ID: Je nach Land oder Region AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER

Unterstützte Länder und Regionen: Australien, Brasilien, Frankreich, Deutschland, Indien, Italien, Spanien, Großbritannien, USA

Schlüsselwort erforderlich: Ja. In der folgenden Tabelle sind die Schlüsselwörter aufgeführt, die Macie für bestimmte Länder und Regionen erkennt.

Land oder Region	Schlüsselwörter
Australien	tax file number, tfn
Brasilien	cadastro de pessoa física, cadastro de pessoa fisica, cadastro de pessoas físicas, cadastro de pessoas fisicas, cadastro nacional da pessoa jurídica, cadastro nacional da pessoa juridica, cnpj, cpf
Frankreich	numéro d'identification fiscal, tax id, tax identification number, tax number, tin, tin#
Deutschland	identifikationsnummer, steuer id, steueridentifikationsnummer, steuernummer, tax id, tax identification number, tax number
Indien	e-pan, pan card, pan number, permanent account number
Italien	codice fiscal, dati anagrafici, ehic, health card, health insurance card, p. iva, partita i.v.a., personal data, tax code, tessera sanitaria
Spanien	cif, cif número, cifnúmero#, nie, nif, número de contribuyente, número de identidad de extranjero, número de identificación fiscal, número de impuesto corporativo, personal tax number, tax id, tax identification number, tax number, tin, tin#
UK	paye, tax id, tax id no., tax id number, tax identification, tax identification#, tax no., tax number, tax reference, tax#, taxid#, temporary

Land oder Region	Schlüsselwörter
	reference number, tin, trn, unique tax reference, unique taxpayer reference, utr
US	i.t.i.n., individuelle Steueridentifikationsnummer, itin

Kommentare: Keine

Fahrzeug-Identifikationsnummer (VIN)

ID der verwalteten Daten-ID: VEHICLE_IDENTIFICATION_NUMBER

Unterstützte Länder und Regionen: Alle, wenn sich die Fahrgestellnummer in der Nähe eines Schlüsselworts in einer der folgenden Sprachen befindet: Englisch, Französisch, Deutsch, Litauisch, Polnisch, Portugiesisch, Rumänisch oder Spanisch.

Schlüsselwort erforderlich: Ja. Zu den Schlüsselwörtern gehören: Fahrgestellnummer, niv, numarul de identificare, numarul seriei de sasiu, numer VIN, Número de Identificação do Veículo, Número de Identificación de Automóviles, numéro d'identification du véhicule, vehicle identification number, vin, VIN numeris

Kommentare: Macie kann VINs erkennen, die aus einer Sequenz von 17 Zeichen bestehen und den Normen ISO 3779 und 3780 entsprechen. Diese Standards wurden für den weltweiten Einsatz konzipiert.

Erstellen benutzerdefinierter Datenkennungen in Amazon Macie

EINbenutzerdefinierter Datenbezeichnerist eine Reihe von Kriterien, die Sie definieren, um vertrauliche Daten in Amazon Simple Storage Service (Amazon S3) -Objekten zu erkennen. Die Kriterien bestehen aus einem regulären Ausdruck (Regex), der ein zu suchendes Textmuster definiert und optional Zeichenfolgen und eine Näherungsregel zur Eingrenzung der Ergebnisse festlegt.

Mit benutzerdefinierten Datenkennungen können Sie Erkennungskriterien definieren, die die speziellen Szenarien Ihres Unternehmens, geistiges Eigentum oder proprietäre Daten widerspiegeln, z. B. Mitarbeiter-IDs, Kundenkontonummern oder interne Datenklassifizierungen. Wenn Sie konfigurierenAufgaben zur Erkennung vertraulicher Datenoderautomatische Erkennung vertraulicher

DatenUm diese Identifikatoren zu verwenden, können Sie S3-Objekte auf eine Weise analysieren, die dieIdentifikatoren für verwaltete Datendas Amazon Macie bietet.

Zusätzlich zu den Erkennungskriterien können Sie benutzerdefinierte Schweregradeinstellungen für sensible Datenfunde definieren, die ein benutzerdefinierter Datenidentifikator generiert. Standardmäßig weist Macie dieMittelSchweregrad aller Ergebnisse, die ein benutzerdefinierter Datenbezeichner liefert — der Schweregrad ändert sich nicht anhand der Anzahl der Textvorkommen, die den Erkennungskriterien einer benutzerdefinierten Daten-ID entsprechen. Durch die Definition benutzerdefinierter Schweregradeinstellungen können Sie anhand der Anzahl der Textvorkommen, die den Kriterien entsprechen, angeben, welcher Schweregrad zugewiesen werden soll.

Themen

- Definition von Erkennungskriterien für benutzerdefinierte Datenkennungen
- Definieren von Einstellungen für den Schweregrad der Suche für benutzerdefinierte Datenkennungen
- Erstellen benutzerdefinierter Datenkennungen
- Regex-Unterstützung in benutzerdefinierten Datenkennungen

Definition von Erkennungskriterien für benutzerdefinierte Datenkennungen

Wenn Sie einen benutzerdefinierten Datenbezeichner erstellen, geben Sie einen regulären Ausdruck an (Regex), das ein Textmuster definiert, das in S3-Objekten übereinstimmt. Macie unterstützt eine Teilmenge der Regex-Mustersyntax, die von derPerl-Bibliothek für kompatible reguläre Ausdrücke (PCRE). Weitere Informationen finden Sie unterRegex-Unterstützungspäter in diesem Abschnitt.

Sie können auch Zeichenfolgen wie Wörter und Phrasen sowie eine Näherungsregel angeben, um die Ergebnisse zu verfeinern.

Stichwörter

Dies sind spezifische Zeichenfolgen, die sich in der Nähe von Text befinden müssen, der dem Regex-Muster entspricht. Die Anforderungen an die Nähe variieren je nach Speicherformat oder Dateityp eines S3-Objekts:

- Bei strukturierten, spaltenförmigen Daten fügt Macie ein Ergebnis ein, wenn der Text dem Regex-Muster entspricht und ein Schlüsselwort im Namen des Felds oder der Spalte enthalten ist, in der der Text gespeichert ist, oder wenn dem Text ein Schlüsselwort vorangestellt ist

und innerhalb des maximalen Übereinstimmungsabstands eines Schlüsselworts in demselben Feld oder Zellenwert liegt. Dies gilt für Microsoft Excel-Arbeitsmappen, CSV-Dateien und TSV-Dateien.

- Bei strukturierten, datensatzbasierten Daten fügt Macie ein Ergebnis ein, wenn der Text dem Regex-Muster entspricht und der Text innerhalb der maximalen Übereinstimmungsdistanz eines Schlüsselworts liegt. Das Schlüsselwort kann im Namen eines Elements im Pfad zu dem Feld oder Array enthalten sein, in dem der Text gespeichert ist, oder es kann in dem Feld oder Array, in dem der Text gespeichert ist, vor demselben Wert stehen und Teil desselben Werts sein. Dies gilt für Apache Avro-Objektcontainer, Apache Parquet-Dateien, JSON-Dateien und JSON Lines-Dateien.
- Bei unstrukturierten Daten fügt Macie ein Ergebnis ein, wenn der Text dem Regex-Muster entspricht und dem Text ein Schlüsselwort vorangestellt ist und innerhalb des maximalen Übereinstimmungsabstands liegt. Dies gilt für Dateien im Adobe Portable Document Format, Microsoft Word-Dokumente, E-Mail-Nachrichten und nicht-binäre Textdateien mit Ausnahme von CSV-, JSON-, JSON Lines- und TSV-Dateien. Dazu gehören alle strukturierten Daten, wie z. B. Tabellen, in diesen Dateitypen.

Sie können bis zu 50 Keywords angeben. Jedes Schlüsselwort kann 3—90 UTF-8-Zeichen enthalten. Bei Schlüsselwörtern muss die Groß- und Kleinschreibung nicht beachtet werden.

Maximale Spieldistanz

Dies ist eine zeichenbasierte Näherungsregel für Keywords. Macie verwendet diese Einstellung, um festzustellen, ob ein Schlüsselwort vor Text steht, der dem Regex-Muster entspricht. Die Einstellung definiert die maximale Anzahl von Zeichen, die zwischen dem Ende eines vollständigen Schlüsselworts und dem Ende eines Textes existieren können, das dem Regex-Muster entspricht. Wenn der Text dem Regex-Muster entspricht, nach mindestens einem vollständigen Schlüsselwort steht und innerhalb der angegebenen Entfernung zum Schlüsselwort vorkommt, nimmt Macie ihn in die Ergebnisse auf. Andernfalls schließt Macie es von den Ergebnissen aus.

Sie können einen Abstand von 1—300 Zeichen angeben. Der Standardabstand beträgt 50 Zeichen. Um optimale Ergebnisse zu erzielen, sollte dieser Abstand größer sein als die Mindestanzahl von Textzeichen, die der Regex erkennen soll. Wenn nur ein Teil des Textes innerhalb der maximalen Trefferentfernung eines Keywords liegt, nimmt Macie es nicht in die Ergebnisse auf.

Wörter ignorieren

Dies sind spezifische Zeichenfolgen, die aus den Ergebnissen ausgeschlossen werden sollen. Wenn der Text dem Regex-Muster entspricht, aber ein Ignorierwort enthält, nimmt Macie es nicht in die Ergebnisse auf.

Sie können bis zu 10 Ignorierwörter angeben. Jedes Ignorierwort kann 4—90 UTF-8-Zeichen enthalten. Die zu ignorierenden Wörter unterscheiden zwischen Groß- und Kleinschreibung.

Beispielsweise haben viele Unternehmen eine spezifische Syntax für Mitarbeiter-IDs. Eine solche Syntax könnte lauten: ein Großbuchstabe, der angibt, ob der Mitarbeiter in Vollzeit beschäftigt ist (F) oder Teilzeit (P) Mitarbeiter, gefolgt von einem Bindestrich (-), gefolgt von einer achtstelligen Sequenz, die den Mitarbeiter identifiziert. Beispiele sind:F-12345678, für einen Vollzeitbeschäftigten undP-87654321, für einen Teilzeitbeschäftigten.

Wenn Sie einen benutzerdefinierten Datenbezeichner erstellen, um Mitarbeiter-IDs zu erkennen, die diese Syntax verwenden, können Sie den folgenden Regex verwenden:`[A-Z]-\d{8}`. Um die Analyse zu verfeinern und Fehlalarme zu vermeiden, können Sie den benutzerdefinierten Datenbezeichner auch so konfigurieren, dass er die Schlüsselwörter verwendetMitarbeiterundMitarbeiter-IDund eine maximale Übereinstimmungsdistanz von 20 Zeichen. Bei diesen Kriterien enthalten die Ergebnisse nur dann Text, der dem Regex entspricht, wenn der Text nach dem Schlüsselwort stehtMitarbeiteroderMitarbeiter-IDund der gesamte Text kommt innerhalb von 20 Zeichen von einem dieser Schlüsselwörter entfernt vor.

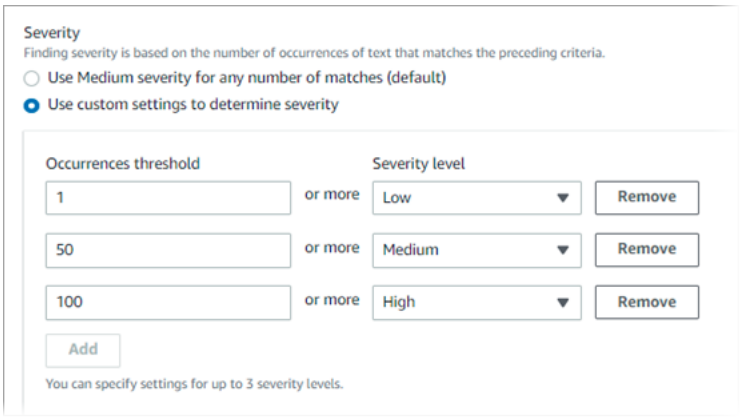
Sehen Sie sich das folgende Video an, wie Keywords Ihnen helfen können, vertrauliche Daten zu finden und Fehlalarme zu vermeiden:Wie Amazon Macie Stichwörter verwendet, um sensible Daten zu entdecken.

Definieren von Einstellungen für den Schweregrad der Suche für benutzerdefinierte Datenkennungen

Wenn Sie eine benutzerdefinierte Daten-ID erstellen, können Sie auch benutzerdefinierte Einstellungen für den Schweregrad für die Ergebnisse sensibler Daten definieren, die der Identifier generiert. Standardmäßig weist Macie dieMittelSchweregrad aller Ergebnisse, die ein benutzerdefinierter Datenbezeichner liefert — wenn ein S3-Objekt mindestens ein Vorkommen von Text enthält, der den Erkennungskriterien einer benutzerdefinierten Daten-ID entspricht, weist Macie automatisch denMittelSchweregrad des resultierenden Befundes.

Mit benutzerdefinierten Schweregradeinstellungen können Sie anhand der Anzahl von Textvorkommen, die den Erkennungskriterien der benutzerdefinierten Daten-ID entsprechen, angeben, welcher Schweregrad zugewiesen werden soll. Um das zu tun, definierst duSchwellenwerte für Vorkommnissefür bis zu drei Schweregrade:Niedrig(am wenigsten schwerwiegend),Mittel, undHoch(am schwersten). EinSchwellenwert für Vorkommenist die Mindestanzahl von Übereinstimmungen, die in einem S3-Objekt vorhanden sein müssen, um ein Ergebnis mit dem angegebenen Schweregrad zu erhalten. Wenn Sie mehr als einen Schwellenwert angeben, müssen die Schwellenwerte in aufsteigender Reihenfolge nach Schweregrad angeordnet sein, und zwar vonNiedrigzuHoch.

Die folgende Abbildung zeigt beispielsweise die Schweregradeinstellungen für eine benutzerdefinierte Daten-ID, die drei Schwellenwerte für Vorkommen angibt, einen für jeden Schweregrad, den Macie unterstützt.



In der folgenden Tabelle wird der Schweregrad der Ergebnisse angegeben, zu denen der benutzerdefinierte Datenbezeichner führt.

Schwellenwert für Vorkommen	Schweregrad	Ergebnis
1	Niedrig	Wenn ein S3-Objekt 1—49 Textvorkommen enthält, die den Erkennungskriterien entsprechen, ist der Schweregrad des resultierenden ErgebnissesNiedrig.
50	Medium	Wenn ein S3-Objekt 50—99 Textvorkommen enthält, die den Erkennungskriterie

Schwellenwert für Vorkommen	Schweregrad	Ergebnis
		n entsprechen, ist der Schweregrad des resultier enden ErgebnissesMittel.
100	Hoch	Wenn ein S3-Objekt 100 oder mehr Textvorkommen enthält, die den Erkennung skriterien entsprechen, ist der Schweregrad des resultier enden ErgebnissesHoch.

Sie können auch die Einstellungen für den Schweregrad verwenden, um festzulegen, ob überhaupt ein Ergebnis erstellt werden soll. Wenn ein S3-Objekt weniger Vorkommen enthält als der niedrigste Schwellenwert für Vorkommen, erstellt Macie keinen Befund.

Erstellen benutzerdefinierter Datenkennungen

Gehen Sie wie folgt vor, um mithilfe der Amazon Macie-Konsole eine benutzerdefinierte Daten-ID zu erstellen. Um programmgesteuert einen benutzerdefinierten Datenbezeichner zu erstellen, verwenden Sie denCreateCustomDataIdentifierBetrieb der Amazon Macie API.

Um einen benutzerdefinierten Datenbezeichner zu erstellen

1. Öffnen Sie die Amazon Macie-Konsole unterhttps://console.aws.amazon.com/macie/.
2. Im Navigationsbereich unterEinstellungen, wähleBenutzerdefinierte Datenkennungen.
3. Wählen Sie Erstellen aus.
4. FürName, geben Sie einen Namen für die benutzerdefinierte Daten-ID ein. Der Name darf maximal 128 Zeichen enthalten.

   Vermeiden Sie es, vertrauliche Daten in den Namen aufzunehmen. Andere Benutzer Ihres Kontos können den Namen möglicherweise sehen, je nachdem, welche Aktionen sie in Macie ausführen dürfen.
5. (Optional) FürBeschreibung, geben Sie eine kurze Beschreibung der benutzerdefinierten Daten-ID ein. Die Beschreibung darf maximal 512 Zeichen enthalten.

Vermeiden Sie es, sensible Daten in die Beschreibung aufzunehmen. Andere Benutzer Ihres Kontos können die Beschreibung möglicherweise sehen, je nachdem, welche Aktionen sie in Macie ausführen dürfen.

6. FürRegulärer Ausdruck, geben Sie den regulären Ausdruck ein (Regex), das das passende Textmuster definiert. Der Regex kann bis zu 512 Zeichen enthalten. Weitere Informationen zu unterstützter Syntax und Einschränkungen finden Sie unterRegex-Unterstützungspäter in diesem Abschnitt.
7. (Optional) FürStichwörter, geben Sie bis zu 50 Zeichenfolgen (durch Kommas getrennt) ein, um einen bestimmten Text zu definieren, der sich in der Nähe von Text befinden muss, der dem Regex-Muster entspricht. Jedes Schlüsselwort kann 3—90 UTF-8-Zeichen enthalten. Bei Schlüsselwörtern muss die Groß- und Kleinschreibung nicht beachtet werden.

   Macie nimmt nur dann ein Vorkommen in die Ergebnisse auf, wenn der Text dem Regex-Muster entspricht und der Text innerhalb der maximalen Übereinstimmungsdistanz eines dieser Schlüsselwörter liegt, wie in dervorheriges Thema.
8. (Optional) FürWörter ignorieren, geben Sie bis zu 10 Zeichenfolgen (durch Kommas getrennt) ein, die einen bestimmten Text definieren, der aus den Ergebnissen ausgeschlossen werden soll. Jedes Ignorierwort kann 4—90 UTF-8-Zeichen enthalten. Die zu ignorierenden Wörter unterscheiden zwischen Groß- und Kleinschreibung.

   Macie schließt ein Ereignis aus den Ergebnissen aus, wenn der Text dem Regex-Muster entspricht, aber eines dieser Ignorierwörter enthält.
9. (Optional) FürMaximale Spieldistanz, geben Sie die maximale Anzahl von Zeichen ein, die zwischen dem Ende eines Schlüsselworts und dem Textende liegen können, das dem Regex-Muster entspricht. Der Abstand kann 1—300 Zeichen betragen. Der Standardabstand beträgt 50 Zeichen.

   Macie nimmt nur dann ein Vorkommen in die Ergebnisse auf, wenn der Text dem Regex-Muster entspricht und der Text innerhalb dieser Entfernung von einem vollständigen Schlüsselwort liegt, wie in dervorheriges Thema.
10. FürSchweregrad, wählen Sie aus, wie Macie den Ergebnissen vertraulicher Daten, die der benutzerdefinierte Datenidentifikator liefert, einen Schweregrad zuweisen soll:

    - Um das automatisch zuzuweisenMittelSchweregrad aller Befunde, wählen SieFür beliebig viele Treffer den Schweregrad „Mittel“ verwenden (Standard). Mit dieser Option weist Macie

automatisch dieMittelSchweregrad eines Befundes, wenn das betroffene S3-Objekt ein oder mehrere Textvorkommen enthält, die den Erkennungskriterien entsprechen.

- Um den Schweregrad auf der Grundlage der von Ihnen angegebenen Schwellenwerte für Ereignisse zuzuweisen, wählen SieVerwenden Sie benutzerdefinierte Einstellungen, um den Schweregrad zu bestimmen. Dann benutze denSchwellenwert für VorkommenundSchweregradOptionen zur Angabe der Mindestanzahl von Übereinstimmungen, die in einem S3-Objekt vorhanden sein müssen, um ein Ergebnis mit einem ausgewählten Schweregrad zu erhalten.

  Zum Beispiel, um die zuzuweisenHochSchweregrad eines Ergebnisses, das 100 oder mehr Textvorkommen meldet, die den Erkennungskriterien entsprechen, geben Sie ein**`100`**in derSchwellenwert für VorkommenKästchen und wählen Sie dannHochvon derSchweregradListe.

  Sie können bis zu drei Schwellenwerte für das Auftreten angeben, einen für jeden Schweregrad, den Macie unterstützt:Niedrig(bei geringstem Schweregrad),Mittel, oderHoch(für die schwersten). Wenn Sie mehr als einen angeben, müssen die Schwellenwerte in aufsteigender Reihenfolge nach Schweregrad angeordnet sein, und zwar ausgehend vonNiedrigzuHoch. Wenn ein S3-Objekt weniger Vorkommen als der niedrigste angegebene Schwellenwert enthält, erstellt Macie keinen Befund.

11. (Optional) FürSchlagworte, wähleTag hinzufügen, und geben Sie dann bis zu 50 Tags ein, um sie der benutzerdefinierten Daten-ID zuzuweisen.

    EINTagist ein Label, das Sie definieren und bestimmten Typen zuweisenAWSRessourcen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Mithilfe von Tags können Sie Ressourcen auf unterschiedliche Weise identifizieren, kategorisieren und verwalten, z. B. nach Zweck, Eigentümer, Umgebung oder anderen Kriterien. Weitere Informationen hierzu finden Sie unter Kennzeichnen von Amazon Macie-Ressourcen.

12. (Optional) FürEvaluieren, geben Sie bis zu 1.000 Zeichen in dasBeispieldatenKästchen, und wählen Sie dannTestenum die Erkennungskriterien zu testen. Macie wertet die Beispieldaten aus und gibt an, wie oft Text vorkommt, der den Kriterien entspricht. Sie können diesen Schritt beliebig oft wiederholen, um die Kriterien zu verfeinern und zu optimieren.

    > **Note**
    >
    > Es wird dringend empfohlen, die Erkennungskriterien zu testen und zu verfeinern, bevor Sie die benutzerdefinierte Daten-ID speichern. Da benutzerdefinierte Datenkennungen

von Aufträgen zur Erkennung vertraulicher Daten verwendet werden, können Sie eine benutzerdefinierte Daten-ID nicht bearbeiten, nachdem Sie sie gespeichert haben. Auf diese Weise können Sie sicherstellen, dass Sie über eine unveränderliche Historie vertraulicher Datenfunde und Ermittlungsergebnisse für Datenschutz- und Datenschutzaudits oder Untersuchungen verfügen, die Sie durchführen.

13. Wenn Sie fertig sind, klicken Sie auf Submit (Absenden).

Macie testet die Einstellungen und überprüft, ob sie den Regex kompilieren kann. Wenn es ein Problem mit einer der Einstellungen oder dem Regex gibt, tritt ein Fehler auf, der auf die Art des Problems hinweist. Nachdem Sie alle Probleme behoben haben, können Sie die benutzerdefinierte Daten-ID speichern.

Regex-Unterstützung in benutzerdefinierten Datenkennungen

Macie unterstützt eine Teilmenge der Regex-Mustersyntax, die von derPerl-Bibliothek für kompatible reguläre Ausdrücke (PCRE). Von den von der PCRE-Bibliothek bereitgestellten Konstrukten unterstützt Macie die folgenden Musterelemente nicht:

- Rückverweise
- Gruppen erfassen
- Bedingungsmuster
- Eingebetteter Code
- Globale Musterflaggen, wie`/i`,`/m`, und`/x`
- Rekursive Muster
- Positive und negative Behauptungen mit Rückblick und Ausblick auf die Zukunft mit Nullbreite, wie`?=`,`?!`,`?<=`, und`?<!`

Beachten Sie außerdem die folgenden Tipps und Empfehlungen, um effektive Regex-Muster für benutzerdefinierte Datenkennungen zu erstellen:

- Anker— Verwenden Sie Anker (^oder$) nur, wenn Sie erwarten, dass das Muster am Anfang oder Ende einer Datei erscheint, nicht am Anfang oder Ende einer Zeile.
- Begrenzte Wiederholungen— Aus Leistungsgründen begrenzt Macie die Größe begrenzter Wiederholungsgruppen. Zum Beispiel`\d{100,1000}`wird in Macie nicht kompiliert. Um diese

Funktionalität annähernd zu erreichen, können Sie eine Wiederholung mit offenem Ende verwenden, z. B.`\d{100,}`.

- Groß- und Kleinschreibung nicht beachten— Um Teile eines Musters nicht zwischen Groß- und Kleinschreibung zu unterscheiden, können Sie den`(?i)`konstruieren statt des`/i`Flagge.
- Leistung— Präfixe oder Alternativen müssen nicht manuell optimiert werden. Zum Beispiel ändern`/hello|hi|hey/`zu`/h(?:ello|i|ey)/`wird die Leistung nicht verbessern.
- Platzhalter— Aus Leistungsgründen begrenzt Macie die Anzahl der wiederholten Platzhalter. Zum Beispiel`a*b*a*`wird in Macie nicht kompiliert.

Zum Schutz vor falsch formatierten oder lang andauernden Ausdrücken testet Macie automatisch Regex-Muster anhand einer Sammlung von Beispieltexten.

Definition von Ausnahmen für sensible Daten mit Amazon Macie Allow Lists

Mit Zulassungslisten in Amazon Macie können Sie bestimmten Text und Textmustern definieren, die Macie bei der Überprüfung von Amazon Simple Storage Service (Amazon S3) auf sensible Daten auf sensible Daten auf sensible Daten auf sensible Daten auf sensible Daten auf sensible Daten auf sensible Daten auf sensible Daten auf sensible Daten auf sensible Daten auf sensible Daten auf sensible Daten auf sensible Daten auf sensible Daten auf sensible Daten auf sensible Daten Dies sind in der Regel Ausnahmen für sensible Daten für Ihre speziellen Szenarien oder Umgebungen. Wenn Daten mit Text oder Textmustern in einer Zulassungsliste übereinstimmen, meldet Macie die Daten nicht Suchergebnissen, selbst wenn die Daten den Kriterien einer verwalteten Datenkennung entsprechen. Mithilfe von Zulassungslisten können Sie Ihre Analyse von Amazon S3 S3-Daten verfeinern und das Rauschen reduzieren.

Sie können zwei Arten von Zulassungslisten erstellen und verwenden:

- Vordefinierter Text — Für diesen Listentyp geben Sie bestimmte Zeichenfolgen an, die ignoriert werden sollen, z. B. die Namen von Vertretern des öffentlichen Rechts Ihrer Organisation, bestimmte Telefonnummern oder bestimmte Beispieldaten, die Ihre Organisation für Tests verwendet. Wenn Sie diesen Listentyp verwenden, ignoriert Macie den Text, der genau mit einem Eintrag in der Liste übereinstimmen.

Dieser Zulassungslistentyp ist hilfreich, wenn Sie Wörter, Ausdrücke und andere Arten von Zeichenfolgen angeben möchten, die nicht sensibel sind, sich wahrscheinlich nicht ändern und nicht zwingend einem gemeinsamen Muster entsprechen.

- Regulärer Ausdruck — Für diesen Listentyp geben Sie einen regulären Ausdruck (Regex) an, der ein Textmuster definiert, das ignoriert werden soll, z. B. öffentliche Telefonnummern für Ihre Organisation, E-Mail-Adressen für die Domain Ihrer Organisation oder gemusterte Beispieldaten, die Ihre Organisation zum Testen verwendet. Wenn Sie diesen Listentyp verwenden, ignoriert Macie Text, der in der Liste genau mit dem Muster in der Liste übereinstimmen.

  Dieser Zulassungslistentyp ist hilfreich, wenn Sie Text angeben möchten, der nicht sensibel ist, aber variiert werden soll.

Nachdem Sie eine Zulassungsliste erstellt haben, können Sie Aufträge zur Erkennung vertraulicher Daten erstellen und konfigurieren, um sie zu verwenden, oder sie zu Ihren Einstellungen für die automatische Erkennung vertraulicher Daten hinzufügen. Macie verwendet die Liste dann, wenn sie Daten analysiert. Wenn Macie Text findet, der einem Eintrag oder Muster in einer Zulassungsliste entspricht, meldet Macie das Vorkommen von Text in vertraulichen Datenergebnissen, Statistiken und anderen Arten von Ergebnissen nicht.

Sie können Zulassungslisten in allen AWS-Regionen erstellen und verwenden, in denen Macie derzeit verfügbar ist, mit Ausnahme der Region Asien-Pazifik (Osaka).

Themen

- Optionen und Anforderungen für Zulassungslisten in Amazon Macie
- Erlaubte Listen in Amazon Macie erstellen und verwalten

Optionen und Anforderungen für Zulassungslisten in Amazon Macie

In Amazon Macie können Sie Zulassungslisten verwenden, um Text oder Textmuster anzugeben, die Macie ignorieren soll, wenn es Amazon Simple Storage Service (Amazon S3)-Objekte auf sensible Daten prüft. Macie bietet Optionen für zwei Arten von Zulassungslisten, vordefinierten Text und reguläre Ausdrücke.

Eine Liste vordefinierter Texte ist hilfreich, wenn Macie bestimmte Wörter, Wortgruppen und andere Arten von Zeichenfolgen ignorieren soll, die Sie nicht als empfindlich betrachten. Beispiele hierfür sind die Namen öffentlicher Stellvertreter für Ihre Organisation, bestimmte Telefonnummern oder

bestimmte Beispieldaten, die Ihre Organisation zum Testen verwendet. Wenn Macie Text findet, der den Kriterien einer verwalteten Datenkennung oder einer benutzerdefinierten Datenkennung entspricht, und der Text auch einem Eintrag in einer Zulassungsliste entspricht, meldet Macie dieses Auftreten von Text in Ergebnissen, Statistiken und anderen Ergebnistypen für sensible Daten nicht.

Ein regulärer Ausdruck (Regex) ist hilfreich, wenn Macie Text ignorieren soll, der variiert oder sich wahrscheinlich ändern wird, während er gleichzeitig ein gemeinsames Muster einhält. Die Regex gibt ein zu ignorierendes Textmuster an. Beispiele hierfür sind öffentliche Telefonnummern für Ihre Organisation, E-Mail-Adressen für die Domain Ihrer Organisation oder musterhafte Beispieldaten, die Ihre Organisation zum Testen verwendet. Wenn Macie Text findet, der den Kriterien einer verwalteten Datenkennung oder einer benutzerdefinierten Datenkennung entspricht, und der Text auch einem Regex-Muster in einer Zulassungsliste entspricht, meldet Macie dieses Auftreten von Text in Ergebnissen, Statistiken und anderen Ergebnistypen nicht.

Sie können beide Arten von Zulassungslisten in allen erstellen und verwenden, in AWS-Regionen denen Macie derzeit verfügbar ist, mit Ausnahme der Region Asien-Pazifik (Osaka). Beachten Sie beim Erstellen und Verwalten von Zulassungslisten die folgenden Optionen und Anforderungen. Beachten Sie auch, dass Zulassungslisteneinträge und Regex-Muster für Mailing-Adressen nicht unterstützt werden.

Themen

- Optionen und Anforderungen für Listen vordefinierter Texte
  - Syntaxanforderungen
  - Speicheranforderungen
  - Anforderungen an die Verschlüsselung/Entschlüsselung
  - Überlegungen und Empfehlungen zum Design
- Optionen und Anforderungen für reguläre Ausdrücke in Zulassungslisten
  - Syntaxunterstützung und Empfehlungen
  - Beispiele

Optionen und Anforderungen für Listen vordefinierter Texte

Für diese Art von Zulassungsliste stellen Sie eine durch Zeilen getrennte Klartextdatei bereit, die bestimmte Zeichenfolgen auflistet, die ignoriert werden sollen. Bei den Listeneinträgen handelt es sich in der Regel um Wörter, Wortgruppen und andere Arten von Zeichenfolgen, die Sie nicht als empfindlich betrachten, sich wahrscheinlich nicht ändern werden und nicht unbedingt einem

bestimmten Muster entsprechen. Wenn Sie diese Art von Liste verwenden, meldet Amazon Macie keine Textvorkommen, die genau mit einem Eintrag in der Liste übereinstimmen. Macie behandelt jeden Listeneintrag als Zeichenfolgeliteralwert.

Um diese Art von Zulassungsliste zu verwenden, erstellen Sie zunächst die Liste in einem Texteditor und speichern Sie sie als Klartextdatei. Laden Sie dann die Liste in einen S3-Bucket hoch und stellen Sie sicher, dass die Speicher- und Verschlüsselungseinstellungen für den Bucket und das Objekt es Macie ermöglichen, die Liste abzurufen und zu entschlüsseln. Erstellen und konfigurieren Sie dann Einstellungen für die Liste in Macie.

Nachdem Sie die Einstellungen in Macie konfiguriert haben, empfehlen wir Ihnen, die Zulassungsliste mit einem kleinen, repräsentativen Datensatz für Ihr Konto oder Ihre Organisation zu testen. Um eine Liste zu testen, können Sie einen einmaligen Auftrag erstellen und den Auftrag so konfigurieren, dass er die Liste zusätzlich zu den verwalteten Datenkennungen und benutzerdefinierten Datenkennungen verwendet, die Sie normalerweise zum Analysieren von Daten verwenden. Anschließend können Sie die Ergebnisse des Auftrags überprüfen – Ergebnisse zu sensiblen Daten, Ergebnisse zur Erkennung sensibler Daten oder beides. Wenn sich die Ergebnisse des Auftrags von Ihren Erwartungen unterscheiden, können Sie die Liste ändern und testen, bis die Ergebnisse Ihren Erwartungen entsprechen.

Nachdem Sie mit der Konfiguration und dem Testen einer Zulassungsliste fertig sind, können Sie zusätzliche Aufträge erstellen und konfigurieren, um sie zu verwenden, oder sie zu den automatisierten Einstellungen für die Erkennung sensibler Daten für Ihr Konto hinzufügen. Wenn diese Aufträge ausgeführt werden oder der nächste automatisierte Erkennungsanalysezyklus beginnt, ruft Macie die neueste Version der Liste von Amazon S3 ab und speichert sie im temporären Speicher. Macie verwendet dann diese temporäre Kopie der Liste, wenn es S3-Objekte auf sensible Daten prüft. Wenn ein Auftrag abgeschlossen ist oder der Analysezyklus abgeschlossen ist, löscht Macie seine Kopie der Liste dauerhaft aus dem Speicher. Die Liste bleibt in Macie nicht bestehen. Nur die Einstellungen der Liste bleiben in Macie bestehen.

> **Important**
>
> Da vordefinierte Textlisten in Macie nicht bestehen bleiben, ist es wichtig, den Status Ihrer Zulassungslisten regelmäßig zu überprüfen. Wenn Macie eine Liste, die Sie für einen Auftrag oder eine automatische Erkennung konfiguriert haben, nicht abrufen oder analysieren kann, verwendet Macie die Liste nicht. Dies kann zu unerwarteten Ergebnissen führen, z. B. zu Ergebnissen sensibler Daten für Text, den Sie in der Liste angegeben haben.

Themen

- Syntaxanforderungen
- Speicheranforderungen
- Anforderungen an die Verschlüsselung/Entschlüsselung
- Überlegungen und Empfehlungen zum Design

Syntaxanforderungen

Wenn Sie diese Art von Zulassungsliste erstellen, beachten Sie die folgenden Anforderungen für die -Datei der Liste:

- Die Liste muss als Klartextdatei (`text/plain`) gespeichert werden, z. B. als .txt-, .text- oder .plain-Datei.
- Die Liste muss Zeilenumbrüche verwenden, um einzelne Einträge zu trennen. Beispielsweise:

  ```
  Akua Mansa
  John Doe
  Martha Rivera
  425-555-0100
  425-555-0101
  425-555-0102
  ```

  Macie behandelt jede Zeile als einen einzelnen, eindeutigen Eintrag in der Liste. Die Datei kann auch leere Zeilen enthalten, um die Lesbarkeit zu verbessern. Macie überspringt leere Zeilen beim Parsen der Datei.
- Jeder Eintrag kann 1–90 UTF–8 Zeichen enthalten.
- Jeder Eintrag muss eine vollständige, exakte Übereinstimmung sein, damit der Text ignoriert werden kann. Macie unterstützt nicht die Verwendung von Platzhalterzeichen oder Teilwerten für Einträge. Macie behandelt jeden Eintrag als Zeichenfolgeliteralwert. Bei Übereinstimmungen wird die Groß- und Kleinschreibung ignoriert.
- Die Datei kann 1–100.000 Einträge enthalten.
- Die Gesamtspeichergröße der Datei darf 35 MB nicht überschreiten.

Speicheranforderungen

Beachten Sie beim Hinzufügen und Verwalten von Zulassungslisten in Amazon S3 die folgenden Speicheranforderungen und Empfehlungen:

- Regionale Unterstützung – Eine Zulassungsliste muss in einem S3-Bucket gespeichert werden, der sich in derselben AWS-Region wie Ihr Macie-Konto befindet. Macie kann nicht auf eine Zulassungsliste zugreifen, wenn sie in einer anderen Region gespeichert ist.
- Bucket-Eigentümerschaft – Eine Zulassungsliste muss in einem S3-Bucket gespeichert werden, der Ihrem gehörtAWS-Konto. Wenn Sie möchten, dass andere Konten dieselbe Zulassungsliste verwenden, sollten Sie erwägen, eine Amazon S3-Replikationsregel zu erstellen, um die Liste in Buckets zu replizieren, die diesen Konten gehören. Informationen zum Replizieren von S3-Objekten finden Sie unter Replizieren von Objekten im Benutzerhandbuch für Amazon Simple Storage Service.

  Darüber hinaus muss Ihre AWS Identity and Access Management (IAM)-Identität über Lesezugriff auf den S3-Bucket und das Objekt verfügen, in dem die Liste gespeichert ist. Andernfalls können Sie die Einstellungen der Liste nicht erstellen oder aktualisieren oder den Status der Liste mithilfe von Macie überprüfen.
- Bucket-Richtlinien – Wenn Sie eine Zulassungsliste in einem S3-Bucket speichern, der über eine restriktive Bucket-Richtlinie verfügt, stellen Sie sicher, dass die Richtlinie es Macie ermöglicht, die Liste abzurufen. Dazu können Sie der Bucket-Richtlinie eine Bedingung für die serviceverknüpfte Macie-Rolle hinzufügen. Weitere Informationen finden Sie unter Macie den Zugriff von S3-Buckets und -Objekten erlauben.

  Stellen Sie außerdem sicher, dass die Richtlinie Ihrer IAM-Identität Lesezugriff auf den Bucket gewährt. Andernfalls können Sie die Einstellungen der Liste nicht erstellen oder aktualisieren oder den Status der Liste mithilfe von Macie überprüfen.
- Objektpfade – Wenn Sie mehr als eine Zulassungsliste in Amazon S3 speichern, muss der Objektpfad für jede Liste eindeutig sein. Mit anderen Worten, jede Zulassungsliste muss separat als eigenes S3-Objekt gespeichert werden.
- Speicherklassen – Eine Zulassungsliste muss direkt in Amazon S3 mit einer der folgenden Speicherklassen gespeichert werden: Reduced Redundancy (RRS), S3 Glacier Instant Retrieval, S3 Intelligent-Tiering, S3 One Zone-IA, S3 Standard oder S3 Standard-IA.
- Versioning – Wenn Sie einem S3-Bucket eine Zulassungsliste hinzufügen, empfehlen wir Ihnen, auch das Versioning für den Bucket zu aktivieren. Anschließend können Sie Datums- und Zeitwerte verwenden, um Versionen der Liste mit den Ergebnissen von Erkennungsaufträgen für sensible

Daten und automatisierten Erkennungszyklen für sensible Daten zu korrelieren, die die Liste verwenden. Dies kann bei Datenschutz- und Schutzprüfungen oder Untersuchungen helfen, die Sie durchführen.

- Objektsperre – Um zu verhindern, dass eine Zulassungsliste für einen bestimmten Zeitraum oder auf unbestimmte Zeit gelöscht oder überschrieben wird, können Sie die Objektsperre für den S3-Bucket aktivieren, in dem die Liste gespeichert ist. Durch Aktivieren dieser Einstellung wird Macie nicht daran gehindert, auf die Liste zuzugreifen. Informationen zu dieser Einstellung finden Sie unter Verwenden der S3-Objektsperre im Benutzerhandbuch für Amazon Simple Storage Service.

Anforderungen an die Verschlüsselung/Entschlüsselung

Wenn Sie eine Zulassungsliste in Amazon S3 verschlüsseln, gewährt die Berechtigungsrichtlinie für die serviceverknüpfte Macie-Rolle Macie in der Regel die Berechtigungen, die es zum Entschlüsseln der Liste benötigt. Dies hängt jedoch von der Art der verwendeten Verschlüsselung ab:

- Wenn eine Liste mit serverseitiger Verschlüsselung mit einem von Amazon S3 verwalteten Schlüssel (SSE-S3) verschlüsselt wird, kann Macie die Liste entschlüsseln. Die serviceverknüpfte Rolle für Ihr Macie-Konto gewährt Macie die erforderlichen Berechtigungen.
- Wenn eine Liste mit serverseitiger Verschlüsselung mit einem -AWSverwalteten AWS KMS key (DSSE-KMS oder SSE-KMS) verschlüsselt wird, kann Macie die Liste entschlüsseln. Die serviceverknüpfte Rolle für Ihr Macie-Konto gewährt Macie die erforderlichen Berechtigungen.
- Wenn eine Liste mit serverseitiger Verschlüsselung mit einem vom Kunden verwalteten AWS KMS key (DSSE-KMS oder SSE-KMS) verschlüsselt wird, kann Macie die Liste nur entschlüsseln, wenn Sie Macie erlauben, den Schlüssel zu verwenden. Weitere Informationen zur Vorgehensweise finden Sie unter Macie erlauben, einen vom Kunden verwalteten zu verwenden AWS KMS key.

> **Note**
>
> Sie können eine Liste mit einem Kunden verschlüsseln, der AWS KMS key in einem externen Schlüsselspeicher verwaltet wird. Der Schlüssel kann dann jedoch langsamer und weniger zuverlässig sein als ein Schlüssel, der vollständig innerhalb von verwaltet wirdAWS KMS. Wenn Macie durch Latenz- oder Verfügbarkeitsprobleme daran gehindert wird, die Liste zu entschlüsseln, verwendet Macie die Liste nicht, wenn es S3-Objekte analysiert. Dies kann zu unerwarteten Ergebnissen führen, z. B. zu Ergebnissen sensibler Daten für Text, den Sie in der Liste angegeben haben. Um dieses Risiko zu verringern, sollten Sie die Liste in einem S3-Bucket speichern, der für die Verwendung des Schlüssels als S3-Bucket-Schlüssel konfiguriert ist.

Informationen zur Verwendung von KMS-Schlüsseln in externen Schlüsselspeichern finden Sie unter Externe Schlüsselspeicher im AWS Key Management Service Entwicklerhandbuch für . Informationen zur Verwendung von S3-Bucket-Schlüsseln finden Sie unter Reduzieren der Kosten für SSE-KMS mit Amazon S3-Bucket-Schlüsseln im Benutzerhandbuch für Amazon Simple Storage Service.

- Wenn eine Liste mit serverseitiger Verschlüsselung mit einem vom Kunden bereitgestellten Schlüssel (SSE-C) oder clientseitiger Verschlüsselung verschlüsselt wird, kann Macie die Liste nicht entschlüsseln. Ziehen Sie stattdessen die Verwendung von SSE-S3-, DSSE-KMS- oder SSE-KMS-Verschlüsselung in Betracht.

Wenn eine Liste mit einem von AWS verwalteten KMS-Schlüssel oder einem vom Kunden verwalteten KMS-Schlüssel verschlüsselt ist, muss Ihre AWS Identity and Access Management (IAM)-Identität auch den Schlüssel verwenden dürfen. Andernfalls können Sie die Einstellungen der Liste nicht erstellen oder aktualisieren oder den Status der Liste mithilfe von Macie überprüfen. Informationen zum Überprüfen oder Ändern der Berechtigungen für einen KMS-Schlüssel finden Sie unter Schlüsselrichtlinien in AWS KMS im AWS Key Management Service -Entwicklerhandbuch.

Ausführliche Informationen zu Verschlüsselungsoptionen für Amazon S3-Daten finden Sie unter Schützen von Daten durch Verschlüsselung im Benutzerhandbuch für Amazon Simple Storage Service.

Überlegungen und Empfehlungen zum Design

Im Allgemeinen behandelt Macie jeden Eintrag in einer Zulassungsliste als Zeichenfolgeliteralwert. Das heißt, Macie ignoriert jedes Vorkommen von Text, der genau mit einem vollständigen Eintrag in einer Zulassungsliste übereinstimmt. Bei Übereinstimmungen wird die Groß- und Kleinschreibung ignoriert.

Macie verwendet die Einträge jedoch als Teil eines größeren Datenextraktions- und Analyse-Frameworks. Das Framework umfasst Funktionen für Machine Learning und Musterabgleich, die Dimensionen wie grammatische und syntaktische Variationen und in vielen Fällen die Nähe von Schlüsselwörtern berücksichtigen. Das Framework berücksichtigt auch den Dateityp oder das Speicherformat eines S3-Objekts. Berücksichtigen Sie daher die folgenden Überlegungen und Empfehlungen, wenn Sie die Einträge in einer Zulassungsliste hinzufügen und verwalten.

Bereiten Sie sich auf verschiedene Dateitypen und Speicherformate vor

Für unstrukturierte Daten, wie Text in einer Adobe portable Document Format (.pdf)-Datei, ignoriert Macie Text, der genau mit einem vollständigen Eintrag in einer Zulassungsliste übereinstimmt, einschließlich Text, der sich über mehrere Zeilen oder Seiten erstreckt.

Bei strukturierten Daten, wie z. B. spaltenbasierten Daten in einer CSV-Datei oder datensatzbasierten Daten in einer JSON-Datei, ignoriert Macie Text, der genau mit einem vollständigen Eintrag in einer Zulassungsliste übereinstimmt, wenn der gesamte Text in einem einzigen Feld, einer Zelle oder einem Array gespeichert ist. Diese Anforderung gilt nicht für strukturierte Daten, die in einer ansonsten unstrukturierten Datei gespeichert sind, z. B. einer Tabelle in einer PDF-Datei.

Betrachten Sie beispielsweise den folgenden Inhalt in einer CSV-Datei:

```
Name,Account ID
Akua Mansa,111111111111
John Doe,222222222222
```

Wenn `Akua Mansa` und Einträge in einer Zulassungsliste `John Doe` sind, ignoriert Macie diese Namen in der CSV-Datei. Der vollständige Text jedes Listeneintrags wird in einem einzigen `Name` Feld gespeichert.

Umgekehrt sollten Sie eine CSV-Datei in Betracht ziehen, die die folgenden Spalten und Felder enthält:

```
First Name,Last Name,Account ID
Akua,Mansa,111111111111
John,Doe,222222222222
```

Wenn `Akua Mansa` und Einträge in einer Zulassungsliste `John Doe` sind, ignoriert Macie diese Namen in der CSV-Datei nicht. Keines der Felder in der CSV-Datei enthält den vollständigen Text eines Eintrags in der Zulassungsliste.

Einschließen gängiger Varianten

Fügen Sie Einträge für gängige Variationen numerischer Daten, richtige Substantive, Begriffe und alphanumerische Zeichenfolgen hinzu. Wenn Sie beispielsweise Namen oder Wortgruppen hinzufügen, die nur ein Leerzeichen zwischen Wörtern enthalten, fügen Sie auch Varianten hinzu, die zwei Leerzeichen zwischen Wörtern enthalten. Fügen Sie auf ähnliche Weise Wörter und

Wortgruppen hinzu, die Sonderzeichen enthalten und keine enthalten, und erwägen Sie, gängige syntaktische und semantische Variationen einzubeziehen.

Für die US-Telefonnummer 425-555-0100 können Sie beispielsweise diese Einträge zu einer Zulassungsliste hinzufügen:

```
425-555-0100
425.555.0100
(425) 555-0100
+1-425-555-0100
```

Für das Datum 1. Februar 2022 im Kontext können Sie Einträge hinzufügen, die gängige syntaktische Varianten für Englisch und Französisch enthalten, einschließlich Varianten, die Sonderzeichen enthalten und keine Sonderzeichen enthalten:

```
February 1, 2022
1 février 2022
1 fevrier 2022
Feb 01, 2022
1 fév 2022
1 fev 2022
02/01/2022
01/02/2022
```

Fügen Sie für Personennamen Einträge für verschiedene Formen eines Namens hinzu, die Sie nicht als sensibel betrachten. Nehmen Sie beispielsweise Folgendes auf: den Vornamen gefolgt von Nachnamen, den Nachnamen gefolgt von Vornamen, den Vor- und Nachnamen getrennt durch ein Leerzeichen, den Vor- und Nachnamen getrennt durch zwei Leerzeichen und Spitznamen.

Für den Namen Martha Bola können Sie beispielsweise Folgendes hinzufügen:

```
Martha Rivera
Martha  Rivera
Rivera, Martha
Rivera,  Martha
Rivera Martha
Rivera  Martha
```

Wenn Sie Varianten eines bestimmten Namens ignorieren möchten, der viele Teile enthält, erstellen Sie stattdessen eine Zulassungsliste, die einen regulären Ausdruck verwendet.

Beispielsweise können Sie für den Namen Dr. Martha Bolda Bola, PhD, den folgenden regulären Ausdruck verwenden: `^(Dr. )?Martha\s(Lyda|L\.)?\s?Rivera,?( PhD)?$`.

Optionen und Anforderungen für reguläre Ausdrücke in Zulassungslisten

Für diese Art von Zulassungsliste geben Sie einen regulären Ausdruck (Regex) an, der ein zu ignorierendes Textmuster definiert, z. B. öffentliche Telefonnummern für Ihre Organisation, E-Mail-Adressen für die Domain Ihrer Organisation oder musterhafte Beispieldaten, die Ihre Organisation zum Testen verwendet. Der Regex definiert ein gemeinsames Muster für eine bestimmte Art von Daten, die Sie nicht als empfindlich betrachten. Wenn Sie diese Art von Zulassungsliste verwenden, meldet Amazon Macie keine Textvorkommen, die vollständig mit dem angegebenen Muster übereinstimmen. Im Gegensatz zu einer Zulassungsliste, die vordefinierten zu ignorierenden Text angibt, erstellen und speichern Sie den Regex und alle anderen Listeneinstellungen in Macie.

Wenn Sie diese Art von Zulassungsliste erstellen oder aktualisieren, können Sie den Regex der Liste mit Beispieldaten testen, bevor Sie die Liste speichern. Wir empfehlen Ihnen, dies mit mehreren Sätzen von Beispieldaten zu tun. Wenn Sie eine zu allgemeine Regex erstellen, ignoriert Macie möglicherweise Textereignisse, die Sie als empfindlich betrachten. Wenn ein Regex zu spezifisch ist, ignoriert Macie möglicherweise keine Textvorkommen, die Sie nicht als empfindlich betrachten. Um sich vor fehlerhaften oder lang andauernden Ausdrücken zu schützen, kompiliert und testet Macie den Regex automatisch anhand einer Sammlung von Beispieltext und benachrichtigt Sie über zu behebende Probleme.

Für weitere Tests empfehlen wir Ihnen, auch die Regex der Liste mit einem kleinen, repräsentativen Datensatz für Ihr Konto oder Ihre Organisation zu testen. Dazu können Sie einen einmaligen Auftrag erstellen und den Auftrag so konfigurieren, dass er zusätzlich zu den verwalteten Datenkennungen und benutzerdefinierten Datenkennungen, die Sie normalerweise zur Analyse von Daten verwenden, die Liste verwendet. Anschließend können Sie die Ergebnisse des Auftrags überprüfen – Ergebnisse zu sensiblen Daten, Ergebnisse zur Erkennung sensibler Daten oder beides. Wenn sich die Ergebnisse des Auftrags von Ihren Erwartungen unterscheiden, können Sie die Regex ändern und testen, bis die Ergebnisse Ihren Erwartungen entsprechen.

Nachdem Sie eine Zulassungsliste konfiguriert und getestet haben, können Sie zusätzliche Aufträge erstellen und konfigurieren, um sie zu verwenden, oder sie zu den automatisierten Einstellungen für die Erkennung sensibler Daten für Ihr Konto hinzufügen. Wenn diese Aufträge ausgeführt werden oder Macie eine automatische Erkennung für Ihr Konto durchführt, verwendet Macie die neueste Version der Regex der Liste, um Daten zu analysieren.

Themen

- Syntaxunterstützung und Empfehlungen
- Beispiele

Syntaxunterstützung und Empfehlungen

Eine Zulassungsliste kann einen regulären Ausdruck (Regex) angeben, der bis zu 512 Zeichen enthält. Macie unterstützt eine Teilmenge der Regex-Mustersyntax, die von der Perl Compatible Regular Expressions (PCRE)-Bibliothek bereitgestellt wird. Macie unterstützt von den Konstrukten der PCRE-Bibliothek die folgenden Musterelemente nicht:

- Rückreferenzen
- Erfassen von Gruppen
- Bedingungsmuster
- Eingebetteter Code
- Globale Muster-Flags wie `/i/m`, und `/x`
- Rekursive Muster
- Positive und negative Look-Thind- und Look-Ahead-Null-Breite-Assertionen wie `?=`, `?!?<=`, und `?<!`

Um effektive Regex-Muster für Zulassungslisten zu erstellen, beachten Sie auch die folgenden Tipps und Empfehlungen:

- Anchors – Verwenden Sie Anchors (`^` oder `$`) nur, wenn Sie erwarten, dass das Muster am Anfang oder Ende einer Datei erscheint, nicht am Anfang oder Ende einer Linie.
- Begrenzte Wiederholungen – Aus Leistungsgründen begrenzt Macie die Größe begrenzter Wiederholungsgruppen. Beispielsweise `\d{100,1000}` wird nicht in Macie kompiliert. Um diese Funktionalität anzunähern, können Sie eine offene Wiederholung verwenden, z. B. `\d{100,}`.
- Nichtbeachtung der Groß-/Kleinschreibung – Um Teile eines Musters ohne Berücksichtigung der Groß-/Kleinschreibung zu bereinigen, können Sie das `(?i)`Konstrukt anstelle des `-/i`Flags verwenden.
- Leistung – Präfixe oder Änderungen müssen nicht manuell optimiert werden. Wenn Sie beispielsweise `/hello|hi|hey/` auf ändern, `/h(?:ello|i|ey)/` wird die Leistung nicht verbessert.

- Platzhalter – Aus Leistungsgründen begrenzt Macie die Anzahl der wiederholten Platzhalter. Beispielsweise `a*b*a*` wird nicht in Macie kompiliert.
- Alternation – Um mehr als ein Muster in einer einzigen Zulassungsliste anzugeben, können Sie den Alternationsoperator (`|`) verwenden, um die Muster zu verketten. In diesem Fall verwendet Macie die ODER-Logik, um die Muster zu kombinieren und ein neues Muster zu bilden. Wenn Sie beispielsweise angeben`(apple|orange)`, erkennt Macie sowohl Äpfel als auch Orange als Übereinstimmung und ignoriert Vorkommen beider Wörter. Wenn Sie Muster verketten, achten Sie darauf, die Gesamtlänge des verketteten Ausdrucks auf 512 oder weniger Zeichen zu beschränken.

Wenn Sie den Regex entwickeln, entwerfen Sie ihn schließlich so, dass er verschiedene Dateitypen und Speicherformate berücksichtigt. Macie verwendet den Regex als Teil eines größeren Frameworks für Datenextraktion und -analyse. Das Framework beeinflusst den Dateityp oder das Speicherformat eines S3-Objekts. Bei strukturierten Daten, wie z. B. spaltenbasierten Daten in einer CSV-Datei oder datensatzbasierten Daten in einer JSON-Datei, ignoriert Macie nur dann Text, der vollständig mit dem Muster übereinstimmt, wenn der gesamte Text in einem einzigen Feld, einer Zelle oder einem Array gespeichert ist. Diese Anforderung gilt nicht für strukturierte Daten, die in einer ansonsten unstrukturierten Datei gespeichert sind, z. B. einer Tabelle in einer Adobe portable Document Format (.pdf)-Datei. Für unstrukturierte Daten, wie Text in einer PDF-Datei, ignoriert Macie Text, der vollständig mit dem Muster übereinstimmt, einschließlich Text, der sich über mehrere Zeilen oder Seiten erstreckt.

Beispiele

Die folgenden Beispiele zeigen gültige Regex-Muster für einige gängige Szenarien.

E-Mail-Adressen

Wenn Sie eine benutzerdefinierte Datenkennung verwenden, um E-Mail-Adressen zu erkennen, können Sie E-Mail-Adressen ignorieren, die Sie nicht als sensibel betrachten, z. B. E-Mail-Adressen für Ihre Organisation.

Um E-Mail-Adressen für eine bestimmte Domain der zweiten Ebene und der obersten Ebene zu ignorieren, können Sie dieses Muster verwenden:

```
[a-zA-Z0-9_.+\\-]+@example\.com
```

Wobei *Beispiel* der Name der Domain der zweiten Ebene und *com* die Domain der obersten Ebene ist. In diesem Fall gleicht Macie Adressen wie johndoe@example.com und john.doe@example.com ab und ignoriert sie.

Um E-Mail-Adressen für eine bestimmte Domain in einer generischen Top-Level-Domain (gTLD) wie .com oder .gov zu ignorieren, können Sie dieses Muster verwenden:

```
[a-zA-Z0-9_.+\\-]+@example\.[a-zA-Z]{2,}
```

Wobei *das Beispiel* der Name der Domain ist. In diesem Fall gleicht Macie Adressen wie johndoe@example.com, john.doe@example.gov und johndoe@example.edu ab und ignoriert sie.

Um E-Mail-Adressen für eine bestimmte Domain in einer beliebigen Top-Level-Domain (ccTLD) zu ignorieren, z. B. .ca für Kanada oder .au für Australien, können Sie dieses Muster verwenden:

```
[a-zA-Z0-9_.+\\-]+@example\.(ca|au)
```

Wobei *beispielsweise* der Name der Domain und *ca* und *au* bestimmte ccTLDs sind, die ignoriert werden sollen. In diesem Fall gleicht Macie Adressen wie johndoe@example.ca und john.doe@example.au ab und ignoriert sie.

Um E-Mail-Adressen zu ignorieren, die für eine bestimmte Domäne und gTLD gelten und Domains der dritten und vierten Ebene enthalten, können Sie dieses Muster verwenden:

```
[a-zA-Z0-9_.+\\-]+@([a-zA-Z0-9-]+\.)?[a-zA-Z0-9-]+\.example\.com
```

Wobei *Beispiel* der Name der Domain und *com* die gTLD ist. In diesem Fall gleicht Macie Adressen wie johndoe@www.example.com und john.doe@www.team.example.com ab und ignoriert sie.

Phone numbers (Telefonnummern)

Macie stellt verwaltete Datenkennungen bereit, die Telefonnummern für mehrere Länder und Regionen erkennen können. Um bestimmte Telefonnummern zu ignorieren, z. B. gebührenfreie Nummern oder öffentliche Telefonnummern für Ihre Organisation, können Sie Muster wie die folgenden verwenden.

Um gebührenfreie Telefonnummern zu ignorieren, verwenden US-Telefonnummern die Vorwahl 800 und sind als (800) ###-#### formatiert:

```
^\(?800\)?[ -]?\d{3}[ -]?\d{4}$
```

Um gebührenfreie Telefonnummern zu ignorieren, verwenden US-Telefonnummern die Vorwahl 888 und sind als (888) ###-#### formatiert:

```
^\(?888\)?[ -]?\d{3}[ -]?\d{4}$
```

Um 10-stellige, englische Telefonnummern zu ignorieren, die die 33-Ländervorwahl enthalten und als +33 Bol Bol Bol formatiert sind:

```
^\+33 \d( \d\d){4}$
```

Um US- und japanische Telefonnummern zu ignorieren, die bestimmte Gebiets- und Austauschcodes verwenden, geben Sie keine Landesvorwahl an und sind als (###) ###-#### formatiert:

```
^\(?123\)?[ -]?555[ -]?\d{4}$
```

Wobei *123* die Vorwahl und *555* die Austauschvorwahl ist.

Um US-amerikanische und japanische Telefonnummern zu ignorieren, die bestimmte Vorwahlen und Austauschcodes verwenden, geben Sie eine Landesvorwahl an und sind als +1 (###) ###-#### formatiert:

```
^\+1\(?123\)?[ -]?555[ -]?\d{4}$
```

Wobei *123* die Vorwahl und *555* die Austauschvorwahl ist.

Erlaubte Listen in Amazon Macie erstellen und verwalten

In Amazon Macie wird über eine Zulassungsliste festgelegt, welcher Text oder welche Textmuster Macie ignorieren soll, wenn Amazon Simple Storage Service (Amazon S3) auf sensible Daten geprüft werden. Wenn Text mit Text übereinstimmen, meldet Macie den Text nicht Suchergebnissen, selbst wenn der Text den Kriterien einer verwalteten oder benutzerdefinierten Datenkennung entspricht.

In Macie können Sie die folgenden Arten von Zulassungslisten erstellen und verwalten.

Vordefinierter Text

Verwenden Sie diesen Listentyp, um Wörter, Ausdrücke und andere Arten von Zeichenfolgen anzugeben, die nicht sensibel sind, sich wahrscheinlich nicht ändern und nicht unbedingt

einem gemeinsamen Muster entsprechen. Beispiele hierfür sind die Namen von Vertretern des öffentlichen Rechts Ihrer Organisation, bestimmte Telefonnummern und spezifische Beispieldaten, die Ihre Organisation für Tests verwendet. Wenn Sie diesen Listentyp verwenden, ignoriert Macie Text, der genau mit einem Eintrag in der Liste übereinstimmt.

Für diesen Listentyp erstellen Sie eine zeilengetrennte Klartextdatei, die bestimmten Text auflistet, der ignoriert werden soll. Anschließend speichern Sie die Datei in einem S3-Bucket und konfigurieren, wie Macie auf die Liste im Bucket zugreifen soll. Anschließend können Sie Aufträge zur Erkennung vertraulicher Daten erstellen und konfigurieren, um die Liste zu verwenden, oder die Liste zu den Einstellungen für die automatische Erkennung vertraulicher Daten für Ihr Konto hinzufügen. Wenn jeder Job ausgeführt wird oder der nächste automatische Erkennungsanalysezyklus beginnt, ruft Macie die neueste Version der Liste von Amazon S3 ab. Macie verwendet dann diese Version der Liste, wenn sie S3-Objekte auf vertrauliche Daten untersucht. Wenn Macie Text findet, der genau mit einem Eintrag in der Liste übereinstimmen, meldet Macie das Auftreten von Text nicht Suchergebnissen.

Regulärer Ausdruck

Verwenden Sie diesen Listentyp, um einen regulären Ausdruck (RegEx) anzugeben, der ein zu ignorierendes Textmuster definiert. Beispiele hierfür sind öffentliche Telefonnummern für Ihre Organisation, E-Mail-Adressen für die Domain Ihrer Organisation und gemusterte Beispieldaten, die Ihre Organisation für Tests verwendet. Wenn Sie diesen Listentyp verwenden, ignoriert Macie Text, der genau mit dem in der Liste definierten Regex-Muster übereinstimmen.

Für diesen Listentyp erstellen Sie einen RegEx, das ein gemeinsames Muster für Text definiert, das nicht sensibel ist, aber variiert oder sich wahrscheinlich ändern wird. Anders als bei einer Liste mit vordefiniertem Text erstellen und speichern Sie den Regex und alle anderen Listeneinstellungen in Macie. Anschließend können Sie Aufträge zur Erkennung vertraulicher Daten erstellen und konfigurieren, um die Liste zu verwenden, oder die Liste zu den Einstellungen für die automatische Erkennung vertraulicher Daten für Ihr Konto hinzufügen. Wenn diese Jobs ausgeführt werden oder Macie eine automatische Erkennung für Ihr Konto durchführt, verwendet Macie die neueste Version des Regex der Liste, um Daten zu analysieren. Wenn Macie Text findet, der genau mit dem Muster in der Liste übereinstimmen, meldet Macie das Auftreten von Text nicht Suchergebnissen.

Detaillierte Anforderungen, Empfehlungen und Beispiele für die einzelnen Listentypen finden Sie unterOptionen und Anforderungen für Zulassungslisten. In jeder unterstützten Liste können Sie bis zu 10 Zulassungslisten für Ihr Konto erstellenAWS-Region, bis zu fünf Zulassungslisten, die

vordefinierten Text angeben, und bis zu fünf Zulassungslisten, die reguläre Ausdrücke angeben. Sie können Zulassungslisten in allen AWS-Regionen erstellen und verwenden, in denen Macie derzeit verfügbar ist, mit Ausnahme der Region Asien-Pazifik (Osaka).

Um Zulassungslisten zu erstellen und zu verwalten, können Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden. Die folgenden Themen geben Aufschluss, wie. Für die API enthalten die Themen Beispiele dafür, wie diese Aufgaben mithilfe von AWS Command Line Interface(AWS CLI) ausgeführt werden können. Sie können diese Aufgaben auch ausführen, indem Sie eine aktuelle Version eines anderen AWS Befehlszeilentools oder eines AWS SDK verwenden oder HTTPS-Anfragen direkt an Macie senden. Informationen zu AWS Tools und SDKs finden Sie unter Tools, auf AWS denen Sie aufbauen können.

Themen

- Erlaubnislisten erstellen
- Überprüfen des Status der Zulassungslisten
- Zulassungslisten ändern
- Zulässige Listen löschen

Erlaubnislisten erstellen

Wie Sie in Amazon Macie eine Zulassungsliste erstellen, hängt von der Art der Liste ab, die Sie erstellen möchten. Eine Zulassungsliste kann eine Datei sein, die vordefinierten Text auflistet, der ignoriert werden soll, oder es kann sich um einen regulären Ausdruck (Regex) handeln, der ein Textmuster definiert, das ignoriert werden soll. Wählen Sie den Abschnitt für den Listentyp aus, den Sie erstellen möchten.

Vordefinierter Text

Führen Sie in Macie die folgenden Schritte aus, bevor Sie diese Art von Zulassungsliste erstellen, führen Sie in Macie die folgenden Schritte aus:

1. Erstellen Sie mithilfe eines Texteditors eine zeilengetrennte Klartextdatei, die bestimmten Text auflistet, der ignoriert werden soll, z. B. eine TXT-, .text- oder .plain-Datei. Weitere Informationen finden Sie unter Syntaxanforderungen für Listen von vordefiniertem Text.
2. Laden Sie die Datei in einen S3-Bucket hoch und notieren Sie sich den Namen des Buckets und des Objekts. Sie müssen diese Namen eingeben, wenn Sie die Einstellungen in Macie konfigurieren.

3. Stellen Sie sicher, dass die Einstellungen für den S3-Bucket und das Objekt es Ihnen und Macie ermöglichen, die Liste aus dem Bucket abzurufen. Weitere Informationen finden Sie unter Speicheranforderungen für Listen vordefinierter Texte.
4. Wenn Sie das S3-Objekt verschlüsselt haben, sollten Sie sicherstellen, dass Sie und Macie den zugehörigen Schlüssel verwenden dürfen. Weitere Informationen finden Sie unter Verschlüsselungs-/Entschlüsselungsanforderungen für Listen vordefinierter Texte.

Nachdem Sie diese Schritte ausgeführt haben, können Sie die Listeneinstellungen in Macie konfigurieren. Sie können die Einstellungen mithilfe der Amazon-Macie-Konsole oder der Amazon-Macie-API konfigurieren.

Console

Gehen Sie wie folgt vor, um die Einstellungen für eine Zulassungsliste mithilfe der Amazon Macie Macie-Konsole zu konfigurieren.

So konfigurieren Sie die Einstellungen für die Zulassungsliste in Macie

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Listen zulassen aus.
3. Wählen Sie auf der Seite Zulässige Listen die Option Erstellen aus.
4. Wählen Sie unter Wählen Sie einen Listentyp die Option Vordefinierter Text aus.
5. Verwenden Sie unter Listeneinstellungen die folgenden Optionen, um zusätzliche Einstellungen für die Zulassungsliste einzugeben:

   - Geben Sie unter Name einen Namen für die Liste ein. Der Name darf maximal 128 Zeichen enthalten.
   - Geben Sie unter Description (Beschreibung) eine kurze Beschreibung der Liste ein. Die Beschreibung darf maximal 512 Zeichen enthalten.
   - Geben Sie für den S3-Bucket-Namen den vollständigen Namen des Buckets ein, in dem die Liste gespeichert ist.

     In Amazon S3 finden Sie diesen Wert im Feld Name der Bucket-Eigenschaften. Bei diesem Wert ist die Groß- und Kleinschreibung zu beachten. Verwenden Sie außerdem keine Platzhalterzeichen oder Teilwerte, wenn Sie den Namen eingeben.
   - Geben Sie für den S3-Objektnamen den vollständigen Namen des S3-Objekts ein, das die Liste speichert.

In Amazon S3 finden Sie diesen Wert im Schlüsselfeld der Objekteigenschaften. Wenn der Name einen Pfad enthält, sollten Sie beispielsweise bei der Eingabe des Namens den vollständigen Pfad angeben**`allowlists/macie/mylist.txt`**. Bei diesem Wert ist die Groß- und Kleinschreibung zu beachten. Verwenden Sie außerdem keine Platzhalterzeichen oder Teilwerte, wenn Sie den Namen eingeben.

6. (Optional) Wählen Sie unter Schlagworte die Option Tag hinzufügen aus, und geben Sie dann bis zu 50 Tags ein, die Sie der Zulassungsliste zuweisen möchten.

   Ein Tag ist eine Bezeichnung, die Sie definieren und bestimmten Arten von AWS Ressourcen zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Mithilfe von Tags können Sie Ressourcen auf verschiedene Weise identifizieren, kategorisieren und verwalten können, z. B. nach Zweck, Besitzer, Umgebung oder anderen Kriterien. Weitere Informationen hierzu finden Sie unter Kennzeichnen von Amazon Macie-Ressourcen.

7. Wenn Sie fertig sind, klicken Sie auf Create.

Macie testet die Einstellungen der Liste. Macie überprüft außerdem, ob es die Liste von Amazon S3 abrufen und den Inhalt der Liste analysieren kann. Wenn ein Fehler auftritt, zeigt Macie eine Meldung an, die den Fehler beschreibt. Detaillierte Informationen, die Ihnen bei der Problembehebung helfen können, finden Sie unter. Optionen und Anforderungen für Listen vordefinierter Texte Nachdem Sie alle Fehler behoben haben, können Sie die Einstellungen der Liste speichern.

API

Um die Einstellungen der Zulassungsliste programmgesteuert zu konfigurieren, verwenden Sie CreateAllowListdie Amazon Macie Macie-API und geben Sie die entsprechenden Werte für die erforderlichen Parameter an.

Verwenden Sie für den `criteria` Parameter ein `s3WordsList` Objekt, um den Namen des S3-Buckets (`bucketName`) und den Namen des S3-Objekts (`objectKey`) anzugeben, das die Liste speichert. Um den Bucket-Namen zu ermitteln, verwenden Sie das `Name` Feld in Amazon S3. Um den Objektnamen zu ermitteln, verwenden Sie das `Key` Feld in Amazon S3. Beachten Sie, dass bei diesen Werten die Groß-/Kleinschreibung berücksichtigt wird. Verwenden Sie außerdem keine Platzhalterzeichen oder Teilwerte, wenn Sie diese Namen angeben.

Um die Einstellungen mithilfe von zu konfigurierenAWS CLI, führen Sie den create-allow-listBefehl aus und geben Sie die entsprechenden Werte für die erforderlichen Parameter an. Die folgenden

Beispiele zeigen, wie Sie die Einstellungen für eine Zulassungsliste konfigurieren, die in einem S3-Bucket mit dem Namen *DOC-EXAMPLE-BUCKET* gespeichert ist. Der Name des S3-Objekts, das die Liste speichert, ist *allowlists/macie/mylist.txt*.

Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Zeilenfortsetzung, um die Lesbarkeit zu verbessern.

```
$ aws macie2 create-allow-list \
--criteria '{"s3WordsList":{"bucketName":"DOC-EXAMPLE-
BUCKET","objectKey":"allowlists/macie/mylist.txt"}}' \
--name my_allow_list \
--description "Lists public phone numbers and names for Example Corp."
```

Dieses Beispiel ist für Microsoft Windows formatiert und verwendet das Caret-Zeichen (^) zur Zeilenfortsetzung, um die Lesbarkeit zu verbessern.

```
C:\> aws macie2 create-allow-list ^
--criteria={\"s3WordsList\":{\"bucketName\":\"DOC-EXAMPLE-BUCKET\",\"objectKey\":
\"allowlists/macie/mylist.txt\"}} ^
--name my_allow_list ^
--description "Lists public phone numbers and names for Example Corp."
```

Wenn du deine Anfrage absendest, testet Macie die Einstellungen der Liste. Macie überprüft außerdem, ob es die Liste von Amazon S3 abrufen und den Inhalt der Liste analysieren kann. Wenn ein Fehler auftritt, schlägt Ihre Anfrage fehl und Macie gibt eine Nachricht zurück, die den Fehler beschreibt. Detaillierte Informationen, die Ihnen bei der Problembehebung helfen können, finden Sie unter. Optionen und Anforderungen für Listen vordefinierter Texte

Wenn Macie die Liste abrufen und parsen kann, ist Ihre Anfrage erfolgreich und Sie erhalten eine Ausgabe, die der folgenden ähnelt.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
nkr81bmtu2542yyexample",
    "id": "nkr81bmtu2542yyexample"
}
```

Wo `arn` ist der Amazon-Ressourcenname (ARN), der erstellt wurde, und `id` ist die eindeutige Kennung der Liste.

Nachdem Sie die Einstellungen der Liste gespeichert haben, können Sie Aufträge zur Erkennung vertraulicher Daten erstellen und konfigurieren, um die Liste zu verwenden, oder die Liste zu Ihren Einstellungen für die automatische Erkennung vertraulicher Daten hinzufügen. Jedes Mal, wenn diese Jobs ausgeführt werden oder ein automatisierter Discovery-Analysezyklus beginnt, ruft Macie die neueste Version der Liste von Amazon S3 ab. Macie verwendet dann diese Version der Liste, wenn sie Daten analysiert.

Regulärer Ausdruck

Wenn Sie eine Zulassungsliste erstellen, die einen regulären Ausdruck (Regex) angibt, definieren Sie den Regex und alle anderen Listeneinstellungen direkt in Macie. Macie unterstützt einen Teil der Regex-Mustersyntax, die von der Perl Compatible Regular Expressions (PCRE) -Bibliothek bereitgestellt wird. Weitere Informationen finden Sie unter Syntaxunterstützung und Empfehlungen.

Sie können diese Art von Liste mithilfe der Amazon Macie Macie-Konsole oder der Amazon Macie Macie-API erstellen.

Console

Führen Sie die folgenden Schritte aus, um eine Zulassungsliste mit der Amazon-Macie-Konsole zu erstellen.

Um eine Zulassungsliste zu erstellen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Listen zulassen aus.
3. Wählen Sie auf der Seite Zulässige Listen die Option Erstellen aus.
4. Wählen Sie unter Wählen Sie einen Listentyp die Option Regulärer Ausdruck aus.
5. Verwenden Sie unter Listeneinstellungen die folgenden Optionen, um zusätzliche Einstellungen für die Zulassungsliste einzugeben:

   - Geben Sie unter Name einen Namen für die Liste ein. Der Name darf maximal 128 Zeichen enthalten.
   - Geben Sie unter Description (Beschreibung) eine kurze Beschreibung der Liste ein. Die Beschreibung darf maximal 512 Zeichen enthalten.
   - Geben Sie unter Regulärer Ausdruck den Regex ein, der das zu ignorierende Textmuster definiert. Der Regex darf maximal 512 Zeichen enthalten.

6. (Optional) Geben Sie für Evaluieren bis zu 1.000 Zeichen in das Feld Beispieldaten ein und wählen Sie dann Test aus, um den Regex zu testen. Macie wertet die Beispieldaten aus und gibt an, wie oft Text vorkommt, der dem Regex entspricht. Sie können diesen Schritt beliebig oft wiederholen, um den Regex zu verfeinern und zu optimieren.

   > **Note**
   >
   > Wir empfehlen, den Regex mit mehreren Beispieldatensätzen zu testen und zu verfeinern. Wenn Sie einen zu allgemeinen Regex erstellen, ignoriert Macie möglicherweise Textstellen, die Sie für sensibel halten. Wenn ein Regex zu spezifisch ist, ignoriert Macie möglicherweise nicht das Vorkommen von Text, den Sie nicht als sensibel erachten.

7. (Optional) Wählen Sie unter Schlagworte die Option Tag hinzufügen aus, und geben Sie dann bis zu 50 Tags ein, die Sie der Zulassungsliste zuweisen möchten.

   Ein Tag ist eine Bezeichnung, die Sie definieren und bestimmten Arten von AWS Ressourcen zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Mithilfe von Tags können Sie Ressourcen auf verschiedene Weise identifizieren, kategorisieren und verwalten können, z. B. nach Zweck, Besitzer, Umgebung oder anderen Kriterien. Weitere Informationen hierzu finden Sie unter Kennzeichnen von Amazon Macie-Ressourcen.

8. Wenn Sie fertig sind, klicken Sie auf Create.

Macie testet die Einstellungen der Liste. Macie testet auch den Regex, um zu überprüfen, ob er den Ausdruck kompilieren kann. Wenn ein Fehler auftritt, zeigt Macie eine Meldung an, die den Fehler beschreibt. Detaillierte Informationen, die Ihnen bei der Problembehebung helfen können, finden Sie unter. Optionen und Anforderungen für reguläre Ausdrücke in Zulassungslisten Nachdem Sie alle Fehler behoben haben, können Sie die Zulassungsliste speichern.

API

Bevor Sie diese Art von Zulassungsliste in Macie erstellen, empfehlen wir, den regulären Ausdruck mit mehreren Beispieldatensätzen zu testen und zu verfeinern. Wenn Sie einen zu allgemeinen Regex erstellen, ignoriert Macie möglicherweise Textstellen, die Sie für sensibel halten. Wenn ein Regex zu spezifisch ist, ignoriert Macie möglicherweise nicht das Vorkommen von Text, den Sie nicht als sensibel erachten.

Um einen Ausdruck mit Macie zu testen, können Sie den TestCustomDataIdentifierBetrieb der Amazon Macie Macie-API verwenden oder für den den den AWS CLI Befehl ausführen. test-custom-data-identifier Macie verwendet denselben zugrunde liegenden Code, um Ausdrücke für Zulassungslisten und benutzerdefinierte Datenkennungen zu kompilieren. Wenn Sie einen Ausdruck auf diese Weise testen, stellen Sie sicher, dass Sie nur Werte für die `sampleText` Parameter `regex` und angeben. Andernfalls erhalten Sie ungenaue Ergebnisse.

Wenn Sie bereit sind, diese Art von Zulassungsliste zu erstellen, verwenden Sie die CreateAllowListBedienung der Amazon Macie Macie-API und geben Sie die entsprechenden Werte für die erforderlichen Parameter an. Verwenden Sie `criteria` das `regex` Feld, um den regulären Ausdruck anzugeben, der das zu ignorierende Textmuster definiert. Der Ausdruck darf maximal 512 Zeichen enthalten.

Um diese Art von Liste mithilfe von zu erstellenAWS CLI, führen Sie den create-allow-listBefehl aus und geben Sie die entsprechenden Werte für die erforderlichen Parameter an. In den folgenden Beispielen wird eine Zulassungsliste mit dem Namen *`my_allow_list`* erstellt. Der Regex ist dafür ausgelegt, alle E-Mail-Adressen zu ignorieren, die eine benutzerdefinierte Datenkennung andernfalls für die `example.com` Domäne erkennen könnte.

Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Zeilenfortsetzung, um die Lesbarkeit zu verbessern.

```
$ aws macie2 create-allow-list \
--criteria '{"regex":"[a-z]@example.com"}' \
--name my_allow_list \
--description "Ignores all email addresses for Example Corp."
```

Dieses Beispiel ist für Microsoft Windows formatiert und verwendet das Caret-Zeichen (^) zur Zeilenfortsetzung, um die Lesbarkeit zu verbessern.

```
C:\> aws macie2 create-allow-list ^
--criteria={\"regex\":\"[a-z]@example.com\"} ^
--name my_allow_list ^
--description "Ignores all email addresses for Example Corp."
```

Wenn du deine Anfrage absendest, testet Macie die Einstellungen der Liste. Macie testet auch den Regex, um zu überprüfen, ob er den Ausdruck kompilieren kann. Tritt ein Fehler auf, schlägt die Anfrage fehl und Macie gibt eine Meldung zurück, die den Fehler beschreibt. Detaillierte

Informationen, die Ihnen bei der Problembehebung helfen können, finden Sie unter. Optionen und Anforderungen für reguläre Ausdrücke in Zulassungslisten

Wenn Macie den Ausdruck kompilieren kann, ist die Anfrage erfolgreich und Sie erhalten eine Ausgabe, die der folgenden ähnelt:

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
km2d4y22hp6rv05example",
    "id": "km2d4y22hp6rv05example"
}
```

Wo `arn` ist der Amazon-Ressourcenname (ARN), der erstellt wurde, und `id` ist die eindeutige Kennung der Liste.

Nachdem Sie die Liste gespeichert haben, können Sie Aufträge zur Erkennung vertraulicher Daten erstellen und konfigurieren, um sie zu verwenden, oder sie zu Ihren Einstellungen für die automatische Erkennung vertraulicher Daten hinzufügen. Wenn diese Jobs ausgeführt werden oder Macie eine automatische Erkennung für Ihr Konto durchführt, verwendet Macie die neueste Version des Regex der Liste, um Daten zu analysieren.

Überprüfen des Status der Zulassungslisten

Es ist wichtig, den Status Ihrer Zulassungslisten regelmäßig zu überprüfen. Andernfalls könnten Fehler dazu führen, dass Amazon Macie unerwartete Analyseergebnisse liefert, wie z. B. Ergebnisse vertraulicher Daten für Text, den Sie in einer Zulassungsliste angegeben haben.

Wenn Sie einen Job zur Erkennung vertraulicher Daten so konfigurieren, dass er eine Zulassungsliste verwendet und Macie nicht auf die Liste zugreifen oder sie verwenden kann, wenn der Job ausgeführt wird, wird der Job weiterhin ausgeführt. Macie verwendet die Liste jedoch nicht, wenn sie S3-Objekte analysiert. In ähnlicher Weise wird die Analyse fortgesetzt, wenn ein Analysezyklus für die automatische Erkennung vertraulicher Daten beginnt und Macie nicht auf eine angegebene Zulassungsliste zugreifen oder diese verwenden kann, aber Macie verwendet die Liste nicht.

Es ist unwahrscheinlich, dass Fehler bei einer Zulassungsliste auftreten, die einen regulären Ausdruck (Regex) angibt. Dies liegt zum Teil daran, dass Macie den Regex automatisch testet, wenn Sie die Einstellungen der Liste erstellen oder aktualisieren. Darüber hinaus speichern Sie den Regex und alle anderen Listeneinstellungen in Macie.

Bei einer Zulassungsliste, die vordefinierten Text angibt, können jedoch Fehler auftreten, was zum Teil darauf zurückzuführen ist, dass Sie die Liste in Amazon S3 und nicht in Macie speichern. Häufige Fehlerursachen sind:

- Der S3-Bucket oder das S3-Objekt wird gelöscht.
- Der S3-Bucket oder das S3-Objekt wird umbenannt und die Listeneinstellungen in Macie geben den neuen Namen nicht an.
- Die Berechtigungseinstellungen des S3-Buckets werden geändert und Macie verliert den Zugriff auf den Bucket und das Objekt.
- Die Verschlüsselungseinstellungen für den S3-Bucket wurden geändert und Macie kann das Objekt, das die Liste speichert, nicht entschlüsseln.
- Die Richtlinie für den Verschlüsselungsschlüssel wird geändert und Macie verliert den Zugriff auf den Schlüssel. Macie kann das S3-Objekt, das die Liste speichert, nicht entschlüsseln.

> **Important**
>
> Da sich diese Fehler auf die Ergebnisse Ihrer Analysen auswirken, empfehlen wir Ihnen, den Status Ihrer Zulassungslisten regelmäßig zu überprüfen. Wir empfehlen, dass Sie dies auch tun, wenn Sie die Berechtigungen oder Verschlüsselungseinstellungen für einen S3-Bucket ändern, der eine Zulassungsliste speichert, oder wenn Sie die Richtlinie für einen AWS Key Management Service (AWS KMS) -Schlüssel ändern, der zum Verschlüsseln einer Liste verwendet wird.

Sie können den Status Ihrer Zulassungslisten mithilfe der Amazon Macie Macie-Konsole oder der Amazon Macie Macie-API überprüfen. Detaillierte Informationen, die Ihnen bei der Behebung von auftretenden Fehlern helfen können, finden Sie unter. Optionen und Anforderungen für Listen vordefinierter Texte

Console

Gehen Sie wie folgt vor, um den Status Ihrer Zulassungslisten mithilfe der Amazon Macie Macie-Konsole zu überprüfen.

So überprüfen Sie den Status Ihrer Zulassungslisten

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.

2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Listen zulassen aus.
3. Wählen Sie auf der Seite „Listen zulassen“ die Option „Aktualisieren“ ()
   Macie testet die Einstellungen für alle Ihre Zulassungslisten und aktualisiert das Statusfeld, um den aktuellen Status jeder Liste anzuzeigen.

   Wenn eine Liste einen regulären Ausdruck angibt, ist ihr Status normalerweise OK. Dies bedeutet, dass Macie den Ausdruck kompilieren kann. Wenn eine Liste vordefinierten Text angibt, kann ihr Status einen der folgenden Werte haben.

   OK

   Macie kann den Inhalt der Liste abrufen und parsen.

   Zugriff verweigert

   Macie darf nicht auf das S3-Objekt zugreifen, das die Liste speichert. Amazon S3 hat die Anforderung zum Abrufen des Objekts abgelehnt. Eine Liste kann diesen Status auch haben, wenn das Objekt verschlüsselt ist und Macie nicht verwenden darf. AWS KMS key

   Um diesen Fehler zu beheben, überprüfen Sie die Bucket-Richtlinie und andere Berechtigungseinstellungen für den Bucket und das Objekt. Stellen Sie sicher, dass Macie auf das Objekt zugreifen und es abrufen darf. Wenn das Objekt mit einem vom Kunden verwalteten AWS KMS -Schlüssel verschlüsselt ist, sollten Sie außerdem die Schlüsselrichtlinie überprüfen und sicherstellen, dass Macie den Schlüssel verwenden darf.

   Fehler

   Macie hat versucht, den Inhalt der Liste abzurufen oder zu parsen. Dabei ist ein vorübergehender oder interner Fehler aufgetreten. Eine Zulassungsliste kann diesen Status auch haben, wenn sie mit einem Verschlüsselungsschlüssel verschlüsselt ist, auf den Amazon S3 und Macie nicht zugreifen oder den sie nicht verwenden können.

   Wenn Sie diesen Fehler beheben möchten, warten Sie einige Minuten und wählen Sie dann erneut aktualisieren (). Wenn der Status weiterhin Fehler lautet, überprüfen Sie die Verschlüsselungseinstellungen für das S3-Objekt. Stellen Sie sicher, dass das Objekt

mit einem Schlüssel verschlüsselt ist, auf den Amazon S3 und Macie und den sie nicht verwenden können.

Objekt ist leer

Macie kann die Liste von Amazon S3 abrufen, aber die Liste enthält keine Einträge.

Um diesen Fehler zu beheben, laden Sie das Objekt von Amazon S3 herunter und stellen Sie sicher, dass es die richtigen Einträge enthält. Wenn die Einträge korrekt sind, überprüfen Sie die Einstellungen der Liste in Macie. Stellen Sie sicher, dass die angegebenen Bucket- und Objektnamen korrekt sind.

Objekt wurde nicht gefunden

Die Liste ist in Amazon S3 nicht vorhanden.

Um diesen Fehler zu beheben, überprüfen Sie die Listeneinstellungen in Macie. Stellen Sie sicher, dass die angegebenen Bucket- und Objektnamen korrekt sind.

Kontingent überschritten

Macie kann in Amazon S3 auf die Liste zugreifen. Die Anzahl der Einträge in der Liste oder die Speichergröße der Liste überschreiten jedoch das Kontingent für eine Zulassungsliste.

Um diesen Fehler zu beheben, teilen Sie die Liste in mehrere Dateien auf. Stellen Sie sicher, dass jede Datei weniger als 100.000 Einträge enthält. Stellen Sie außerdem sicher, dass die Größe jeder Datei weniger als 35 MB beträgt. Laden Sie anschließend jede Datei in Amazon S3 hoch. Wenn Sie fertig sind, konfigurieren Sie in Macie für jede Datei die Zulassungsliste. Sie können bis zu fünf Listen mit vordefiniertem Text in jeder Liste unterstützenAWS-Region.

Gedrosselt

Amazon S3 hat die Anforderung zum Abrufen der Liste gedrosselt.

Wenn Sie diesen Fehler beheben möchten, warten Sie einige Minuten und wählen Sie dann erneut aktualisieren ().

Benutzerzugriff verweigert

Amazon S3 hat die Anforderung zum Abrufen des Objekts abgelehnt. Wenn das angegebene Objekt vorhanden ist, haben Sie keinen Zugriff oder keine Berechtigung, den AWS KMS-Schlüssel zu verwenden, mit dem es verschlüsselt wurde.

Um diesen Fehler zu beheben, sollten Sie mit Ihrem AWS Administrator zusammenarbeiten, um sicherzustellen, dass in den Einstellungen der Liste die richtigen Bucket- und Objektnamen angegeben sind und dass Sie Lesezugriff auf den Bucket und das Objekt haben. Wenn das Objekt verschlüsselt ist, sollten Sie außerdem sicherstellen, dass Sie den zugehörigen Schlüssel verwenden dürfen.

4. Um die Einstellungen und den Status einer bestimmten Liste zu überprüfen, wählen Sie den Namen der Liste.

API

Um den Status einer Zulassungsliste programmgesteuert zu überprüfen, verwenden Sie den GetAllowListVorgang der Amazon Macie Macie-API oder führen Sie für die den den AWS CLI get-allow-listBefehl aus.

Geben Sie für den `id` Parameter den eindeutigen Bezeichner für die Zulassungsliste an, deren Status Sie überprüfen möchten. Um diese Kennung abzurufen, können Sie die ListAllowListsOperation verwenden. Der ListAllowLists Vorgang ruft Informationen zu allen Zulassungslisten für Ihr Konto ab. Wenn Sie den verwendenAWS CLI, können Sie den list-allow-listsBefehl ausführen, um diese Informationen abzurufen.

Wenn Sie eine GetAllowList Anfrage einreichen, testet Macie alle Einstellungen für die Zulassungsliste. Wenn die Einstellungen einen regulären Ausdruck (Regex) angeben, überprüft Macie, ob der Ausdruck kompiliert werden kann. Wenn die Einstellungen eine Liste mit vordefiniertem Text angeben, überprüft Macie, ob die Liste abgerufen und analysiert werden kann.

Macie gibt dann ein `GetAllowListResponse` Objekt zurück, das die Details der Zulassungsliste bereitstellt. Im `GetAllowListResponse` Objekt gibt das `status` Objekt den aktuellen Status der Liste an: einen Statuscode (`code`) und, je nach Statuscode, eine kurze Beschreibung des Status der Liste (`description`).

Wenn die Zulassungsliste einen Regex angibt, lautet der Statuscode normalerweise `OK` und es gibt keine zugehörige Beschreibung. Das bedeutet, dass Macie den Ausdruck erfolgreich kompiliert hat.

Wenn die Zulassungsliste vordefinierten Text angibt, variiert der Statuscode je nach Testergebnis:

- Wenn Macie die Liste erfolgreich abgerufen und analysiert hat, lautet der Statuscode 0K und es gibt keine zugehörige Beschreibung.
- Wenn Macie aufgrund eines Fehlers die Liste nicht abrufen oder analysieren konnte, geben der Statuscode und die Beschreibung die Art des aufgetretenen Fehlers an.

Eine Liste möglicher Statuscodes und eine Beschreibung der einzelnen Codes finden Sie AllowListStatusin der Amazon Macie API-Referenz.

Zulassungslisten ändern

Nachdem Sie eine Zulassungsliste erstellt haben, können Sie die meisten Einstellungen der Liste in Amazon Macie ändern. Sie können beispielsweise den Namen und die Beschreibung der Liste ändern und die Tags der Liste hinzufügen und bearbeiten. Die einzige Einstellung, die Sie nicht ändern können, ist der Typ einer Liste. Wenn eine bestehende Zulassungsliste beispielsweise einen regulären Ausdruck angibt, können Sie seinen Typ nicht in vordefinierten Text ändern.

Wenn eine Zulassungsliste vordefinierten Text angibt, können Sie auch die Einträge in der Liste ändern. Aktualisieren Sie dazu die Datei, die die Einträge enthält, und laden Sie dann die neue Version der Datei auf Amazon S3 hoch. Wenn Macie sich das nächste Mal auf die Verwendung der Liste vorbereitet, ruft Macie die neueste Version der Datei von Amazon S3 ab. Wenn Sie die neue Datei hochladen, stellen Sie sicher, dass Sie sie im selben S3-Bucket und Objekt speichern. Oder, wenn Sie den Namen des Buckets oder Objekts ändern, stellen Sie sicher, dass Sie die Einstellungen der Liste in Macie aktualisieren.

Sie können die Einstellungen einer Zulassungsliste mithilfe der Amazon Macie Macie-Konsole oder der Amazon Macie Macie-API ändern.

Console

Führen Sie die folgenden Schritte aus, um die Einstellungen für eine Zulassungsliste mithilfe der Amazon-Macie-Konsole zu ändern.

Um eine Zulassungsliste zu ändern

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Listen zulassen aus.

3. Wählen Sie auf der Seite Zulassungslisten den Namen der Zulassungsliste aus, die Sie ändern möchten. Die Seite „Zulassen“ wird geöffnet und zeigt die aktuellen Einstellungen für die Liste an.
4. Um der Zulassungsliste Schlagworte zuzuweisen oder zu bearbeiten, wählen Sie im Bereich Schlagworte die Option Schlagworte verwalten aus. Ändern Sie dann die Tags nach Bedarf. Wählen Sie Save (Speichern) aus, wenn Sie fertig sind.
5. Um andere Einstellungen für die Zulassungsliste zu ändern, wählen Sie im Abschnitt Listeneinstellungen die Option Bearbeiten aus. Ändern Sie dann die gewünschten Einstellungen:

   - Name — Geben Sie einen neuen Namen für die Liste ein. Der Name darf maximal 128 Zeichen enthalten.
   - Beschreibung — Geben Sie eine neue Beschreibung der Liste ein. Die Beschreibung darf maximal 512 Zeichen enthalten.
   - Wenn die Zulassungsliste vordefinierten Text angibt:
     - S3-Bucket-Name — Geben Sie den vollständigen Namen des Buckets ein, in dem die Liste derzeit gespeichert ist.

       In Amazon S3 finden Sie diesen Wert im Feld Name der Bucket-Eigenschaften. Bei diesem Wert ist die Groß- und Kleinschreibung zu beachten. Verwenden Sie außerdem keine Platzhalterzeichen oder Teilwerte, wenn Sie den Namen eingeben.
     - S3-Objektname — Geben Sie den vollständigen Namen des S3-Objekts ein, in dem die Liste derzeit gespeichert ist.

       In Amazon S3 finden Sie diesen Wert im Schlüsselfeld der Objekteigenschaften. Wenn der Name einen Pfad enthält, sollten Sie beispielsweise bei der Eingabe des Namens den vollständigen Pfad angeben**`allowlists/macie/mylist.txt`**. Bei diesem Wert ist die Groß- und Kleinschreibung zu beachten. Verwenden Sie außerdem keine Platzhalterzeichen oder Teilwerte, wenn Sie den Namen eingeben.
   - Wenn die Zulassungsliste einen regulären Ausdruck (Regex) angibt, geben Sie einen neuen Regex in das Feld Regulärer Ausdruck ein. Der Regex darf maximal 512 Zeichen enthalten.

     Nachdem Sie den neuen Regex eingegeben haben, testen Sie ihn optional. Geben Sie dazu bis zu 1.000 Zeichen in das Feld Beispieldaten ein und wählen Sie dann Test aus. Macie wertet die Beispieldaten aus und gibt an, wie oft Text vorkommt, der dem Regex

entspricht. Sie können diesen Schritt beliebig oft wiederholen, um den Regex zu verfeinern und zu optimieren, bevor Sie Ihre Änderungen speichern.

Wenn Sie mit dem Ändern der Einstellungen fertig sind, wählen Sie Speichern.

Macie testet die Einstellungen der Liste. Bei einer Liste mit vordefiniertem Text überprüft Macie außerdem, ob die Liste von Amazon S3 abgerufen und der Inhalt der Liste analysiert werden kann. Für einen Regex überprüft Macie auch, ob er den Ausdruck kompilieren kann. Wenn ein Fehler auftritt, zeigt Macie eine Meldung an, die den Fehler beschreibt. Detaillierte Informationen, die Ihnen bei der Problembehebung helfen können, finden Sie unter. Optionen und Anforderungen für Zulassungslisten Nachdem Sie alle Fehler behoben haben, können Sie Ihre Änderungen speichern.

API

Um eine Zulassungsliste programmgesteuert zu ändern, verwenden Sie den UpdateAllowListVorgang der Amazon Macie Macie-API oder führen Sie für die den den AWS CLI update-allow-listBefehl aus. Verwenden Sie in Ihrer Anfrage die unterstützten Parameter, um für jede Einstellung, die Sie ändern möchten, einen neuen Wert anzugeben. Beachten Sie`criteria`, dass die `name` Parameter`id`,, und erforderlich sind. Wenn Sie den Wert für einen erforderlichen Parameter nicht ändern möchten, geben Sie den aktuellen Wert für den Parameter an.

Mit dem folgenden Befehl werden beispielsweise den Namen und die Beschreibung einer vorhandenen Zulassungsliste geändert. Das Beispiel ist für Microsoft Windows formatiert und verwendet das Caret-Zeichen (^) zur Zeilenfortsetzung, um die Lesbarkeit zu verbessern.

```
C:\> aws macie2 update-allow-list ^
--id km2d4y22hp6rv05example ^
--name my_allow_list-email ^
--criteria={\"regex\":\"[a-z]@example.com\"} ^
--description "Ignores all email addresses for the example.com domain"
```

Wobei gilt:

- *`km2d4y22hp6rv05example`* ist die eindeutige Kennung für die Liste.
- *`my_allow_list-email`* ist der neue Name für die Liste.
- *`[a-z] @example .com`* ist das Kriterium der Liste, ein regulärer Ausdruck.

- *`Ignoriert alle E-Mail-Adressen für die Domäne example.com`* ist die neue Beschreibung für die Liste.

Wenn du deine Anfrage absendest, testet Macie die Einstellungen der Liste. Wenn die Liste vordefinierten Text angibt, muss überprüft werden, ob Macie die Liste von Amazon S3 abrufen und den Inhalt der Liste analysieren kann. Wenn in der Liste ein Regex angegeben ist, muss überprüft werden, ob Macie den Ausdruck kompilieren kann.

Tritt beim Testen der Einstellungen durch Macie ein Fehler auf, schlägt Ihre Anfrage fehl und Macie gibt eine Meldung zurück, in der der Fehler beschrieben wird. Detaillierte Informationen, die Ihnen bei der Problembehebung helfen können, finden Sie unter. Optionen und Anforderungen für Zulassungslisten Wenn die Anfrage aus einem anderen Grund fehlschlägt, gibt Macie eine HTTP 4 xx - oder 500-Antwort zurück, die angibt, warum der Vorgang fehlgeschlagen ist.

Wenn Ihre Anfrage erfolgreich ist, aktualisiert Macie die Einstellungen der Liste, und Sie erhalten eine Ausgabe, die der folgenden ähnelt.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
km2d4y22hp6rv05example",
    "id": "km2d4y22hp6rv05example"
}
```

Wo `arn` ist der Amazon-Ressourcenname (ARN) der Zulassungsliste, die aktualisiert wurde, und `id` ist die eindeutige Kennung der Liste.

Zulässige Listen löschen

Wenn Sie eine Zulassungsliste in Amazon Macie löschen, löschen Sie dauerhaft alle Einstellungen der Liste. Diese Einstellungen können nach dem Löschen nicht wiederhergestellt werden. Wenn die Einstellungen eine Liste mit vordefiniertem Text angeben, den Sie in Amazon S3 speichern, löscht Macie das S3-Objekt, das die Liste speichert, nicht. Nur die Einstellungen in Macie werden gelöscht.

Wenn Sie Aufträge zur Erkennung vertraulicher Daten so konfigurieren, dass sie eine Zulassungsliste verwenden und die Liste anschließend löschen, werden die Jobs wie geplant ausgeführt. Ihre Arbeitsergebnisse, sowohl Ergebnisse vertraulicher Daten als auch Ergebnisse der Erkennung vertraulicher Daten, enthalten jedoch möglicherweise Text, den Sie zuvor in einer Zulassungsliste angegeben haben. In ähnlicher Weise werden die täglichen Analysezyklen fortgesetzt, wenn Sie

die automatische Erkennung vertraulicher Daten für die Verwendung einer Liste konfigurieren und die Liste anschließend löschen. Bei sensiblen Daten, Ergebnissen, Statistiken oder anderen Arten von Ergebnissen kann es jedoch vorkommen, dass Text angezeigt wird, den Sie zuvor in einer Zulassungsliste angegeben haben.

Bevor Sie eine Zulassungsliste löschen, empfehlen wir Ihnen, Ihr Jobinventar zu überprüfen, um Jobs zu identifizieren, die die Liste verwenden und deren Ausführung in der future geplant ist. Im Inventar gibt der Detailbereich an, ob ein Job so konfiguriert ist, dass er erlaubte Listen verwendet, und wenn ja, welche. Überprüfen Sie außerdem Ihre Einstellungen für die automatische Erkennung vertraulicher Daten. Sie könnten entscheiden, dass es am besten ist, eine Liste zu ändern, anstatt sie zu löschen.

Als zusätzlichen Schutz überprüft Macie die Einstellungen für all Ihre Jobs, wenn Sie versuchen, eine Zulassungsliste zu löschen. Wenn Sie Jobs für die Verwendung der Liste konfiguriert haben und einer dieser Jobs einen anderen Status als Abgeschlossen oder Storniert hat, löscht Macie die Liste nicht, es sei denn, Sie geben eine zusätzliche Bestätigung.

Sie können eine Zulassungsliste löschen, indem Sie die Amazon-Macie-Konsole oder die Amazon-Macie-API verwenden.

Console

Gehen Sie wie folgt vor, um eine Zulassungsliste mithilfe der Amazon Macie Macie-Konsole zu löschen.

So löschen Sie eine Zulassungsliste

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Listen zulassen aus.
3. Aktivieren Sie auf der Seite Zulassungslisten das Kontrollkästchen für die Zulassungsliste, die Sie löschen möchten.
4. Wählen Sie im Menü Actions die Option Delete.
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein und wählen Sie dann Delete (Löschen) aus.

API

Um eine Zulassungsliste programmgesteuert zu löschen, verwenden Sie den DeleteAllowListVorgang der Amazon Macie Macie-API. Geben Sie für den `id` Parameter den

eindeutigen Bezeichner für die zu löschende Zulassungsliste an. Sie können diese Kennung mithilfe der ListAllowListsOperation abrufen. Der ListAllowLists Vorgang ruft Informationen zu allen Zulassungslisten für Ihr Konto ab. Wenn Sie den verwendenAWS CLI, können Sie den list-allow-listsBefehl ausführen, um diese Informationen abzurufen.

Geben Sie für den `ignoreJobChecks` Parameter an, ob das Löschen der Liste erzwungen werden soll, auch wenn Aufträge zur Erkennung vertraulicher Daten so konfiguriert sind, dass sie die Liste verwenden:

- Wenn Sie angeben`false`, überprüft Macie die Einstellungen für alle Ihre Jobs, die einen anderen Status als `COMPLETE` oder `CANCELLED` haben. Wenn keiner dieser Jobs für die Verwendung der Liste konfiguriert ist, löscht Macie die Liste dauerhaft. Wenn einer dieser Jobs für die Verwendung der Liste konfiguriert ist, lehnt Macie Ihre Anfrage ab und gibt einen HTTP 400 (`ValidationException`) -Fehler zurück. Die Fehlermeldung gibt die Anzahl der zutreffenden Jobs für bis zu 200 Jobs an.
- Wenn Sie angeben`true`, löscht Macie die Liste dauerhaft, ohne die Einstellungen für einen Ihrer Jobs zu überprüfen.

Führen Sie den delete-allow-listBefehl ausAWS CLI, um eine Zulassungsliste mit dem zu löschen. Beispiel:

```
C:\> aws macie2 delete-allow-list --id nkr81bmtu2542yyexample --ignore-job-checks
 false
```

Wobei *`nkr81bmtu2542yyexample`* die eindeutige Kennung für die zu löschende Liste ist.

Wenn Ihre Anfrage erfolgreich ist, gibt Macie eine leere HTTP 200-Antwort zurück. Andernfalls gibt Macie eine HTTP 4 xx - oder 500-Antwort zurück, die angibt, warum der Vorgang fehlgeschlagen ist.

Wenn in der Zulassungsliste vordefinierten Text angegeben ist, können Sie optional das S3-Objekt löschen, das die Liste speichert. Wenn Sie dieses Objekt behalten, können Sie jedoch sicherstellen, dass Sie über einen unveränderlichen Verlauf der Ergebnisse, die mit sensiblen Daten und Ermittlungsergebnissen übereinstimmen.

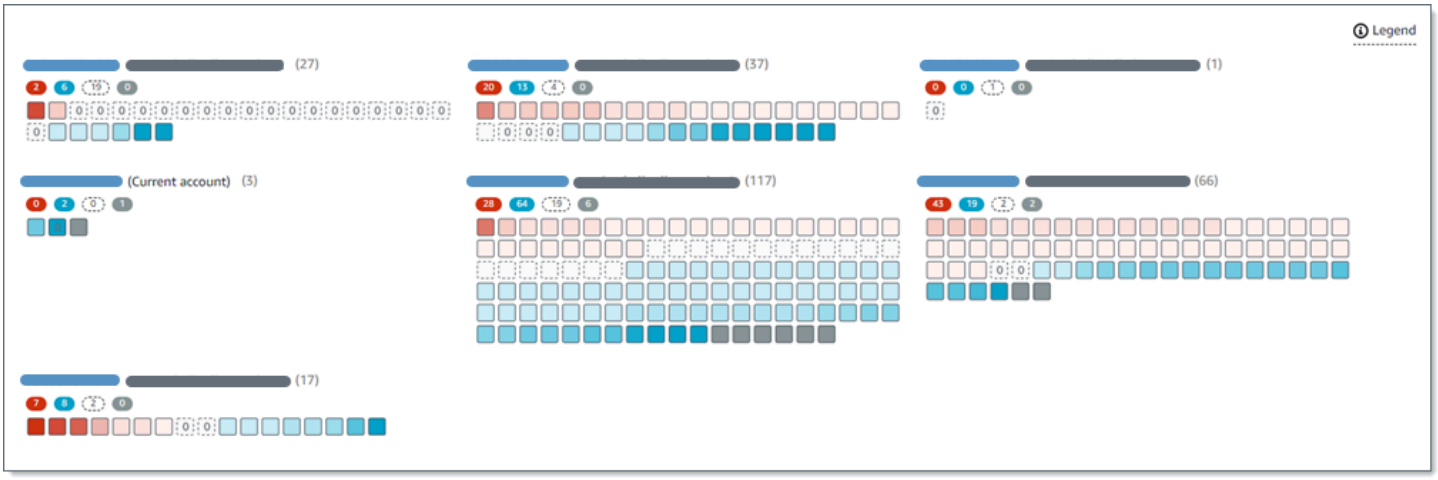
Durchführung automatisierter Erkennung vertraulicher Daten mit Amazon Macie

Um einen umfassenden Überblick darüber zu erhalten, wo sich sensible Daten in Ihrem Amazon Simple Storage Service (Amazon S3) -Datenbestand befinden könnten, konfigurieren Sie Amazon Macie so, dass es die automatische Erkennung vertraulicher Daten für Ihr Konto oder Ihre Organisation durchführt. Mit der automatisierten Erkennung vertraulicher Daten wertet Macie kontinuierlich Ihr S3-Bucket-Inventar aus und verwendet Stichprobenverfahren, um repräsentative S3-Objekte in Ihren Buckets zu identifizieren und auszuwählen. Macie ruft dann die ausgewählten Objekte ab, analysiert sie und untersucht sie auf sensible Daten.

Standardmäßig analysiert Macie S3-Objekte mithilfe des Satzes von verwalteten Datenkennungen, die wir für die automatische Erkennung vertraulicher Daten empfehlen. Sie können die Analysen anpassen, indem Sie Macie so konfigurieren, dass sie bestimmteIdentifikatoren für verwaltete Daten,benutzerdefinierte Datenkennungen, undListen zulassenwenn es die automatische Erkennung vertraulicher Daten für Ihr Konto oder Ihre Organisation durchführt. Darüber hinaus wählt Macie automatisch Objekte aus all Ihren S3-Buckets aus und analysiert sie. Wenn Sie der Macie-Administrator für eine Organisation sind, schließt dies Objekte in S3-Buckets ein, die Ihren Mitgliedskonten gehören. Sie können den Umfang der Analysen anpassen, indem Sie bestimmte Buckets ausschließen, z. B. S3-Buckets, die normalerweise speichernAWSDaten protokollieren.

Im Laufe der täglichen Analyse erstellt Macie Aufzeichnungen über die sensiblen Daten, die sie findet, und die Analysen, die sie durchführt: Ergebnisse sensibler Daten, die Macie in einzelnen S3-Objekten findet, und Ergebnisse der Erkennung vertraulicher Daten, in denen Details über die Analyse einzelner S3-Objekte protokolliert werden. Macie aktualisiert auch Statistiken, Inventardaten und andere Informationen, die es über Ihre Amazon S3-Daten bereitstellt.

Eine interaktive Heatmap auf der Konsole bietet beispielsweise eine visuelle Darstellung der Datensensitivität in Ihrem gesamten Datenbestand:



Diese Funktionen sollen Ihnen helfen, die Datensensitivität in Ihrem Amazon S3-Datenbestand zu bewerten und detaillierte Analysen durchzuführen, um einzelne Konten, Buckets und Objekte zu untersuchen und zu bewerten. Sie können Ihnen auch dabei helfen, herauszufinden, wo Sie eingehendere, unmittelbarere Analysen durchführen sollten, indemAusführen von Aufträgen zur Erkennung vertraulicher Daten. In Kombination mit den Informationen, die Macie über die Sicherheit und den Datenschutz Ihrer Amazon S3-Daten bereitstellt, können Sie diese Funktionen auch verwenden, um Fälle zu identifizieren, in denen eine sofortige Korrektur erforderlich sein könnte — zum Beispiel ein öffentlich zugänglicher Bucket, in dem Macie vertrauliche Daten gefunden hat.

Um die automatische Erkennung vertraulicher Daten zu konfigurieren und zu verwenden, muss Ihr Konto ein eigenständiges Macie-Konto oder das Macie-Administratorkonto für eine Organisation sein.

Themen

- So funktioniert die automatische Erkennung vertraulicher Daten
- Konfiguration der automatischen Erkennung sensibler Daten für Ihr Konto
- Verwaltung der automatisierten Erkennung vertraulicher Daten für einzelne S3-Buckets
- Bewertung des Umfangs automatisierter Erkennung vertraulicher Daten
- Überprüfung automatisierter Statistiken und Ergebnisse zur Erkennung sensibler Daten
- Empfindlichkeitsbewertung für S3-Buckets
- Standardeinstellungen für die automatische Erkennung vertraulicher Daten

So funktioniert die automatische Erkennung vertraulicher Daten

Wenn Sie Amazon Macie für Ihren aktivierenAWS-Konto, Macie erstellt eineAWS Identity and Access Management(ICH BIN)Rolle im Zusammenhang mit Dienstleistungenfür Ihr Konto in der

aktuellenAWS-Region. Die Berechtigungsrichtlinie für diese Rolle ermöglicht es Macie, andere anzurufenAWS-Servicesund überwachenAWSRessourcen in Ihrem Namen. Mithilfe dieser Rolle generiert und verwaltet Macie ein vollständiges Inventar Ihrer Amazon Simple Storage Service (Amazon S3) -Buckets in der Region. Das Inventar enthält Informationen zu jedem Ihrer S3-Buckets und den Objekten in den Buckets. Wenn Sie der Macie-Administrator einer Organisation sind, enthält das Inventar Informationen über S3-Buckets, die Ihren Mitgliedskonten gehören. Weitere Informationen finden Sie unter Verwalten mehrerer Konten.

Wenn die automatische Erkennung vertraulicher Daten für Ihr Macie-Konto aktiviert ist, wertet Macie die Inventardaten täglich aus, um S3-Objekte zu identifizieren, die für die automatische Erkennung in Frage kommen. Im Rahmen der Bewertung wählt Macie auch eine Stichprobe repräsentativer Objekte zur Analyse aus. Macie ruft dann die neueste Version jedes ausgewählten Objekts von Amazon S3 ab und analysiert sie und überprüft jedes Objekt auf vertrauliche Daten.

Im Verlauf der Analyse aktualisiert Macie die Statistiken, Inventardaten und andere Informationen, die es über Ihre Amazon S3-Daten bereitstellt. Macie erstellt auch Aufzeichnungen über die sensiblen Daten, die sie findet, und über die Analysen, die sie durchführt. Die daraus resultierenden Daten geben Aufschluss darüber, wo Macie sensible Daten in Ihrem Amazon S3-Datenbestand gefunden hat. Sie umfassen alle S3-Buckets, die Macie für Ihr Konto überwacht und analysiert. Die Daten können Ihnen dabei helfen, die Sicherheit und den Datenschutz Ihrer sensiblen Daten zu beurteilen, festzustellen, wo eine eingehendere Untersuchung durchzuführen ist, und Fälle zu identifizieren, in denen Abhilfemaßnahmen erforderlich sind.

Eine kurze Demonstration der Funktionsweise der automatisierten Erkennung vertraulicher Daten finden Sie im folgenden Video:Überblick über die automatische Datenerkennung von Amazon Macie.

Um die automatische Erkennung vertraulicher Daten zu konfigurieren und zu verwenden, muss Ihr Konto ein eigenständiges Macie-Konto oder das Macie-Administratorkonto für eine Organisation sein.

Themen

- Zentrale Komponenten
- Überlegungen

Zentrale Komponenten

Amazon Macie verwendet eine Kombination von Funktionen und Techniken, um die automatische Erkennung vertraulicher Daten für Ihre Amazon S3-Daten durchzuführen. Diese funktionieren

zusammen mit Funktionen und Techniken, die Macie verwendet, um Ihnen zu helfen.Überwachen Sie Ihre Amazon S3-Daten für Sicherheit und Zugriffskontrolle.

S3-Objekte zur Analyse auswählen

Macie wertet täglich Ihre Amazon S3-Inventardaten aus, um S3-Objekte zu identifizieren, die für eine Analyse durch die automatische Erkennung vertraulicher Daten in Frage kommen. Wenn Sie der Macie-Administrator einer Organisation sind, gehören dazu auch Inventardaten für S3-Buckets, die Ihren Mitgliedskonten gehören.

Im Rahmen der Bewertung verwendet Macie Stichprobenverfahren, um repräsentative Objekte für die Analyse auszuwählen. Die Techniken definieren Gruppen von Objekten, die ähnliche Metadaten und wahrscheinlich ähnlichen Inhalt haben. Die Gruppen basieren auf Dimensionen wie Bucket-Name, Präfix, Speicherklasse, Dateinamenerweiterung und Datum der letzten Änderung. Macie wählt dann einen repräsentativen Satz von Stichproben aus jeder Gruppe aus, ruft die neueste Version jedes ausgewählten Objekts von Amazon S3 ab und analysiert jedes ausgewählte Objekt, um festzustellen, ob das Objekt vertrauliche Daten enthält. Wenn die Analyse abgeschlossen ist, verwirft Macie seine Kopie des Objekts.

Die Stichprobenstrategie priorisiert verteilte Analysen. Im Allgemeinen verwendet es einen Ansatz, bei dem die Breite an erster Stelle steht, für Ihren Amazon S3-Datenbestand. Jeden Tag wird ein repräsentativer Satz von S3-Objekten aus so vielen Ihrer Buckets wie möglich ausgewählt, basierend auf der Gesamtspeichergröße aller klassifizierbaren Objekte in Ihrem Amazon S3-Datenbestand. Wenn Macie beispielsweise bereits vertrauliche Daten in Objekten in einem S3-Bucket analysiert und in einem anderen Bucket noch keine Objekte analysiert hat, hat der letztere Bucket eine höhere Priorität für die Analyse. Mit diesem Ansatz erhalten Sie schneller einen umfassenden Einblick in die Sensitivität Ihrer Amazon S3-Daten. Abhängig von der Größe Ihres Datenbestands können die Analyseergebnisse innerhalb von 48 Stunden nach Aktivierung der automatischen Erkennung vertraulicher Daten für Ihr Konto erscheinen.

Die Stichprobenstrategie priorisiert auch die Analyse verschiedener Arten von S3-Objekten und Objekten, die kürzlich erstellt oder geändert wurden. Es kann nicht garantiert werden, dass ein einzelnes Objektmuster aussagekräftig ist. Daher kann die Analyse einer Vielzahl von Objekten einen besseren Einblick in die Art und Menge vertraulicher Daten liefern, die ein S3-Bucket enthalten könnte. Darüber hinaus hilft die Priorisierung neuer oder kürzlich geänderter Objekte der Analyse, sich an Änderungen an Ihrem Bucket-Inventar anzupassen. Wenn Objekte beispielsweise nach einer vorherigen Analyse erstellt oder geändert werden, haben diese Objekte für die nachfolgende Analyse eine höhere Priorität. Umgekehrt, wenn ein Objekt zuvor analysiert wurde und sich seit dieser Analyse nicht geändert hat, analysiert Macie das Objekt

nicht erneut. Dieser Ansatz hilft Ihnen dabei, Sensitivitäts-Baselines für einzelne S3-Buckets festzulegen. Im Zuge der fortlaufenden, inkrementellen Analysen für Ihr Konto können Ihre Sensibilitätseinschätzungen einzelner Bereiche dann in einem vorhersehbaren Tempo immer detaillierter und detaillierter werden.

Definition des Umfangs der Analysen

Standardmäßig schließt Macie alle S3-Buckets ein, die es für Ihr Konto überwacht und analysiert, wenn es Ihre Inventardaten auswertet und S3-Objekte zur Analyse auswählt. Wenn Sie der Macie-Administrator einer Organisation sind, gehören dazu auch Buckets, die Ihren Mitgliedskonten gehören.

Sie können bestimmte S3-Buckets von den Analysen ausschließen. Sie könnten es beispielsweise vorziehen, Eimer auszuschließen, in denen normalerweise gespeichert wirdAWSProtokollierung von Daten, wieAWS CloudTrailEreignisprotokolle. Um einen Bucket auszuschließen, können Sie die Einstellungen für die automatische Erkennung vertraulicher Daten für Ihr Konto oder den Bucket ändern. Wenn Sie dies tun, beginnt Macie, den Bucket auszuschließen, wenn der nächste tägliche Auswertungs- und Analysezyklus beginnt. Sie können bis zu 1.000 Buckets von den Analysen ausschließen.

Wenn Sie einen Bucket ausschließen, können Sie ihn anschließend erneut einschließen. Ändern Sie dazu erneut die Einstellungen für die automatische Erkennung vertraulicher Daten für Ihr Konto oder den Bucket. Macie beginnt dann mit der Aufnahme des Buckets, wenn der nächste tägliche Auswertungs- und Analysezyklus beginnt.

Festlegen, welche Arten von sensiblen Daten erkannt und gemeldet werden sollen

Standardmäßig überprüft Macie S3-Objekte mithilfe des Satzes verwalteter Datenkennungen, die wir für die automatische Erkennung vertraulicher Daten empfehlen. Eine Liste dieser verwalteten Datenkennungen finden Sie unterStandardeinstellungen für die automatische Erkennung vertraulicher Daten.

Sie können die Analysen so anpassen, dass sie sich auf bestimmte Arten sensibler Daten konzentrieren. Ändern Sie dazu die Einstellungen für die automatische Erkennung vertraulicher Daten für Ihr Konto auf eine der folgenden Arten:

- Bestimmte Identifikatoren für verwaltete Daten hinzufügen oder entfernen — AIdentifier für verwaltete Datenist eine Reihe integrierter Kriterien und Techniken, die darauf ausgelegt sind, eine bestimmte Art von sensiblen Daten wie Kreditkartennummern zu erkennen,AWSgeheime Zugangsschlüssel oder Passnummern für ein bestimmtes Land oder eine bestimmte Region. Weitere Informationen finden Sie unter Verwenden von verwalteten Datenbezeichnern.

- Benutzerdefinierte Datenkennungen hinzufügen oder anschließend entfernen — Abenutzerdefinierter Datenbezeichnerist eine Reihe von Kriterien, die Sie definieren, um vertrauliche Daten zu erkennen. Mit benutzerdefinierten Datenkennungen können Sie sensible Daten erkennen, die die speziellen Szenarien Ihres Unternehmens, geistiges Eigentum oder proprietäre Daten wie Mitarbeiter-IDs, Kundenkontonummern oder interne Datenklassifizierungen widerspiegeln. Weitere Informationen finden Sie unter Erstellen von benutzerdefinierten Datenbezeichnern.
- Zulassungslisten hinzufügen oder anschließend entfernen — In Macie gibt eine Zulassungsliste Text oder ein Textmuster an, das Macie in S3-Objekten ignorieren soll. Dabei handelt es sich in der Regel um Ausnahmen für sensible Daten für Ihre speziellen Szenarien oder Umgebungen, wie öffentliche Namen oder Telefonnummern für Ihr Unternehmen oder Beispieldaten, die Ihre Organisation zum Testen verwendet. Weitere Informationen finden Sie unter Definition von Ausnahmen für sensible Daten mit Zulassungslisten.

Wenn Sie die Einstellungen ändern, wendet Macie Ihre Änderungen an, wenn der nächste tägliche Analysezyklus beginnt.

Sie können auch Einstellungen auf Bucket-Ebene anpassen, die festlegen, ob bestimmte Arten vertraulicher Daten in die Bewertung der Sensitivität eines Buckets einbezogen werden. Um zu erfahren wie dies geht, vgl. Verwaltung der automatisierten Erkennung vertraulicher Daten für einzelne S3-Buckets.

Berechnung der Sensitivitätswerte

Standardmäßig berechnet Macie automatisch einen Sensitivitätswert für jeden S3-Bucket, den es für Ihr Konto überwacht und analysiert. Wenn Sie der Macie-Administrator einer Organisation sind, gehören dazu auch Buckets, die Ihren Mitgliedskonten gehören.

In Macie,Empfindlichkeitswertist ein quantitatives Maß für den Schnittpunkt zweier Hauptdimensionen: der Menge vertraulicher Daten, die Macie in einem Bucket gefunden hat, und der Datenmenge, die Macie in einem Bucket analysiert hat. Der Sensitivitätswert eines Buckets bestimmt, welches Sensitivitätslabel Macie dem Bucket zuweist. EINEmpfindlichkeitslabelist eine qualitative Darstellung des Sensitivitätswerts eines Buckets — zum BeispielSensibel,Nicht empfindlich, undNoch nicht analysiert. Einzelheiten zu dem von Macie definierten Bereich der Empfindlichkeitswerte und Bezeichnungen finden Sie unterEmpfindlichkeitsbewertung für S3-Buckets.

> **Important**
>
> Der Sensitivitätswert und die Bezeichnung eines S3-Buckets deuten nicht auf die Wichtigkeit oder Bedeutung hin, die der Bucket oder die Objekte des Buckets für Ihr Unternehmen haben könnten. Stattdessen sollen sie Referenzpunkte bieten, anhand derer Sie potenzielle Sicherheitsrisiken erkennen und überwachen können.

Wenn Sie die automatische Erkennung vertraulicher Daten für Ihr Konto zum ersten Mal aktivieren, weist Macie automatisch einen Sensibilitätswert von50und derNoch nicht analysiertEtikett für jeden S3-Bucket. Die Ausnahme bilden leere Eimer. Einleerer Eimerist ein Bucket, der keine Objekte enthält oder alle Objekte des Buckets enthalten null (0) Byte an Daten. Wenn dies bei einem Bucket der Fall ist, weist Macie eine Punktzahl von zu1dem Bucket und es weist dieNicht empfindlichEtikett auf den Eimer.

Während die automatische Erkennung für Ihr Konto voranschreitet, aktualisiert Macie die Sensitivitätswerte und Labels entsprechend den Analyseergebnissen. Beispiele:

- Wenn Macie in einem Objekt keine vertraulichen Daten findet, verringert Macie den Sensitivitätswert des Buckets und aktualisiert die Sensitivitätsbezeichnung des Buckets nach Bedarf.
- Wenn Macie sensible Daten in einem Objekt findet, erhöht Macie den Sensitivitätswert des Buckets und aktualisiert die Sensitivitätsbezeichnung des Buckets nach Bedarf.
- Wenn Macie sensible Daten in einem Objekt findet, das anschließend geändert wurde, entfernt Macie die Erkennung vertraulicher Daten für das Objekt aus dem Sensitivitätswert des Buckets und aktualisiert die Sensitivitätsbezeichnung des Buckets nach Bedarf.
- Wenn Macie vertrauliche Daten in einem Objekt findet, das anschließend gelöscht wird, entfernt Macie die Erkennung vertraulicher Daten für das Objekt aus dem Sensitivitätswert des Buckets und aktualisiert die Sensitivitätskennzeichnung des Buckets nach Bedarf.

Sie können die Einstellungen für die Sensitivitätsbewertung für einzelne S3-Buckets anpassen, indem Sie bestimmte Arten vertraulicher Daten in die Bewertung eines Buckets einbeziehen oder ausschließen. Sie können die berechnete Punktzahl eines Buckets auch überschreiben, indem Sie die maximale Punktzahl manuell zuweisen (100) zum Eimer. Wenn Sie die maximale Punktzahl zuweisen, wird der Bucket beschriftetSensibel. Weitere Informationen finden Sie unter Verwaltung der automatisierten Erkennung für einzelne S3-Buckets.

Generierung von Metadaten, Statistiken und Ergebnissen

Wenn die automatische Erkennung vertraulicher Daten für Ihr Konto aktiviert ist, generiert und verwaltet Macie automatisch zusätzliche Inventardaten, Statistiken und andere Informationen über die S3-Buckets, die es für Ihr Konto überwacht und analysiert. Wenn Sie der Macie-Administrator einer Organisation sind, gehören dazu auch Buckets, die Ihren Mitgliedskonten gehören.

Die zusätzlichen Informationen erfassen die Ergebnisse der automatisierten Aktivitäten zur Erkennung vertraulicher Daten, die Macie bisher für Ihr Konto durchgeführt hat. Es ergänzt auch andere Informationen, die Macie über Ihre Amazon S3-Daten bereitstellt, z. B. die Einstellungen für den öffentlichen Zugriff und den gemeinsamen Zugriff für einzelne Buckets. Zu den zusätzlichen Informationen gehören:

- Aggregierte Statistiken zur Datensensitivität, z. B. die Gesamtzahl der Buckets, in denen Macie sensible Daten gefunden hat, und wie viele dieser Buckets öffentlich zugänglich sind.
- Eine interaktive, visuelle Darstellung der Datensensitivität in Ihrem Amazon S3-Datenbestand.
- Details auf Bucketebene, die den aktuellen Status der Analysen angeben, z. B. eine Liste der Objekte, die Macie in einem Bucket analysiert hat, die Typen sensibler Daten, die Macie in einem Bucket gefunden hat, und die Anzahl der Vorkommen jedes Typs vertraulicher Daten, die Macie gefunden hat.

Weitere Informationen finden Sie unter Überprüfung automatisierter Statistiken und Ergebnisse zur Erkennung sensibler Daten.

Zu den zusätzlichen Informationen gehören auch Statistiken und Details, anhand derer Sie die Reichweite Ihrer Amazon S3-Daten beurteilen und überwachen können. Sie können den Status der Analysen für Ihren Datenbestand insgesamt und für einzelne S3-Buckets in Ihrem Bucket-Inventar überprüfen. Sie können auch Probleme identifizieren, die Macie daran gehindert haben, Objekte in bestimmten Buckets zu analysieren. Wenn Sie die Probleme beheben, können Sie die Abdeckung Ihrer Amazon S3-Daten in den nachfolgenden Analysezyklen erhöhen. Weitere Informationen finden Sie unter Bewertung des Umfangs automatisierter Erkennung vertraulicher Daten.

Macie berechnet und aktualisiert diese Informationen automatisch neu und führt gleichzeitig eine automatische Erkennung vertraulicher Daten für Ihr Konto durch. Wenn Macie beispielsweise sensible Daten in einem Objekt findet, das anschließend geändert oder gelöscht wurde, aktualisiert Macie die Metadaten des entsprechenden Buckets: entfernt das Objekt aus der Liste der analysierten Objekte; entfernt sensible Daten, die Macie in dem Objekt gefunden hat;

berechnet den Sensitivitätswert neu, falls der Wert automatisch berechnet wird; und aktualisiert die Sensitivitätskennzeichnung nach Bedarf, um die neue Bewertung widerzuspiegeln.

Zusätzlich zu Metadaten und Statistiken erstellt Macie Aufzeichnungen über die sensiblen Daten, die es findet, und die Analysen, die es durchführt: Ergebnisse sensibler Daten, die Macie in einzelnen S3-Objekten findet, und vertrauliche Datenerfassungsergebnisse, in denen Details über die Analyse einzelner S3-Objekte protokolliert werden.

Überlegungen

Beachten Sie Folgendes, wenn Sie Amazon Macie verwenden, um die automatische Erkennung vertraulicher Daten für Ihre Amazon S3-Daten durchzuführen:

- Ihre Einstellungen für die automatische Erkennung gelten nur für die aktuelleAWS-Region. Folglich gelten die resultierenden Analysen und Daten nur für S3-Buckets und Objekte in der aktuellen Region. Um die automatische Erkennung durchzuführen und auf die resultierenden Daten in zusätzlichen Regionen zuzugreifen, aktivieren und konfigurieren Sie die automatische Erkennung in jeder weiteren Region.
- Wenn Sie der Macie-Administrator für eine Organisation sind:
  - Sie können die automatische Erkennung für ein Mitgliedskonto nur durchführen, wenn Macie für das Konto in der aktuellen Region aktiviert ist. Mitgliedskonten können keine automatische Erkennung für ihre eigenen Konten durchführen.
  - Mitgliedskonten können nicht auf automatische Discovery-Einstellungen zugreifen, die für ihre S3-Buckets gelten. Nur der Macie-Administrator kann auf diese Einstellungen zugreifen.
  - Mitgliedskonten können nicht auf Statistiken zur Erkennung vertraulicher Daten und andere Ergebnisse zugreifen, die Macie direkt für ihre S3-Buckets bereitstellt. Beispielsweise kann ein Mitgliedskonto die Amazon Macie-Konsole nicht verwenden, um die Sensibilitätswerte für seine S3-Buckets zu überprüfen. Nur der Macie-Administrator kann auf diese Daten zugreifen.
- Wenn die Berechtigungseinstellungen eines S3-Buckets Macie daran hindern, Informationen über den Bucket oder die Objekte des Buckets abzurufen oder darauf zuzugreifen, kann Macie keine automatische Erkennung für den Bucket durchführen. Macie kann nur einen Teil der Informationen über den Bucket bereitstellen, z. B. die Konto-ID für denAWS-Kontodem der Bucket gehört, der Name des Buckets und wann Macie zuletzt Bucket- und Objektmetadaten für den Bucket als Teil des abgerufen hattäglicher Auffrischungszyklus. In Ihrem Bucket-Inventar lautet der Sensitivitätswert für diese Buckets50und ihr Empfindlichkeitslabel istNoch nicht analysiert.

Um schnell S3-Buckets zu identifizieren, in denen dies der Fall ist, sehen Sie in Ihren Coverage-Daten zur automatisierten Erkennung nach. Weitere Informationen finden Sie unter Bewertung des Umfangs automatisierter Erkennung vertraulicher Daten. Um das Problem für einen bestimmten Bucket zu untersuchen, überprüfen Sie die Richtlinien- und Berechtigungseinstellungen des Buckets in Amazon S3. Beispielsweise könnte der Bucket eine restriktive Bucket-Richtlinie haben. Weitere Informationen finden Sie unter Macie den Zugriff von S3-Buckets und -Objekten erlauben.

- Um für die Auswahl und Analyse in Frage zu kommen, muss ein S3-Objektklassifizierbar. EINklassifizierbares Objektverwendet eine unterstützte Amazon S3-Speicherklasse und hat eine Dateinamenerweiterung für eine unterstützte Datei oder ein unterstütztes Speicherformat. Weitere Informationen finden Sie unter Unterstützte Speicherklassen und -formate.
- Wenn ein S3-Objekt verschlüsselt ist, kann Macie es nur analysieren, wenn es mit einem Schlüssel verschlüsselt ist, auf den Macie zugreifen kann und den er verwenden darf. Weitere Informationen finden Sie unter Analysieren verschlüsselter S3-Objekte. Informationen zu den Fällen, in denen die Verschlüsselungseinstellungen Macie daran hinderten, ein oder mehrere Objekte in einem Bucket zu analysieren, finden Sie in Ihren Coverage-Daten zur automatisierten Erkennung. Weitere Informationen finden Sie unter Bewertung des Umfangs automatisierter Erkennung vertraulicher Daten.

Konfiguration der automatischen Erkennung sensibler Daten für Ihr Konto

Mit der automatisierten Erkennung sensibler Daten wählt Amazon Macie kontinuierlich Beispielobjekte aus Ihren Amazon Simple Storage Service (Amazon S3) -Buckets aus und analysiert die Objekte, um festzustellen, ob sie sensible Daten enthalten. Wenn Sie der Macie-Administrator einer Organisation sind, umfasst dies auch Objekte in S3-Buckets, die Ihren Mitgliedskonten gehören. Im Verlauf der Analysen aktualisiert Macie Statistiken, Inventardaten und andere Informationen, die Macie zu Ihren Amazon S3 S3-Daten bereitstellt. Macie erstellt auch Aufzeichnungen über die sensiblen Daten, die es findet, und über die Analysen, die es durchführt.

Um die automatische Erkennung vertraulicher Daten konfigurieren und verwenden zu können, muss es sich bei Ihrem Konto um ein eigenständiges Macie-Konto oder um das Macie-Administratorkonto einer Organisation handeln. Wenn Sie über ein Mitgliedskonto verfügen und eine automatische Erkennung Ihrer S3-Buckets durchführen möchten, wenden Sie sich an den Macie-Administrator Ihrer Organisation. Weitere Informationen finden Sie unter Verwalten mehrerer Konten.

Themen

- Bevor Sie beginnen

- Aktivieren Sie die automatische Erkennung sensibler Daten für Ihr Konto
- Konfiguration der Einstellungen für die automatische Erkennung sensibler Daten für Ihr Konto
- Deaktivierung der automatischen Erkennung sensibler Daten für Ihr Konto

Wenn Sie die automatische Erkennung sensibler Daten für Ihr Konto aktivieren, konfigurieren oder deaktivieren, gelten Ihre Änderungen nur für das aktuelle Konto. AWS-Region Um dieselben Änderungen in weiteren Regionen vorzunehmen, wiederholen Sie die entsprechenden Schritte in jeder weiteren Region.

Bevor Sie beginnen

Bevor Sie die automatische Erkennung sensibler Daten für Ihr Konto konfigurieren, stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen verfügen. Stellen Sie außerdem sicher, dass Sie ein Repository für Ihre Ergebnisse der Erkennung sensibler Daten konfiguriert haben.

Um Ihre Berechtigungen zu überprüfen, verwenden Sie AWS Identity and Access Management (IAM), um die IAM-Richtlinien zu überprüfen, die mit Ihrer IAM-Identität verknüpft sind. Vergleichen Sie dann die Informationen in diesen Richtlinien mit der folgenden Liste von Aktionen, die Sie ausführen dürfen müssen:

- `macie2:GetMacieSession`
- `macie2:UpdateAutomatedDiscoveryConfiguration`

Mit der ersten Aktion können Sie auf Ihr Amazon Macie Macie-Konto zugreifen. Mit der zweiten Aktion können Sie die Konfigurationseinstellungen für die automatische Erkennung sensibler Daten für Ihr Konto ändern. Dies beinhaltet das Aktivieren und Deaktivieren der Konfiguration. Stellen Sie optional sicher, dass Sie die `macie2:GetAutomatedDiscoveryConfiguration` Aktion auch ausführen dürfen. Mit dieser Aktion können Sie die aktuellen Konfigurationseinstellungen und den aktuellen Status der Konfiguration abrufen.

Überprüfen Sie nicht nur Ihre Berechtigungen, sondern stellen Sie auch sicher, dass Sie ein Repository zum Speichern Ihrer Discovery-Ergebnisse für sensible Daten konfiguriert haben. Ein Erkennungsergebnis vertraulicher Daten ist ein Datensatz, der Details zu der Analyse protokolliert, die Macie an einem S3-Objekt durchgeführt hat. Macie erstellt für jedes S3-Objekt, das es analysiert, ein Erkennungsergebnis für sensible Daten und führt gleichzeitig eine automatische Erkennung sensibler Daten durch. Dazu gehören Objekte, in denen Macie keine sensiblen Daten findet und die daher keine Ergebnisse für vertrauliche Daten liefern, sowie Objekte, die Macie aufgrund von Fehlern

oder Problemen wie Berechtigungseinstellungen nicht analysieren kann. Wenn Macie sensible Daten in einem Objekt findet, umfasst das Ergebnis der Erkennung sensibler Daten auch Daten aus dem entsprechenden Befund. Es enthält auch zusätzliche Informationen. Diese Ergebnisse liefern Ihnen Analyseaufzeichnungen, die für Prüfungen oder Untersuchungen zum Datenschutz hilfreich sein können.

Macie speichert Ihre Ergebnisse der Entdeckung sensibler Daten nur 90 Tage lang. Um auf die Ergebnisse zuzugreifen und sie langfristig zu speichern und aufzubewahren, konfigurieren Sie Macie so, dass die Ergebnisse in einem S3-Bucket gespeichert werden. Der Bucket kann als definitives, langfristiges Repository für all Ihre Erkennungsergebnisse sensibler Daten dienen.

Um zu überprüfen, ob Sie dieses Repository für Ihr Konto konfiguriert haben, wählen Sie im Navigationsbereich der Amazon Macie Macie-Konsole Discovery-Ergebnisse aus. Wenn Sie dies lieber programmgesteuert tun möchten, verwenden Sie den GetClassificationExportConfigurationBetrieb der Amazon Macie Macie-API. Informationen zur Konfiguration dieses Repositorys finden Sie unter. Speicherung und Beibehaltung der Erkennungsergebnisse von vertraulichen Daten

Wenn Sie das Repository konfiguriert haben, erstellt Macie einen Ordner mit dem Namen automated-sensitive-data-discoveryim Repository, wenn die automatische Erkennung sensibler Daten zunächst für Ihr Konto aktiviert ist. In diesem Ordner werden die Ergebnisse der Erkennung sensibler Daten gespeichert, die Macie bei der automatischen Erkennung für Ihr Konto erstellt.

Aktivieren Sie die automatische Erkennung sensibler Daten für Ihr Konto

Wenn Sie die automatische Erkennung sensibler Daten für Ihr Konto aktivieren, beginnt Amazon Macie, Ihre Amazon S3 S3-Inventardaten auszuwerten und derzeit AWS-Region weitere automatisierte Erkennungsaktivitäten für Ihr Konto durchzuführen. Abhängig von der Größe Ihres Amazon S3 S3-Datenbestands können Statistiken zur Erkennung sensibler Daten und andere Ergebnisse innerhalb von 48 Stunden nach Aktivierung der automatischen Erkennung für Ihr Konto angezeigt werden.

Gehen Sie wie folgt vor, um die automatische Erkennung sensibler Daten für Ihr Konto mithilfe der Amazon Macie Macie-Konsole zu aktivieren. Verwenden Sie den UpdateAutomatedDiscoveryConfigurationBetrieb der Amazon Macie Macie-API, um die automatische Erkennung programmgesteuert zu aktivieren.

Um die automatische Erkennung sensibler Daten für Ihr Konto zu aktivieren

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.

2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie die automatische Erkennung sensibler Daten aktivieren möchten.
3. Wählen Sie im Navigationsbereich unter Einstellungen die Option Automatisierte Erkennung aus.
4. Wählen Sie im Abschnitt Status die Option Aktivieren aus.
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie aktivieren aus.

Nachdem Sie die automatische Erkennung sensibler Daten aktiviert haben, überprüfen und konfigurieren Sie Ihre Einstellungen, um die Analysen zu verfeinern, die Macie anschließend durchführt.

Konfiguration der Einstellungen für die automatische Erkennung sensibler Daten für Ihr Konto

Wenn die automatische Erkennung sensibler Daten für Ihr Konto aktiviert ist, können Sie die Einstellungen für die automatische Erkennung für Ihr Konto anpassen, um die von Amazon Macie durchgeführten Analysen zu verfeinern. Diese Einstellungen geben an, welche S3-Buckets Sie in die Analysen einbeziehen möchten. Sie geben auch an, welche Arten und Vorkommen vertraulicher Daten Macie erkennen und melden soll — die verwalteten Datenkennungen, die benutzerdefinierten Datenkennungen und die Zulässigkeitslisten, die bei der Analyse von S3-Objekten verwendet werden sollen.

Standardmäßig führt Macie die automatische Erkennung sensibler Daten für alle S3-Buckets durch, die es für Ihr Konto überwacht und analysiert. Wenn Sie der Macie-Administrator einer Organisation sind, schließt dies auch S3-Buckets ein, die Ihren Mitgliedskonten gehören. Sie können bestimmte Buckets von den Analysen ausschließen. Sie können beispielsweise Buckets ausschließen, in denen normalerweise AWS Protokolldaten gespeichert werden, wie z. B. AWS CloudTrail Ereignisprotokolle. Wenn Sie einen Bucket ausschließen, können Sie ihn anschließend wieder einbeziehen.

Darüber hinaus analysiert Macie S3-Objekte, indem es nur den Satz verwalteter Datenbezeichner verwendet, den wir für die automatische Erkennung sensibler Daten empfehlen. Macie verwendet keine benutzerdefinierten Datenbezeichner und erlaubt auch keine von Ihnen definierten Listen. Um die Analysen anzupassen, können Sie Macie so konfigurieren, dass es spezifische Zulassungslisten, benutzerdefinierte Datenkennungen und verwaltete Datenkennungen verwendet.

Die folgenden Abschnitte enthalten zusätzliche Informationen zu den einzelnen Einstellungstypen und erklären, wie Sie eine Einstellung mithilfe der Amazon Macie Macie-Konsole ändern können. Wählen Sie einen Abschnitt aus, um mehr zu erfahren. Um die Einstellungen programmgesteuert zu überprüfen oder zu ändern, können Sie die folgenden Operationen der Amazon Macie

Macie-API verwenden: UpdateClassificationScope, um anzugeben, welche S3-Buckets von den Analysen ausgeschlossen werden sollen, und, um anzugeben, welche Zulassungslisten UpdateSensitivityInspectionTemplate, benutzerdefinierten Datenbezeichner und verwalteten Datenbezeichner verwendet werden sollen.

Wenn Sie eine Einstellung ändern, wendet Macie Ihre Änderung an, wenn der nächste Bewertungs- und Analysezyklus für die automatische Erkennung sensibler Daten beginnt, normalerweise innerhalb von 24 Stunden.

Schließen Sie S3-Buckets aus oder beziehen Sie sie in die Analysen ein

Standardmäßig führt Macie die automatische Erkennung sensibler Daten für alle S3-Buckets durch, die es für Ihr Konto überwacht und analysiert. Wenn Sie der Macie-Administrator einer Organisation sind, schließt dies auch S3-Buckets ein, die Ihren Mitgliedskonten gehören. Um den Umfang zu verfeinern, können Sie bis zu 1.000 Buckets von den Analysen ausschließen.

Wenn Sie einen S3-Bucket ausschließen, beendet Macie die Analyse der Objekte im Bucket, wenn die automatische Erkennung sensibler Daten für Ihr Konto durchgeführt wird. Bestehende Statistiken zur Erkennung sensibler Daten und Details für den Bucket bleiben bestehen. Beispielsweise bleibt der aktuelle Sensibilitätswert des Buckets unverändert. Nachdem Sie einen Bucket ausgeschlossen haben, können Sie ihn anschließend wieder aufnehmen.

Um bestimmte S3-Buckets auszuschließen oder einzubeziehen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie bestimmte S3-Buckets ausschließen oder in automatisierte Discovery-Analysen einbeziehen möchten.
3. Wählen Sie im Navigationsbereich unter Einstellungen die Option Automatisierte Erkennung aus. Die Seite Automatisierte Erkennung vertraulicher Daten wird mit Ihren aktuellen Einstellungen angezeigt. Auf dieser Seite werden im Abschnitt S3-Buckets S3-Buckets aufgeführt, die derzeit ausgeschlossen sind, oder es wird angegeben, dass alle Buckets derzeit enthalten sind.
4. Wählen Sie im Abschnitt S3-Buckets die Option Bearbeiten aus.
5. Führen Sie eine der folgenden Aktionen aus:

    - Um einen oder mehrere S3-Buckets auszuschließen, wählen Sie Buckets zur Ausschlussliste hinzufügen. Aktivieren Sie dann in der Tabelle S3-Buckets das Kontrollkästchen für jeden Bucket, den Sie ausschließen möchten. In der Tabelle sind alle S3-Buckets für Ihr Konto in der aktuellen Region aufgeführt.

- Um einen oder mehrere S3-Buckets einzubeziehen, die Sie zuvor ausgeschlossen haben, wählen Sie in der Ausschlussliste die Option Buckets entfernen aus. Aktivieren Sie dann in der S3-Bucket-Tabelle das Kontrollkästchen für jeden Bucket, den Sie einbeziehen möchten. In der Tabelle sind alle Buckets aufgeführt, die derzeit von der automatisierten Erkennung sensibler Daten ausgeschlossen sind.

Um bestimmte Buckets einfacher zu finden, geben Sie Suchkriterien in das Suchfeld über der Tabelle ein. Sie können die Tabelle auch nach dem Bucket-Namen sortieren.

6. Wenn Sie mit der Auswahl der Buckets fertig sind, wählen Sie Hinzufügen oder Entfernen, je nachdem, welche Option Sie im vorherigen Schritt ausgewählt haben.

Fügen Sie verwaltete Datenkennungen zu den Analysen hinzu oder entfernen Sie sie

Ein verwalteter Datenbezeichner besteht aus einer Reihe integrierter Kriterien und Techniken, mit denen ein bestimmter Typ sensibler Daten erkannt werden kann, z. B. Kreditkartennummern, AWS geheime Zugangsschlüssel oder Passnummern für ein bestimmtes Land oder eine bestimmte Region. Standardmäßig analysiert Macie S3-Objekte mithilfe der Gruppe verwalteter Datenkennungen, die wir für die automatische Erkennung sensibler Daten empfehlen. Eine Liste der in diesem Satz enthaltenen Identifikatoren finden Sie unter. Standardeinstellungen für die automatische Erkennung vertraulicher Daten

Sie können die Analysen so anpassen, dass sie sich auf bestimmte Typen vertraulicher Daten konzentrieren: Fügen Sie verwaltete Datenkennungen für die Arten von vertraulichen Daten hinzu, die Macie erkennen und melden soll, und entfernen Sie verwaltete Datenkennungen für die Typen vertraulicher Daten, die Macie nicht erkennen und melden soll. Wenn Sie eine verwaltete Daten-ID entfernen, hat Ihre Änderung keine Auswirkungen auf bestehende Statistiken und Details zur Erkennung sensibler Daten für Ihre S3-Buckets. Wenn Sie beispielsweise die verwaltete Daten-ID entfernen, die AWS geheime Zugriffsschlüssel erkennt, und Macie zuvor diese Art von sensiblen Daten in einem Bucket entdeckt hat, meldet Macie diese Erkennungen weiterhin für den Bucket.

> **Tip**
>
> Anstatt eine verwaltete Daten-ID aus nachfolgenden Analysen aller S3-Buckets zu entfernen, können Sie diese Art der Erkennung aus der Sensitivitätsbewertung für bestimmte Buckets ausschließen. Weitere Informationen finden Sie unter Verwaltung der automatisierten Erkennung vertraulicher Daten für einzelne S3-Buckets.

Um verwaltete Datenkennungen hinzuzufügen oder zu entfernen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie verwaltete Datenkennungen hinzufügen oder aus automatisierten Discovery-Analysen entfernen möchten.
3. Wählen Sie im Navigationsbereich unter Einstellungen die Option Automatisierte Erkennung aus. Auf der Seite Automatisierte Erkennung vertraulicher Daten werden im Abschnitt Verwaltete Datenkennungen Ihre aktuellen Einstellungen angezeigt, die in zwei Registerkarten unterteilt sind:

   - Zur Standardeinstellung hinzugefügt — Auf dieser Registerkarte werden verwaltete Datenkennungen aufgeführt, die Sie explizit hinzugefügt haben. Macie verwendet diese verwalteten Datenkennungen zusätzlich zu denen, die im Standardsatz enthalten sind und die Sie nicht explizit entfernt haben.
   - Aus der Standardeinstellung entfernt — Auf dieser Registerkarte werden verwaltete Datenkennungen aufgeführt, die Sie ausdrücklich entfernt haben. Macie verwendet diese verwalteten Datenkennungen nicht.
4. Wählen Sie im Abschnitt Verwaltete Datenkennungen die Option Bearbeiten aus.
5. Führen Sie eine der folgenden Aktionen aus:

   - Um eine oder mehrere verwaltete Datenkennungen hinzuzufügen, wählen Sie die Registerkarte Zur Standardeinstellung hinzugefügt. Aktivieren Sie dann in der Tabelle das Kontrollkästchen für jeden verwalteten Datenbezeichner, den Sie hinzufügen möchten. Wenn bereits ein Kontrollkästchen aktiviert ist, haben Sie diesen Bezeichner bereits hinzugefügt.
   - Um eine oder mehrere verwaltete Datenkennungen zu entfernen, wählen Sie die Registerkarte Aus Standard entfernt. Aktivieren Sie dann in der Tabelle das Kontrollkästchen für jeden verwalteten Datenbezeichner, den Sie entfernen möchten. Wenn bereits ein Kontrollkästchen aktiviert ist, haben Sie diesen Bezeichner bereits entfernt.

   Auf jeder Registerkarte wird in der Tabelle eine Liste aller verwalteten Datenkennungen angezeigt, die Macie derzeit bereitstellt. In der Tabelle beschreibt die ID jedes verwalteten Datenbezeichners den Typ der sensiblen Daten, für die der Identifier konzipiert ist, z. B. USA_PASSPORT_NUMBER für US-Passnummern. Um bestimmte verwaltete Datenkennungen einfacher zu finden, geben Sie Suchkriterien in das Suchfeld über der Tabelle ein. Sie können

die Tabelle auch sortieren, indem Sie eine Spaltenüberschrift auswählen. Einzelheiten zu den einzelnen Bezeichnern finden Sie unterVerwenden von verwalteten Datenbezeichnern.

6. Wählen Sie Save (Speichern) aus, wenn Sie fertig sind.

Fügen Sie benutzerdefinierte Datenkennungen zu den Analysen hinzu oder entfernen Sie sie

Ein benutzerdefinierter Datenbezeichner besteht aus einer Reihe von Kriterien, die Sie definieren, um vertrauliche Daten zu erkennen. Die Kriterien bestehen aus einem regulären Ausdruck (Regex), der ein zu suchendes Textmuster definiert und optional Zeichenfolgen und eine Näherungsregel zur Eingrenzung der Ergebnisse festlegt. Weitere Informationen hierzu finden Sie unter Erstellen von benutzerdefinierten Datenbezeichnern.

Standardmäßig verwendet Amazon Macie keine benutzerdefinierten Datenbezeichner, wenn es die automatische Erkennung sensibler Daten durchführt. Wenn Sie möchten, dass Macie bestimmte benutzerdefinierte Datenkennungen verwendet, können Sie sie zu den Analysen hinzufügen. Macie verwendet dann die benutzerdefinierten Datenkennungen zusätzlich zu allen verwalteten Datenkennungen, für deren Verwendung Sie Macie ebenfalls konfiguriert haben.

Wenn Sie den Analysen eine benutzerdefinierte Daten-ID hinzufügen, können Sie diese anschließend entfernen. Ihre Änderung wirkt sich nicht auf bestehende Statistiken und Details zur Erkennung sensibler Daten für Ihre S3-Buckets aus. Wenn Sie beispielsweise eine benutzerdefinierte Daten-ID entfernen, die zuvor Erkennungen für einen Bucket ausgelöst hat, meldet Macie diese Erkennungen weiterhin für den Bucket. Erwägen Sie jedoch, diese Art der Erkennung aus der Sensitivitätsbewertung für bestimmte Buckets auszuschließen, anstatt die Kennung aus nachfolgenden Analysen aller Buckets zu entfernen. Weitere Informationen finden Sie unter Verwaltung der automatisierten Erkennung vertraulicher Daten für einzelne S3-Buckets.

Um benutzerdefinierte Datenkennungen hinzuzufügen oder zu entfernen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie benutzerdefinierte Datenkennungen zu automatisierten Discovery-Analysen hinzufügen oder daraus entfernen möchten.
3. Wählen Sie im Navigationsbereich unter Einstellungen die Option Automatisierte Erkennung aus. Die Seite Automatisierte Erkennung vertraulicher Daten wird mit Ihren aktuellen Einstellungen angezeigt. Auf dieser Seite werden im Abschnitt Benutzerdefinierte Datenbezeichner benutzerdefinierte Datenbezeichner aufgeführt, die Sie hinzugefügt haben, oder es wird

darauf hingewiesen, dass Sie keine benutzerdefinierten Datenbezeichner für die automatische Erkennung ausgewählt haben.

4. Wählen Sie im Abschnitt Benutzerdefinierte Datenkennungen die Option Bearbeiten aus.
5. Führen Sie eine der folgenden Aktionen aus:

   - Um einen oder mehrere benutzerdefinierte Datenbezeichner hinzuzufügen, aktivieren Sie das Kontrollkästchen für jede benutzerdefinierte Daten-ID, die Sie hinzufügen möchten. Wenn bereits ein Kontrollkästchen aktiviert ist, haben Sie diesen Bezeichner bereits hinzugefügt.
   - Um einen oder mehrere benutzerdefinierte Datenbezeichner zu entfernen, deaktivieren Sie das Kontrollkästchen für jeden benutzerdefinierten Datenbezeichner, den Sie entfernen möchten. Wenn ein Kontrollkästchen bereits deaktiviert ist, verwendet Macie diesen Bezeichner derzeit nicht bei der automatischen Erkennung.

   > **Tip**
   >
   > Um die Einstellungen für eine benutzerdefinierte Daten-ID zu überprüfen oder zu testen, bevor Sie sie hinzufügen oder entfernen, wählen Sie das Linksymbol () neben dem Namen der Kennung. Macie öffnet eine Seite, auf der die Einstellungen der Kennung angezeigt werden.
   >
   > Sie können diese Seite auch verwenden, um den Identifier anhand von Beispieldaten zu testen. Geben Sie dazu bis zu 1.000 Zeichen Text in das Feld Beispieldaten ein und wählen Sie dann Test aus. Macie wertet die Beispieldaten anhand der Kennung aus und meldet dann die Anzahl der Treffer.

6. Wählen Sie Save (Speichern) aus, wenn Sie fertig sind.

Fügen Sie Zulassungslisten zu den Analysen hinzu oder entfernen Sie sie

In Amazon Macie definiert eine Zulassungsliste einen bestimmten Text oder ein Textmuster, das Macie ignorieren soll, wenn es S3-Objekte auf sensible Daten untersucht. Wenn Text mit einem Eintrag oder einem Muster in einer Zulassungsliste übereinstimmt, meldet Macie den Text nicht, auch wenn der Text den Kriterien einer verwalteten Daten-ID oder einer benutzerdefinierten Daten-ID entspricht. Weitere Informationen hierzu finden Sie unter Definition von Ausnahmen für sensible Daten mit Zulassungslisten.

Standardmäßig verwendet Macie bei der automatischen Erkennung vertraulicher Daten keine Zulassungslisten. Wenn Sie möchten, dass Macie bestimmte Zulassungslisten verwendet, können Sie sie zu den Analysen hinzufügen. Wenn Sie den Analysen eine Zulassungsliste hinzufügen, können Sie sie anschließend entfernen.

Um Zulassungslisten hinzuzufügen oder zu entfernen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie Zulassungslisten zu automatisierten Discovery-Analysen hinzufügen oder daraus entfernen möchten.
3. Wählen Sie im Navigationsbereich unter Einstellungen die Option Automatisierte Erkennung aus. Die Seite Automatisierte Erkennung vertraulicher Daten wird mit Ihren aktuellen Einstellungen angezeigt. Auf dieser Seite gibt der Abschnitt Zulassungslisten an, welche Zulassungslisten Sie hinzugefügt haben, oder es gibt an, dass Sie keine Zulassungslisten für die automatische Erkennung ausgewählt haben.
4. Wählen Sie im Abschnitt Zulassungslisten die Option Bearbeiten aus.
5. Führen Sie eine der folgenden Aktionen aus:

   - Um eine oder mehrere Zulassungslisten hinzuzufügen, aktivieren Sie das Kontrollkästchen für jede Zulassungsliste, die Sie hinzufügen möchten. Wenn bereits ein Kontrollkästchen aktiviert ist, haben Sie diese Liste bereits hinzugefügt.
   - Um eine oder mehrere Zulassungslisten zu entfernen, deaktivieren Sie das Kontrollkästchen für jede Zulassungsliste, die Sie entfernen möchten. Wenn ein Kontrollkästchen bereits deaktiviert ist, verwendet Macie diese Liste derzeit nicht für die automatische Erkennung.

   > **Tip**
   >
   > Um die Einstellungen für eine Zulassungsliste zu überprüfen, bevor Sie sie hinzufügen oder entfernen, wählen Sie das Linksymbol () neben dem Namen der Liste. Macie öffnet eine Seite, auf der die Einstellungen der Liste angezeigt werden.

6. Wählen Sie Save (Speichern) aus, wenn Sie fertig sind.

Deaktivierung der automatischen Erkennung sensibler Daten für Ihr Konto

Sie können die automatische Erkennung sensibler Daten für Ihr Konto jederzeit deaktivieren. Wenn Sie die automatische Erkennung sensibler Daten deaktivieren, beendet Macie die Durchführung aller automatisierten Erkennungsaktivitäten für Ihr Konto, bevor der nächste Bewertungs- und Analysezyklus beginnt, normalerweise innerhalb von 24 Stunden. Darüber hinaus verlieren Sie den Zugriff auf alle statistischen Daten, Inventardaten und andere Informationen, die Macie im Rahmen dieser Aktivitäten erstellt und direkt bereitgestellt hat. Ihr S3-Bucket-Inventar enthält beispielsweise keine Sensitivitätswerte und Visualisierungen mehr und analysiert auch keine Statistiken und Details für einzelne S3-Buckets mehr.

Sie können weiterhin auf die Ergebnisse sensibler Daten zugreifen, die Macie bei der automatischen Erkennung für Ihr Konto erstellt hat. Macie speichert Ihre Ergebnisse 90 Tage lang. Darüber hinaus bleiben Daten, die Sie gespeichert oder für andere veröffentlicht haben, AWS-Services intakt und sind nicht betroffen, wie z. B. die Ergebnisse der Entdeckung sensibler Daten in Amazon S3 und die Suche nach Ereignissen in Amazon EventBridge.

Wenn Sie die automatische Erkennung sensibler Daten für Ihr Konto deaktivieren, können Sie sie wieder aktivieren. Macie nimmt dann alle automatisierten Erkennungsaktivitäten für Ihr Konto wieder auf. Wenn Sie es innerhalb von 30 Tagen wieder aktivieren, erhalten Sie wieder Zugriff auf alle statistischen Daten, Inventardaten und andere Informationen, die Macie zuvor im Rahmen dieser Aktivitäten erstellt und direkt bereitgestellt hat. Wenn Sie es nicht innerhalb von 30 Tagen wieder aktivieren, löscht Macie die statistischen Daten und andere Informationen, die es zuvor erstellt und direkt bereitgestellt hat, dauerhaft.

Gehen Sie wie folgt vor, um die automatische Erkennung sensibler Daten für Ihr Konto mithilfe der Amazon Macie Macie-Konsole zu deaktivieren. Verwenden Sie den UpdateAutomatedDiscoveryConfigurationBetrieb der Amazon Macie Macie-API, um die automatische Erkennung programmgesteuert zu deaktivieren.

Um die automatische Erkennung sensibler Daten für Ihr Konto zu deaktivieren

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie die automatische Erkennung sensibler Daten deaktivieren möchten.
3. Wählen Sie im Navigationsbereich unter Einstellungen die Option Automatisierte Erkennung aus.
4. Wählen Sie im Abschnitt Status die Option Deaktivieren aus.
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie deaktivieren aus.

Verwaltung der automatisierten Erkennung vertraulicher Daten für einzelne S3-Buckets

Während Sie Ihre Statistiken und Ergebnisse zur automatischen Erkennung vertraulicher Daten überprüfen und auswerten, können Sie die Sensitivitätsbewertung und andere Einstellungen für einzelne Amazon Simple Storage Service (Amazon S3) -Buckets anpassen. Durch die Anpassung dieser Einstellungen können Sie die Sensitivitätsbeurteilungen Ihres Amazon S3-Datenbestands insgesamt und bestimmter Buckets innerhalb dieses Datenbestands optimieren. Sie können auch die Ergebnisse von Untersuchungen erfassen, die Sie für bestimmte Bereiche durchführen.

Sie können die Einstellungen für die automatische Erkennung vertraulicher Daten für einen S3-Bucket auf folgende Weise anpassen.

Weisen Sie einen Empfindlichkeitswert zu

Standardmäßig berechnet Amazon Macie automatisch den Sensitivitätswert eines Buckets. Die Bewertung basiert in erster Linie auf der Menge sensibler Daten, die Macie in einem Bucket gefunden hat, und auf der Datenmenge, die Macie in einem Bucket analysiert hat. Weitere Informationen finden Sie unter Empfindlichkeitsbewertung für S3-Buckets.

Sie können die berechnete Punktzahl eines Buckets überschreiben und die maximale Punktzahl manuell zuweisen (100), was auch gilt fürSensibelEtikett auf den Eimer. Wenn Sie dies tun, führt Macie weiterhin die automatische Erkennung für den Bucket durch. Nachfolgende Analysen haben jedoch keinen Einfluss auf die Punktzahl des Buckets. Um das Ergebnis erneut automatisch zu berechnen, ändern Sie die Einstellung erneut.

Bestimmte sensible Datentypen in den Sensitivitätswert ausschließen oder in diesen aufnehmen

Bei automatischer Berechnung basiert der Sensitivitätswert eines Buckets teilweise auf der Menge sensibler Daten, die Macie im Bucket gefunden hat. Dies ist hauptsächlich auf die Art und Anzahl der vertraulichen Datentypen zurückzuführen, die Macie im Bucket gefunden hat, sowie auf die Anzahl der Vorkommen der einzelnen Typen. Standardmäßig berücksichtigt Macie das Vorkommen aller Arten vertraulicher Daten, wenn es den Sensitivitätswert eines Buckets berechnet.

Sie können die Berechnung anpassen, indem Sie bestimmte Arten vertraulicher Daten in die Bewertung eines Buckets ausschließen oder einbeziehen. Wenn Macie beispielsweise Postanschriften in einem Bucket erkannt hat und Sie feststellen, dass dies akzeptabel ist, können Sie alle Vorkommen von Postanschriften von der Bewertung des Buckets ausschließen. Wenn Sie einen vertraulichen Datentyp ausschließen, untersucht Macie den Bucket weiterhin auf diesen

Datentyp und meldet gefundene Vorkommnisse. Diese Vorkommnisse wirken sich jedoch nicht auf die berechnete Punktzahl des Buckets aus. Um einen vertraulichen Datentyp wieder in den berechneten Speicher aufzunehmen, ändern Sie die Einstellung erneut.

Den Bucket in nachfolgende Analysen ausschließen oder einbeziehen

Standardmäßig führt Macie eine automatische Erkennung für alle S3-Buckets durch, die es für Ihr Konto überwacht und analysiert. Wenn Sie der Macie-Administrator einer Organisation sind, gehören dazu auch S3-Buckets, die Ihren Mitgliedskonten gehören. Sie können bestimmte Buckets von den Analysen ausschließen. Sie können beispielsweise Eimer ausschließen, in denen normalerweise gespeichert wirdAWSProtokollierung von Daten, wieAWS CloudTrailEreignisprotokolle.

Wenn Sie einen Bucket ausschließen, bleiben die vorhandenen Statistiken zur Erkennung vertraulicher Daten und Details für den Bucket erhalten. Beispielsweise bleibt der aktuelle Sensitivitätswert des Buckets unverändert. Macie beendet jedoch die Analyse von Objekten im Bucket, wenn es eine automatische Erkennung für Ihr Konto durchführt. Nachdem Sie einen Bucket ausgeschlossen haben, können Sie ihn anschließend erneut einschließen.

Wenn Sie eine Einstellung ändern, die sich auf den Sensitivitätswert eines S3-Buckets auswirkt, beginnt Macie sofort mit der Neuberechnung und Aktualisierung relevanter Statistiken zur Erkennung vertraulicher Daten und anderer Informationen, die es über Ihre Amazon S3-Daten bereitstellt. Wenn Sie beispielsweise einem Bucket die maximale Punktzahl zuweisen, erhöht Macie die Anzahl vonSensibelBuckets in aggregierten Statistiken für Ihr Konto.

Gehen Sie wie folgt vor, um eine Einstellung mithilfe der Amazon Macie-Konsole zu ändern. Um eine Einstellung programmgesteuert zu ändern, können Sie die folgenden Operationen der Amazon Macie-API verwenden:UpdateResourceProfile, um einem Bucket einen Sensitivitätswert zuzuweisen;UpdateResourceProfileDetections, sensible Datentypen auszuschließen oder nachträglich in die Bewertung eines Buckets aufzunehmen; undUpdateClassificationScopeum einen Bucket in nachfolgende Analysen auszuschließen oder einzubeziehen.

So ändern Sie die Einstellungen für die automatische Erkennung vertraulicher Daten für einen S3-Bucket

1. Öffnen Sie die Amazon Macie-Konsole unterhttps://console.aws.amazon.com/macie/.
2. Wählen Sie im NavigationsbereichS3-Eimer.
3. Auf derS3-EimerSeite, wählen Sie den S3-Bucket aus, dessen Einstellungen Sie ändern möchten. Sie können den Bucket auswählen, indem Sie entweder die Tabellenansicht

verwenden
( )
oder die interaktive Karte
( ).

4. Führen Sie im Detailbereich einen der folgenden Schritte aus:

   - Um den berechneten Wert zu überschreiben und dem Bucket manuell einen Sensitivitätswert zuzuweisen, aktivieren SieHöchstpunktzahl zuweisen(
     Dadurch ändert sich die Punktzahl des Buckets auf100und wendet dieSensibelEtikett auf den Eimer.

     Um eine Punktzahl zuzuweisen, die Macie automatisch berechnet, schalten Sie die Option ausHöchstpunktzahl zuweisen(
   - Um den Bucket von nachfolgenden Analysen auszuschließen, aktivieren SieVon der automatisierten Erkennung ausschließen(

     Wenn Sie den Bucket zuvor von Analysen ausgeschlossen haben, deaktivieren SieVon der automatisierten Erkennung ausschließen(
     um es wieder aufzunehmen.
   - Um das Vorkommen bestimmter Arten vertraulicher Daten auszuschließen oder in die Sensitivitätsbewertung des Buckets aufzunehmen, wählen Sie dieSensitivitätTab. In derErkennungenTabelle, aktivieren Sie das Kontrollkästchen für den vertraulichen Datentyp, den Sie ausschließen oder einschließen möchten. Dann, auf derAktionenMenü, wählenVom Ergebnis ausschließenum den Typ auszuschließen oder zu wählenIn die Partitur aufnehmenum den Typ einzubeziehen.

     In der Tabelle ist derVertraulicher DatentypDas Feld gibt den eindeutigen Identifier (ID) für den verwalteten Datenbezeichner an, der die Daten erkannt hat, oder den Namen der benutzerdefinierten Daten-ID, die die Daten erkannt hat. Die ID eines verwalteten Datenbezeichners beschreibt die Art der sensiblen Daten, die der Identifier erkennen soll, z. B.USA_REISEPASSNUMMERfür US-Passnummern. Einzelheiten zu den einzelnen verwalteten Datenkennungen finden Sie unterVerwenden von verwalteten Datenbezeichnern.

Wenn Sie eine Einstellung geändert haben, die sich auf den Sensitivitätswert des S3-Buckets auswirkt, beginnt Macie sofort mit der Neuberechnung und Aktualisierung relevanter Statistiken zur Erkennung vertraulicher Daten und anderer Informationen über den S3-Bucket.

Bewertung des Umfangs automatisierter Erkennung vertraulicher Daten

Während die automatische Erkennung vertraulicher Daten für Ihr Konto voranschreitet, stellt Amazon Macie Statistiken und Details bereit, anhand derer Sie den Umfang Ihres Amazon Simple Storage Service (Amazon S3) -Datenbestands beurteilen und überwachen können. Mit diesen Daten können Sie den Status der automatisierten Erkennung vertraulicher Daten für Ihren gesamten Datenbestand und für einzelne S3-Buckets in Ihrem Bucket-Inventar überprüfen. Sie können auch Probleme identifizieren, die Macie daran gehindert haben, Objekte in bestimmten Buckets zu analysieren. Wenn Sie die Probleme beheben, können Sie die Abdeckung Ihrer Amazon S3-Daten in den nachfolgenden Analysezyklen erhöhen.

Die Coverage-Daten bieten eine Momentaufnahme des aktuellen Status der automatisierten Erkennung vertraulicher Daten für Ihre S3-Buckets in der aktuellen AWS-Region Version. Wenn Sie der Macie-Administrator einer Organisation sind, gehören dazu auch S3-Buckets, die Ihren Mitgliedskonten gehören. Für jeden Bucket geben die Daten an, ob Probleme aufgetreten sind, als Macie versuchte, Objekte im Bucket zu analysieren. Wenn Probleme aufgetreten sind, geben die Daten die Art der einzelnen Probleme und in bestimmten Fällen die Anzahl der Vorfälle an. Die Daten werden aktualisiert, während die automatische Erkennung vertraulicher Daten für Ihr Konto täglich voranschreitet. Wenn Macie während eines täglichen Analysezyklus ein oder mehrere Objekte in einem Bucket analysiert oder versucht, diese zu analysieren, aktualisiert Macie die Abdeckung und andere Daten entsprechend den Ergebnissen.

Bei bestimmten Arten von Problemen können Sie die Daten für alle Ihre S3-Buckets zusammenfassen und optional zusätzliche Details zu jedem Bucket abrufen. Mithilfe von Deckungsdaten können Sie beispielsweise schnell alle Bereiche identifizieren, auf die Macie für Ihr Konto nicht zugreifen darf. Die Coverage-Daten berichten auch über aufgetretene Probleme auf Objektebene. Diese als Klassifikationsfehler bezeichneten Probleme hinderten Macie daran, bestimmte Objekte in einem Bucket zu analysieren. Sie können beispielsweise ermitteln, wie viele Objekte Macie in einem Bucket nicht analysieren konnte, weil die Objekte mit einem AWS Key Management Service (AWS KMS) -Schlüssel verschlüsselt sind, der nicht mehr verfügbar ist.

Wenn Sie die Amazon Macie-Konsole verwenden, um die Versicherungsdaten zu überprüfen, enthält Ihre Ansicht der Daten Hinweise zur Behebung der einzelnen Arten von Problemen. Die nachfolgenden Themen in diesem Abschnitt enthalten auch Anleitungen zur Problembehebung für jeden Typ.

Themen

- Überprüfung der Deckungsdaten zur automatisierten Erkennung vertraulicher Daten
- Behebung von Deckungsproblemen bei automatisierter Erkennung vertraulicher Daten
  - Zugriff verweigert
  - Klassifizierungsfehler: Ungültiger Inhalt
  - Klassifizierungsfehler: Ungültige Verschlüsselung
  - Klassifizierungsfehler: Ungültiger KMS-Schlüssel
  - Klassifizierungsfehler: Erlaubnis verweigert
  - Nicht klassifizierbar

Überprüfung der Deckungsdaten zur automatisierten Erkennung vertraulicher Daten

Um den Umfang der automatisierten Erkennung vertraulicher Daten für Ihr Konto zu überprüfen und zu bewerten, können Sie die Amazon Macie-Konsole oder die Amazon Macie-API verwenden. Sowohl die Konsole als auch die API stellen Daten bereit, die den aktuellen Status der Analysen für Ihre Amazon Simple Storage Service (Amazon S3) -Buckets angeben. AWS-Region Die Daten enthalten Informationen zu Problemen, die zu Lücken in den Analysen führen:

- S3-Buckets, auf die Macie nicht zugreifen darf. Macie kann keine Objekte in diesen Buckets analysieren, da die Berechtigungseinstellungen der Buckets Macie daran hindern, auf die Buckets und die Objekte der Buckets zuzugreifen.
- S3-Buckets, die keine klassifizierbaren Objekte speichern. Macie kann keine Objekte in diesen Buckets analysieren, da alle Objekte Amazon S3-Speicherklassen verwenden, die Macie nicht unterstützt, oder weil sie Dateinamenerweiterungen für Datei- oder Speicherformate haben, die Macie nicht unterstützt.
- S3-Buckets, die Macie aufgrund von Klassifizierungsfehlern auf Objektebene noch nicht analysieren konnte. Macie versuchte, ein oder mehrere Objekte in diesen Buckets zu analysieren. Macie konnte die Objekte jedoch aufgrund von Problemen mit den Berechtigungseinstellungen auf Objektebene, dem Objektinhalt oder den Kontingenten nicht analysieren.

Die Deckungsdaten werden aktualisiert, während die automatische Erkennung vertraulicher Daten für Ihr Konto täglich voranschreitet. Wenn Sie der Macie-Administrator einer Organisation sind, enthalten die Daten Informationen für S3-Buckets, die Ihren Mitgliedskonten gehören.

> **Note**
>
> Zu den Coverage-Daten gehören nicht explizit Ergebnisse von Aufträgen zur Erkennung vertraulicher Daten, die Sie erstellt und ausgeführt haben. Die Behebung von Deckungsproblemen, die sich auf die Ergebnisse der automatisierten Erkennung vertraulicher Daten auswirken, erhöht jedoch wahrscheinlich auch die Reichweite der Aufgaben zur Erkennung vertraulicher Daten, die Sie anschließend ausführen. Um den Versicherungsschutz für eine Stelle zu ermitteln, überprüfen Sie die Statistiken und Ergebnisse der Stelle. Wenn die Protokollereignisse eines Jobs oder andere Ergebnisse auf Probleme mit der Abdeckung hinweisen, können Ihnen die Anleitungen zur Problembehebung weiter unten in diesem Abschnitt helfen, einige der Probleme zu lösen.

Zur Überprüfung automatisierter Deckungsdaten zur Erkennung vertraulicher Daten

Sie können die Amazon Macie-Konsole oder die Amazon Macie-API verwenden, um die Deckungsdaten für Ihr Konto oder Ihre Organisation zu überprüfen. In der Konsole bietet eine einzige Seite eine einheitliche Ansicht der Coverage-Daten für alle Ihre S3-Buckets, einschließlich einer Zusammenfassung der Probleme, die kürzlich für jeden Bucket aufgetreten sind. Die Seite bietet auch Optionen zum Überprüfen von Datengruppen nach Problemtyp. Um Ihre Untersuchung von Problemen für bestimmte Buckets nachzuverfolgen, können Sie Daten von der Seite in eine Datei mit kommagetrennten Werten (CSV) exportieren.

Console

Gehen Sie wie folgt vor, um mithilfe der Amazon Macie-Konsole Daten zur automatischen Erkennung vertraulicher Daten zu überprüfen.

Um die Deckungsdaten zu überprüfen

1. Öffnen Sie die Amazon Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich die Option Resource coverage aus.
3. Wählen Sie auf der Seite Ressourcenabdeckung die Registerkarte für die Art der Deckungsdaten aus, die Sie überprüfen möchten:

- Alle — Listet alle S3-Buckets auf, die Macie für Ihr Konto überwacht und analysiert.

  Für jeden Bucket gibt das Feld Probleme an, ob Probleme Macie daran gehindert haben, Objekte im Bucket zu analysieren. Wenn der Wert für dieses Feld None ist, hat Macie mindestens eines der Objekte des Buckets analysiert oder Macie hat noch nicht versucht, eines der Objekte des Buckets zu analysieren. Wenn es Probleme gibt, gibt dieses Feld die Art der Probleme an und gibt an, wie die Probleme behoben werden können. Bei Klassifizierungsfehlern auf Objektebene kann es auch (in Klammern) angeben, wie oft der Fehler aufgetreten ist.

- Zugriff verweigert — Listet S3-Buckets auf, auf die Macie nicht zugreifen darf. Die Berechtigungseinstellungen für diese Buckets verhindern, dass Macie auf die Buckets und die Objekte der Buckets zugreift. Folglich kann Macie keine Objekte in diesen Buckets analysieren.

- Klassifizierungsfehler — Listet S3-Buckets auf, die Macie aufgrund von Klassifizierungsfehlern auf Objektebene noch nicht analysiert hat. Dies sind Probleme mit den Berechtigungseinstellungen auf Objektebene, Objektinhalten oder Kontingenten.

  Für jeden Bucket gibt das Feld Probleme die Art der einzelnen Fehlertypen an, die aufgetreten sind und Macie daran gehindert haben, ein Objekt im Bucket zu analysieren. Es zeigt auch, wie die einzelnen Fehlertypen behoben werden können. Je nach Fehler kann es auch (in Klammern) angeben, wie oft der Fehler aufgetreten ist.

- Nicht klassifizierbar — Listet S3-Buckets auf, die Macie nicht analysieren kann, da sie keine klassifizierbaren Objekte speichern. Alle Objekte in diesen Buckets verwenden nicht unterstützte Amazon S3-Speicherklassen oder haben Dateinamenerweiterungen für nicht unterstützte Datei- oder Speicherformate. Folglich kann Macie keine Objekte in diesen Buckets analysieren.

4. Um die unterstützenden Daten für einen S3-Bucket aufzuschlüsseln und zu überprüfen, wählen Sie den Namen des Buckets aus. Statistiken und andere Informationen zum Bucket finden Sie dann im Bereich mit den Bucket-Details.
5. Um die Tabelle in eine CSV-Datei zu exportieren, wählen Sie oben auf der Seite In CSV exportieren aus. Die resultierende CSV-Datei enthält eine Teilmenge von Metadaten für jeden S3-Bucket in der Tabelle, für bis zu 50.000 Buckets. Die Datei enthält ein Feld mit Coverage-Problemen. Der Wert für dieses Feld gibt an, ob Probleme Macie daran gehindert haben, Objekte im Bucket zu analysieren, und wenn ja, welche Art der Probleme waren.

API

Um die Deckungsdaten programmgesteuert zu überprüfen, geben Sie Filterkriterien in Abfragen an, die Sie mithilfe DescribeBucketsder Amazon Macie-API einreichen. Diese Operation gibt ein Array von Objekten zurück. Jedes Objekt enthält statistische Daten und andere Informationen über einen S3-Bucket, der den Filterkriterien entspricht.

Fügen Sie in die Filterkriterien eine Bedingung für die Art der Deckungsdaten ein, die Sie überprüfen möchten:

- Um Buckets zu identifizieren, auf die Macie aufgrund der Berechtigungseinstellungen der Buckets nicht zugreifen darf, fügen Sie eine Bedingung hinzu, bei der der Wert für das Feld gleich ist. `errorCode` `ACCESS_DENIED`
- Um Buckets zu identifizieren, auf die Macie zugreifen darf und die sie noch nicht analysiert hat, fügen Sie Bedingungen hinzu, bei denen der Wert für das `sensitivityScore` Feld gleich `50` und der Wert für das `errorCode` Feld ungleich ist. `ACCESS_DENIED`
- Um Buckets zu identifizieren, die Macie nicht analysieren kann, weil alle Objekte der Buckets nicht unterstützte Speicherklassen oder Formate verwenden, fügen Sie Bedingungen hinzu, bei denen der Wert für das `classifiableSizeInBytes` Feld gleich `0` und der Wert für das `sizeInBytes` Feld größer ist als. `0`
- Um Buckets zu identifizieren, für die Macie mindestens ein Objekt analysiert hat, schließen Sie Bedingungen ein, bei denen der Wert für das `sensitivityScore` Feld im Bereich von 1—99 liegt, aber nicht gleich ist. `50` Um auch Buckets einzubeziehen, denen Sie manuell die maximale Punktzahl zugewiesen haben, sollte der Bereich zwischen 1 und 100 liegen.
- Um Buckets zu identifizieren, die Macie aufgrund von Klassifizierungsfehlern auf Objektebene noch nicht analysiert hat, fügen Sie eine Bedingung hinzu, bei der der Wert für das Feld gleich ist. `sensitivityScore` `-1` Verwenden Sie den GetResourceProfileVorgang, um anschließend eine Aufschlüsselung der Typen und der Anzahl der Fehler zu überprüfen, die für einen bestimmten Bucket aufgetreten sind.

Wenn Sie die AWS Command Line Interface(AWS CLI) verwenden, geben Sie Filterkriterien in Abfragen an, die Sie einreichen, indem Sie den Befehl describe-buckets ausführen. Führen Sie den get-resource-profileBefehl aus, um eine Aufschlüsselung der Arten und der Anzahl der Fehler zu überprüfen, die für einen bestimmten S3-Bucket aufgetreten sind, sofern vorhanden.

Die folgenden AWS CLI Befehle verwenden beispielsweise Filterkriterien, um die Details aller S3-Buckets abzurufen, auf die Macie aufgrund der Berechtigungseinstellungen der Buckets nicht zugreifen darf.

Dieses Beispiel ist für Linux, macOS oder Unix formatiert:

```
$ aws macie2 describe-buckets --criteria '{"errorCode":{"eq":["ACCESS_DENIED"]}}'
```

Dieses Beispiel ist für Microsoft Windows formatiert:

```
C:\> aws macie2 describe-buckets --criteria={\"errorCode\":{\"eq\":[\"ACCESS_DENIED
\"]}}
```

Wenn Ihre Anfrage erfolgreich ist, gibt Macie ein `buckets` Array zurück. Das Array enthält ein Objekt für jeden S3-Bucket, der sich im aktuellen Bucket befindet AWS-Region und den Filterkriterien entspricht.

Wenn keine S3-Buckets den Filterkriterien entsprechen, gibt Macie ein leeres `buckets` Array zurück.

```
{
    "buckets": []
}
```

Weitere Informationen zur Angabe von Filterkriterien in Abfragen, einschließlich Beispielen für allgemeine Kriterien, finden Sie unterFiltern Ihres S3-Bucket-Inventars.

Behebung von Deckungsproblemen bei automatisierter Erkennung vertraulicher Daten

Amazon Macie meldet verschiedene Arten von Problemen, die den Umfang Ihrer Amazon Simple Storage Service (Amazon S3) -Daten durch die automatische Erkennung vertraulicher Daten einschränken. Die folgenden Informationen können Ihnen helfen, diese Probleme zu untersuchen und zu beheben.

Problemtypen und Details

- Zugriff verweigert
- Klassifizierungsfehler: Ungültiger Inhalt
- Klassifizierungsfehler: Ungültige Verschlüsselung

- Klassifizierungsfehler: Ungültiger KMS-Schlüssel
- Klassifizierungsfehler: Erlaubnis verweigert
- Nicht klassifizierbar

> **Tip**
>
> Um Klassifizierungsfehler auf Objektebene für einen S3-Bucket zu untersuchen, überprüfen Sie zunächst die Liste der Objektbeispiele für den Bucket. Diese Liste gibt an, welche Objekte Macie im Bucket analysiert oder zu analysieren versucht hat, für bis zu 100 Objekte. Um die Liste auf der Amazon Macie-Konsole zu überprüfen, wählen Sie den Bucket auf der Seite mit den S3-Buckets und dann im Bereich mit den Bucket-Details den Tab Objektbeispiele aus. Verwenden Sie die Amazon Macie-API, um die ListResourceProfileArtifactsListe programmgesteuert zu überprüfen. Wenn der Status der Analyse für ein Objekt Skipped (`SKIPPED`) lautet, hat das Objekt möglicherweise den Fehler verursacht.

Zugriff verweigert

Dieses Problem weist darauf hin, dass die Berechtigungseinstellungen eines S3-Buckets Macie daran hindern, auf den Bucket und die Objekte des Buckets zuzugreifen. Macie kann keine Objekte im Bucket abrufen und analysieren.

Details

Die häufigste Ursache für diese Art von Problem ist eine restriktive Bucket-Richtlinie. Eine Bucket-Richtlinie ist eine ressourcenbasierte AWS Identity and Access Management (IAM) -Richtlinie, die festlegt, welche Aktionen ein Principal (Benutzer, Konto, Dienst oder andere Entität) in einem S3-Bucket ausführen kann und unter welchen Bedingungen ein Principal diese Aktionen ausführen kann. Eine restriktive Bucket-Richtlinie verwendet explizite `Deny` Anweisungen `Allow` oder Anweisungen, die den Zugriff auf die Daten eines Buckets unter bestimmten Bedingungen gewähren oder einschränken. Eine Bucket-Richtlinie kann beispielsweise eine `Deny` ODER-Anweisung enthalten, die den Zugriff auf einen Bucket verweigert, sofern nicht bestimmte Quell-IP-Adressen für den Zugriff auf den Bucket verwendet werden. `Allow`

Wenn die Bucket-Richtlinie für einen S3-Bucket eine explizite `Deny` Anweisung mit einer oder mehreren Bedingungen enthält, darf Macie die Objekte des Buckets möglicherweise nicht abrufen

und analysieren, um vertrauliche Daten zu erkennen. Macie kann nur einen Teil der Informationen über den Bucket bereitstellen, z. B. den Namen und das Erstellungsdatum des Buckets.

Hinweise zur Problembehebung

Um dieses Problem zu beheben, aktualisieren Sie die Bucket-Richtlinie für den S3-Bucket. Stellen Sie sicher, dass die Richtlinie Macie den Zugriff auf den Bucket und die Objekte des Buckets ermöglicht. Um diesen Zugriff zuzulassen, fügen Sie der Richtlinie eine Bedingung für die dienstverknüpfte Macie-Rolle (`AWSServiceRoleForAmazonMacie`) hinzu. Diese Bedingung sollte verhindern, dass die dienstverknüpfte Macie-Rolle der `Deny` Einschränkung in der Richtlinie entspricht. Dazu verwendet es den `aws:PrincipalArn` globalen Bedingungskontextschlüssel und den Amazon-Ressourcennamen (ARN) der Macie-Rolle, die mit dem Service verknüpft ist, für Ihr Konto.

Wenn Sie die Bucket-Richtlinie aktualisieren und Macie Zugriff auf den S3-Bucket erhält, erkennt Macie die Änderung. In diesem Fall aktualisiert Macie Statistiken, Inventardaten und andere Informationen, die Macie über Ihre Amazon S3-Daten bereitstellt. Darüber hinaus wird den Objekten des Buckets in einem nachfolgenden Analysezyklus eine höhere Priorität für die Analyse eingeräumt.

Zusätzliche Referenz

Weitere Informationen zur Aktualisierung einer S3-Bucket-Richtlinie, um Macie den Zugriff auf einen Bucket zu ermöglichen, finden Sie unterErmöglichen Sie Amazon Macie den Zugriff auf S3-Buckets und -Objekte. Informationen zur Verwendung von Bucket-Richtlinien zur Steuerung des Zugriffs auf Buckets finden Sie unter Bucket-Richtlinien und Benutzerrichtlinien und Wie Amazon S3 eine Anfrage autorisiert im Amazon Simple Storage Service-Benutzerhandbuch.

Klassifizierungsfehler: Ungültiger Inhalt

Diese Art von Klassifizierungsfehler tritt auf, wenn Macie versucht, ein Objekt in einem S3-Bucket zu analysieren, und das Objekt falsch formatiert ist oder wenn das Objekt Inhalt enthält, der eine Quote für die Erkennung vertraulicher Daten überschreitet. Macie kann das Objekt nicht analysieren.

Details

Dieser Fehler tritt normalerweise auf, weil es sich bei einem S3-Objekt um eine falsch formatierte oder beschädigte Datei handelt. Folglich kann Macie nicht alle Daten in der Datei analysieren und analysieren.

Dieser Fehler kann auch auftreten, wenn die Analyse eines S3-Objekts die Quote für die Erkennung vertraulicher Daten für eine einzelne Datei überschreiten würde. Beispielsweise übersteigt die Speichergröße des Objekts das Größenkontingent für diesen Dateityp.

In beiden Fällen kann Macie die Analyse des S3-Objekts nicht abschließen und der Status der Analyse für das Objekt lautet Skipped ()`SKIPPED`.

Hinweise zur Problembehebung

Um diesen Fehler zu untersuchen, laden Sie das S3-Objekt herunter und überprüfen Sie die Formatierung und den Inhalt der Datei. Prüfen Sie außerdem den Inhalt der Datei anhand der Macie-Kontingente für die Erkennung vertraulicher Daten.

Wenn Sie diesen Fehler nicht beheben, versucht Macie, andere Objekte im S3-Bucket zu analysieren. Wenn Macie ein anderes Objekt erfolgreich analysiert, aktualisiert Macie die Coverage-Daten und andere Informationen, die Macie über den Bucket bereitstellt.

Zusätzliche Referenz

Eine Liste der Kontingente für die Erkennung vertraulicher Daten, einschließlich der Kontingente für bestimmte Dateitypen, finden Sie unter. Amazon Macie Macie-Kontingente Informationen darüber, wie Macie die Empfindlichkeitswerte aktualisiert, und andere Informationen, die es zu S3-Buckets bereitstellt, finden Sie unter. So funktioniert die automatische Erkennung vertraulicher Daten

Klassifizierungsfehler: Ungültige Verschlüsselung

Diese Art von Klassifizierungsfehler tritt auf, wenn Macie versucht, ein Objekt in einem S3-Bucket zu analysieren und das Objekt mit einem vom Kunden bereitgestellten Schlüssel verschlüsselt wird. Das Objekt verwendet SSE-C-Verschlüsselung, was bedeutet, dass Macie das Objekt nicht abrufen und analysieren kann.

Details

Amazon S3 unterstützt mehrere Verschlüsselungsoptionen für S3-Objekte. Bei den meisten dieser Optionen kann Macie ein Objekt entschlüsseln, indem er die mit dem Macie-Dienst verknüpfte Rolle für Ihr Konto verwendet. Dies hängt jedoch von der Art der verwendeten Verschlüsselung ab.

Damit Macie ein S3-Objekt entschlüsseln kann, muss das Objekt mit einem Schlüssel verschlüsselt werden, auf den Macie zugreifen kann und den er verwenden darf. Wenn ein Objekt

mit einem vom Kunden bereitgestellten Schlüssel verschlüsselt ist, kann Macie das erforderliche Schlüsselmaterial nicht bereitstellen, um das Objekt von Amazon S3 abzurufen. Folglich kann Macie das Objekt nicht analysieren und der Status der Analyse für das Objekt lautet Skipped ()`SKIPPED`.

Hinweise zur Problembehebung

Um diesen Fehler zu beheben, verschlüsseln Sie S3-Objekte mit von Amazon S3 verwalteten Schlüsseln oder AWS Key Management Service (AWS KMS) -Schlüsseln. Wenn Sie Schlüssel bevorzugen, können die Schlüssel AWS verwaltete KMS-Schlüssel oder kundenverwaltete KMS-Schlüssel sein, die Macie verwenden AWS KMS darf.

Um vorhandene S3-Objekte mit Schlüsseln zu verschlüsseln, auf die Macie zugreifen und die Macie verwenden kann, können Sie die Verschlüsselungseinstellungen für die Objekte ändern. Um neue Objekte mit Schlüsseln zu verschlüsseln, auf die Macie zugreifen und die Macie verwenden kann, ändern Sie die Standardverschlüsselungseinstellungen für den S3-Bucket. Stellen Sie außerdem sicher, dass die Richtlinie des Buckets nicht vorschreibt, dass neue Objekte mit einem vom Kunden bereitgestellten Schlüssel verschlüsselt werden.

Wenn Sie diesen Fehler nicht beheben, versucht Macie, andere Objekte im S3-Bucket zu analysieren. Wenn Macie ein anderes Objekt erfolgreich analysiert, aktualisiert Macie die Coverage-Daten und andere Informationen, die Macie über den Bucket bereitstellt.

Zusätzliche Referenz

Hinweise zu den Anforderungen und Optionen für die Verwendung von Macie zur Analyse verschlüsselter S3-Objekte finden Sie unterAnalysieren verschlüsselter Amazon S3-Objekte mit Amazon Macie. Informationen zu Verschlüsselungsoptionen und Einstellungen für S3-Buckets finden Sie im Amazon Simple Storage Service-Benutzerhandbuch unter Schützen von Daten durch Verschlüsselung und Festlegen des standardmäßigen serverseitigen Verschlüsselungsverhaltens für S3-Buckets.

Klassifizierungsfehler: Ungültiger KMS-Schlüssel

Diese Art von Klassifizierungsfehler tritt auf, wenn Macie versucht, ein Objekt in einem S3-Bucket zu analysieren und das Objekt mit einem AWS Key Management Service (AWS KMS) -Schlüssel verschlüsselt wird, der nicht mehr verfügbar ist. Macie kann das Objekt nicht abrufen und analysieren.

Details

AWS KMSbietet Optionen zum Deaktivieren und Löschen von AWS KMS keys Kundenverwaltungen. Wenn ein S3-Objekt mit einem deaktivierten KMS-Schlüssel verschlüsselt ist, für das Löschen geplant ist oder gelöscht wurde, kann Macie das Objekt nicht abrufen und entschlüsseln. Folglich kann Macie das Objekt nicht analysieren und der Status der Analyse für das Objekt lautet Skipped ()`SKIPPED`. Damit Macie ein verschlüsseltes Objekt analysieren kann, muss das Objekt mit einem Schlüssel verschlüsselt werden, auf den Macie zugreifen kann und den er verwenden darf.

Hinweise zur Problembehebung

Um diesen Fehler zu beheben, aktivieren Sie das geplante Löschen des entsprechenden Schlüssels erneut oder brechen Sie es abAWS KMS key, je nach aktuellem Status des Schlüssels. Wenn der entsprechende Schlüssel bereits gelöscht wurde, kann dieser Fehler nicht behoben werden.

Um festzustellen, welches Objekt zum Verschlüsseln eines S3-Objekts verwendet AWS KMS key wurde, können Sie zunächst Macie verwenden, um die serverseitigen Verschlüsselungseinstellungen für den S3-Bucket zu überprüfen. Wenn die Standardverschlüsselungseinstellungen für den Bucket so konfiguriert sind, dass sie einen KMS-Schlüssel verwenden, geben die Details des Buckets an, welcher Schlüssel verwendet wird. Sie können dann den Status dieses Schlüssels überprüfen. Alternativ können Sie Amazon S3 verwenden, um die Verschlüsselungseinstellungen für den Bucket und einzelne Objekte im Bucket zu überprüfen.

Wenn Sie diesen Fehler nicht beheben, versucht Macie, andere Objekte im S3-Bucket zu analysieren. Wenn Macie ein anderes Objekt erfolgreich analysiert, aktualisiert Macie die Coverage-Daten und andere Informationen, die Macie über den Bucket bereitstellt.

Zusätzliche Referenz

Hinweise zur Verwendung von Macie zur Überprüfung der serverseitigen Verschlüsselungseinstellungen für einen S3-Bucket finden Sie unter. Überprüfen der Details von S3-Buckets Informationen zur erneuten Aktivierung oder Stornierung des geplanten Löschvorgangs eines Schlüssels finden Sie im AWS KMS key Entwicklerhandbuch unter Schlüssel aktivieren und deaktivieren und Löschen von Schlüsseln planen und stornieren. AWS Key Management Service

Klassifizierungsfehler: Erlaubnis verweigert

Diese Art von Klassifizierungsfehler tritt auf, wenn Macie versucht, ein Objekt in einem S3-Bucket zu analysieren, und Macie das Objekt aufgrund der Berechtigungseinstellungen für das Objekt oder der Berechtigungseinstellungen für den Schlüssel, der zum Verschlüsseln des Objekts verwendet wurde, nicht abrufen oder entschlüsseln kann. Macie kann das Objekt nicht abrufen und analysieren.

Details

Dieser Fehler tritt normalerweise auf, weil ein S3-Objekt mit einem vom Kunden verwalteten AWS Key Management Service (AWS KMS) Schlüssel verschlüsselt ist, den Macie nicht verwenden darf. Wenn ein Objekt mit einem vom Kunden verwalteten Objekt verschlüsselt wirdAWS KMS key, muss die Richtlinie des Schlüssels es Macie ermöglichen, Daten mithilfe des Schlüssels zu entschlüsseln.

Dieser Fehler kann auch auftreten, wenn die Amazon S3-Berechtigungseinstellungen Macie daran hindern, ein S3-Objekt abzurufen. Die Bucket-Richtlinie für den S3-Bucket kann den Zugriff auf bestimmte Bucket-Objekte einschränken oder nur bestimmten Prinzipalen (Benutzern, Konten, Diensten oder anderen Entitäten) den Zugriff auf die Objekte ermöglichen. Oder die Zugriffskontrollliste (ACL) für ein Objekt schränkt möglicherweise den Zugriff auf das Objekt ein. Folglich darf Macie möglicherweise nicht auf das Objekt zugreifen.

In keinem der vorherigen Fälle kann Macie das Objekt abrufen und analysieren, und der Status der Analyse für das Objekt lautet Skipped ()`SKIPPED`.

Hinweise zur Problembehebung

Um diesen Fehler zu beheben, stellen Sie fest, ob das S3-Objekt mit einem vom Kunden verwalteten AWS KMS key Objekt verschlüsselt ist. Ist dies der Fall, stellen Sie sicher, dass die Richtlinie des Schlüssels es der dienstverknüpften Macie-Rolle (`AWSServiceRoleForAmazonMacie`) ermöglicht, Daten mit dem Schlüssel zu entschlüsseln. Wie Sie diesen Zugriff gewähren, hängt davon ab, ob das Konto, dem das gehört, AWS KMS key auch den S3-Bucket besitzt, in dem das Objekt gespeichert ist. Wenn dasselbe Konto den KMS-Schlüssel und den Bucket besitzt, muss ein Benutzer des Kontos die Richtlinie des Schlüssels aktualisieren. Wenn ein Konto den KMS-Schlüssel besitzt und ein anderes Konto den Bucket besitzt, muss ein Benutzer des Kontos, dem der Schlüssel gehört, kontenübergreifenden Zugriff auf den Schlüssel gewähren.

> **Tip**
>
> Sie können automatisch eine Liste aller verwalteten Kunden erstellen, auf AWS KMS keys die Macie zugreifen muss, um Objekte in den S3-Buckets für Ihr Konto zu analysieren. Führen Sie dazu das AWS KMS Permission Analyzer-Skript aus, das im Amazon Macie Scripts-Repository unter verfügbar ist. GitHub Das Skript kann auch ein zusätzliches Skript mit AWS Command Line Interface (AWS CLI) -Befehlen generieren. Sie können diese Befehle optional ausführen, um die erforderlichen Konfigurationseinstellungen und Richtlinien für von Ihnen angegebene KMS-Schlüssel zu aktualisieren.

Wenn Macie das entsprechende Objekt bereits verwenden darf AWS KMS key oder das S3-Objekt nicht mit einem vom Kunden verwalteten KMS-Schlüssel verschlüsselt ist, stellen Sie sicher, dass die Richtlinie des Buckets Macie den Zugriff auf das Objekt ermöglicht. Stellen Sie außerdem sicher, dass die ACL des Objekts es Macie ermöglicht, die Daten und Metadaten des Objekts zu lesen.

Für die Bucket-Richtlinie können Sie diesen Zugriff zulassen, indem Sie der Richtlinie eine Bedingung für die dienstverknüpfte Macie-Rolle hinzufügen. Diese Bedingung sollte verhindern, dass die dienstverknüpfte Macie-Rolle der `Deny` Einschränkung in der Richtlinie entspricht. Dazu verwendet es den `aws:PrincipalArn` globalen Bedingungskontextschlüssel und den Amazon-Ressourcennamen (ARN) der Macie-Rolle, die mit dem Service verknüpft ist, für Ihr Konto.

Für die Objekt-ACL können Sie diesen Zugriff gewähren, indem Sie mit dem Objekteigentümer zusammenarbeiten, um Sie AWS-Konto als Empfänger mit `READ` Berechtigungen für das Objekt hinzuzufügen. Macie kann dann die dienstverknüpfte Rolle für Ihr Konto verwenden, um das Objekt abzurufen und zu analysieren. Erwägen Sie auch, die Objektbesitzeinstellungen für den Bucket zu ändern. Sie können diese Einstellungen verwenden, um ACLs für alle Objekte im Bucket zu deaktivieren und dem Konto, dem der Bucket gehört, Eigentumsberechtigungen zu gewähren.

Wenn Sie diesen Fehler nicht beheben, versucht Macie, andere Objekte im S3-Bucket zu analysieren. Wenn Macie ein anderes Objekt erfolgreich analysiert, aktualisiert Macie die Coverage-Daten und andere Informationen, die Macie über den Bucket bereitstellt.

Zusätzliche Referenz

Weitere Informationen darüber, wie Macie Daten mit einem vom Kunden verwalteten Code entschlüsseln kannAWS KMS key, finden Sie unter. Amazon Macie erlauben, einen vom Kunden

verwalteten zu verwenden AWS KMS key Hinweise zur Aktualisierung einer S3-Bucket-Richtlinie, um Macie den Zugriff auf einen Bucket zu ermöglichen, finden Sie unterErmöglichen Sie Amazon Macie den Zugriff auf S3-Buckets und -Objekte.

Informationen zur Aktualisierung einer Schlüsselrichtlinie finden Sie unter Ändern einer Schlüsselrichtlinie im AWS Key Management ServiceEntwicklerhandbuch. Informationen zur vom Kunden verwalteten AWS KMS keys Verschlüsselung von S3-Objekten finden Sie unter Verwenden der serverseitigen Verschlüsselung mit AWS KMS Schlüsseln im Amazon Simple Storage Service-Benutzerhandbuch.

Informationen zur Verwendung von Bucket-Richtlinien zur Steuerung des Zugriffs auf S3-Buckets finden Sie unter Bucket-Richtlinien und Benutzerrichtlinien und Wie Amazon S3 eine Anfrage autorisiert im Amazon Simple Storage Service-Benutzerhandbuch. Informationen zur Verwendung von ACLs oder Objektbesitzeinstellungen zur Steuerung des Zugriffs auf S3-Objekte finden Sie im Amazon Simple Storage Service-Benutzerhandbuch unter Zugriff mit ACLs verwalten und Eigentümer von Objekten kontrollieren und ACLs für Ihren Bucket deaktivieren.

Nicht klassifizierbar

Dieses Problem weist darauf hin, dass alle Objekte in einem S3-Bucket mit nicht unterstützten Amazon S3-Speicherklassen oder nicht unterstützten Datei- oder Speicherformaten gespeichert werden. Macie kann keine Objekte im Bucket analysieren.

Details

Um für die Auswahl und Analyse in Frage zu kommen, muss ein S3-Objekt eine Amazon S3-Speicherklasse verwenden, die Macie unterstützt. Das Objekt muss auch eine Dateinamenerweiterung für ein Datei- oder Speicherformat haben, das Macie unterstützt. Wenn ein Objekt diese Kriterien nicht erfüllt, wird das Objekt als nicht klassifizierbares Objekt behandelt. Macie versucht nicht, Daten in nicht klassifizierbaren Objekten abzurufen oder zu analysieren.

Wenn alle Objekte in einem S3-Bucket nicht klassifizierbare Objekte sind, ist der gesamte Bucket ein nicht klassifizierbarer Bucket. Macie kann keine automatische Erkennung vertraulicher Daten für den Bucket durchführen.

Hinweise zur Problembehebung

Um dieses Problem zu beheben, überprüfen Sie die Lebenszykluskonfigurationsregeln und andere Einstellungen, die bestimmen, welche Speicherklassen zum Speichern von

Objekten im S3-Bucket verwendet werden. Erwägen Sie, diese Einstellungen anzupassen, um Speicherklassen zu verwenden, die Macie unterstützt. Sie können auch die Speicherklasse vorhandener Objekte im Bucket ändern.

Beurteilen Sie auch die Datei- und Speicherformate vorhandener Objekte im S3-Bucket. Um die Objekte zu analysieren, sollten Sie erwägen, die Daten vorübergehend oder dauerhaft auf neue Objekte zu übertragen, die ein unterstütztes Format verwenden.

Wenn Objekte zum S3-Bucket hinzugefügt werden und sie eine unterstützte Speicherklasse und ein unterstütztes Format verwenden, erkennt Macie die Objekte, wenn es Ihr Bucket-Inventar das nächste Mal auswertet. In diesem Fall meldet Macie nicht mehr, dass der Bucket in den Statistiken, Deckungsdaten und anderen Informationen, die er über Ihre Amazon S3-Daten bereitstellt, nicht klassifizierbar ist. Darüber hinaus wird den neuen Objekten in einem nachfolgenden Analysezyklus eine höhere Priorität bei der Analyse eingeräumt.

Zusätzliche Referenz

Informationen zu den Amazon S3-Speicherklassen und den von Macie unterstützten Datei- und Speicherformaten finden Sie unterVon Amazon Macie unterstützte Speicherklassen und -formate. Informationen zu den Lebenszykluskonfigurationsregeln und den von Amazon S3 bereitgestellten Speicherklassenoptionen finden Sie unter Verwaltung Ihres Speicherlebenszyklus und Verwenden von Amazon S3-Speicherklassen im Amazon Simple Storage Service-Benutzerhandbuch.

Überprüfung automatisierter Statistiken und Ergebnisse zur Erkennung sensibler Daten

Wenn die automatische Erkennung sensibler Daten für Ihr Konto aktiviert ist, generiert und verwaltet Amazon Macie automatisch zusätzliche Inventardaten, Statistiken und andere Informationen über die Amazon Simple Storage Service (Amazon S3) -Buckets, die es für Ihr Konto überwacht und analysiert. Wenn Sie der Macie-Administrator einer Organisation sind, schließt dies auch S3-Buckets ein, die Ihren Mitgliedskonten gehören.

Die zusätzlichen Informationen erfassen die Ergebnisse der automatisierten Aktivitäten zur Erkennung sensibler Daten, die Macie bisher für Ihr Konto durchgeführt hat. Es ergänzt auch andere Informationen, die Macie zu Ihren Amazon S3 S3-Daten bereitstellt, z. B. öffentliche Zugriffs- und Verschlüsselungseinstellungen für einzelne S3-Buckets. Zusätzlich zu Metadaten und Statistiken erstellt Macie Aufzeichnungen über die gefundenen sensiblen Daten und die durchgeführten Analysen — Ergebnisse sensibler Daten und Ergebnisse der Entdeckung sensibler Daten.

Während die automatische Erkennung sensibler Daten den Fortschritt Ihres Kontos analysiert, können Ihnen die folgenden Funktionen und Daten dabei helfen, die Ergebnisse zu überprüfen und auszuwerten:

- Übersichts-Dashboard — Bietet aggregierte Statistiken für Ihren Amazon S3 S3-Datenbestand. Die Statistiken enthalten Daten für wichtige Kennzahlen wie die Gesamtzahl der Buckets, in denen Macie sensible Daten gefunden hat, und wie viele dieser Buckets öffentlich zugänglich sind. Sie enthalten auch Daten zu Problemen, die sich auf die Abdeckung Ihres Datenbestands auswirken.
- S3-Buckets-Heatmap — Bietet eine interaktive, visuelle Darstellung der Datensensitivität in Ihrem gesamten Datenbestand, gruppiert AWS-Konto nach. Für jedes Konto enthält die Map aggregierte Sensitivitätsstatistiken und zeigt anhand von Farben den aktuellen Sensibilitätswert für jeden Bucket an, den das Konto besitzt. In der Karte werden außerdem Symbole verwendet, um Ihnen dabei zu helfen, Buckets zu identifizieren, die öffentlich zugänglich sind, von Macie nicht analysiert werden können und vieles mehr.
- Tabelle mit S3-Buckets — Bietet zusammenfassende Informationen für jeden S3-Bucket in Ihrem Inventar. Für jeden Bucket enthält die Tabelle Daten wie den Namen und die aktuelle Sensitivitätsbewertung des Buckets, die Anzahl der Objekte, die Macie im Bucket analysieren kann, und ob Sie irgendwelche Discovery-Jobs für sensible Daten konfiguriert haben, um Objekte im Bucket regelmäßig zu analysieren. Sie können optional Daten aus der Tabelle in eine Datei mit kommagetrennten Werten (CSV) exportieren.
- Bereich „Details“ — Enthält Details und Statistiken für einen S3-Bucket, den Sie in der Heatmap oder Tabelle auswählen. Zu den Details gehören eine Liste der Objekte, die Macie im Bucket analysiert hat, sowie eine Aufschlüsselung der Typen und der Anzahl der Vorkommen sensibler Daten, die Macie im Bucket gefunden hat. Sie können das Panel auch verwenden, um die Einstellungen für die automatische Erkennung für einzelne Buckets zu verwalten.
- Ergebnisse sensibler Daten — Stellen Sie detaillierte Berichte über sensible Daten bereit, die Macie in einzelnen S3-Objekten findet. Zu den Einzelheiten gehören, wann Macie die sensiblen Daten gefunden hat, sowie die Art und Anzahl der Vorkommen der sensiblen Daten, die Macie gefunden hat. Die Details enthalten auch Informationen über den betroffenen S3-Bucket und das betroffene S3-Objekt, einschließlich der Einstellungen für den öffentlichen Zugriff des Buckets und wann das Objekt zuletzt geändert wurde.
- Ergebnisse der Erkennung sensibler Daten — Stellen Sie Aufzeichnungen über die Analyse bereit, die Macie für einzelne S3-Objekte durchführt. Dazu gehören Objekte, in denen Macie keine sensiblen Daten findet und die daher keine Ergebnisse für sensible Daten liefern, sowie Objekte, die Macie aufgrund von Problemen oder Fehlern nicht analysieren kann.

Mit diesen Daten können Sie die Datensensitivität Ihres gesamten Amazon S3 S3-Datenbestands bewerten und einzelne S3-Buckets und Objekte detailliert auswerten und untersuchen. In Kombination mit den Informationen, die Macie zur Sicherheit und zum Datenschutz Ihrer Amazon S3 S3-Daten bereitstellt, können Sie auch Fälle identifizieren, in denen sofortige Abhilfemaßnahmen erforderlich sein könnten, z. B. ein öffentlich zugängliches Bucket, in dem Macie sensible Daten gefunden hat.

Zusätzliche Daten können Ihnen helfen, die Abdeckung Ihres Amazon S3 S3-Datenbestands zu beurteilen und zu überwachen. Mithilfe von Abdeckungsdaten können Sie den Status der Analysen für Ihren gesamten Datenbestand und für einzelne S3-Buckets in Ihrem Bucket-Inventar überprüfen. Sie können auch Probleme identifizieren, die Macie daran gehindert haben, Objekte in bestimmten Buckets zu analysieren. Wenn Sie die Probleme beheben, können Sie die Abdeckung Ihrer Amazon S3 S3-Daten in nachfolgenden Analysezyklen erhöhen. Weitere Informationen finden Sie unter Bewertung des Umfangs automatisierter Erkennung vertraulicher Daten.

Themen

- Überprüfung der aggregierten Statistiken zur Datensensitivität im Übersichts-Dashboard
- Visualisierung der Datensensitivität mit der S3-Buckets-Map
- Bewertung der Datensensitivität anhand der S3-Buckets-Tabelle
- Überprüfung der Details zur Datensensitivität für einzelne S3-Buckets
- Analyse sensibler Daten — Ergebnisse, die durch automatische Erkennung gewonnen wurden
- Zugriff auf Ergebnisse der Erkennung sensibler Daten, die durch automatische Erkennung generiert wurden

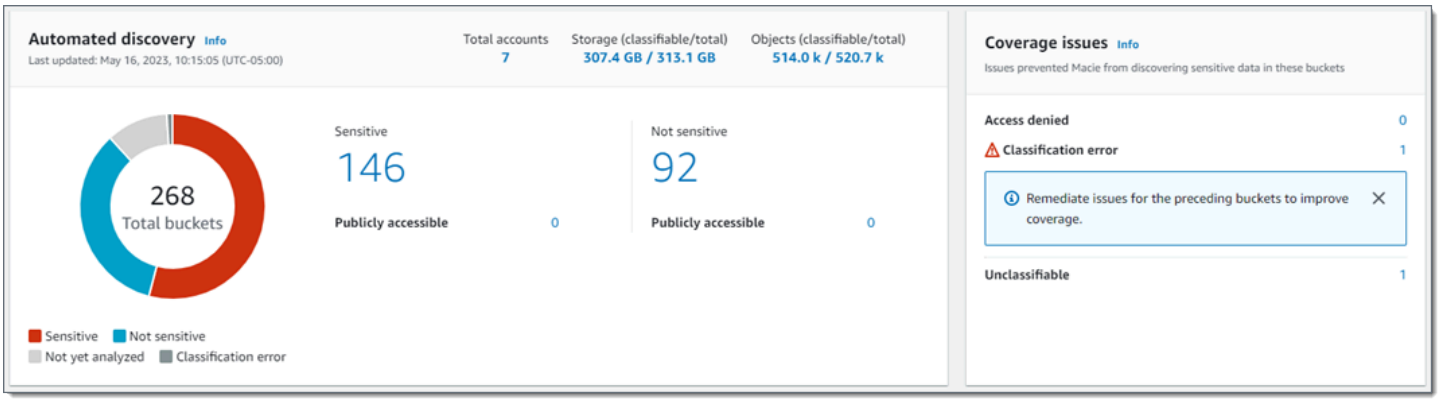
Überprüfung der aggregierten Statistiken zur Datensensitivität im Übersichts-Dashboard

In der Amazon Macie Macie-Konsole bietet das Übersichts-Dashboard eine Momentaufnahme der aggregierten Statistiken und Ergebnisdaten für Ihre aktuellen Amazon Simple Storage Service (Amazon S3) -Daten. AWS-Region Es soll Ihnen helfen, den allgemeinen Sicherheitsstatus Ihrer Amazon S3 S3-Daten zu beurteilen.

Die Dashboard-Statistiken enthalten Daten für wichtige Sicherheitsmetriken wie die Anzahl der S3-Buckets, auf die öffentlich zugegriffen werden kann oder die mit anderen AWS-Konten geteilt werden. Das Dashboard zeigt auch Gruppen von aggregierten Ergebnisdaten für Ihr Konto an, z. B. die S3-Buckets, die in den letzten sieben Tagen die meisten Ergebnisse generiert haben. Wenn Sie der

Macie-Administrator einer Organisation sind, bietet das Dashboard aggregierte Statistiken und Daten für alle Konten in Ihrer Organisation. Sie können die Daten optional nach Konto filtern.

Wenn die automatische Erkennung sensibler Daten für Ihr Konto aktiviert ist, enthält das Übersichts-Dashboard automatische Statistiken zur Erkennung sensibler Daten. Die Statistiken erfassen den Status und die Ergebnisse der automatisierten Erkennungsaktivitäten, die Macie bisher für Ihre Amazon S3 S3-Daten durchgeführt hat. Beispielsweise:



Die Statistiken im Abschnitt Automatisierte Erkennung bieten einen Überblick über den aktuellen Status und die Ergebnisse automatisierter Aktivitäten zur Erkennung sensibler Daten. Die Daten enthalten nicht die Ergebnisse von Aufträgen zur Erkennung sensibler Daten, die Sie erstellt und ausgeführt haben.

Statistiken im Abschnitt Probleme mit der Abdeckung geben Aufschluss darüber, ob Macie aufgrund von Problemen Objekte in einzelnen S3-Buckets nicht analysieren kann. Diese Statistiken enthalten nicht ausdrücklich Daten für Discovery-Jobs, die Sie erstellt und ausgeführt haben. Durch die Behebung von Deckungsproblemen, die sich auf Ihre Ergebnisse bei der automatisierten Erkennung vertraulicher Daten auswirken, wird jedoch wahrscheinlich auch die Abdeckung durch Jobs erhöht, die Sie anschließend ausführen.

Themen

- Das Übersichts-Dashboard anzeigen
- Grundlegendes zu Statistiken zur automatisierten Erkennung sensibler Daten im Übersichts-Dashboard

Das Übersichts-Dashboard anzeigen

Gehen Sie wie folgt vor, um das Übersichts-Dashboard auf der Amazon Macie Macie-Konsole anzuzeigen. Wenn Sie die Statistiken lieber programmgesteuert abfragen möchten, können Sie den GetBucketStatisticsBetrieb der Amazon Macie Macie-API verwenden.

Um das Übersichts-Dashboard anzuzeigen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich Zusammenfassung aus. Macie zeigt das Übersichts-Dashboard an.
3. Um die unterstützenden Daten für ein Element auf dem Dashboard aufzuschlüsseln und zu überprüfen, wählen Sie das Element aus.

Wenn Sie der Macie-Administrator einer Organisation sind, zeigt das Dashboard aggregierte Statistiken und Daten für Ihr Konto und Ihre Mitgliedskonten in Ihrer Organisation an. Um das Dashboard zu filtern und Daten nur für ein bestimmtes Konto anzuzeigen, geben Sie die Konto-ID in das Feld Konto über dem Dashboard ein.

Grundlegendes zu Statistiken zur automatisierten Erkennung sensibler Daten im Übersichts-Dashboard

Das Übersichts-Dashboard auf der Amazon Macie Macie-Konsole enthält aggregierte Statistiken, mit deren Hilfe Sie die automatische Erkennung sensibler Daten für Ihre Amazon S3 S3-Daten überwachen können. Mithilfe von Dashboard-Statistiken können Sie beispielsweise schnell ermitteln, in wie vielen S3-Buckets Amazon Macie sensible Daten gefunden hat und wie viele dieser Buckets öffentlich zugänglich sind. Das Dashboard bietet eine Momentaufnahme des aktuellen Status und der aktuellen Ergebnisse der Analysen Ihrer Amazon S3 S3-Daten AWS-Region.

Sie können auch Dashboard-Statistiken verwenden, um die Reichweite Ihrer Amazon S3 S3-Daten zu bewerten und Probleme zu identifizieren, die Macie daran hindern, Objekte in einzelnen S3-Buckets zu analysieren. Sie können beispielsweise feststellen, auf wie viele Buckets Macie für Ihr Konto nicht zugreifen darf.

Auf dem Dashboard sind die automatisierten Statistiken zur Erkennung sensibler Daten hauptsächlich in die folgenden Abschnitte unterteilt:

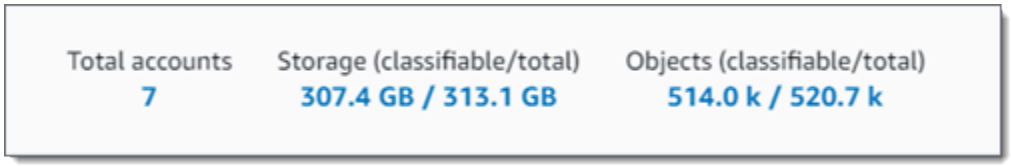
- Speicherung und Erkennung sensibler Daten

- Automatisierte Erkennung
- Probleme mit der Berichterstattung

Die einzelnen Statistiken in den einzelnen Abschnitten lauten wie folgt. Informationen zu Statistiken in anderen Abschnitten des Übersichts-Dashboards finden Sie unterGrundlegendes zu den Komponenten des Übersichts-Dashboards.

Speicherung und Erkennung sensibler Daten

Oben im Abschnitt Automatisierte Erkennung finden Sie Statistiken, die angeben, wie viele Daten Sie in Amazon S3 speichern und wie viele dieser Daten Macie analysieren kann, um sensible Daten zu erkennen. Beispielsweise:



In diesem Abschnitt:

- Konten insgesamt — Die Gesamtzahl AWS-Konten dieser eigenen Buckets in Ihrem S3-Bucket-Inventar. Wenn Sie der Macie-Administrator einer Organisation sind, ist dies die Gesamtzahl der Macie-Konten, die Sie für Ihre Organisation verwalten. Wenn Sie ein eigenständiges Macie-Konto haben, ist dieser Wert 1.
- Speicherung
  - Klassifizierbar — Die Gesamtspeichergröße aller Objekte, die Macie in den Buckets analysieren kann.
  - Insgesamt — Die Gesamtspeichergröße aller Objekte in den Buckets, einschließlich der Objekte, die Macie nicht analysieren kann.

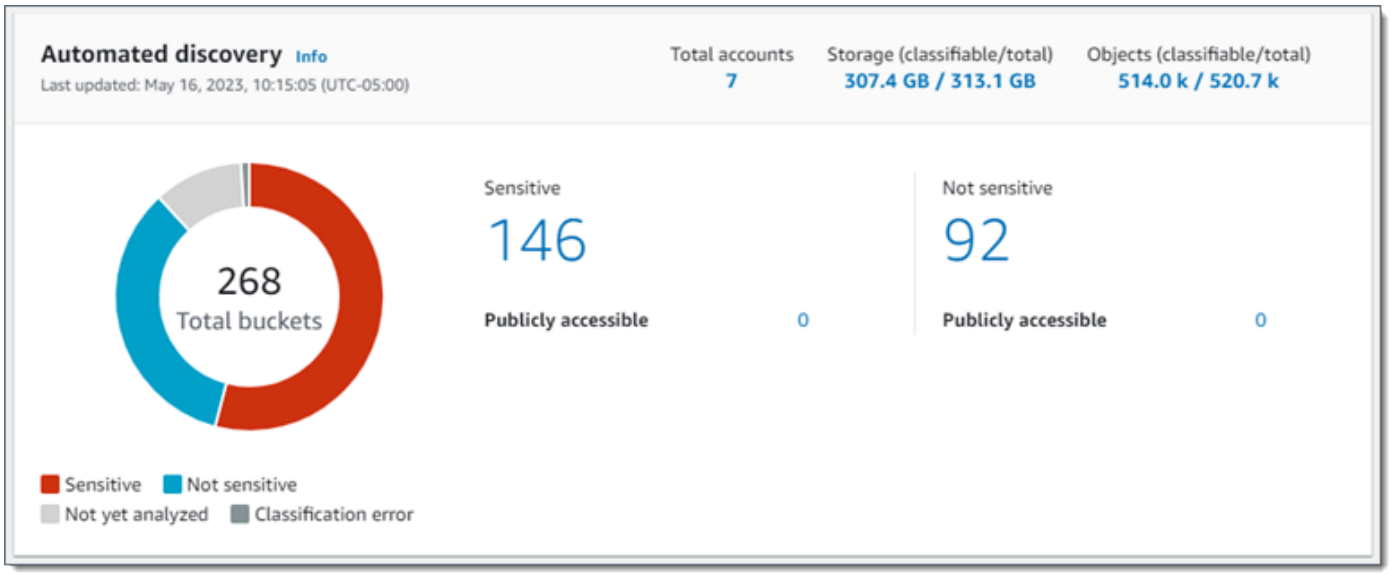
  Wenn es sich bei den Objekten um komprimierte Dateien handelt, geben diese Werte nicht die tatsächliche Größe dieser Dateien nach der Dekomprimierung wieder. Wenn die Versionsverwaltung für einen der Buckets aktiviert ist, basieren diese Werte auf der Speichergröße der neuesten Version jedes Objekts in diesen Buckets.
- Objekte
  - Klassifizierbar — Die Gesamtzahl der Objekte, die Macie in den Buckets analysieren kann.
  - Insgesamt — Die Gesamtzahl der Objekte in den Buckets, einschließlich der Objekte, die Macie nicht analysieren kann.

In den obigen Statistiken sind Daten und Objekte klassifizierbar, wenn sie eine unterstützte Amazon S3 S3-Speicherklasse verwenden und eine Dateinamenerweiterung für ein unterstütztes Datei- oder Speicherformat haben. Weitere Informationen finden Sie unter Unterstützte Speicherklassen und -formate.

Beachten Sie, dass die Speicher - und Objektstatistiken keine Daten über Objekte in Buckets enthalten, auf die Macie nicht zugreifen darf. Um Bereiche zu identifizieren, in denen dies der Fall ist, wählen Sie die Statistik Zugriff verweigert im Bereich Coverage issues des Dashboards aus.

Automatisierte Erkennung

Diese Statistiken erfassen in erster Linie den Status und die Ergebnisse der automatisierten Erkennungsaktivitäten, die Macie bisher für Ihre Amazon S3 S3-Daten durchgeführt hat. Beispielsweise:



Die einzelnen Statistiken in diesem Abschnitt lauten wie folgt.

Gesamtzahl der Buckets

Das Donut-Diagramm zeigt die Gesamtzahl der Buckets in Ihrem S3-Bucket-Inventar. Das Diagramm gruppiert die Buckets auf der Grundlage der aktuellen Sensitivitätsbewertung jedes Buckets in Kategorien:

- Sensitiv (rot) — Die Gesamtzahl der Buckets, deren Sensitivitätswert zwischen 51 und 100 liegt.
- Nicht empfindlich (blau) — Die Gesamtzahl der Buckets, deren Sensitivitätswert zwischen 1 und 49 liegt.

- Noch nicht analysiert (hellgrau) — Die Gesamtzahl der Buckets, deren Sensitivitätswert 50 ist.
- Klassifizierungsfehler (dunkelgrau) — Die Gesamtzahl der Buckets, deren Sensitivitätswert -1 ist.

Einzelheiten zum Bereich der Sensitivitätswerte und Bezeichnungen, die Macie definiert, finden Sie unter. Empfindlichkeitsbewertung für S3-Buckets

Um zusätzliche Statistiken für eine Gruppe anzuzeigen, bewegen Sie den Mauszeiger über die Gruppe:

- Buckets — Die Gesamtzahl der Buckets.
- Öffentlich zugänglich — Die Gesamtzahl der Buckets, die der Öffentlichkeit Lese- oder Schreibzugriff auf den Bucket ermöglichen.
- Klassifizierbare Byte — Die Gesamtspeichergröße aller Objekte, die Macie in den Buckets analysieren kann. Diese Objekte verwenden unterstützte Amazon S3 S3-Speicherklassen und haben Dateinamenerweiterungen für unterstützte Datei- oder Speicherformate. Weitere Informationen finden Sie unter Unterstützte Speicherklassen und -formate.
- Byte insgesamt — Die Gesamtspeichergröße aller Buckets.

In den vorherigen Statistiken basieren die Speichergrößenwerte auf der Speichergröße der neuesten Version jedes Objekts in den Buckets. Wenn es sich bei den Objekten um komprimierte Dateien handelt, geben diese Werte nicht die tatsächliche Größe dieser Dateien nach der Dekomprimierung wieder.

Sensibel

Dieser Bereich gibt die Gesamtzahl der S3-Buckets an, für die derzeit eine Sensitivitätsbewertung zwischen 51 und 100 vorliegt. Innerhalb dieser Gruppe gibt Öffentlich zugänglich die Gesamtzahl der Buckets an, die auch der Öffentlichkeit Lese- oder Schreibzugriff auf den Bucket ermöglichen.

Nicht sensibel

Dieser Bereich gibt die Gesamtzahl der S3-Buckets an, für die derzeit eine Sensitivitätsbewertung zwischen 1 und 49 vorliegt. Innerhalb dieser Gruppe gibt Öffentlich zugänglich die Gesamtzahl der Buckets an, die auch der Öffentlichkeit Lese- oder Schreibzugriff auf den Bucket ermöglichen.

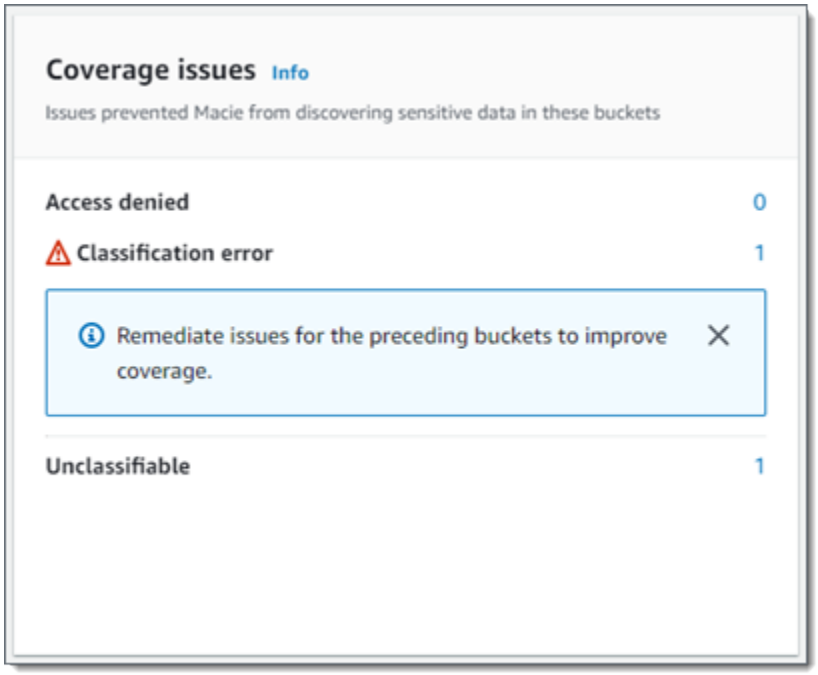
Um Werte für öffentlich zugängliche Statistiken zu ermitteln und zu berechnen, analysiert Macie für jeden Bucket eine Kombination von Einstellungen auf Konto- und Bucket-Ebene, wie z. B.

die Einstellungen zum Sperren des öffentlichen Zugriffs für das Konto und den Bucket und die Bucket-Richtlinie für den Bucket. Weitere Informationen finden Sie unter So überwacht Macie die Amazon S3 S3-Datensicherheit.

Beachten Sie, dass die Statistiken im Abschnitt Automatisierte Erkennung nicht die Ergebnisse von Discovery-Jobs für sensible Daten enthalten, die Sie erstellt und ausgeführt haben.

Probleme mit der Abdeckung

Diese Statistiken geben Aufschluss darüber, ob Macie aufgrund bestimmter Probleme Objekte in einzelnen S3-Buckets nicht analysieren kann. Beispielsweise:



In diesem Abschnitt:

- Zugriff verweigert — Die Gesamtzahl der Buckets, auf die Macie nicht zugreifen darf. Macie kann keine Objekte in diesen Buckets analysieren. Die Berechtigungseinstellungen der Buckets verhindern, dass Macie auf die Buckets und die Objekte der Buckets zugreift.
- Klassifizierungsfehler — Die Gesamtzahl der Buckets, die Macie aufgrund von Klassifizierungsfehlern auf Objektebene noch nicht analysiert hat. Macie hat versucht, ein oder mehrere Objekte in diesen Buckets zu analysieren. Macie konnte die Objekte jedoch aufgrund von Problemen mit den Berechtigungseinstellungen auf Objektebene, dem Objektinhalt oder den Kontingenten nicht analysieren.
- Nicht klassifizierbar — Die Gesamtzahl der Buckets, in denen keine klassifizierbaren Objekte gespeichert sind. Macie kann keine Objekte in diesen Buckets analysieren. Alle Objekte

verwenden Amazon S3 S3-Speicherklassen, die Macie nicht unterstützt, oder sie haben Dateinamenerweiterungen für Datei- oder Speicherformate, die Macie nicht unterstützt.

Wählen Sie den Wert für eine Statistik aus, um zusätzliche Details und gegebenenfalls Hinweise zur Problembehebung anzuzeigen. Wenn Sie Zugriffsprobleme und Klassifizierungsfehler beheben, können Sie die Abdeckung Ihrer Amazon S3 S3-Daten in nachfolgenden Analysezyklen erhöhen. Weitere Informationen finden Sie unter Bewertung des Umfangs automatisierter Erkennung vertraulicher Daten.

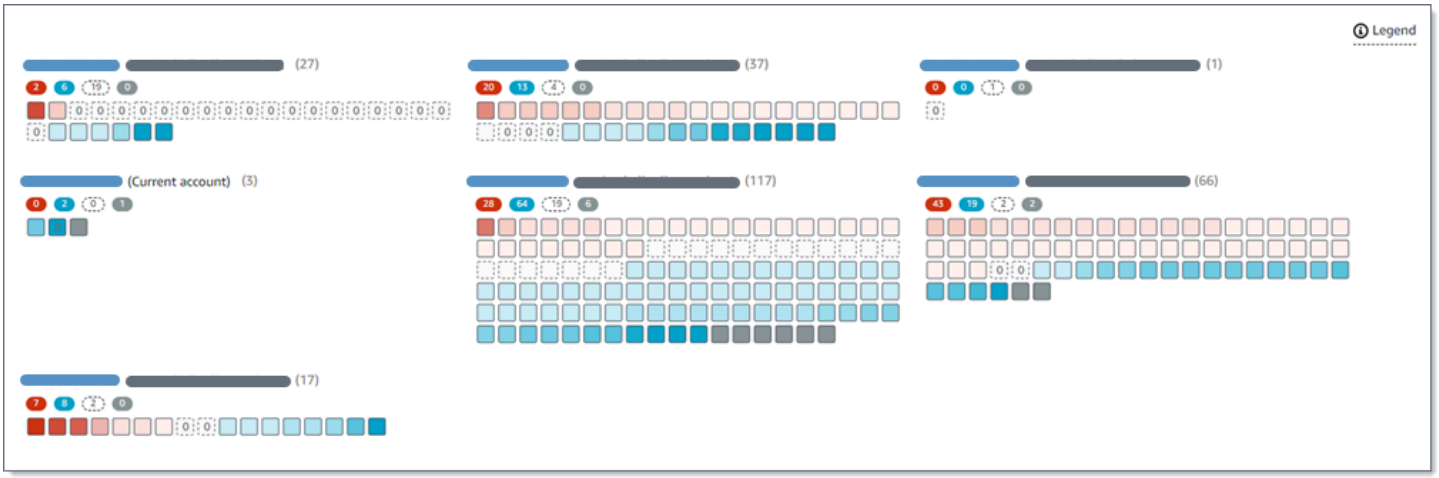
Beachten Sie, dass die Statistiken im Abschnitt Probleme mit der Abdeckung nicht ausdrücklich Daten für Discovery-Jobs enthalten, die Sie erstellt und ausgeführt haben. Durch die Behebung von Deckungsproblemen, die sich auf Ihre Ergebnisse bei der automatisierten Erkennung vertraulicher Daten auswirken, wird jedoch wahrscheinlich auch die Abdeckung durch Jobs erhöht, die Sie anschließend ausführen.

Informationen zu anderen Abschnitten des Übersichts-Dashboards finden Sie unterGrundlegendes zu den Komponenten des Übersichts-Dashboards.

Visualisierung der Datensensitivität mit der S3-Buckets-Map

Auf der Amazon Macie Macie-Konsole bietet die S3-Buckets-Heatmap eine interaktive, visuelle Darstellung der aktuellen Datensensitivität Ihres gesamten Amazon Simple Storage Service (Amazon S3) -Datenbestands. AWS-Region Sie erfasst die Ergebnisse automatisierter Aktivitäten zur Erkennung sensibler Daten, die Macie bisher für Ihr Konto durchgeführt hat.

Wenn Sie der Macie-Administrator einer Organisation sind, enthält die Map Ergebnisse für S3-Buckets, die Ihren Mitgliedskonten gehören, gruppiert AWS-Konto und sortiert nach Konto-ID. Beispielsweise:



Auf jeder Seite der Karte werden Daten für bis zu 99 Konten oder 1.000 Buckets angezeigt, abhängig von der Größe Ihrer Organisation oder Ihres Amazon S3 S3-Datenbestands.

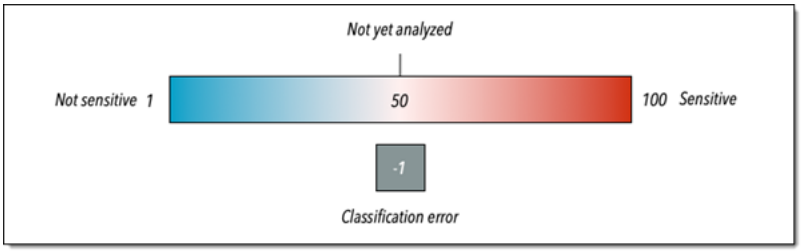
Um die Karte anzuzeigen, wählen Sie im Navigationsbereich der Konsole S3-Buckets aus. Wählen Sie dann oben auf der Seite Karte ( ).
Die Karte ist nur verfügbar, wenn die automatische Erkennung sensibler Daten derzeit für Ihr Konto aktiviert ist. Sie enthält keine Ergebnisse von Aufträgen zur Erkennung sensibler Daten, die Sie erstellt und ausgeführt haben.

Themen

- Interpretieren von Daten in der S3-Buckets-Map
- Interaktion mit der S3-Buckets-Map

Interpretieren von Daten in der S3-Buckets-Map

In der S3-Buckets-Map steht jedes Quadrat für einen S3-Bucket in Ihrem Bucket-Inventar. Die Farbe eines Quadrats steht für den aktuellen Sensitivitätswert eines Buckets, der den Schnittpunkt zweier primärer Dimensionen misst: die Menge sensibler Daten, die Macie in dem Bucket gefunden hat, und die Datenmenge, die Macie in dem Bucket analysiert hat. Die Intensität des Farbtons gibt an, wo der Punktewert eines Buckets innerhalb eines Bereichs von Datensensitivitätswerten liegt, wie in der folgenden Abbildung dargestellt.



Im Allgemeinen können Sie die Farb- und Farbtonintensität wie folgt interpretieren:

- Blau — Wenn der aktuelle Empfindlichkeitswert eines Buckets zwischen 1 und 49 liegt, ist das Quadrat des Buckets blau und das Empfindlichkeitslabel des Buckets ist Nicht sensitiv. Die Intensität des blauen Farbtons spiegelt die Anzahl der eindeutigen Objekte, die Macie im Bucket analysiert hat, im Verhältnis zur Gesamtzahl der eindeutigen Objekte im Bucket wider. Ein dunklerer Farbton weist auf einen niedrigeren Sensitivitätswert hin.

- Keine Farbe — Wenn der aktuelle Sensitivitätswert eines Buckets 50 ist, ist das Quadrat des Buckets nicht farbig und das Sensitivitätslabel des Buckets ist noch nicht analysiert. Darüber hinaus hat das Quadrat einen gestrichelten Rand.
- Rot — Wenn der aktuelle Empfindlichkeitswert eines Buckets zwischen 51 und 100 liegt, ist das Quadrat des Buckets rot und das Empfindlichkeitslabel des Buckets ist Sensitiv. Die Intensität des roten Farbtons spiegelt die Menge sensibler Daten wider, die Macie in dem Bucket gefunden hat. Ein dunklerer Farbton weist auf einen höheren Sensitivitätswert hin.
- Grau — Wenn der aktuelle Sensitivitätswert eines Buckets -1 ist, ist das Quadrat des Buckets dunkelgrau und die Sensitivitätsbezeichnung des Buckets lautet Classification error. Die Farbtonintensität variiert nicht.

Einzelheiten zu den von Macie definierten Empfindlichkeitswerten und Bezeichnungen finden Sie unterEmpfindlichkeitsbewertung für S3-Buckets.

In der Karte kann das Quadrat für einen S3-Bucket auch ein Symbol enthalten. Das Symbol weist auf einen Fehler, ein Problem oder eine andere Art von Überlegung hin, die sich auf Ihre Einschätzung der Sensitivität eines Buckets auswirken könnte. Ein Symbol kann auch auf ein potenzielles Problem mit der Sicherheit des Buckets hinweisen, z. B. wenn der Bucket öffentlich zugänglich ist. In der folgenden Tabelle sind die Symbole aufgeführt, die Macie verwendet, um Sie über diese Fälle zu informieren.

Symbol	Definition	Beschreibung
	Zugriff verweigert	Macie darf nicht auf den Bucket oder die Objekte des Buckets zugreifen. Folglich kann Macie keine Objekte im Bucket analysieren. Dieses Problem tritt normalerweise auf, weil für einen Bucket eine restriktive Bucket-Richtlinie gilt. Informationen zur Behebung dieses Problems finden Sie unterMacie den

Symbol	Definition	Beschreibung
		Zugriff von S3-Buckets und -Objekten erlauben.
	Öffentlich zugänglich	Die allgemeine Öffentlichkeit hat Lese- oder Schreibzugriff auf den Bucket. Um diese Entscheidung zu treffen, analysiert Macie für jeden Bucket eine Kombination von Einstellungen auf Konto- und Bucket-Ebene, z. B. die Einstellungen zum Sperren des öffentlichen Zugriffs für das Konto und den Bucket und die Bucket-Richtlinie für den Bucket. Weitere Informationen finden Sie unter So überwacht Macie die Amazon S3 S3-Datensicherheit.

Symbol	Definition	Beschreibung
?	Nicht klassifizierbar	Macie kann keine Objekte im Bucket analysieren. Alle Objekte des Buckets verwenden Amazon S3 S3-Speicherklassen, die Macie nicht unterstützt, oder sie haben Dateiname nerweiterungen für Datei- oder Speicherformate, die Macie nicht unterstützt. Damit Macie ein Objekt analysieren kann, muss das Objekt eine unterstützte Speicherklasse verwenden und eine Dateinamenerweiter ung für ein unterstütztes Datei- oder Speicherformat haben. Weitere Informationen finden Sie unter Unterstützte Speicherklassen und -formate.
0	Null Byte	Der Bucket enthält keine Objekte, die Macie analysier en könnte. Der Bucket ist leer oder alle Objekte im Bucket enthalten null (0) Datenbytes.

Interaktion mit der S3-Buckets-Map

Bei der Überprüfung der S3-Buckets-Map können Sie auf unterschiedliche Weise mit ihr interagieren, um zusätzliche Daten und Details für einzelne Konten und Buckets aufzudecken und auszuwerten. Gehen Sie wie folgt vor, um die Karte auf der Amazon Macie Macie-Konsole anzuzeigen und mit den verschiedenen Funktionen der Karte zu interagieren.

Um mit der S3-Buckets-Map zu interagieren

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich S3-Buckets aus. Auf der Seite S3-Buckets wird eine Übersicht Ihres Bucket-Inventars angezeigt. Wenn auf der Seite Ihr Inventar stattdessen im Tabellenformat angezeigt wird, wählen Sie oben auf der Seite Karte () aus.
3. Wählen Sie oben auf der Seite optional refresh (), um die neuesten Bucket-Metadaten von Amazon S3 abzurufen.
4. Führen Sie in der S3-Buckets-Map einen der folgenden Schritte aus:

   - Anhand der farbigen Markierungen direkt unter einer ID können Sie ermitteln, wie viele Buckets ein bestimmtes Sensibilitätslabel haben. AWS-Konto Die Badges zeigen die aggregierte Anzahl der Buckets an, aufgeschlüsselt nach Sensibilitätskennzeichen.

     Das rote Badge gibt beispielsweise die Gesamtzahl der Buckets an, die dem Konto gehören und die Kennzeichnung „Vertraulich“ tragen. Der Sensibilitätswert für diese Buckets reicht von 51 bis 100. Das blaue Abzeichen gibt die Gesamtzahl der Buckets an, die dem Konto gehören und die Kennzeichnung Nicht vertraulich tragen. Der Sensibilitätswert für diese Buckets reicht von 1 bis 49.

   - Um eine Teilmenge der Informationen zu einem Bucket zu überprüfen, bewegen Sie den Mauszeiger über das Quadrat des Buckets. In einem Popover werden der Name des Buckets und die aktuelle Vertraulichkeitsbewertung angezeigt.

     Das Popover zeigt auch die Gesamtzahl der Objekte, die Macie im Bucket analysieren kann, sowie die Gesamtspeichergröße der neuesten Version dieser Objekte an. Diese Objekte sind klassifizierbar. Sie verwenden unterstützte Amazon S3 S3-Speicherklassen und haben Dateinamenerweiterungen für unterstützte Datei- oder Speicherformate. Weitere Informationen finden Sie unter Unterstützte Speicherklassen und -formate.

   - Um die Map zu filtern und nur die Buckets anzuzeigen, die einen bestimmten Wert für ein Feld haben, platzieren Sie den Cursor in das Filterfeld und fügen Sie dann eine Filterbedingung für das Feld hinzu. Macie wendet die Kriterien der Bedingung an und zeigt die Bedingung unter dem Filterfeld an. Um die Ergebnisse weiter zu verfeinern, fügen Sie Filterbedingungen für weitere Felder hinzu. Weitere Informationen finden Sie unter Filtern Ihres S3-Bucket-Inventars.

- Um eine Aufschlüsselung durchzuführen und nur die Buckets anzuzeigen, die einem bestimmten Konto gehören, wählen Sie die Konto-ID für das Konto aus. Macie öffnet eine neue Registerkarte, auf der nur Daten für dieses Konto gefiltert und angezeigt werden.

5. Um alle Statistiken zur Entdeckung vertraulicher Daten und anderer Informationen zu überprüfen, die Macie zu einem bestimmten Bucket bereitstellt, wählen Sie das Quadrat des Buckets aus und schauen Sie dann im Detailbereich nach. Weitere Informationen finden Sie unter Überprüfung der Details zur Datensensitivität für einzelne S3-Buckets.

> **Tip**
>
> Auf der Registerkarte „Bucket-Details“ des Fensters können Sie viele Felder per Pivot und Drilldown betrachten. Um Buckets anzuzeigen, die denselben Wert für ein Feld haben, wählen Sie  in dem Feld die Option. Um Buckets anzuzeigen, die andere Werte für ein Feld haben, wählen Sie  in dem Feld aus.

Bewertung der Datensensitivität anhand der S3-Buckets-Tabelle

In der Amazon Macie Macie-Konsole werden in der Tabelle S3-Buckets zusammenfassende Informationen zu jedem Ihrer aktuellen Amazon Simple Storage Service (Amazon S3) -Buckets angezeigt. AWS-Region Wenn Sie der Macie-Administrator einer Organisation sind, gehören dazu auch Informationen zu S3-Buckets, die Ihren Mitgliedskonten gehören. Wenn Sie lieber programmgesteuert auf die Daten zugreifen möchten, können Sie den DescribeBucketsBetrieb der Amazon Macie Macie-API verwenden.

Auf der Konsole können Sie die Tabelle sortieren und filtern, um Ihre Ansicht anzupassen. Sie können auch Daten aus der Tabelle in eine Datei mit kommagetrennten Werten (CSV) exportieren. Wenn Sie in der Tabelle einen S3-Bucket auswählen, werden im Detailbereich zusätzliche Informationen zum Bucket angezeigt. Dazu gehören Details und Statistiken, die die Ergebnisse der automatisierten Aktivitäten zur Erkennung sensibler Daten erfassen, die Macie bisher für den Bucket durchgeführt hat. Es enthält auch Daten für Einstellungen und Metriken, die Aufschluss über die Sicherheit und den Datenschutz der Bucket-Daten geben. Sie können nicht nur die Details eines Buckets überprüfen, sondern auch den Bereich „Details“ verwenden, um die automatische Erkennung

sensibler Daten für den Bucket anzupassen. Um zu erfahren wie dies geht, vgl. Verwaltung der automatisierten Erkennung vertraulicher Daten für einzelne S3-Buckets.

Um die Datensensitivität anhand der S3-Bucket-Tabelle zu beurteilen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich S3-Buckets aus.
3. Wählen Sie auf der Seite S3-Buckets oben auf der Seite die Option Tabelle
   ()
   aus. Macie zeigt die Anzahl der Buckets in Ihrem Inventar und eine Tabelle der Buckets an.
4. Wählen Sie oben auf der Seite optional refresh
   (),
   um die neuesten Bucket-Metadaten von Amazon S3 abzurufen.

   Wenn das Informationssymbol
   ()
   neben Bucket-Namen angezeigt wird, empfehlen wir Ihnen, dies zu tun. Dieses Symbol weist darauf hin, dass in den letzten 24 Stunden ein Bucket erstellt wurde, möglicherweise nachdem Macie im Rahmen des täglichen Aktualisierungszyklus das letzte Mal Bucket- und Objektmetadaten von Amazon S3 abgerufen hat.
5. Sehen Sie sich in der Tabelle mit den S3-Buckets die zusammenfassenden Informationen zu jedem Bucket in Ihrem Inventar an:

   - Sensitivität — Der aktuelle Sensitivitätswert des Buckets. Informationen über den von Macie definierten Bereich der Sensitivitätswerte finden Sie unterEmpfindlichkeitsbewertung für S3-Buckets.
   - Bucket — Der Name des Buckets.
   - Konto — Die Konto-ID für den AWS-Konto , dem der Bucket gehört.
   - Klassifizierbare Objekte — Die Gesamtzahl der Objekte, die Macie analysieren kann, um sensible Daten im Bucket zu erkennen.
   - Klassifizierbare Größe — Die Gesamtspeichergröße aller Objekte, die Macie analysieren kann, um sensible Daten im Bucket zu erkennen.

     Dieser Wert gibt nicht die tatsächliche Größe komprimierter Objekte nach der Dekomprimierung wieder. Wenn die Versionierung für den Bucket aktiviert ist, basiert dieser Wert außerdem auf der Speichergröße der neuesten Version jedes Objekts im Bucket.

- Auftragsweise überwacht — Gibt an, ob alle Discovery-Jobs für sensible Daten so konfiguriert sind, dass Objekte im Bucket regelmäßig täglich, wöchentlich oder monatlich analysiert werden.

  Wenn der Wert für dieses Feld Ja lautet, ist der Bucket explizit in einem periodischen Job enthalten oder der Bucket hat innerhalb der letzten 24 Stunden die Kriterien für einen periodischen Job erfüllt. Darüber hinaus lautet der Status von mindestens einem dieser Jobs nicht Storniert. Macie aktualisiert diese Daten täglich.
- Letzte Auftragsausführung — Wenn einmalige oder regelmäßige Discovery-Jobs für sensible Daten so konfiguriert sind, dass Objekte im Bucket analysiert werden, gibt der Wert für dieses Feld das Datum und die Uhrzeit an, an dem einer dieser Jobs zuletzt gestartet wurde. Andernfalls ist dieses Feld leer.

In den obigen Daten sind Objekte klassifizierbar, wenn sie eine unterstützte Amazon S3 S3-Speicherklasse verwenden und eine Dateinamenerweiterung für ein unterstütztes Datei- oder Speicherformat haben. Mithilfe von Macie können Sie sensible Daten in den Objekten erkennen. Weitere Informationen finden Sie unter Unterstützte Speicherklassen und -formate.

6. Gehen Sie wie folgt vor, um Ihr Inventar anhand der Tabelle zu analysieren:

   - Um die Tabelle nach einem bestimmten Feld zu sortieren, klicken Sie auf die Spaltenüberschrift für das Feld. Um die Sortierreihenfolge zu ändern, klicken Sie erneut auf die Spaltenüberschrift.
   - Um die Tabelle zu filtern und nur die Buckets anzuzeigen, die einen bestimmten Wert für ein Feld haben, platzieren Sie den Cursor in das Filterfeld und fügen Sie dann eine Filterbedingung für das Feld hinzu. Macie wendet die Kriterien der Bedingung an und zeigt die Bedingung unter dem Filterfeld an. Um die Ergebnisse weiter zu verfeinern, fügen Sie Filterbedingungen für weitere Felder hinzu. Weitere Informationen finden Sie unter Filtern Ihres S3-Bucket-Inventars.
   - Um Details und Statistiken für einen bestimmten Bucket zu überprüfen, wählen Sie den Namen des Buckets in der Tabelle aus und gehen dann zum Detailbereich. Weitere Informationen finden Sie unter Überprüfung der S3-Bucket-Details.

   > **Tip**
   >
   > Auf der Registerkarte „Bucket-Details“ des Fensters können Sie viele Felder per Pivot und Drilldown betrachten. Um Buckets

anzuzeigen, die denselben Wert für ein Feld haben, wählen Sie

in dem Feld die Option. Um Buckets anzuzeigen, die andere Werte für ein Feld haben, wählen Sie

in dem Feld aus.

7. Um Daten aus der Tabelle in eine CSV-Datei zu exportieren, aktivieren Sie das Kontrollkästchen für jede Zeile, die Sie exportieren möchten, oder aktivieren Sie das Kontrollkästchen in der Überschrift der Auswahlspalte, um alle Zeilen auszuwählen. Wählen Sie dann oben auf der Seite Nach CSV exportieren aus. Sie können bis zu 50.000 Zeilen aus der Tabelle exportieren.
8. Um eine tiefere und unmittelbarere Analyse von Objekten in einem oder mehreren Buckets durchzuführen, aktivieren Sie das Kontrollkästchen für jeden Bucket und wählen Sie dann Job erstellen. Weitere Informationen finden Sie unter Erstellen einer Aufgabe zur Erkennung vertraulicher Daten.

Überprüfung der Details zur Datensensitivität für einzelne S3-Buckets

In der Amazon Macie Macie-Konsole können Sie den Detailbereich auf der Seite S3-Buckets verwenden, um Statistiken und andere Informationen zu einzelnen Amazon Simple Storage Service (Amazon S3) -Buckets einzusehen, die Macie für Ihr Konto überwacht und analysiert. Wenn Sie der Macie-Administrator einer Organisation sind, umfasst dies auch S3-Buckets, die Ihren Mitgliedskonten gehören.

Die Statistiken und Informationen enthalten Details, die Aufschluss über die Sicherheit und den Datenschutz der Daten eines S3-Buckets geben. Wenn die automatische Erkennung sensibler Daten für Ihr Konto aktiviert ist, erfassen sie auch die Ergebnisse der automatisierten Erkennungsaktivitäten, die Macie bisher für einen Bucket durchgeführt hat. Beispielsweise finden Sie in einem Bucket eine Liste von Objekten, die Macie analysiert hat, sowie eine Aufschlüsselung der Typen und der Anzahl der Vorkommen sensibler Daten, die Macie in einem Bucket gefunden hat. Beachten Sie, dass die Daten nicht die Ergebnisse von Discovery-Jobs für sensible Daten enthalten, die Sie erstellt und ausgeführt haben.

Macie berechnet und aktualisiert diese Statistiken und Details automatisch und führt gleichzeitig eine automatische Erkennung sensibler Daten für Ihr Konto durch. Beispielsweise:

- Wenn Macie keine sensiblen Daten in einem S3-Objekt findet, senkt Macie den Vertraulichkeitswert des Buckets und aktualisiert bei Bedarf das Vertraulichkeitslabel des Buckets. Macie fügt das Objekt auch der Liste der Objekte hinzu, die es im Bucket analysiert hat.
- Wenn Macie sensible Daten in einem S3-Objekt findet, fügt Macie diese Vorkommen der Aufschlüsselung der sensiblen Datentypen hinzu, die Macie im Bucket gefunden hat. Macie erhöht außerdem den Sensitivitätswert des Buckets und aktualisiert bei Bedarf das Sensitivitätslabel des Buckets. Darüber hinaus fügt Macie das Objekt der Liste der Objekte hinzu, die es im Bucket analysiert hat. Diese Aufgaben dienen zusätzlich zur Erstellung einer Suche nach sensiblen Daten für das Objekt.
- Wenn Macie sensible Daten in einem S3-Objekt findet, das anschließend geändert oder gelöscht wurde, entfernt Macie vertrauliche Datenvorkommen für dieses Objekt aus der Aufschlüsselung sensibler Datentypen im Bucket. Macie senkt außerdem den Sensitivitätswert des Buckets und aktualisiert bei Bedarf das Sensitivitätslabel des Buckets. Darüber hinaus entfernt Macie das Objekt aus der Liste der Objekte, die es im Bucket analysiert hat.
- Wenn Macie versucht, ein S3-Objekt zu analysieren, Macie jedoch aufgrund eines Problems oder Fehlers daran gehindert wird, fügt Macie das Objekt der Liste der Objekte hinzu, die im Bucket analysiert wurden, und gibt an, dass das Objekt nicht analysiert werden konnte.

Neben der Überprüfung von Statistiken und Details können Sie das Bedienfeld verwenden, um die Einstellungen für die automatische Erkennung sensibler Daten für einen S3-Bucket anzupassen. Sie können beispielsweise bestimmte Arten sensibler Daten in die Bewertung eines Buckets aufnehmen oder daraus ausschließen. Weitere Informationen finden Sie unter Verwaltung der automatisierten Erkennung für einzelne S3-Buckets.

Um die Details zur Datensensitivität für einen S3-Bucket zu überprüfen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich S3-Buckets aus. Auf der Seite S3-Buckets wird eine interaktive Karte Ihres Bucket-Inventars angezeigt. Wählen Sie optional Tabelle () oben auf der Seite aus, um Ihr Inventar stattdessen in tabellarischer Form anzuzeigen.
3. Wählen Sie in der Karte oder Tabelle der S3-Buckets den Namen des S3-Buckets aus, dessen Details Sie überprüfen möchten. Im Detailbereich werden Statistiken und andere Informationen zum Bucket angezeigt.

Im oberen Bereich des Fensters werden allgemeine Informationen zum Bucket angezeigt: der Name des Buckets und die Konto-ID des Buckets AWS-Konto , dem der Bucket gehört. Es bietet auch Optionen zum Ändern bestimmter Einstellungen für die automatische Erkennung sensibler Daten für den Bucket. Zusätzliche Einstellungen und Informationen zum Bucket sind in den folgenden Tabs organisiert:

- Sensitivität
- Einzelheiten zum Eimer
- Beispiele für Objekte
- Entdeckung sensibler Daten

Die einzelnen Einstellungen und Informationen auf jeder Registerkarte lauten wie folgt.

Empfindlichkeit

Auf dieser Registerkarte wird der aktuelle Sensitivitätswert des Buckets angezeigt, der zwischen -1 und 100 liegt. Informationen über den von Macie definierten Bereich der Sensitivitätswerte finden Sie unterEmpfindlichkeitsbewertung für S3-Buckets.

Die Registerkarte enthält auch eine Aufschlüsselung der Typen sensibler Daten, die Macie in den Objekten des Buckets gefunden hat, sowie die Anzahl der Vorkommen der einzelnen Typen:

- Vertraulicher Datentyp — Der eindeutige Bezeichner (ID) für den verwalteten Datenbezeichner, der die Daten erkannt hat, oder der Name des benutzerdefinierten Datenbezeichners, der die Daten erkannt hat.

  Die ID eines verwalteten Datenbezeichners beschreibt den Typ der sensiblen Daten, die mit dem Identifier erkannt werden sollen — zum Beispiel USA_PASSPORT_NUMBER für US-Passnummern. Einzelheiten zu den einzelnen verwalteten Datenkennungen finden Sie unter. Verwenden von verwalteten Datenbezeichnern
- Anzahl — Die Gesamtzahl der Vorkommen der Daten, die von der verwalteten oder benutzerdefinierten Daten-ID erkannt wurden.
- Bewertungsstatus — Gibt an, ob Vorkommen der Daten in die Vertraulichkeitsbewertung des Buckets ein- oder ausgeschlossen werden.

  Wenn Sie Macie so konfiguriert haben, dass der Bucket-Score automatisch berechnet wird, können Sie die Berechnung anpassen, indem Sie bestimmte Arten sensibler Daten in den Bucket-Score ein- oder ausschließen: Aktivieren Sie das Kontrollkästchen für die Daten-ID, die

Sie ein- oder ausschließen möchten, und wählen Sie dann im Menü Aktionen die gewünschte Option aus. Weitere Informationen finden Sie unter Verwaltung der automatisierten Erkennung für einzelne S3-Buckets.

Wenn Macie keine vertraulichen Daten in Objekten gefunden hat, die der Bucket derzeit speichert, wird in diesem Abschnitt die Meldung Keine Erkennungen gefunden angezeigt.

Beachten Sie, dass die Registerkarte „Sensitivität“ keine Daten für Objekte enthält, die Macie analysiert hat und die anschließend geändert oder gelöscht wurden. Wenn Objekte geändert oder aus einem Bucket gelöscht werden, nachdem Macie sie analysiert hat, berechnet Macie automatisch die entsprechenden Statistiken und Daten neu und aktualisiert sie, um die Objekte auszuschließen.

Einzelheiten zum Bucket

Auf dieser Registerkarte finden Sie Details zu den Einstellungen des Buckets, einschließlich der Einstellungen für Datensicherheit und Datenschutz. Sie können beispielsweise die Aufschlüsselung der öffentlichen Zugriffseinstellungen des Buckets überprüfen und feststellen, ob der Bucket Objekte repliziert oder mit anderen gemeinsam genutzt wird. AWS-Konten

Besonders hervorzuheben ist, dass das Feld Letzte Aktualisierung angibt, wann Macie zuletzt Metadaten von Amazon S3 für den Bucket oder die Objekte des Buckets abgerufen hat. Das Feld Letzte automatische Erkennungsausführung gibt an, wann Macie zuletzt Objekte im Bucket analysiert hat, während er die automatische Erkennung durchgeführt hat.

Die Registerkarte enthält auch Statistiken auf Objektebene, anhand derer Sie beurteilen können, wie viele Daten Macie im Bucket analysieren kann. Außerdem wird angezeigt, ob alle Discovery-Jobs für sensible Daten so konfiguriert sind, dass Objekte im Bucket analysiert werden. Wenn ja, können Sie auf Details zu dem Job zugreifen, der zuletzt ausgeführt wurde, und sich dann optional alle Ergebnisse anzeigen lassen, die der Job erbracht hat.

Weitere Informationen zu den Informationen auf dieser Registerkarte finden Sie unterÜberprüfen der Details von S3-Buckets.

Beispiele für Objekte

Auf dieser Registerkarte werden Objekte aufgeführt, die Macie im Bucket analysiert hat, während er die automatische Erkennung sensibler Daten durchgeführt hat. Wählen Sie optional den Namen eines Objekts, um die Amazon S3 S3-Konsole zu öffnen und die Eigenschaften des Objekts anzuzeigen.

Die Liste enthält Daten für bis zu 100 Objekte. Die Liste wird auf der Grundlage des Werts für das Feld Objektempfindlichkeit aufgefüllt: Sensitiv, gefolgt von Nicht sensibel, gefolgt von Objekten, die Macie nicht analysieren konnte.

In der Liste gibt das Feld Objektempfindlichkeit an, ob Macie sensible Daten in einem Objekt gefunden hat:

- Sensibel — Macie hat mindestens ein Vorkommen sensibler Daten in dem Objekt gefunden.
- Nicht sensibel — Macie hat keine sensiblen Daten im Objekt gefunden.
- — (Strich) — Macie konnte die Analyse des Objekts aufgrund eines Problems oder Fehlers nicht abschließen.

Das Feld Klassifizierungsergebnis gibt an, ob Macie ein Objekt analysieren konnte:

- Vollständig — Macie hat die Analyse des Objekts abgeschlossen.
- Teilweise — Macie hat aufgrund eines Problems oder Fehlers nur eine Teilmenge der Daten im Objekt analysiert. Das Objekt ist beispielsweise eine Archivdatei, die Dateien in einem nicht unterstützten Format enthält.
- Übersprungen — Macie konnte aufgrund eines Problems oder Fehlers keine Daten im Objekt analysieren. Das Objekt ist beispielsweise mit einem Schlüssel verschlüsselt, den Macie nicht verwenden darf.

Beachten Sie, dass die Liste keine Objekte enthält, die geändert oder gelöscht wurden, nachdem Macie sie analysiert oder versucht hat, sie zu analysieren. Macie entfernt ein Objekt automatisch aus der Liste, wenn das Objekt anschließend geändert oder gelöscht wird.

Entdeckung sensibler Daten

Auf dieser Registerkarte finden Sie aggregierte, automatisierte Statistiken zur Erkennung sensibler Daten für den Bucket:

- Analysierte Byte — Die Gesamtmenge der Daten in Byte, die Macie im Bucket analysiert hat.
- Klassifizierbare Byte — Die Gesamtspeichergröße aller Objekte, die Macie im Bucket analysieren kann, in Byte. Diese Objekte verwenden unterstützte Amazon S3 S3-Speicherklassen und haben Dateinamenerweiterungen für unterstützte Datei- oder Speicherformate. Weitere Informationen finden Sie unter Unterstützte Speicherklassen und -formate.
- Gesamtzahl der Entdeckungen — Die Gesamtzahl der Vorkommen sensibler Daten, die Macie im Bucket gefunden hat. Dies schließt Ereignisse ein, die derzeit durch die Einstellungen für die Vertraulichkeitsbewertung für den Bucket unterdrückt werden.

Das Diagramm „Analysierte Objekte“ gibt die Gesamtzahl der Objekte an, die Macie im Bucket analysiert hat. Es bietet auch eine visuelle Darstellung der Anzahl der Objekte, in denen Macie sensible Daten gefunden hat oder nicht. Die Legende unter dem Diagramm zeigt eine Aufschlüsselung dieser Ergebnisse:

- Vertrauliche Objekte (rot) — Die Gesamtzahl der Objekte, in denen Macie mindestens ein Vorkommen vertraulicher Daten gefunden hat.
- Nicht sensible Objekte (blau) — Die Gesamtzahl der Objekte, in denen Macie keine sensiblen Daten gefunden hat.
- Übersprungene Objekte (dunkelgrau) — Die Gesamtzahl der Objekte, die Macie aufgrund eines Problems oder Fehlers nicht analysieren konnte.

Der Bereich unter der Legende des Diagramms enthält eine Aufschlüsselung der Fälle, in denen Macie Objekte nicht analysieren konnte, weil bestimmte Arten von Berechtigungsproblemen oder kryptografischen Fehlern aufgetreten sind:

- Übersprungen: Ungültige Verschlüsselung — Die Gesamtzahl der Objekte, die mit vom Kunden bereitgestellten Schlüsseln verschlüsselt wurden. Macie kann nicht auf diese Schlüssel zugreifen.
- Übersprungen: Ungültiges KMS — Die Gesamtzahl der Objekte, die mit AWS Key Management Service (AWS KMS) -Schlüsseln verschlüsselt wurden, die nicht mehr verfügbar sind. Diese Objekte sind mit Objekten verschlüsselt AWS KMS keys , die deaktiviert wurden, deren Löschung geplant ist oder die gelöscht wurden. Macie kann diese Schlüssel nicht benutzen.
- Übersprungen: Zugriff verweigert — Die Gesamtzahl der Objekte, auf die Macie aufgrund der Berechtigungseinstellungen für das Objekt oder der Berechtigungseinstellungen für den Schlüssel, mit dem das Objekt verschlüsselt wurde, nicht zugreifen darf.

Einzelheiten zu diesen und anderen Arten von Problemen und Fehlern, die auftreten können, finden Sie unter. Behebung von Deckungsproblemen bei automatisierter Erkennung vertraulicher Daten Wenn Sie die Probleme und Fehler beheben, können Sie die Abdeckung der Daten des Buckets in nachfolgenden Analysezyklen erhöhen.

Die Statistiken auf der Registerkarte Erkennung vertraulicher Daten enthalten keine Daten für Objekte, die geändert oder gelöscht wurden, nachdem Macie sie analysiert oder versucht hat, sie zu analysieren. Wenn Objekte in einem Bucket geändert oder gelöscht werden, nachdem Macie sie analysiert oder versucht hat, sie zu analysieren, berechnet Macie diese Statistiken automatisch neu, um die Objekte auszuschließen.

Analyse sensibler Daten — Ergebnisse, die durch automatische Erkennung gewonnen wurden

Bei der automatisierten Erkennung sensibler Daten erstellt Amazon Macie für jedes Amazon Simple Storage Service (Amazon S3) -Objekt, in dem sensible Daten gefunden werden, eine Suche nach vertraulichen Daten. Eine Entdeckung sensibler Daten ist ein detaillierter Bericht über sensible Daten, die Macie in einem S3-Objekt gefunden hat. Jeder Fund sensibler Daten enthält eine Bewertung des Schweregrads und weitere Informationen wie:

- Datum und Uhrzeit, an dem Macie die sensiblen Daten gefunden hat.
- Die Kategorie und die Arten sensibler Daten, die Macie gefunden hat.
- Die Anzahl der Vorkommen der einzelnen Arten vertraulicher Daten, die Macie gefunden hat.
- Wie Macie die sensiblen Daten gefunden hat, automatisierte Erkennung sensibler Daten oder Auftrag zur Erkennung sensibler Daten.
- Der Name, die Einstellungen für den öffentlichen Zugriff, der Verschlüsselungstyp und andere Informationen zum betroffenen S3-Bucket und Objekt.

Je nach Dateityp oder Speicherformat des betroffenen S3-Objekts können die Details auch den Speicherort von bis zu 15 Vorkommen der sensiblen Daten beinhalten, die Macie gefunden hat. Eine Entdeckung sensibler Daten umfasst nicht die sensiblen Daten, die Macie gefunden hat. Stattdessen enthält es Informationen, die Sie bei Bedarf für weitere Untersuchungen und Problembehebungen verwenden können.

Macie speichert Ihre Erkenntnisse zu sensiblen Daten 90 Tage lang. Sie können über die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API darauf zugreifen. Sie können die Ergebnisse auch mithilfe anderer Anwendungen, Dienste und Systeme überwachen und verarbeiten. Weitere Informationen finden Sie unter Analyse der Ergebnisse.

Um Ergebnisse zu analysieren, die durch die automatisierte Erkennung sensibler Daten gewonnen wurden

Um die Ergebnisse sensibler Daten zu identifizieren und zu analysieren, die Macie bei der automatischen Erkennung sensibler Daten für Ihr Konto erstellt, können Sie Ihre Ergebnisse filtern. Mithilfe von Filtern verwenden Sie bestimmte Ergebnisattribute, um benutzerdefinierte Ansichten und Abfragen für Ergebnisse zu erstellen. Sie können die Amazon Macie Macie-Konsole verwenden, um Ergebnisse zu filtern, oder Abfragen programmgesteuert über die Amazon Macie Macie-API einreichen.

Console

Gehen Sie wie folgt vor, um die Ergebnisse mithilfe der Amazon Macie Macie-Konsole zu identifizieren und zu analysieren.

Um Ergebnisse zu analysieren, die durch automatische Erkennung erzielt wurden

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich Findings aus.
3. (Optional) Um Ergebnisse anzuzeigen, die durch eine Unterdrückungsregel unterdrückt wurden, ändern Sie die Einstellung für den Suchstatus. Wählen Sie Alle, um sowohl unterdrückte als auch nicht unterdrückte Ergebnisse anzuzeigen, oder wählen Sie Archiviert, um nur unterdrückte Ergebnisse anzuzeigen. Um die unterdrückten Ergebnisse anschließend wieder auszublenden, wählen Sie „Aktuell“.
4. Platzieren Sie den Cursor im Feld Filterkriterien. Wählen Sie in der angezeigten Feldliste den Typ Origin aus.

   In diesem Feld wird angegeben, wie Macie die sensiblen Daten gefunden hat, die zu einem Ergebnis, einer automatisierten Erkennung vertraulicher Daten oder einer Aufgabe zur Erkennung vertraulicher Daten geführt haben. Um dieses Feld in der Liste der Filterfelder zu finden, können Sie die gesamte Liste durchsuchen oder einen Teil des Feldnamens eingeben, um die Liste der Felder einzugrenzen.
5. Wählen Sie AUTOMATED_SENSITIVE_DATA_DISCOVERY als Wert für das Feld aus, und klicken Sie dann auf Anwenden. Macie wendet die Filterkriterien an und fügt die Bedingung einem Filtertoken im Feld Filterkriterien hinzu.
6. (Optional) Um die Ergebnisse zu verfeinern, fügen Sie Filterbedingungen für weitere Felder hinzu, z. B. „Erstellt am“ für den Zeitraum, in dem ein Ergebnis erstellt wurde, „S3-Bucket-Name“ für den Namen eines betroffenen Buckets oder „Erkennungstyp für sensible Daten“ für den Typ sensibler Daten, der erkannt wurde und zu einem Ergebnis geführt hat. Weitere Informationen finden Sie unter Filtern von Ergebnissen.

Wenn Sie diesen Satz von Bedingungen später erneut verwenden möchten, können Sie ihn als Filterregel speichern. Wählen Sie dazu im Feld Filterkriterien die Option Regel speichern aus. Geben Sie anschließend einen Namen und optional eine Beschreibung für die Regel ein. Wählen Sie Save (Speichern) aus, wenn Sie fertig sind.

API

Um die Ergebnisse programmatisch zu identifizieren und zu analysieren, geben Sie Filterkriterien in Abfragen an, die Sie mithilfe der ListFindingsAmazon GetFindingStatisticsMacie Macie-API einreichen. Der ListFindings Vorgang gibt eine Reihe von Such-IDs zurück, eine ID für jedes Ergebnis, das den Filterkriterien entspricht. Sie können diese IDs dann verwenden, um die Details jedes Ergebnisses abzurufen. Der GetFindingStatistics Vorgang gibt aggregierte statistische Daten zu allen Ergebnissen zurück, die den Filterkriterien entsprechen, gruppiert nach einem Feld, das Sie in Ihrer Anfrage angeben. Weitere Informationen zum programmgesteuerten Filtern von Ergebnissen finden Sie unter Filtern von Ergebnissen

Fügen Sie in den Filterkriterien eine Bedingung für das `originType` Feld ein. In diesem Feld wird angegeben, wie Macie die sensiblen Daten gefunden hat, die zu einem Ergebnis, einer automatisierten Erkennung vertraulicher Daten oder einer Aufgabe zur Erkennung vertraulicher Daten geführt haben. Der Wert für dieses Feld gibt an`AUTOMATED_SENSITIVE_DATA_DISCOVERY`, ob bei der automatischen Erkennung ein Ergebnis erzielt wurde.

Um die Ergebnisse mithilfe von AWS Command Line Interface (AWS CLI) zu identifizieren und zu analysieren, führen Sie den Befehl list-findings or get-finding-statisticsaus. In den folgenden Beispielen wird der list-findings Befehl verwendet, um Such-IDs für alle Ergebnisse mit hohem Schweregrad abzurufen, die bei der automatischen Erkennung sensibler Daten in der aktuellen Version erstellt wurden. AWS-Region

Verwenden Sie für Linux, macOS oder Unix den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit:

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":{"classificationDetails.originType":{"eq":
["AUTOMATED_SENSITIVE_DATA_DISCOVERY"]},"severity.description":{"eq":["High"]}}}'
```

Verwenden Sie für Microsoft Windows das Zeilenfortsetzungszeichen Caret (^), um die Lesbarkeit zu verbessern:

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":{\"classificationDetails.originType\":{\"eq
\":[\"AUTOMATED_SENSITIVE_DATA_DISCOVERY\"]},\"severity.description\":{\"eq\":
[\"High\"]}}}
```

Wobei gilt:

- `classificationDetails.originType`gibt den JSON-Namen des Felds vom Typ Origin an und:
  - `eq`gibt den Gleichheitsoperator an.
  - `AUTOMATED_SENSITIVE_DATA_DISCOVERY`ist ein Aufzählungswert für das Feld.
- *`severity.description`*gibt den JSON-Namen des Schweregradfeldes an und:
  - *`eq`*gibt den Gleichheitsoperator an.
  - *`High`*ist ein Aufzählungswert für das Feld.

Wenn der Befehl erfolgreich ausgeführt wird, gibt Macie ein Array zurück. `findingIds` Das Array listet den eindeutigen Bezeichner für jedes Ergebnis auf, das den Filterkriterien entspricht, wie im folgenden Beispiel gezeigt.

```
{
    "findingIds": [
        "1f1c2d74db5d8caa76859ec52example",
        "6cfa9ac820dd6d55cad30d851example",
        "702a6fd8750e567d1a3a63138example",
        "826e94e2a820312f9f964cf60example",
        "274511c3fdcd87010a19a3a42example"
    ]
}
```

Wenn keine Ergebnisse den Filterkriterien entsprechen, gibt Macie ein leeres `findingIds` Array zurück.

```
{
    "findingIds": []
}
```

Zugriff auf Ergebnisse der Erkennung sensibler Daten, die durch automatische Erkennung generiert wurden

Amazon Macie erstellt einen Analysedatensatz für jedes Amazon Simple Storage Service (Amazon S3) -Objekt, das es für die Analyse auswählt, und führt gleichzeitig die automatische Erkennung sensibler Daten für Ihr Konto oder Ihre Organisation durch. Diese Datensätze, die als Erkennungsergebnisse sensibler Daten bezeichnet werden, protokollieren Details über die Analyse, die Macie an einzelnen S3-Objekten durchführt. Dazu gehören Objekte, in denen Macie keine

sensiblen Daten erkennt und daher keine Ergebnisse liefert, sowie Objekte, die Macie aufgrund von Fehlern oder Problemen nicht analysieren kann, z. B. aufgrund von Berechtigungseinstellungen oder der Verwendung eines nicht unterstützten Datei- oder Speicherformats.

Wenn Macie sensible Daten in einem S3-Objekt entdeckt, umfasst das Ergebnis der Erkennung sensibler Daten Daten aus dem entsprechenden Befund. Es bietet auch zusätzliche Informationen, z. B. den Standort von bis zu 1.000 Vorkommen jedes Typs sensibler Daten, die Macie in dem Objekt gefunden hat. Beispielsweise:

- Die Spalten- und Zeilennummer für eine Zelle oder ein Feld in einer Microsoft Excel-Arbeitsmappe, CSV-Datei oder TSV-Datei
- Der Pfad zu einem Feld oder Array in einer JSON- oder JSON Lines-Datei
- Die Zeilennummer für eine Zeile in einer nicht-binären Textdatei, bei der es sich nicht um eine CSV-, JSON-, JSON-Zeilen- oder TSV-Datei handelt, z. B. eine HTML-, TXT- oder XML-Datei
- Die Seitennummer für eine Seite in einer PDF-Datei (Adobe Portable Document Format)
- Der Datensatzindex und der Pfad zu einem Feld in einem Datensatz in einem Apache Avro-Objektcontainer oder einer Apache Parquet-Datei

Handelt es sich bei dem betroffenen S3-Objekt um eine Archivdatei, z. B. eine .tar- oder .zip-Datei, liefert das Ergebnis der Erkennung sensibler Daten auch detaillierte Standortdaten für das Vorkommen sensibler Daten in einzelnen Dateien, die Macie aus dem Archiv extrahiert. Macie nimmt diese Informationen nicht in die Ergebnisse sensibler Daten für Archivdateien auf. Um Standortdaten zu melden, verwenden die Ergebnisse der Erkennung sensibler Daten ein standardisiertes JSON-Schema.

Ein Ermittlungsergebnis für sensible Daten beinhaltet nicht die sensiblen Daten, die Macie gefunden hat. Stattdessen erhalten Sie einen Analysedatensatz, der für Prüfungen oder Untersuchungen zum Datenschutz hilfreich sein kann.

Macie speichert Ihre Ergebnisse der Entdeckung sensibler Daten 90 Tage lang. Sie können nicht direkt über die Amazon Macie Macie-Konsole oder mit der Amazon Macie Macie-API darauf zugreifen. Stattdessen konfigurieren Sie Macie so, dass sie verschlüsselt und in einem S3-Bucket gespeichert werden. Der Bucket kann als definitives, langfristiges Repository für all Ihre Erkennungsergebnisse sensibler Daten dienen. Anschließend können Sie optional auf die Ergebnisse in diesem Repository zugreifen und diese abfragen.

Um zu ermitteln, wo sich dieses Repository für Ihr Konto befindet, wählen Sie im Navigationsbereich der Amazon Macie Macie-Konsole Discovery-Ergebnisse aus. Um dies programmgesteuert zu tun,

verwenden Sie den GetClassificationExportConfigurationBetrieb der Amazon Macie Macie-API. Wenn Sie dieses Repository nicht für Ihr Konto konfiguriert haben, erfahren Sie unter, wie Speicherung und Beibehaltung der Erkennungsergebnisse von vertraulichen Daten das geht.

Nachdem Sie Macie so konfiguriert haben, dass Ihre Erkennungsergebnisse vertraulicher Daten in einem S3-Bucket gespeichert werden, schreibt Macie die Ergebnisse in JSON-Lines-Dateien (.jsonl), verschlüsselt diese Dateien und fügt sie dem Bucket als GNU-Zip-Dateien (.gz) hinzu. Für die automatische Erkennung sensibler Daten fügt Macie die Dateien einem Ordner hinzu, der im Bucket benannt ist. automated-sensitive-data-discovery

Wie bei Ergebnissen sensibler Daten entsprechen auch die Ergebnisse der Erkennung sensibler Daten einem standardisierten Schema. Auf diese Weise können Sie sie optional mithilfe anderer Anwendungen, Dienste und Systeme abfragen, überwachen und verarbeiten.

> **Tip**
>
> Ein detailliertes, anschauliches Beispiel dafür, wie Sie die Ergebnisse der Erkennung sensibler Daten abfragen und verwenden können, um potenzielle Datensicherheitsrisiken zu analysieren und zu melden, finden Sie im QuickSight Blogbeitrag So fragen Sie die Ergebnisse der Erkennung sensibler Daten von Macie mit Amazon Athena und Amazon ab und visualisieren Sie sie im Security Blog.AWS
> Beispiele für Athena-Abfragen, mit denen Sie Erkennungsergebnisse sensibler Daten analysieren können, finden Sie im Amazon Macie Results Analytics-Repository unter. GitHub Dieses Repository enthält auch Anweisungen zur Konfiguration von Athena zum Abrufen und Entschlüsseln Ihrer Ergebnisse sowie Skripten zum Erstellen von Tabellen für die Ergebnisse.

Empfindlichkeitsbewertung für S3-Buckets

Wenn die automatische Erkennung vertraulicher Daten für Ihr Konto aktiviert ist, berechnet Amazon Macie automatisch einen Sensibilitätswert und weist jedem Amazon Simple Storage Service (Amazon S3) -Bucket, den es für Ihr Konto überwacht und analysiert, eine Vertraulichkeitsbewertung zu. Ein Sensitivitätswert ist eine quantitative Darstellung der Menge an sensiblen Daten, die ein S3-Bucket enthalten kann. Basierend auf dieser Bewertung weist Macie jedem Bucket außerdem ein Sensitivitätslabel zu. Ein Sensitivitätslabel ist eine qualitative Darstellung des Sensitivitätswerts eines Buckets. Diese Werte können als Bezugspunkte dienen, um festzustellen, wo sich sensible Daten in Ihrem Amazon S3-Datenbestand befinden könnten, und um potenzielle Sicherheitsrisiken für diese Daten zu identifizieren und zu überwachen.

Standardmäßig spiegeln der Sensitivitätswert und die Bezeichnung eines S3-Buckets die Ergebnisse automatisierter Aktivitäten zur Erkennung vertraulicher Daten wider, die Macie bisher für den Bucket durchgeführt hat. Sie spiegeln nicht die Ergebnisse von Aufträgen zur Erkennung vertraulicher Daten wider, die Sie erstellt und ausgeführt haben. Darüber hinaus implizieren weder die Bewertung noch das Label die Wichtigkeit oder Bedeutung, die ein Bucket oder die Objekte eines Buckets für Ihr Unternehmen haben könnten, oder geben auf andere Weise an. Sie können jedoch die berechnete Bewertung eines Buckets überschreiben, indem Sie dem Bucket manuell die maximale Punktzahl (100) zuweisen, wodurch dem Bucket auch das Label Sensitiv zugewiesen wird.

Themen

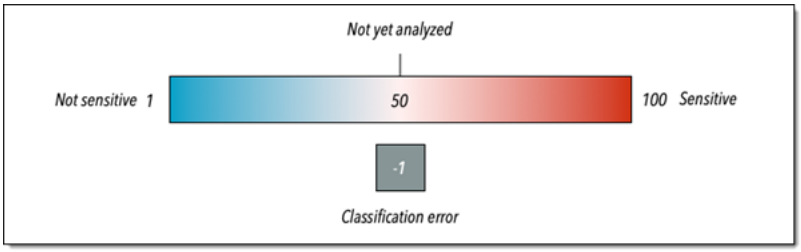
- Dimensionen und Bereiche der Empfindlichkeitsbewertung
- Überwachung der Empfindlichkeitswerte

Dimensionen und Bereiche der Empfindlichkeitsbewertung

Wenn er von Amazon Macie berechnet wird, ist der Sensitivitätswert eines S3-Buckets ein quantitatives Maß für den Schnittpunkt zweier primärer Dimensionen:

- Die Menge an sensiblen Daten, die Macie im Eimer gefunden hat. Dies ist hauptsächlich auf die Art und Anzahl der vertraulichen Datentypen zurückzuführen, die Macie im Bucket gefunden hat, sowie auf die Anzahl der Vorkommen der einzelnen Typen.
- Die Datenmenge, die Macie im Bucket analysiert hat. Dies ergibt sich hauptsächlich aus der Anzahl der eindeutigen Objekte, die Macie im Bucket analysiert hat, im Verhältnis zur Gesamtzahl der eindeutigen Objekte im Bucket.

Der Sensitivitätswert eines S3-Buckets bestimmt auch, welches Sensitivitätslabel Macie dem Bucket zuweist. Das Sensitivitätslabel ist eine qualitative Darstellung des Ergebnisses, z. B. Sensitiv oder Nicht empfindlich. In der Amazon Macie-Konsole bestimmt der Empfindlichkeitswert eines Buckets auch, welche Farbe Macie verwendet, um den Bucket in Datenvisualisierungen darzustellen, wie in der folgenden Abbildung dargestellt.



Die Sensitivitätswerte reichen von -1 bis 100, wie in der folgenden Tabelle beschrieben. Um die Eingaben für die Bewertung eines S3-Buckets zu bewerten, können Sie auf Statistiken zur Erkennung vertraulicher Daten und andere Details zurückgreifen, die Macie über den Bucket bereitstellt.

Empfindlichkeitswert	Empfindlichkeitslabel	Zusätzliche Informationen
-1	Fehler bei der Klassifizierung	Macie hat aufgrund von Klassifizierungsfehlern auf Objektebene — Problemen mit den Berechtigungseinstellungen auf Objektebene, Objektinhalt oder Kontingenten — noch keines der Objekte des Buckets analysiert. Als Macie versuchte, ein oder mehrere Objekte im Bucket zu analysieren, traten Fehler auf. Beispielsweise handelt es sich bei einem Objekt um eine falsch formatierte Datei, oder ein Objekt ist mit einem Schlüssel verschlüsselt, auf den Macie nicht zugreifen kann oder den er nicht verwenden darf. Die Deckungsdaten für den Bucket können Ihnen helfen, die Fehler zu untersuchen und zu beheben. Weitere Informationen finden Sie unter Bewertung des Umfangs automatisierter Erkennung vertraulicher Daten.

Empfindlichkeitswert	Empfindlichkeitslabel	Zusätzliche Informationen
		Macie wird weiterhin versuchen, Objekte im Bucket zu analysieren. Wenn Macie ein Objekt erfolgreich analysiert, aktualisiert Macie den Sensitivitätswert und die Bezeichnung des Buckets entsprechend den Ergebnissen der Analyse.

Empfindlichkeitswert	Empfindlichkeitslabel	Zusätzliche Informationen
1-49	Nicht empfindlich	In diesem Bereich bedeutet ein höherer Wert, z. B. 49, dass Macie relativ wenige Objekte im Bucket analysier t hat. Ein niedrigerer Wert, z. B. 1, bedeutet, dass Macie viele Objekte im Bucket analysiert hat (im Verhältnis zur Gesamtzahl der Objekte im Bucket) und relativ wenige Arten und Vorkommen vertraulicher Daten in diesen Objekten erkannt hat. Ein Wert von 1 kann auch bedeuten, dass der Bucket keine Objekte enthält oder dass alle Objekte im Bucket null (0) Byte an Daten enthalten. Mithilfe von Objektstatistiken in den Details des Buckets können Sie feststellen, ob dies der Fall ist. Weitere Informationen finden Sie unter Überprüfung der S3-Bucket-Details.

Empfindlichkeitswert	Empfindlichkeitslabel	Zusätzliche Informationen
50	Noch nicht analysiert	Macie hat noch nicht versucht, eines der Objekte des Buckets zu analysieren oder zu analysieren. Macie weist diese Punktzahl automatisch einem Bucket zu, wenn Sie die automatische Erkennung für Ihr Konto zum ersten Mal aktivieren oder Ihrem Bucket-Inventar ein Bucket hinzugefügt wird. Ein Wert von 50 kann auch darauf hinweisen, dass die Berechtigungseinstellungen des Buckets Macie daran hindern, auf den Bucket oder die Objekte des Buckets zuzugreifen. Dies ist in der Regel auf eine restriktive Bucket-Richtlinie zurückzuführen. Anhand der Details des Buckets können Sie feststellen, ob dies der Fall ist, da Macie nur einen Teil der Informationen über den Bucket bereitstellen kann. Informationen zur Behebung dieses Problems finden Sie unterMacie den Zugriff von S3-Buckets und -Objekten erlauben.

Empfindlichkeitswert	Empfindlichkeitslabel	Zusätzliche Informationen
51-99	Sensibel	In diesem Bereich bedeutet ein höherer Wert, z. B. 99, dass Macie viele Objekte im Bucket analysiert hat (im Verhältnis zur Gesamtzahl der Objekte im Bucket) und viele Arten und Vorkommen vertraulicher Daten in diesen Objekten erkannt hat. Ein niedrigerer Wert, z. B. 51, weist darauf hin, dass Macie eine moderate Anzahl von Objekten im Bucket analysier t hat (im Verhältnis zur Gesamtzahl der Objekte im Bucket) und mindestens einige Arten und Vorkommen vertraulicher Daten in diesen Objekten erkannt hat.
100	Sensibel	Die Punktzahl wurde dem Bucket manuell zugewiese n und hat Vorrang vor der berechneten Punktzahl. Macie weist diesen Punktestand nicht Eimern zu.

Überwachung der Empfindlichkeitswerte

Wenn Sie zunächst die automatische Erkennung vertraulicher Daten für Ihr Konto aktivieren, weist Amazon Macie jedem S3-Bucket automatisch einen Sensibilitätswert von 50 zu. Macie weist diese Punktzahl auch einem Bucket zu, wenn der Bucket zu Ihrem Bucket-Inventar hinzugefügt wird. Basierend auf dieser Bewertung wird das Sensitivitätslabel jedes Buckets noch nicht analysiert. Die Ausnahme ist ein leerer Bucket, bei dem es sich um einen Bucket handelt, der keine Objekte enthält,

oder alle Objekte im Bucket enthalten null (0) Byte an Daten. Wenn dies bei einem Bucket der Fall ist, weist Macie dem Bucket eine Punktzahl von 1 zu und das Sensitivitätslabel des Buckets lautet Nicht empfindlich.

Während die automatische Erkennung vertraulicher Daten für Ihr Konto täglich voranschreitet, aktualisiert Macie die Sensibilitätswerte und Labels für Ihre S3-Buckets, um die Ergebnisse der Analyse widerzuspiegeln. Beispiele:

- Wenn Macie in einem Objekt keine vertraulichen Daten findet, verringert Macie den Sensitivitätswert des Buckets und aktualisiert die Sensitivitätsbezeichnung des Buckets nach Bedarf.
- Wenn Macie sensible Daten in einem Objekt findet, erhöht Macie den Sensitivitätswert des Buckets und aktualisiert die Sensitivitätsbezeichnung des Buckets nach Bedarf.
- Wenn Macie sensible Daten in einem Objekt findet, das anschließend geändert wurde, entfernt Macie die Erkennung vertraulicher Daten für das Objekt aus dem Sensitivitätswert des Buckets und aktualisiert die Sensitivitätsbezeichnung des Buckets nach Bedarf.
- Wenn Macie vertrauliche Daten in einem Objekt findet, das anschließend gelöscht wird, entfernt Macie die Erkennung vertraulicher Daten für das Objekt aus dem Sensitivitätswert des Buckets und aktualisiert die Sensitivitätskennzeichnung des Buckets nach Bedarf.
- Wenn ein Objekt zu einem Bucket hinzugefügt wird, der zuvor leer war, und Macie sensible Daten in dem Objekt findet, erhöht Macie den Sensitivitätswert des Buckets und aktualisiert die Sensitivitätsbezeichnung des Buckets nach Bedarf.
- Wenn die Berechtigungseinstellungen eines Buckets Macie daran hindern, Informationen über den Bucket oder die Objekte des Buckets abzurufen oder darauf zuzugreifen, ändert Macie den Sensitivitätswert des Buckets auf 50 und ändert die Sensitivitätsbezeichnung des Buckets in Noch nicht analysiert.

Abhängig von der Datenmenge, die Sie in Amazon S3 speichern, können die Analyseergebnisse innerhalb von 48 Stunden nach Aktivierung der automatischen Erkennung vertraulicher Daten für Ihr Konto erscheinen.

Sie können die Einstellungen für die Sensitivitätsbewertung für Ihr Konto anpassen, wodurch die Einstellungen für nachfolgende Analysen all Ihrer S3-Buckets geändert werden. Sie können auch die Einstellungen für einzelne S3-Buckets anpassen. Für Einstellungen auf Kontoebene können Sie damit beginnen, bestimmte Zulassungslisten, benutzerdefinierte Datenkennungen oder verwaltete Datenkennungen in die Analysen aufzunehmen oder auszuschließen. Sie können auch bestimmte

Buckets von den Analysen ausschließen. Weitere Informationen finden Sie unter Konfiguration der Einstellungen für die automatische Erkennung für Ihr Konto.

Um die Bewertungseinstellungen für einen bestimmten Bucket anzupassen, können Sie bestimmte Arten vertraulicher Daten in die Bewertung des Buckets einbeziehen oder davon ausschließen. Sie können auch angeben, ob dem Bucket eine automatisch berechnete Punktzahl zugewiesen werden soll. Weitere Informationen finden Sie unter Verwaltung der automatisierten Erkennung für einzelne S3-Buckets.

Standardeinstellungen für die automatische Erkennung vertraulicher Daten

Wenn die automatische Erkennung vertraulicher Daten für Ihr Konto aktiviert ist, wählt Amazon Macie automatisch Beispielobjekte aus allen Amazon Simple Storage Service (Amazon S3) - Buckets aus, die es für Ihr Konto überwacht und analysiert. Wenn Sie der Macie-Administrator einer Organisation sind, gehören dazu auch S3-Buckets, die Ihren Mitgliedskonten gehören. Um den Umfang der Analysen zu verfeinern, können Sie bestimmte Buckets von der automatisierten Erkennung vertraulicher Daten ausschließen. Sie können dies auf zwei Arten tun: durchÄnderung der Einstellungen für die automatische Erkennung vertraulicher Daten für Ihr Konto, und vonÄnderung der Einstellungen für die automatische Erkennung vertraulicher Daten für einzelne Buckets.

Standardmäßig analysiert Macie S3-Objekte, indem er nur den Satz verwalteter Datenkennungen verwendet, die wir für die automatische Erkennung vertraulicher Daten empfehlen. Macie verwendet keine benutzerdefinierten Datenkennungen und erlaubt keine Listen, die Sie definiert haben. Um die Analysen anzupassen, können Sie Macie so konfigurieren, dass es bestimmte verwaltete Datenkennungen, benutzerdefinierte Datenkennungen und Zulassungslisten verwendet. Sie können das tun, indem SieÄnderung der Einstellungen für die automatische Erkennung vertraulicher Daten für Ihr Konto.

Themen

- Standardkennungen für verwaltete Daten für die automatische Erkennung vertraulicher Daten
- Aktualisierungen der Standardeinstellungen für die automatische Erkennung vertraulicher Daten

Standardkennungen für verwaltete Daten für die automatische Erkennung vertraulicher Daten

Standardmäßig analysiert Amazon Macie S3-Objekte, indem es nur den Satz verwalteter Datenkennungen verwendet, die wir für die automatische Erkennung vertraulicher Daten empfehlen.

Dieser Standardsatz verwalteter Datenkennungen wurde entwickelt, um gängige Kategorien und Typen vertraulicher Daten zu erkennen. Basierend auf unseren Recherchen kann es allgemeine Kategorien und Typen sensibler Daten erkennen und gleichzeitig Ihre automatisierten Erkennungsergebnisse optimieren, indem es das Rauschen reduziert.

Die Standardeinstellung ist dynamisch. Sobald wir neue Identifikatoren für verwaltete Daten veröffentlichen, fügen wir sie dem Standardsatz hinzu, wenn sie Ihre automatisierten Ergebnisse zur Erkennung vertraulicher Daten voraussichtlich weiter optimieren werden. Im Laufe der Zeit können wir dem Set auch bestehende Identifikatoren für verwaltete Daten hinzufügen oder daraus entfernen. Das Entfernen einer verwalteten Daten-ID hat keinen Einfluss auf die vorhandenen Statistiken zur Erkennung vertraulicher Daten und Details für Ihre S3-Buckets. Wenn wir beispielsweise die verwaltete Daten-ID für einen Typ vertraulicher Daten entfernen, den Macie zuvor in einem Bucket erkannt hat, meldet Macie diese Erkennungen weiterhin für den Bucket. Wenn wir eine verwaltete Daten-ID zur Standardeinstellung hinzufügen oder daraus entfernen, aktualisieren wir diese Seite, um die Art und den Zeitpunkt der Änderung anzugeben. Um automatische Benachrichtigungen über diese Änderungen zu erhalten, können Sie den RSS-Feed auf der[Geschichte des Macie-Dokuments](#)Seite.

In den folgenden Themen sind die verwalteten Datenkennungen aufgeführt, die derzeit im Standardsatz enthalten sind, und zwar geordnet nach Kategorie und Typ vertraulicher Daten. Sie geben den eindeutigen Identifier (ID) für jeden verwalteten Datenbezeichner im Satz an. Diese ID beschreibt die Art sensibler Daten, die ein verwalteter Datenbezeichner erkennen soll, zum Beispiel:`PGP_PRIVATE_KEY`für private PGP-Schlüssel und`USA_PASSPORT_NUMBER`für US-Passnummern. Wenn Sie die Einstellungen für die automatische Erkennung vertraulicher Daten für Ihr Konto ändern, können Sie diese ID verwenden, um eine verwaltete Daten-ID explizit von nachfolgenden Analysen auszuschließen.

Themen

- [Anmeldeinformationen](#)
- [Finanzinformationen](#)
- [Persönlich Identifizierbare Informationen (PII)](#)

Einzelheiten zu bestimmten Identifikatoren für verwaltete Daten oder eine vollständige Liste aller Identifikatoren für verwaltete Daten, die Macie derzeit bereitstellt, finden Sie unter[Verwenden von verwalteten Datenbezeichnern](#).

Anmeldeinformationen

Um das Vorkommen von Anmeldeinformationsdaten in S3-Objekten zu erkennen, verwendet Macie standardmäßig die folgenden verwalteten Datenkennungen.

Vertraulicher Datentyp	ID der verwalteten Datenkennung
Geheimer AWS-Zugriffsschlüssel	`AWS_CREDENTIALS`
Header für die HTTP-Standardautorisierung	`HTTP_BASIC_AUTH_HEADER`
Privater OpenSSH-Schlüssel	`OPENSSH_PRIVATE_KEY`
Privater PGP-Schlüssel	`PGP_PRIVATE_KEY`
Privater Schlüssel des Public Key Cryptography Standard (PKCS)	`PKCS`
Privater PuTTY-Schlüssel	`PUTTY_PRIVATE_KEY`

Finanzinformationen

Um das Vorkommen von Finanzinformationen in S3-Objekten zu erkennen, verwendet Macie standardmäßig die folgenden verwalteten Datenkennungen.

Vertraulicher Datentyp	ID der verwalteten Datenkennung
Kreditkarten-Magnetstreifendaten	`CREDIT_CARD_MAGNETIC_STRIPE`
Kreditkartennummer	`CREDIT_CARD_NUMBER` (für Kreditkartennummern in der Nähe eines Schlüsselworts)

Persönlich Identifizierbare Informationen (PII)

Um das Vorkommen personenbezogener Daten (PII) in S3-Objekten zu erkennen, verwendet Macie standardmäßig die folgenden verwalteten Datenkennungen.

Vertraulicher Datentyp	ID der verwalteten Datenkennung
Identifikationsnummer des Führerscheins	`CANADA_DRIVERS_LICENSE`, `DRIVERS_LICENSE` (für die USA), `UK_DRIVERS_LICENSE`
Nummer der Wählerliste	`UK_ELECTORAL_ROLL_NUMBER`
Nationale Identifikationsnummern	`FRANCE_NATIONAL_IDENTIFICATION_NUMBER`, `GERMANY_NATIONAL_IDENTIFICATION_NUMBER`, `ITALY_NATIONAL_IDENTIFICATION_NUMBER`, `SPAIN_DNI_NUMBER`
Landesversicherungsnummer (NINO)	`UK_NATIONAL_INSURANCE_NUMBER`
Passnummer	`CANADA_PASSPORT_NUMBER`, `FRANCE_PASSPORT_NUMBER`, `GERMANY_PASSPORT_NUMBER`, `ITALY_PASSPORT_NUMBER`, `SPAIN_PASSPORT_NUMBER`, `UK_PASSPORT_NUMBER`, `USA_PASSPORT_NUMBER`
Sozialversicherungsnummer (SIN)	`CANADA_SOCIAL_INSURANCE_NUMBER`
Sozialversicherungsnummer (SSN)	`SPAIN_SOCIAL_SECURITY_NUMBER`, `USA_SOCIAL_SECURITY_NUMBER`
Steuerpflichtigen-Identifikationsnummer oder Referenznummer	`AUSTRALIA_TAX_FILE_NUMBER`, `BRAZIL_CPF_NUMBER`, `FRANCE_TAX_IDENTIFICATION_NUMBER`, `GERMANY_TAX_IDENTIFICATION_NUMBER`, `SPAIN_NIE_NUMBER`, `SPAIN_NIF_NUMBER`, `SPAIN_TAX_IDENTIFICATION_NUMBER`, `USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER`

Aktualisierungen der Standardeinstellungen für die automatische Erkennung vertraulicher Daten

In der folgenden Tabelle werden Änderungen an den Einstellungen beschrieben, die Amazon Macie standardmäßig für die automatische Erkennung vertraulicher Daten verwendet. Um automatische Benachrichtigungen über diese Änderungen zu erhalten, abonnieren Sie den RSS-Feed auf derGeschichte des Macie-DokumentsSeite.

Änderung	Beschreibung	Datum
Es wurde ein neuer, dynamischer Satz standardmäßiger verwalteter Datenkennungen implementiert	Neue Konfigurationen für die automatische Erkennung sensibler Daten basieren jetzt auf einer dynamischen enStandardsatz verwalteter Datenkennungen. Wenn Sie die automatische Erkennung vertraulicher Daten zum ersten Mal an oder nach diesem Datum aktivieren, basiert Ihre Konfiguration auf dem dynamischen Satz. Wenn Sie die automatische Erkennung vertraulicher Daten vor diesem Datum zum ersten Mal aktiviert haben, basiert Ihre Konfiguration auf einem anderen Satz verwalteter Datenkennungen. Weitere Informationen finden Sie in den Anmerkungen nach dieser Tabelle.	02. August 2023
Allgemeine Verfügbarkeit	Erste Version der automatisierten Erkennung vertraulicher Daten.	28. November 2022

Wenn Sie die automatische Erkennung vertraulicher Daten für Ihr Konto ursprünglich vor dem 2. August 2023 aktiviert haben, basiert Ihre Konfiguration nicht auf den dynamischen Standardkennungen für verwaltete Daten. Ihre Konfiguration basiert stattdessen auf einem statischen Satz verwalteter Datenkennungen, die wir für die erste Version der automatisierten Erkennung vertraulicher Daten definiert haben, wie in der folgenden Tabelle aufgeführt.

Um festzustellen, wann Sie die automatische Erkennung vertraulicher Daten für Ihr Konto zum ersten Mal aktiviert haben, wählen SieAutomatisierte Erkennungim Navigationsbereich der Amazon Macie-Konsole und geben Sie dann das Aktivierungsdatum in derStatusAbschnitt. Um dies programmgesteuert zu tun, verwenden Sie denGetAutomatedDiscoveryConfigurationBetrieb der Amazon Macie API und beziehen Sie sich auf den Wert für`firstEnabledAt`Feld. Wenn das Datum vor dem 2. August 2023 liegt und Sie mit der Verwendung der dynamischen Standardkennungen für verwaltete Daten beginnen möchten, wenden Sie sich anAWS Supportfür Unterstützung.

In der folgenden Tabelle sind alle verwalteten Datenkennungen aufgeführt, die im statischen Satz enthalten sind. Die Tabelle wird zuerst nach der Kategorie vertraulicher Daten und dann nach dem sensiblen Datentyp sortiert. Einzelheiten zu bestimmten Identifikatoren für verwaltete Daten finden Sie unterVerwenden von verwalteten Datenbezeichnern.

Kategorie vertraulicher Daten	Vertraulicher Datentyp	ID der verwalteten Datenkennung
Anmeldeinformationen	Geheimer AWS-Zugriffsschlüssel	`AWS_CREDENTIALS`
Anmeldeinformationen	Header für die HTTP-Standardautorisierung	`HTTP_BASIC_AUTH_HEADER`
Anmeldeinformationen	Privater OpenSSH-Schlüssel	`OPENSSH_PRIVATE_KEY`
Anmeldeinformationen	Privater PGP-Schlüssel	`PGP_PRIVATE_KEY`
Anmeldeinformationen	Privater Schlüssel des Public Key Cryptography Standard (PKCS)	`PKCS`
Anmeldeinformationen	Privater PuTTY-Schlüssel	`PUTTY_PRIVATE_KEY`

Kategorie vertraulicher Daten	Vertraulicher Datentyp	ID der verwalteten Datenkennung
Finanzinformationen	Bankkontonummer	`BANK_ACCOUNT_NUMBER` (für kanadische und US-amerikanische Bankkontonummern),`FRANCE_BANK_ACCOUNT_NUMBER`, `GERMANY_BANK_ACCOUNT_NUMBER`, `ITALY_BANK_ACCOUNT_NUMBER`, `SPAIN_BANK_ACCOUNT_NUMBER`, `UK_BANK_ACCOUNT_NUMBER`
Finanzinformationen	Ablaufdatum der Kreditkarte	`CREDIT_CARD_EXPIRATION`
Finanzinformationen	Kreditkarten-Magnetstreifendaten	`CREDIT_CARD_MAGNETIC_STRIPE`
Finanzinformationen	Kreditkartennummer	`CREDIT_CARD_NUMBER` (für Kreditkartennummern in der Nähe eines Schlüsselworts)
Finanzinformationen	Bestätigungscode für die Kreditkarte	`CREDIT_CARD_SECURITY_CODE`
Persönliche Daten: Persönliche Gesundheitsinformationen (PHI)	Registrierungsnummer der Drug Enforcement Agency (DEA)	`US_DRUG_ENFORCEMENT_AGENCY_NUMBER`
Persönliche Informationen: PHI	Health Insurance Claim Number (HICN)	`USA_HEALTH_INSURANCE_CLAIM_NUMBER`

Kategorie vertraulicher Daten	Vertraulicher Datentyp	ID der verwalteten Datenkennung
Persönliche Informationen: PHI	Krankenversicherungs- oder medizinische Identifizierungsnummer	`CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER`
Persönliche Informationen: PHI	Standardisierte Codes für medizinische Leistungen (HCPCS)	`USA_HEALTHCARE_PROCEDURE_CODE`
Persönliche Informationen: PHI	National Drug Code (NDC)	`USA_NATIONAL_DRUG_CODE`
Persönliche Informationen: PHI	National Provider Identifier (NPI)	`USA_NATIONAL_PROVIDER_IDENTIFIER`
Persönliche Informationen: PHI	Eindeutige Gerätekennung (UDI)	`MEDICAL_DEVICE_UDI`
Personenbezogene Daten: Persönlich identifizierbare Informationen (PII)	Geburtsdatum	`DATE_OF_BIRTH`

Kategorie vertraulicher Daten	Vertraulicher Datentyp	ID der verwalteten Datenkennung
Persönliche Informationen: PII	Identifikationsnummer des Führerscheins	AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (für die USA),ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICE

Kategorie vertraulicher Daten	Vertraulicher Datentyp	ID der verwalteten Datenkennung
		NSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE
Persönliche Informationen: PII	Nummer der Wählerliste	UK_ELECTORAL_ROLL_NUMBER
Persönliche Informationen: PII	Vollständiger Name	NAME
Persönliche Informationen: PII	Koordinaten des globalen Positionierungssystems (GPS)	LATITUDE_LONGITUDE
Persönliche Informationen: PII	Postanschrift	ADDRESS, BRAZIL_CEP_CODE
Persönliche Informationen: PII	Nationale Identifikationsnummern	BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER

Kategorie vertraulicher Daten	Vertraulicher Datentyp	ID der verwalteten Datenkennung
Persönliche Informationen: PII	Landesversicherungsnummer (NINO)	`UK_NATIONAL_INSURANCE_NUMBER`
Persönliche Informationen: PII	Passnummer	`CANADA_PASSPORT_NUMBER`, `FRANCE_PASSPORT_NUMBER`, `GERMANY_PASSPORT_NUMBER`, `ITALY_PASSPORT_NUMBER`, `SPAIN_PASSPORT_NUMBER`, `UK_PASSPORT_NUMBER`, `USA_PASSPORT_NUMBER`
Persönliche Informationen: PII	Ständige Wohnsitznummer	`CANADA_NATIONAL_IDENTIFICATION_NUMBER`
Persönliche Informationen: PII	Phone number (Telefonnummer)	`BRAZIL_PHONE_NUMBER`, `FRANCE_PHONE_NUMBER`, `GERMANY_PHONE_NUMBER`, `ITALY_PHONE_NUMBER`, `PHONE_NUMBER` (für Kanada und die USA),`SPAIN_PHONE_NUMBER`, `UK_PHONE_NUMBER`
Persönliche Informationen: PII	Sozialversicherungsnummer (SIN)	`CANADA_SOCIAL_INSURANCE_NUMBER`
Persönliche Informationen: PII	Sozialversicherungsnummer (SSN)	`SPAIN_SOCIAL_SECURITY_NUMBER`, `USA_SOCIAL_SECURITY_NUMBER`

Kategorie vertraulicher Daten	Vertraulicher Datentyp	ID der verwalteten Datenkennung
Persönliche Informationen: PII	Steuerpflichtigen-Identifikationsnummer oder Referenznummer	`AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER`
Persönliche Informationen: PII	Fahrgestellnummern (VIN)	`VEHICLE_IDENTIFICATION_NUMBER`

Ausführen von Aufträgen zur Erkennung vertraulicher Daten in Amazon Macie

Mit Amazon Macie können Sie Aufgaben zur Erkennung vertraulicher Daten erstellen und ausführen, um die Erkennung, Protokollierung und Berichterstattung vertraulicher Daten in Amazon Simple Storage Service (Amazon S3) -Buckets zu automatisieren. Ein Job zur Erkennung vertraulicher Daten ist eine Reihe automatisierter Verarbeitungs- und Analyseaufgaben, die Macie ausführt, um sensible Daten in Amazon S3-Objekten zu erkennen und zu melden. Jeder Job enthält detaillierte Berichte über die sensiblen Daten, die Macie findet, und über die Analysen, die Macie durchführt. Durch das Erstellen und Ausführen von Jobs können Sie einen umfassenden Überblick über die Daten, die Ihr Unternehmen in Amazon S3 speichert, sowie über alle Sicherheits- oder Compliance-Risiken, die mit diesen Daten verbunden sind, erstellen und verwalten.

Um Ihnen dabei zu helfen, Ihre Anforderungen an Datensicherheit und Datenschutz zu erfüllen und einzuhalten, bietet Macie verschiedene Optionen für die Planung und Definition des Umfangs eines Auftrags. Sie können einen Job so konfigurieren, dass er nur einmal für Analysen und Bewertungen auf Abruf oder wiederholt für regelmäßige Analysen, Bewertungen und Überwachungen ausgeführt wird. Sie definieren auch den Umfang und die Tiefe der Analyse eines Jobs — bestimmte S3-Buckets, die Sie auswählen, oder Buckets, die bestimmten Kriterien entsprechen. Sie können den Umfang dieser Analyse optional verfeinern, indem Sie zusätzliche Optionen auswählen. Zu den Optionen gehören benutzerdefinierte Ein- und Ausschlusskriterien, die sich von Eigenschaften von S3-Objekten wie Tags, Präfixen und dem Zeitpunkt der letzten Änderung eines Objekts ableiten.

Für jeden Job geben Sie auch die Arten vertraulicher Daten an, die Macie erkennen und melden soll. Sie können einen Job so konfigurieren, dass er verwaltete Datenkennungen verwendet, die Macie bereitstellt, benutzerdefinierte Datenkennungen, die Sie definieren, oder eine Kombination aus beiden. Indem Sie bestimmte verwaltete und benutzerdefinierte Datenkennungen für einen Job auswählen, können Sie die Analyse so anpassen, dass sie sich auf bestimmte Arten vertraulicher Daten konzentriert. Zur Feinabstimmung der Analyse können Sie einen Job auch so konfigurieren, dass er von Ihnen definierte Zulassungslisten verwendet. Zulässige Listen geben Text und Textmuster an, die Macie ignorieren soll. Dabei handelt es sich in der Regel um Ausnahmen für sensible Daten für die speziellen Szenarien oder Umgebungen Ihres Unternehmens.

Bei jedem Auftrag werden die sensiblen Daten, die Macie findet, und die Analysen, die Macie durchführt, aufgezeichnet — Ergebnisse vertraulicher Daten und Ergebnisse der Entdeckung vertraulicher Daten. Ein Ergebnis vertraulicher Daten ist ein detaillierter Bericht über sensible Daten, die Macie in einem S3-Objekt gefunden hat. Ein Ergebnis der Erkennung vertraulicher Daten ist ein Datensatz, der Details zur Analyse eines S3-Objekts protokolliert. Macie erstellt für jedes Objekt, für dessen Analyse Sie einen Job konfigurieren, ein Ermittlungsergebnis vertraulicher Daten. Dazu gehören Objekte, in denen Macie keine vertraulichen Daten findet und daher keine Ergebnisse für sensible Daten liefert, sowie Objekte, die Macie aufgrund von Fehlern oder Problemen nicht analysieren kann. Jeder Datensatztyp entspricht einem standardisierten Schema, mit dem Sie die Datensätze abfragen, überwachen und verarbeiten können, um Ihre Sicherheits- und Compliance-Anforderungen zu erfüllen.

Themen

- Umfangsoptionen für Aufgaben zur Erkennung sensibler Daten
- Erstellen einer Aufgabe zur Erkennung vertraulicher Daten
- Überprüfung von Statistiken und Ergebnissen für Discovery-Jobs im Zusammenhang mit sensiblen Daten

- Überwachung von Aufträgen zur Erkennung sensibler Daten mit Amazon CloudWatch Logs
- Verwaltung von Aufträgen zur Erkennung sensibler Daten
- Prognostizieren und Überwachen der Kosten für Erkennungsaufgaben bei vertraulichen Daten
- Verwaltete Datenkennungen, die für die Erkennung vertraulicher Daten empfohlen werden

Umfangsoptionen für Aufgaben zur Erkennung sensibler Daten

Mit Aufträgen zur Erkennung sensibler Daten definieren Sie den Umfang der Amazon Simple Storage Service (Amazon S3) -Daten, die Amazon Macie analysiert, um sensible Daten zu erkennen und zu melden. Um Ihnen dabei zu helfen, bietet Macie mehrere auftragsspezifische Optionen, die Sie bei der Erstellung und Konfiguration eines Jobs auswählen können.

Optionen für den Geltungsbereich

- S3-Buckets
- Bestehende S3-Objekte einbeziehen
- Tiefe der Probenahme
- S3-Objektkriterien

S3-Buckets

Wenn Sie einen Discovery-Job für sensible Daten erstellen, geben Sie an, welche S3-Buckets Objekte enthalten, die Macie analysieren soll, wenn der Job ausgeführt wird. Sie können dies auf zwei Arten tun, indem Sie bestimmte S3-Buckets aus Ihrem Bucket-Inventar auswählen oder indem Sie benutzerdefinierte Kriterien angeben, die sich aus den Eigenschaften von S3-Buckets ableiten.

Wählen Sie bestimmte Buckets aus

> Mit dieser Option wählen Sie explizit jeden S3-Bucket aus, den der Job analysieren soll. Wenn der Job dann ausgeführt wird, analysiert er nur Objekte in den von Ihnen ausgewählten Buckets. Wenn Sie den Job so konfigurieren, dass er regelmäßig täglich, wöchentlich oder monatlich ausgeführt wird, analysiert der Job bei jeder Ausführung Objekte in denselben Buckets.
>
> Diese Konfiguration ist hilfreich für Fälle, in denen Sie eine gezielte Analyse eines bestimmten Datensatzes bevorzugen. Sie gibt Ihnen eine präzise und vorhersehbare Kontrolle darüber, welche Buckets ein Job analysiert.

Geben Sie Bucket-Kriterien an

Mit dieser Option definieren Sie Laufzeitkriterien, die bestimmen, welche S3-Buckets der Job analysiert. Die Kriterien bestehen aus einer oder mehreren Bedingungen, die sich aus Bucket-Eigenschaften wie Einstellungen und Tags für den öffentlichen Zugriff ergeben. Wenn der Job ausgeführt wird, identifiziert er Buckets, die Ihren Kriterien entsprechen, und analysiert dann Objekte in diesen Buckets. Wenn Sie den Job so konfigurieren, dass er regelmäßig ausgeführt wird, tut er dies bei jeder Ausführung. Folglich analysiert der Job bei jeder Ausführung möglicherweise Objekte in unterschiedlichen Buckets, abhängig von Änderungen an Ihrem Bucket-Inventar und den von Ihnen definierten Kriterien.

Diese Konfiguration ist in Fällen hilfreich, in denen Sie möchten, dass sich der Analyseumfang des Jobs dynamisch an Änderungen an Ihrem Bucket-Inventar anpasst. Wenn Sie einen Job so konfigurieren, dass er Bucket-Kriterien verwendet und regelmäßig ausgeführt wird, identifiziert der Job automatisch neue Buckets, die den Kriterien entsprechen, und überprüft diese Buckets auf sensible Daten.

Die Themen in diesem Abschnitt enthalten zusätzliche Informationen zu den einzelnen Optionen.

Themen

- Auswahl bestimmter S3-Buckets
- Angabe von S3-Bucket-Kriterien

Auswahl bestimmter S3-Buckets

Wenn Sie sich dafür entscheiden, explizit jeden S3-Bucket auszuwählen, den ein Job analysieren soll, stellt Macie Ihnen eine vollständige Bestandsaufnahme Ihrer aktuellen Buckets zur Verfügung. AWS-Region Anschließend können Sie Ihr Inventar überprüfen und die gewünschten Buckets auswählen. Informationen darüber, wie Macie dieses Inventar für Sie generiert und verwaltet, finden Sie unter. So überwacht Macie die Amazon S3 S3-Datensicherheit

Wenn Sie der Macie-Administrator einer Organisation sind, umfasst das Inventar Buckets, die Mitgliedskonten in Ihrer Organisation gehören. Sie können bis zu 1.000 dieser Buckets auswählen, die sich über bis zu 1.000 Konten erstrecken.

Um Ihnen bei der Auswahl Ihrer Buckets zu helfen, enthält das Inventar Details und Statistiken für jeden Bucket. Dazu gehört die Datenmenge, die ein Job in jedem Bucket analysieren kann.

Klassifizierbare Objekte sind Objekte, die eine unterstützte Amazon S3 S3-Speicherklasse verwenden und eine Dateinamenerweiterung für ein unterstütztes Datei- oder Speicherformat haben. Das Inventar gibt auch an, ob bestehende Jobs für die Analyse von Objekten in einem Bucket konfiguriert sind. Anhand dieser Details können Sie den Umfang eines Jobs einschätzen und Ihre Bucket-Auswahl verfeinern.

In der Inventartabelle:

- Sensitivität — Gibt den aktuellen Vertraulichkeitswert eines Buckets an, wenn die automatische Erkennung sensibler Daten für Ihr Konto aktiviert ist.
- Klassifizierbare Objekte — Gibt die Gesamtzahl der Objekte an, die der Job in einem Bucket analysieren kann.
- Klassifizierbare Größe — Gibt die Gesamtspeichergröße aller Objekte an, die der Job in einem Bucket analysieren kann.

  Wenn ein Bucket komprimierte Objekte enthält, gibt dieser Wert nicht die tatsächliche Größe dieser Objekte nach der Dekomprimierung wieder. Wenn die Versionsverwaltung für einen Bucket aktiviert ist, basiert dieser Wert auf der Speichergröße der neuesten Version jedes Objekts im Bucket.
- Auftragsweise überwacht — Gibt an, ob vorhandene Jobs so konfiguriert sind, dass Objekte in einem Bucket regelmäßig täglich, wöchentlich oder monatlich analysiert werden.

  Wenn der Wert für dieses Feld Ja lautet, ist der Bucket explizit in einem periodischen Job enthalten oder der Bucket hat innerhalb der letzten 24 Stunden die Kriterien für einen periodischen Job erfüllt. Darüber hinaus lautet der Status von mindestens einem dieser Jobs nicht Storniert. Macie aktualisiert diese Daten täglich.
- Letzte Auftragsausführung — Wenn bestehende periodische oder einmalige Jobs so konfiguriert sind, dass sie Objekte in einem Bucket analysieren, gibt dieses Feld das Datum und die Uhrzeit an, zu der einer dieser Jobs zuletzt gestartet wurde. Andernfalls ist dieses Feld leer.

Wenn das Informationssymbol
()
neben einem beliebigen Bucket-Namen in der Tabelle angezeigt wird, empfehlen wir Ihnen, die neuesten Bucket-Metadaten von Amazon S3 abzurufen. Wählen Sie dazu über der Tabelle refresh
()
aus. Das Informationssymbol weist darauf hin, dass in den letzten 24 Stunden ein Bucket erstellt wurde, möglicherweise nachdem Macie im Rahmen des täglichen Aktualisierungszyklus das letzte

Mal Bucket- und Objektmetadaten von Amazon S3 abgerufen hat. Weitere Informationen finden Sie unter Datenaktualisierungen.

Wenn das Warnsymbol
(⚠)
neben dem Namen eines Buckets in der Tabelle erscheint, darf Macie nicht auf den Bucket oder die Objekte des Buckets zugreifen. Macie kann nur eine Teilmenge von Informationen über den Bucket bereitstellen, z. B. den Namen des Buckets. Das bedeutet, dass der Job keine Objekte im Bucket analysieren kann. Um das Problem zu untersuchen, überprüfen Sie die Richtlinien- und Berechtigungseinstellungen des Buckets in Amazon S3. Beispielsweise könnte der Bucket eine restriktive Bucket-Richtlinie haben. Weitere Informationen finden Sie unter Macie den Zugriff von S3-Buckets und -Objekten erlauben.

Um Ihre Ansicht des Inventars anzupassen und bestimmte Buckets leichter zu finden, können Sie die Tabelle filtern, indem Sie Filterkriterien in das Filterfeld eingeben. Die folgende Tabelle bietet einige Beispiele.

Um alle Buckets anzuzeigen, die...	Wende diesen Filter an...
Gehören einem bestimmten Konto	Konto-ID = *die 12-stellige ID für das* Konto
Sind öffentlich zugänglich	Wirksame Genehmigung = Öffentlich
Sind in keinen regelmäßigen Jobs enthalten	Aktiv vom Job überwacht = Falsch
Sind nicht in regelmäßigen oder einmaligen Aufträgen enthalten	Definiert in Job = False
Habe einen bestimmten Tag-Schlüssel*	Tag-Schlüssel = *der Tag-Schlüssel*
Habe einen bestimmten Tag-Wert*	Tag-Wert = *der* Tag-Wert
Enthalten unverschlüsselte Objekte (oder verwenden Sie eine clientseitige Verschlüsselung)	Die Anzahl der Objekte bei Verschlüsselung ist Keine Verschlüsselung und Von = 1

* Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden. Außerdem müssen Sie in einem Filter einen vollständigen, gültigen Wert für diese Felder angeben. Sie können keine Teilwerte angeben oder Platzhalterzeichen verwenden.

Um die Details eines Buckets anzuzeigen, wählen Sie den Namen des Buckets aus und schauen Sie im Detailbereich nach. Von dort aus können Sie auch:

- Wählen Sie ein Vergrößerungsglas für das Feld aus, um bestimmte Felder zu öffnen und nach unten zu gelangen. Wählen

  Sie, ob Bereiche mit demselben Wert oder Bereiche mit anderen

  Werten angezeigt werden sollen.
- Rufen Sie die neuesten Metadaten für Objekte im Bucket ab. Dies kann hilfreich sein, wenn Sie kürzlich einen Bucket erstellt haben oder in den letzten 24 Stunden wesentliche Änderungen an den Objekten des Buckets vorgenommen haben. Um die Daten abzurufen, wählen Sie im Bereich Objektstatistiken des Bedienfelds die Option refresh () aus. Diese Option ist für Buckets verfügbar, die 30.000 oder weniger Objekte enthalten.

Angabe von S3-Bucket-Kriterien

Wenn Sie sich dafür entscheiden, Bucket-Kriterien für einen Job anzugeben, bietet Macie Optionen zum Definieren und Testen der Kriterien. Dies sind Laufzeitkriterien, die bestimmen, welche S3-Buckets Objekte enthalten, die der Job analysieren soll. Bei jeder Ausführung des Jobs werden Buckets identifiziert, die Ihren Kriterien entsprechen, und anschließend die Objekte in den entsprechenden Buckets analysiert. Wenn Sie der Macie-Administrator einer Organisation sind, schließt dies auch Buckets ein, die Mitgliedskonten in Ihrer Organisation gehören.

Definition von Bucket-Kriterien

Bucket-Kriterien bestehen aus einer oder mehreren Bedingungen, die sich aus den Eigenschaften von S3-Buckets ergeben. Jede Bedingung, auch als Kriterium bezeichnet, besteht aus den folgenden Teilen:

- Ein eigenschaftsbasiertes Feld, z. B. Konto-ID oder Gültige Berechtigung.
- Ein Operator, entweder gleich (`eq`) oder ungleich (). `neq`
- Ein oder mehrere Werte.

- Eine Include- oder Exclude-Anweisung, die angibt, ob der Job Buckets analysieren (einschließen) oder überspringen (ausschließen) soll, die der Bedingung entsprechen.

Wenn Sie mehr als einen Wert für ein Feld angeben, verwendet Macie die OR-Logik, um die Werte zu verknüpfen. Wenn Sie mehr als eine Bedingung für die Kriterien angeben, verwendet Macie die UND-Logik, um die Bedingungen zu verknüpfen. Außerdem haben Ausschlussbedingungen Vorrang vor Einschlussbedingungen. Wenn Sie beispielsweise öffentlich zugängliche Buckets einbeziehen und Buckets mit bestimmten Tags ausschließen, analysiert der Job Objekte in allen Buckets, auf die öffentlich zugegriffen werden kann, sofern der Bucket nicht über eines der angegebenen Tags verfügt.

Sie können Bedingungen definieren, die sich aus einem der folgenden eigenschaftsbasierten Felder für S3-Buckets ableiten.

Konto-ID

Die eindeutige Kennung (ID) für denAWS-Konto, dem ein Bucket gehört. Um mehrere Werte für dieses Feld anzugeben, geben Sie die ID für jedes Konto ein und trennen Sie jeden Eintrag durch ein Komma.

Beachten Sie, dass Macie die Verwendung von Platzhalterzeichen oder Teilwerten für dieses Feld nicht unterstützt.

Bucket-Name

Der Name eines Buckets. Dieses Feld entspricht dem Feld Name, nicht dem Feld Amazon Resource Name (ARN) in Amazon S3. Um mehrere Werte für dieses Feld anzugeben, geben Sie den Namen jedes Buckets ein und trennen Sie jeden Eintrag durch ein Komma.

Beachten Sie, dass bei Werten zwischen Groß- und Kleinschreibung unterschieden wird. Darüber hinaus unterstützt Macie die Verwendung von Platzhalterzeichen oder Teilwerten für dieses Feld nicht.

Wirksame Erlaubnis

Gibt an, ob ein Bucket öffentlich zugänglich ist. Sie können einen oder mehrere der folgenden Werte für dieses Feld wählen:

- Nicht öffentlich — Die allgemeine Öffentlichkeit hat keinen Lese- oder Schreibzugriff auf den Bucket.
- Öffentlich — Die allgemeine Öffentlichkeit hat Lese- oder Schreibzugriff auf den Bucket.

- Unbekannt — Macie war nicht in der Lage, die Einstellungen für den öffentlichen Zugriff für den Bucket auszuwerten.

Um diesen Wert für einen Bucket zu ermitteln, analysiert Macie eine Kombination von Einstellungen auf Konto- und Bucket-Ebene für den Bucket: die Einstellungen für den Block öffentlichen Zugriff für das Konto, die Einstellungen für den Block öffentlichen Zugriff für den Bucket, die Bucket-Richtlinie für den Bucket und die Zugriffskontrollliste (ACL) für den Bucket.

Gemeinsamer Zugriff

Gibt an, ob ein Bucket mit einem anderenAWS-Konto, einer Amazon CloudFront Origin Access Identity (OAI) oder einer CloudFront Origin Access Control (OAC) geteilt wird. Sie können einen oder mehrere der folgenden Werte für dieses Feld wählen:

- Extern — Der Bucket wird mit einer oder mehreren der folgenden Personen oder einer beliebigen Kombination der folgenden Personen gemeinsam genutzt: eine CloudFront OAI, eine CloudFront OAC oder ein Konto, das extern zu Ihrer Organisation gehört (nicht Teil davon ist).
- Intern — Der Bucket wird mit einem oder mehreren Konten geteilt, die innerhalb (eines Teils) Ihrer Organisation liegen. Es wird nicht mit einer CloudFront OAI oder OAC geteilt.
- Nicht geteilt — Der Bucket wird nicht mit einem anderen Konto, einer CloudFront OAI oder einem OAC geteilt. CloudFront
- Unbekannt — Macie konnte die Einstellungen für den gemeinsamen Zugriff für den Bucket nicht auswerten.

Um festzustellen, ob ein Bucket mit einem anderen gemeinsam genutzt wirdAWS-Konto, analysiert Macie die Bucket-Richtlinie und die ACL für den Bucket. Darüber hinaus ist eine Organisation als eine Gruppe von Macie-Konten definiert, die über AWS Organizations oder auf Einladung von Macie als Gruppe verwandter Konten zentral verwaltet werden. Informationen zu den Amazon S3-Optionen für die gemeinsame Nutzung von Buckets finden Sie unter Identitäts- und Zugriffsverwaltung in Amazon S3 im Amazon Simple Storage Service-Benutzerhandbuch.

Um festzustellen, ob ein Bucket mit einer CloudFront OAI oder OAC gemeinsam genutzt wird, analysiert Macie die Bucket-Richtlinie für den Bucket. Eine CloudFront OAI oder OAC ermöglicht es Benutzern, über eine oder mehrere angegebene Distributionen auf die Objekte eines Buckets zuzugreifen. CloudFront Informationen zu CloudFront OAIs und OACs finden Sie unter Beschränken des Zugriffs auf einen Amazon S3 S3-Ursprung im Amazon CloudFront Developer Guide.

Tags

Die Tags, die einem Bucket zugeordnet sind. Tags sind Labels, die Sie definieren und bestimmten Ressourcentypen, einschließlich S3-Buckets, zuweisen können. AWS Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Informationen zum Taggen von S3-Buckets finden Sie unter Verwenden von S3-Bucket-Tags für die Kostenzuweisung im Amazon Simple Storage Service-Benutzerhandbuch.

Für einen Job zur Erkennung sensibler Daten können Sie diese Art von Bedingung verwenden, um Buckets mit einem bestimmten Tag-Schlüssel, einem bestimmten Tag-Wert oder einem bestimmten Tag-Schlüssel und Tag-Wert (als Paar) ein- oder auszuschließen. Beispiele:

- Wenn Sie einen Tag-Schlüssel angeben **`Project`** und keine Tag-Werte für eine Bedingung angeben, entspricht jeder Bucket, der den Tag-Schlüssel Project enthält, den Kriterien der Bedingung, unabhängig von den Tag-Werten, die diesem Tag-Schlüssel zugeordnet sind.
- Wenn Sie **`Development`** und **`Test`** als Tag-Werte angeben und keine Tag-Schlüssel für eine Bedingung angeben, entspricht jeder Bucket, der den **`Development`** oder **`Test`** -Tag-Wert enthält, den Kriterien der Bedingung, unabhängig von den Tag-Schlüsseln, die diesen Tag-Werten zugeordnet sind.

Um mehrere Tag-Schlüssel in einer Bedingung anzugeben, geben Sie jeden Tag-Schlüssel in das Schlüsselfeld ein und trennen Sie jeden Eintrag durch ein Komma. Um mehrere Tagwerte in einer Bedingung anzugeben, geben Sie jeden Tagwert in das Feld Wert ein und trennen Sie jeden Eintrag durch ein Komma.

Beachten Sie, dass bei Tag-Schlüsseln und -Werten zwischen Groß- und Kleinschreibung unterschieden wird. Darüber hinaus unterstützt Macie die Verwendung von Platzhalterzeichen oder Teilwerten in Tag-Bedingungen nicht.

Bucket-Kriterien testen

Während Sie Ihre Bucket-Kriterien definieren, können Sie die Kriterien testen und verfeinern, indem Sie sich eine Vorschau der Ergebnisse ansehen. Erweitern Sie dazu den Abschnitt Vorschau der Kriterienergebnisse anzeigen, der unter den Kriterien in der Konsole angezeigt wird. In diesem Abschnitt wird eine Tabelle mit allen Buckets angezeigt, die derzeit den Kriterien entsprechen.

Die Tabelle bietet auch einen Einblick in die Datenmenge, die der Job in jedem Bucket analysieren kann. Klassifizierbare Objekte sind Objekte, die eine unterstützte Amazon S3 S3-Speicherklasse verwenden und eine Dateinamenerweiterung für ein unterstütztes Datei- oder Speicherformat haben.

Die Tabelle gibt auch an, ob bestehende Jobs so konfiguriert sind, dass sie Objekte in einem Bucket regelmäßig analysieren.

In der Tabelle:

- Sensitivität — Zeigt den aktuellen Vertraulichkeitswert eines Buckets an, wenn die automatische Erkennung sensibler Daten für Ihr Konto aktiviert ist.
- Klassifizierbare Objekte — Gibt die Gesamtzahl der Objekte an, die der Job in einem Bucket analysieren kann.
- Klassifizierbare Größe — Gibt die Gesamtspeichergröße aller Objekte an, die der Job in einem Bucket analysieren kann.

  Wenn ein Bucket komprimierte Objekte enthält, gibt dieser Wert nicht die tatsächliche Größe dieser Objekte nach der Dekomprimierung wieder. Wenn die Versionsverwaltung für einen Bucket aktiviert ist, basiert dieser Wert auf der Speichergröße der neuesten Version jedes Objekts im Bucket.
- Auftragsweise überwacht — Gibt an, ob vorhandene Jobs so konfiguriert sind, dass Objekte in einem Bucket regelmäßig täglich, wöchentlich oder monatlich analysiert werden.

  Wenn der Wert für dieses Feld Ja lautet, ist der Bucket explizit in einem periodischen Job enthalten oder der Bucket hat innerhalb der letzten 24 Stunden die Kriterien für einen periodischen Job erfüllt. Darüber hinaus lautet der Status von mindestens einem dieser Jobs nicht Storniert. Macie aktualisiert diese Daten täglich.

Wenn das Warnsymbol
(⚠)
neben dem Namen eines Buckets erscheint, darf Macie nicht auf den Bucket oder die Objekte des Buckets zugreifen. Macie kann nur eine Teilmenge von Informationen über den Bucket bereitstellen, z. B. den Namen des Buckets. Das bedeutet, dass der Job keine Objekte im Bucket analysieren kann. Um das Problem zu untersuchen, überprüfen Sie die Richtlinien- und Berechtigungseinstellungen des Buckets in Amazon S3. Beispielsweise könnte der Bucket eine restriktive Bucket-Richtlinie haben. Weitere Informationen finden Sie unter Macie den Zugriff von S3-Buckets und -Objekten erlauben.

Um die Bucket-Kriterien für den Job zu verfeinern, verwenden Sie die Filteroptionen, um Bedingungen zu den Kriterien hinzuzufügen, zu ändern oder zu entfernen. Macie aktualisiert dann die Tabelle, um Ihre Änderungen widerzuspiegeln.

Bestehende S3-Objekte einbeziehen

Sie können Aufgaben zur Erkennung sensibler Daten verwenden, um eine fortlaufende, inkrementelle Analyse von Objekten in S3-Buckets durchzuführen. Wenn Sie einen Job so konfigurieren, dass er regelmäßig ausgeführt wird, erledigt Macie dies automatisch für Sie. Bei jedem Lauf werden nur die Objekte analysiert, die nach dem vorherigen Lauf erstellt oder geändert wurden. Mit der Option Bestehende Objekte einbeziehen wählen Sie den Startpunkt für das erste Inkrement:

- Um alle vorhandenen Objekte unmittelbar nach Abschluss der Erstellung des Jobs zu analysieren, aktivieren Sie das Kontrollkästchen für diese Option.
- Um zu warten und nur die Objekte zu analysieren, die nach der Erstellung des Jobs und vor der ersten Ausführung erstellt oder geändert wurden, deaktivieren Sie das Kontrollkästchen für diese Option.

  Das Deaktivieren dieses Kontrollkästchens ist in Fällen hilfreich, in denen Sie die Daten bereits analysiert haben und sie regelmäßig weiter analysieren möchten. Wenn Sie beispielsweise zuvor einen anderen Dienst oder eine andere Anwendung zum Klassifizieren von Daten verwendet haben und seit Kurzem Macie verwenden, können Sie diese Option verwenden, um sicherzustellen, dass Ihre Daten kontinuierlich erkannt und klassifiziert werden, ohne dass Ihnen unnötige Kosten entstehen oder Klassifizierungsdaten dupliziert werden.

Bei jeder nachfolgenden Ausführung eines periodischen Jobs werden automatisch nur die Objekte analysiert, die nach dem vorherigen Lauf erstellt oder geändert wurden.

Sowohl für periodische als auch für einmalige Jobs können Sie einen Job auch so konfigurieren, dass nur die Objekte analysiert werden, die vor oder nach einer bestimmten Zeit oder in einem bestimmten Zeitraum erstellt oder geändert wurden. Fügen Sie dazu Objektkriterien hinzu, die das Datum der letzten Änderung für Objekte verwenden.

Tiefe der Probenahme

Mit dieser Option geben Sie den Prozentsatz der in Frage kommenden S3-Objekte an, die Macie analysieren soll, wenn ein Discovery-Job für sensible Daten ausgeführt wird. In Frage kommende Objekte sind Objekte, die: eine unterstützte Amazon S3 S3-Speicherklasse verwenden, eine Dateinamenerweiterung für ein unterstütztes Datei- oder Speicherformat haben und andere Kriterien erfüllen, die Sie für den Job angeben.

Wenn dieser Wert unter 100% liegt, wählt Macie nach dem Zufallsprinzip geeignete Objekte für die Analyse bis zum angegebenen Prozentsatz aus und analysiert alle Daten in diesen Objekten.

Wenn Sie beispielsweise einen Job für die Analyse von 10.000 Objekten konfigurieren und eine Stichprobentiefe von 20% angeben, analysiert der Job ungefähr 2.000 zufällig ausgewählte, geeignete Objekte.

Durch die Reduzierung der Stichprobentiefe eines Jobs können die Kosten gesenkt und die Dauer eines Jobs verkürzt werden. Dies ist hilfreich in Fällen, in denen die Daten in Objekten sehr konsistent sind und Sie feststellen möchten, ob ein S3-Bucket und nicht jedes Objekt sensible Daten enthält.

Beachten Sie, dass diese Option den Prozentsatz der analysierten Objekte steuert, nicht den Prozentsatz der analysierten Byte. Wenn Sie eine Stichprobentiefe von weniger als 100% eingeben, analysiert Macie alle Daten in jedem ausgewählten Objekt, nicht den Prozentsatz der Daten in jedem ausgewählten Objekt.

S3-Objektkriterien

Um den Umfang eines Discovery-Jobs für sensible Daten zu optimieren, können Sie auch benutzerdefinierte Kriterien definieren, die bestimmen, welche S3-Objekte Macie in die Analyse eines Jobs einbezieht oder ausschließt. Diese Kriterien bestehen aus einer oder mehreren Bedingungen, die sich aus den Eigenschaften von S3-Objekten ergeben. Die Bedingungen gelten für Objekte in allen S3-Buckets, für deren Analyse ein Job konfiguriert ist. Wenn ein Bucket mehrere Versionen eines Objekts enthält, gelten die Bedingungen für die neueste Version des Objekts.

Wenn Sie mehrere Bedingungen als Objektkriterien definieren, verwendet Macie die UND-Logik, um die Bedingungen zu verknüpfen. Außerdem haben Ausschlussbedingungen Vorrang vor Einschlussbedingungen. Wenn Sie beispielsweise Objekte mit der Dateinamenerweiterung PDF einbeziehen und Objekte ausschließen, die größer als 5 MB sind, analysiert der Job jedes Objekt mit der Dateinamenerweiterung PDF, sofern das Objekt nicht größer als 5 MB ist.

Sie können Bedingungen definieren, die sich aus einer der folgenden Eigenschaften von S3-Objekten ableiten.

Erweiterung des Dateinamens

Dies entspricht der Dateinamenerweiterung eines S3-Objekts. Sie können diese Art von Bedingung verwenden, um Objekte basierend auf dem Dateityp ein- oder auszuschließen. Um dies für mehrere Dateitypen zu tun, geben Sie die Dateinamenerweiterung für jeden Typ ein und trennen Sie jeden Eintrag durch ein Komma, zum Beispiel:. **`docx,pdf,xlsx`** Wenn Sie mehrere Dateinamenerweiterungen als Werte für eine Bedingung eingeben, verwendet Macie die OR-Logik, um die Werte zu verknüpfen.

Beachten Sie, dass bei Werten zwischen Groß- und Kleinschreibung unterschieden wird. Darüber hinaus unterstützt Macie die Verwendung von Teilwerten oder Platzhalterzeichen in dieser Art von Bedingung nicht.

Hinweise zu den Dateitypen, die Macie analysieren kann, finden Sie unter. Unterstützte Datei- und Speicherformate

Zuletzt geändert

Dies entspricht dem Feld Letzte Änderung in Amazon S3. In Amazon S3 speichert dieses Feld das Datum und die Uhrzeit der Erstellung oder letzten Änderung eines S3-Objekts, je nachdem, welcher Zeitpunkt zuletzt ist.

Bei einem Discovery-Job für sensible Daten kann es sich bei dieser Bedingung um ein bestimmtes Datum, ein bestimmtes Datum und eine bestimmte Uhrzeit oder um einen exklusiven Zeitraum handeln:

- Um Objekte zu analysieren, die nach einem bestimmten Datum oder Datum und Uhrzeit zuletzt geändert wurden, geben Sie die Werte in die Felder Von ein.
- Um Objekte zu analysieren, die vor einem bestimmten Datum oder Datum und Uhrzeit zuletzt geändert wurden, geben Sie die Werte in die Felder Bis ein.
- Um Objekte zu analysieren, die in einem bestimmten Zeitraum zuletzt geändert wurden, verwenden Sie die Felder Von, um die Werte für das erste Datum oder Datum und die erste Uhrzeit im Zeitraum einzugeben. Verwenden Sie die Felder Bis, um die Werte für das letzte Datum oder Datum und die letzte Uhrzeit im Zeitraum einzugeben.
- Um Objekte zu analysieren, die zu einem beliebigen Zeitpunkt an einem bestimmten Tag zuletzt geändert wurden, geben Sie das Datum in das Feld Startdatum ein. Geben Sie das Datum für den nächsten Tag in das Feld Bis ein. Vergewissern Sie sich dann, dass beide Zeitfelder leer sind. (Macie behandelt ein leeres Zeitfeld als`00:00:00`.) Um beispielsweise Objekte zu analysieren, die sich am 9. August 2022 geändert haben, geben Sie **`2022/08/09`** in das Feld Startdatum und **`2022/08/10`** in das Feld Bis Datum ein, und geben Sie in keinem der beiden Zeitfelder einen Wert ein.

Geben Sie beliebige Zeitwerte in der koordinierten Weltzeit (UTC) ein und verwenden Sie die 24-Stunden-Notation.

Präfix

Dies entspricht dem Schlüsselfeld in Amazon S3. In Amazon S3 speichert dieses Feld den Namen eines S3-Objekts, einschließlich des Präfixes des Objekts. Ein Präfix ähnelt einem Verzeichnispfad innerhalb eines Buckets. Es ermöglicht Ihnen, ähnliche Objekte in einem

Bucket zu gruppieren, ähnlich wie Sie ähnliche Dateien zusammen in einem Ordner auf einem Dateisystem speichern könnten. Informationen zu Objektpräfixen und Ordnern in Amazon S3 finden Sie unter Organisieren von Objekten in der Amazon S3 S3-Konsole mithilfe von Ordnern im Amazon Simple Storage Service-Benutzerhandbuch.

Sie können diese Art von Bedingung verwenden, um Objekte ein- oder auszuschließen, deren Schlüssel (Namen) mit einem bestimmten Wert beginnen. Um beispielsweise alle Objekte auszuschließen, deren Schlüssel mit 1 beginnt AWSLogs, geben Sie **`AWSLogs`** als Wert für eine Präfix-Bedingung ein und wählen Sie dann Ausschließen.

Wenn Sie mehrere Präfixe als Werte für eine Bedingung eingeben, verwendet Macie die OR-Logik, um die Werte zu verknüpfen. Wenn Sie beispielsweise **`AWSLogs1`** und **`AWSLogs2`** als Werte für eine Bedingung eingeben, entspricht jedes Objekt, dessen Schlüssel mit AWSLogs1 oder AWSLogs2 beginnt, den Kriterien der Bedingung.

Wenn Sie einen Wert für eine Präfix-Bedingung eingeben, sollten Sie Folgendes beachten:

- Bei Werten wird zwischen Groß- und Kleinschreibung unterschieden.
- Macie unterstützt die Verwendung von Platzhalterzeichen in diesen Werten nicht.
- In Amazon S3 enthält der Schlüssel eines Objekts nicht den Namen des Buckets, der das Objekt enthält. Geben Sie aus diesem Grund in diesen Werten keine Bucket-Namen an.
- Wenn ein Präfix ein Trennzeichen enthält, nehmen Sie das Trennzeichen in den Wert auf. Geben Sie beispielsweise ein, ***`AWSLogs/eventlogs`*** um eine Bedingung für alle Objekte zu definieren, deren Schlüssel mit /eventlogs beginnt. AWSLogs Macie unterstützt das standardmäßige Amazon S3 S3-Trennzeichen, bei dem es sich um einen Schrägstrich (/) handelt, und benutzerdefinierte Trennzeichen.

Beachten Sie auch, dass ein Objekt nur dann den Kriterien einer Bedingung entspricht, wenn der Schlüssel des Objekts genau dem von Ihnen eingegebenen Wert entspricht, beginnend mit dem ersten Zeichen im Objektschlüssel. Darüber hinaus wendet Macie eine Bedingung auf den kompletten Schlüsselwert für ein Objekt an, einschließlich des Dateinamens des Objekts.

Wenn der Schlüssel eines Objekts beispielsweise AWSLogs/eventlogs/testlog.csv lautet und Sie einen der folgenden Werte für eine Bedingung eingeben, entspricht das Objekt den Kriterien der Bedingung:

- **`AWSLogs`**
- **`AWSLogs/event`**
- **`AWSLogs/eventlogs/`**

- **AWSLogs/eventlogs/testlog**
- **AWSLogs/eventlogs/testlog.csv**

Wenn Sie jedoch eingeben***eventlogs***, entspricht das Objekt nicht den Kriterien — der Wert der Bedingung enthält nicht den ersten Teil des Schlüssels,AWSLogs/. Ebenso entspricht das Objekt bei der Eingabe **awslogs** aufgrund von Unterschieden in der Groß- und Kleinschreibung nicht den Kriterien.

Größe des Speichers

Dies entspricht dem Feld Größe in Amazon S3. In Amazon S3 gibt dieses Feld die Gesamtspeichergröße eines S3-Objekts an. Wenn es sich bei einem Objekt um eine komprimierte Datei handelt, spiegelt dieser Wert nicht die tatsächliche Größe der Datei nach der Dekomprimierung wider.

Sie können diese Art von Bedingung verwenden, um Objekte ein- oder auszuschließen, die kleiner als eine bestimmte Größe sind, größer als eine bestimmte Größe sind oder in einen bestimmten Größenbereich fallen. Macie wendet diese Art von Bedingung auf alle Objekttypen an, einschließlich komprimierter Dateien oder Archivdateien und der darin enthaltenen Dateien. Informationen zu größenabhängigen Einschränkungen für jedes unterstützte Format finden Sie unter. Amazon Macie Macie-Kontingente

Tags

Die Tags, die einem S3-Objekt zugeordnet sind. Tags sind Beschriftungen, die Sie definieren und bestimmten RessourcentypenAWS, einschließlich S3-Objekten, zuweisen können. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Informationen zum Taggen von S3-Objekten finden Sie unter Kategorisieren Ihres Speichers mithilfe von Tags im Amazon Simple Storage Service-Benutzerhandbuch.

Für einen Job zur Erkennung sensibler Daten können Sie diese Art von Bedingung verwenden, um Objekte mit einem bestimmten Tag ein- oder auszuschließen. Dabei kann es sich um einen bestimmten Tag-Schlüssel oder um einen bestimmten Tag-Schlüssel und Tag-Wert (als Paar) handeln. Wenn Sie mehrere Tags als Werte für eine Bedingung angeben, verwendet Macie die OR-Logik, um die Werte zu verknüpfen. Wenn Sie beispielsweise **Project1** und **Project2** als Tagschlüssel für eine Bedingung angeben, entspricht jedes Objekt, das den Tagschlüssel Project1 oder Project2 besitzt, den Kriterien der Bedingung.

Beachten Sie, dass bei Tag-Schlüsseln und -Werten zwischen Groß- und Kleinschreibung unterschieden wird. Außerdem unterstützt Macie die Verwendung von Teilwerten oder Platzhalterzeichen in dieser Art von Bedingung nicht.

Erstellen einer Aufgabe zur Erkennung vertraulicher Daten

Mit Amazon Macie können Sie Discovery-Jobs für sensible Daten erstellen und ausführen, um die Erkennung, Protokollierung und Berichterstattung sensibler Daten in Amazon Simple Storage Service (Amazon S3) -Buckets zu automatisieren. Ein Discovery-Job für sensible Daten ist eine Reihe automatisierter Verarbeitungs- und Analyseaufgaben, die Macie ausführt, um sensible Daten in Amazon S3 S3-Objekten zu erkennen und zu melden. Im weiteren Verlauf der Analyse erstellt Macie detaillierte Berichte über die gefundenen sensiblen Daten und die durchgeführten Analysen: Ergebnisse sensibler Daten, bei denen sensible Daten gemeldet werden, die Macie in einzelnen S3-Objekten findet, und Ergebnisse der Erkennung sensibler Daten, in denen Details zur Analyse einzelner S3-Objekte protokolliert werden. Weitere Informationen finden Sie unter Überprüfung der Jobstatistiken und Ergebnisse.

Wenn Sie einen Job erstellen, geben Sie zunächst an, welche S3-Buckets Objekte enthalten, die Macie analysieren soll, wenn der Job ausgeführt wird — spezifische Buckets, die Sie auswählen, oder Buckets, die bestimmten Kriterien entsprechen. Anschließend geben Sie an, wie oft der Job ausgeführt werden soll — einmal oder regelmäßig auf täglicher, wöchentlicher oder monatlicher Basis. Sie können auch Optionen wählen, um den Umfang der Analyse des Jobs zu verfeinern. Zu den Optionen gehören benutzerdefinierte Kriterien, die sich aus den Eigenschaften von S3-Objekten ableiten, wie z. B. Tags, Präfixe und wann ein Objekt zuletzt geändert wurde.

Nachdem Sie den Zeitplan und den Umfang des Jobs definiert haben, geben Sie an, welche verwalteten Datenbezeichner und benutzerdefinierten Datenbezeichner der Job verwenden soll:

- Ein verwalteter Datenbezeichner besteht aus einer Reihe integrierter Kriterien und Techniken, mit denen ein bestimmter Typ vertraulicher Daten erkannt werden kann, z. B. Kreditkartennummern, AWS geheime Zugangsschlüssel oder Passnummern für ein bestimmtes Land oder eine bestimmte Region. Diese Identifikatoren können eine große und ständig wachsende Liste sensibler Datentypen für viele Länder und Regionen erkennen, darunter mehrere Arten von Anmeldedaten, Finanzinformationen und personenbezogenen Daten (PII). Weitere Informationen finden Sie unter Verwenden von verwalteten Datenbezeichnern.
- Eine benutzerdefinierte Daten-ID besteht aus einer Reihe von Kriterien, die Sie zur Erkennung vertraulicher Daten definieren. Mithilfe benutzerdefinierter Datenkennungen können Sie sensible Daten erkennen, die bestimmte Szenarien, geistiges Eigentum oder geschützte Daten Ihres Unternehmens widerspiegeln, z. B. Mitarbeiter-IDs, Kundenkontonummern oder interne Datenklassifizierungen. Sie können die von Macie bereitgestellten verwalteten Datenkennungen ergänzen. Weitere Informationen finden Sie unter Erstellen von benutzerdefinierten Datenbezeichnern.

Anschließend wählen Sie optional Zulassungslisten aus, die der Job verwenden soll. Eine Zulassungsliste gibt Text oder ein Textmuster an, das Macie ignorieren soll. Dabei handelt es sich in der Regel um Ausnahmen für sensible Daten für Ihre speziellen Szenarien oder Umgebungen, z. B. öffentliche Namen oder Telefonnummern für Ihre Organisation oder Beispieldaten, die Ihre Organisation für Tests verwendet. Weitere Informationen finden Sie unter Definition von Ausnahmen für sensible Daten mit Zulassungslisten.

Wenn Sie mit der Auswahl dieser Optionen fertig sind, können Sie allgemeine Einstellungen für den Job eingeben, z. B. den Namen und die Beschreibung des Jobs. Anschließend können Sie den Job überprüfen und speichern.

Aufgaben

- Bevor Sie beginnen
- Schritt 1: Wählen Sie S3-Buckets
- Schritt 2: Überprüfen Sie Ihre S3-Bucket-Auswahlen oder -Kriterien
- Schritt 3: Definieren Sie den Zeitplan und verfeinern Sie den Umfang
- Schritt 4: Wählen Sie verwaltete Datenkennungen aus
- Schritt 5: Wählen Sie benutzerdefinierte Datenkennungen
- Schritt 6: Wählen Sie Zulassungslisten aus
- Schritt 7: Geben Sie die allgemeinen Einstellungen ein
- Schritt 8: Überprüfen und erstellen

Bevor Sie beginnen

Bevor Sie einen Job erstellen, sollten Sie die folgenden Schritte ausführen:

- Stellen Sie sicher, dass Sie Macie so konfiguriert haben, dass Ihre Ergebnisse der Erkennung sensibler Daten in einem S3-Bucket gespeichert werden. Wählen Sie dazu im Navigationsbereich der Amazon Macie Macie-Konsole Discovery-Ergebnisse aus. Vergewissern Sie sich dann, dass Sie die Einstellungen eingegeben haben. Weitere Informationen zu diesen Einstellungen finden Sie unterSpeicherung und Beibehaltung der Erkennungsergebnisse von vertraulichen Daten.
- Erstellen Sie alle benutzerdefinierten Datenbezeichner, die der Job verwenden soll. Um zu erfahren wie dies geht, vgl. Erstellen von benutzerdefinierten Datenbezeichnern.
- Erstellen Sie alle Zulassungslisten, die der Job verwenden soll. Um zu erfahren wie dies geht, vgl. Erlaubnislisten erstellen und verwalten.

- Wenn Sie verschlüsselte S3-Objekte analysieren möchten, stellen Sie sicher, dass Macie auf die entsprechenden Verschlüsselungsschlüssel zugreifen und diese verwenden kann. Weitere Informationen finden Sie unter Analysieren verschlüsselter S3-Objekte.
- Wenn Sie Objekte in einem S3-Bucket analysieren möchten, für den eine restriktive Bucket-Richtlinie gilt, stellen Sie sicher, dass Macie auf die Objekte zugreifen darf. Weitere Informationen finden Sie unter Macie den Zugriff von S3-Buckets und -Objekten erlauben.

Wenn Sie diese Dinge tun, bevor Sie einen Job erstellen, optimieren Sie die Erstellung des Jobs und stellen sicher, dass der Job die gewünschten Daten analysieren kann.

Schritt 1: Wählen Sie S3-Buckets

Der erste Schritt beim Erstellen eines Jobs besteht darin, anzugeben, welche S3-Buckets Objekte enthalten, die Macie analysieren soll, wenn der Job ausgeführt wird. Für diesen Schritt haben Sie zwei Möglichkeiten:

- Bestimmte Buckets auswählen — Mit dieser Option wählen Sie explizit jeden S3-Bucket aus, den der Job analysieren soll. Wenn der Job dann ausgeführt wird, analysiert er nur Objekte in den von Ihnen ausgewählten Buckets.
- Bucket-Kriterien angeben — Mit dieser Option definieren Sie Laufzeitkriterien, die bestimmen, welche S3-Buckets der Job analysiert. Die Kriterien bestehen aus einer oder mehreren Bedingungen, die sich aus Bucket-Eigenschaften ergeben. Wenn der Job dann ausgeführt wird, identifiziert er Buckets, die Ihren Kriterien entsprechen, und analysiert Objekte in diesen Buckets.

Ausführliche Informationen zu diesen Optionen finden Sie unter. Bereichsoptionen für Aufgaben

Die folgenden Abschnitte enthalten Anweisungen zur Auswahl und Konfiguration der einzelnen Optionen. Wählen Sie den Abschnitt für die gewünschte Option aus.

Wählen Sie bestimmte Buckets aus

Wenn Sie sich dafür entscheiden, jeden S3-Bucket, den der Job analysieren soll, explizit auszuwählen, stellt Macie Ihnen einen vollständigen Bestand Ihrer aktuellen Buckets zur Verfügung. AWS-Region Sie können dieses Inventar dann verwenden, um einen oder mehrere Buckets für den zu analysierenden Job auszuwählen. Weitere Informationen zu diesem Inventar finden Sie unterAuswahl bestimmter S3-Buckets.

Wenn Sie der Macie-Administrator einer Organisation sind, umfasst das Inventar Buckets, die Mitgliedskonten in Ihrer Organisation gehören. Sie können den Job so konfigurieren, dass Objekte in bis zu 1.000 dieser Buckets analysiert werden, die sich über bis zu 1.000 Konten erstrecken.

Um bestimmte Buckets für den Job auszuwählen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich die Option Jobs (Aufträge) aus.
3. Wählen Sie Create job (Auftrag erstellen) aus.
4. Wählen Sie auf der Seite S3-Buckets auswählen die Option Bestimmte Buckets auswählen aus. Macie zeigt eine Tabelle mit allen Buckets für Ihr Konto in der aktuellen Region an.
5. Wählen Sie im Abschnitt S3-Buckets auswählen optional refresh
   (),
   um die neuesten Bucket-Metadaten von Amazon S3 abzurufen.

   Wenn das Informationssymbol
   ()
   neben Bucket-Namen angezeigt wird, empfehlen wir Ihnen, dies zu tun. Dieses Symbol weist darauf hin, dass in den letzten 24 Stunden ein Bucket erstellt wurde, möglicherweise nachdem Macie im Rahmen des täglichen Aktualisierungszyklus das letzte Mal Bucket- und Objektmetadaten von Amazon S3 abgerufen hat.
6. Aktivieren Sie in der Tabelle das Kontrollkästchen für jeden Bucket, den der Job analysieren soll.

> **Tip**
>
> - Um bestimmte Buckets einfacher zu finden, geben Sie Filterkriterien in das Filterfeld über der Tabelle ein. Sie können die Tabelle auch sortieren, indem Sie eine Spaltenüberschrift auswählen.
> - Informationen darüber, ob Sie bereits einen Job für die regelmäßige Analyse von Objekten in einem Bucket konfiguriert haben, finden Sie im Feld Überwacht durch Job. Wenn in einem Feld Ja angezeigt wird, ist der Bucket explizit in einem periodischen Job enthalten oder der Bucket hat innerhalb der letzten 24 Stunden die Kriterien für einen periodischen Job erfüllt. Darüber hinaus lautet der Status von mindestens einem dieser Jobs nicht Storniert. Macie aktualisiert diese Daten täglich.

- Informationen darüber, wann ein vorhandener periodischer oder einmaliger Job zuletzt Objekte in einem Bucket analysiert hat, finden Sie im Feld Letzte Auftragsausführung. Weitere Informationen zu diesem Job finden Sie in den Details des Buckets.
- Um die Details eines Buckets anzuzeigen, wählen Sie den Namen des Buckets aus. Zusätzlich zu den auftragsbezogenen Informationen bietet das Detailfenster Statistiken und andere Informationen über den Bucket, z. B. die Einstellungen für den öffentlichen Zugriff des Buckets. Weitere Informationen zu diesen Daten finden Sie unterÜberprüfen Ihres S3-Bucket-Bestands.

7. Wenn Sie mit der Auswahl der Buckets fertig sind, wählen Sie Weiter.

Im nächsten Schritt überprüfen und verifizieren Sie Ihre Auswahl.

Geben Sie Bucket-Kriterien an

Wenn Sie Laufzeitkriterien angeben, die bestimmen, welche S3-Buckets der Job analysiert, bietet Macie Optionen, die Sie bei der Auswahl von Feldern, Operatoren und Werten für einzelne Bedingungen in den Kriterien unterstützen. Weitere Informationen zu diesen Optionen finden Sie unter Angabe von S3-Bucket-Kriterien.

Um Bucket-Kriterien für den Job anzugeben

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich die Option Jobs (Aufträge) aus.
3. Wählen Sie Create job (Auftrag erstellen) aus.
4. Wählen Sie auf der Seite S3-Buckets auswählen die Option Bucket-Kriterien angeben aus.
5. Gehen Sie unter Bucket-Kriterien angeben wie folgt vor, um den Kriterien eine Bedingung hinzuzufügen:

   a. Platzieren Sie den Cursor in dem Filterfeld und wählen Sie dann die Bucket-Eigenschaft aus, die für die Bedingung verwendet werden soll.
   b. Wählen Sie im ersten Feld einen Operator für die Bedingung aus: Gleich oder Nicht gleich.
   c. Geben Sie im nächsten Feld einen oder mehrere Werte für die Eigenschaft ein.

      Je nach Typ und Art der Bucket-Eigenschaft zeigt Macie verschiedene Optionen für die Eingabe von Werten an. Wenn Sie beispielsweise die Eigenschaft Effektive Berechtigung wählen, zeigt Macie eine Liste mit Werten an, aus denen Sie wählen können. Wenn Sie die

Eigenschaft Konto-ID wählen, zeigt Macie ein Textfeld an, in das Sie eine oder mehrere AWS-Konto IDs eingeben können. Um mehrere Werte in ein Textfeld einzugeben, geben Sie jeden Wert ein und trennen Sie jeden Eintrag durch ein Komma.

d. Wählen Sie Apply (Anwenden) aus. Macie fügt die Bedingung hinzu und zeigt sie unter dem Filterfeld an.

   Standardmäßig fügt Macie die Bedingung mit einer Include-Anweisung hinzu. Das bedeutet, dass der Job so konfiguriert ist, dass Objekte in Buckets analysiert (eingeschlossen) werden, die der Bedingung entsprechen. Um Buckets zu überspringen (auszuschließen), die der Bedingung entsprechen, wählen Sie Include für die Bedingung und dann Exclude aus.

e. Wiederholen Sie die vorherigen Schritte für jede weitere Bedingung, die Sie zu den Kriterien hinzufügen möchten.

6. Um Ihre Kriterien zu testen, erweitern Sie den Abschnitt Vorschau der Kriterienergebnisse anzeigen. In diesem Abschnitt wird eine Tabelle mit allen Buckets angezeigt, die derzeit den Kriterien entsprechen.
7. Gehen Sie wie folgt vor, um Ihre Kriterien zu verfeinern:

   - Um eine Bedingung zu entfernen, wählen Sie X für die Bedingung aus.
   - Um eine Bedingung zu ändern, entfernen Sie die Bedingung, indem Sie X für die Bedingung wählen. Fügen Sie dann eine Bedingung hinzu, die die richtigen Einstellungen hat.
   - Um alle Bedingungen zu entfernen, wählen Sie Filter löschen.

   Macie aktualisiert die Tabelle mit den Kriterienergebnissen, um Ihre Änderungen widerzuspiegeln.
8. Wenn Sie mit der Angabe der Bucket-Kriterien fertig sind, wählen Sie Weiter.

Im nächsten Schritt überprüfen und verifizieren Sie Ihre Kriterien.

Schritt 2: Überprüfen Sie Ihre S3-Bucket-Auswahlen oder -Kriterien

Stellen Sie für diesen Schritt sicher, dass Sie im vorherigen Schritt die richtigen Einstellungen ausgewählt haben:

- Überprüfen Sie Ihre Bucket-Auswahl — Wenn Sie bestimmte S3-Buckets für den Job ausgewählt haben, überprüfen Sie die Bucket-Tabelle und ändern Sie Ihre Bucket-Auswahl nach Bedarf. Die Tabelle gibt Aufschluss über den voraussichtlichen Umfang und die Kosten der Auftragsanalyse.

Die Daten basieren auf der Größe und Art der Objekte, die derzeit in einem Bucket gespeichert sind.

In der Tabelle gibt das Feld Geschätzte Kosten die geschätzten Gesamtkosten (in US-Dollar) für die Analyse von Objekten in einem S3-Bucket an. Jede Schätzung spiegelt die voraussichtliche Menge an unkomprimierten Daten wider, die der Job in einem Bucket analysieren wird. Handelt es sich bei Objekten um komprimierte Dateien oder Archivdateien, geht die Schätzung davon aus, dass die Dateien ein Komprimierungsverhältnis von 3:1 verwenden und der Job alle extrahierten Dateien analysieren kann. Weitere Informationen finden Sie unter Prognose und Überwachung der Arbeitskosten.

- Überprüfen Sie Ihre Bucket-Kriterien — Wenn Sie Bucket-Kriterien für den Job angegeben haben, überprüfen Sie jede Bedingung in den Kriterien. Um die Kriterien zu ändern, wählen Sie Zurück und verwenden Sie dann die Filteroptionen des vorherigen Schritts, um die richtigen Kriterien einzugeben. Wenn Sie fertig sind, wählen Sie Next (Weiter) aus.

Wenn Sie mit der Überprüfung und Überprüfung der Einstellungen fertig sind, wählen Sie Weiter.

Schritt 3: Definieren Sie den Zeitplan und verfeinern Sie den Umfang

Geben Sie für diesen Schritt an, wie oft der Job ausgeführt werden soll — einmalig oder regelmäßig täglich, wöchentlich oder monatlich. Wählen Sie außerdem verschiedene Optionen, um den Umfang der Jobanalyse zu verfeinern. Weitere Informationen zu diesen Optionen finden Sie unterBereichsoptionen für Aufgaben.

Um den Zeitplan zu definieren und den Umfang des Auftrags zu verfeinern

1. Geben Sie auf der Seite „Umfang verfeinern“ an, wie oft der Job ausgeführt werden soll:

   - Wenn der Job nur einmal ausgeführt werden soll, unmittelbar nachdem Sie ihn erstellt haben, wählen Sie Einmaliger Job.
   - Um den Job regelmäßig und wiederkehrend auszuführen, wählen Sie Geplanter Job. Wählen Sie unter Aktualisierungshäufigkeit aus, ob der Job täglich, wöchentlich oder monatlich ausgeführt werden soll. Verwenden Sie dann die Option Bestehende Objekte einbeziehen, um den Umfang der ersten Ausführung des Jobs zu definieren:
     - Aktivieren Sie dieses Kontrollkästchen, um alle vorhandenen Objekte unmittelbar nach Abschluss der Auftragserstellung zu analysieren. Bei jedem nachfolgenden Lauf werden nur die Objekte analysiert, die nach dem vorherigen Lauf erstellt oder geändert wurden.

- Deaktivieren Sie dieses Kontrollkästchen, um die Analyse aller vorhandenen Objekte zu überspringen. Bei der ersten Ausführung des Jobs werden nur die Objekte analysiert, die erstellt oder geändert wurden, nachdem Sie die Erstellung des Jobs abgeschlossen haben und bevor der erste Lauf gestartet wird. Bei jedem nachfolgenden Lauf werden nur die Objekte analysiert, die nach dem vorherigen Lauf erstellt oder geändert wurden.

  Das Deaktivieren dieses Kästchens ist in Fällen hilfreich, in denen Sie die Daten bereits analysiert haben und sie regelmäßig weiter analysieren möchten. Wenn Sie beispielsweise zuvor einen anderen Dienst oder eine andere Anwendung zum Klassifizieren von Daten verwendet haben und seit Kurzem Macie verwenden, können Sie diese Option verwenden, um sicherzustellen, dass Ihre Daten kontinuierlich erkannt und klassifiziert werden, ohne dass Ihnen unnötige Kosten entstehen oder Klassifizierungsdaten dupliziert werden.

2. (Optional) Um den Prozentsatz der Objekte anzugeben, die der Job analysieren soll, geben Sie den Prozentsatz in das Feld Stichprobentiefe ein.

   Wenn dieser Wert unter 100% liegt, wählt Macie die zu analysierenden Objekte nach dem Zufallsprinzip bis zum angegebenen Prozentsatz aus und analysiert alle Daten in diesen Objekten. Der Standardwert ist 100%.

3. (Optional) Um spezifische Kriterien hinzuzufügen, die bestimmen, welche S3-Objekte in die Analyse des Jobs aufgenommen oder ausgeschlossen werden, erweitern Sie den Abschnitt Zusätzliche Einstellungen und geben Sie dann die Kriterien ein. Diese Kriterien bestehen aus einzelnen Bedingungen, die sich aus den Eigenschaften von Objekten ergeben:

   - Um Objekte zu analysieren (einzubeziehen), die eine bestimmte Bedingung erfüllen, geben Sie den Bedingungstyp und den Wert ein, und wählen Sie dann Einschließen aus.
   - Um Objekte zu überspringen (auszuschließen), die eine bestimmte Bedingung erfüllen, geben Sie den Bedingungstyp und den Wert ein und wählen Sie dann Ausschließen.

   Wiederholen Sie diesen Schritt für jede gewünschte Ein- oder Ausschlussbedingung.

   Wenn Sie mehrere Bedingungen eingeben, haben alle Ausschlussbedingungen Vorrang vor Einschlussbedingungen. Wenn Sie beispielsweise Objekte mit der Dateinamenerweiterung PDF einbeziehen und Objekte ausschließen, die größer als 5 MB sind, analysiert der Job jedes Objekt mit der Dateinamenerweiterung PDF, sofern das Objekt nicht größer als 5 MB ist.

4. Wenn Sie fertig sind, wählen Sie Next (Weiter) aus.

Schritt 4: Wählen Sie verwaltete Datenkennungen aus

Geben Sie für diesen Schritt an, welche verwalteten Datenkennungen der Job bei der Analyse von S3-Objekten verwenden soll. Sie haben hierfür zwei Möglichkeiten:

- Empfohlene Einstellungen verwenden — Mit dieser Option analysiert der Job S3-Objekte anhand der verwalteten Datenbezeichner, die wir für Jobs empfehlen. Dieses Set dient zur Erkennung gängiger Kategorien und Typen vertraulicher Daten. Eine Liste der verwalteten Datenbezeichner, die derzeit in der Gruppe enthalten sind, finden Sie unterFür Jobs empfohlene Identifikatoren verwalteter Daten. Wir aktualisieren diese Liste jedes Mal, wenn wir einen verwalteten Datenbezeichner hinzufügen oder daraus entfernen.
- Benutzerdefinierte Einstellungen verwenden — Bei dieser Option analysiert der Job S3-Objekte mithilfe von ausgewählten verwalteten Datenkennungen. Dies können alle oder nur einige der derzeit verfügbaren verwalteten Datenkennungen sein. Sie können den Job auch so konfigurieren, dass er keine verwalteten Datenkennungen verwendet. Der Job kann stattdessen nur benutzerdefinierte Datenbezeichner verwenden, die Sie im nächsten Schritt auswählen. Eine Liste der derzeit verfügbaren verwalteten Datenkennungen finden Sie unter. Kurzreferenz: Von Amazon Macie verwaltete Datenkennungen Wir aktualisieren diese Liste jedes Mal, wenn wir einen neuen Identifier für verwaltete Daten veröffentlichen.

Wenn Sie sich für eine der Optionen entscheiden, zeigt Macie eine Tabelle mit verwalteten Datenkennungen an. In der Tabelle gibt das Feld Sensibler Datentyp den eindeutigen Bezeichner (ID) für einen verwalteten Datenbezeichner an. Diese ID beschreibt den Typ vertraulicher Daten, die der verwaltete Datenbezeichner erkennen soll, zum Beispiel: USA_PASSPORT_NUMBER für US-Passnummern, CREDIT_CARD_NUMBER für Kreditkartennummern und PGP_PRIVATE_KEY für private PGP-Schlüssel. Um bestimmte Identifikatoren schneller zu finden, können Sie die Tabelle nach Kategorie oder Typ vertraulicher Daten sortieren und filtern.

Um verwaltete Datenkennungen für den Job auszuwählen

1. Führen Sie auf der Seite Verwaltete Datenkennungen auswählen unter Optionen für verwaltete Datenbezeichner eine der folgenden Aktionen aus:

   - Um den Satz verwalteter Datenbezeichner zu verwenden, den wir für Jobs empfehlen, wählen Sie Empfohlen aus.

     Wenn Sie diese Option wählen und den Job so konfiguriert haben, dass er mehr als einmal ausgeführt wird, verwendet jeder Lauf automatisch alle verwalteten Datenbezeichner, die

zu Beginn der Ausführung im empfohlenen Satz enthalten sind. Dazu gehören auch neue Kennungen für verwaltete Daten, die wir veröffentlichen und dem Satz hinzufügen. Davon ausgenommen sind verwaltete Datenkennungen, die wir aus dem Set entfernen und die wir nicht mehr für Jobs empfehlen.

- Um nur bestimmte von Ihnen ausgewählte verwaltete Datenkennungen zu verwenden, wählen Sie Benutzerdefiniert und dann Bestimmte verwaltete Datenkennungen verwenden aus. Aktivieren Sie dann in der Tabelle das Kontrollkästchen für jede verwaltete Daten-ID, die der Job verwenden soll.

  Wenn Sie diese Option wählen und den Job so konfiguriert haben, dass er mehr als einmal ausgeführt wird, verwendet jeder Lauf nur die von Ihnen ausgewählten verwalteten Datenbezeichner. Mit anderen Worten, der Job verwendet bei jeder Ausführung dieselben verwalteten Datenbezeichner.

- Um alle verwalteten Datenkennungen zu verwenden, die Macie derzeit bereitstellt, wählen Sie Benutzerdefiniert und dann Bestimmte verwaltete Datenkennungen verwenden aus. Aktivieren Sie dann in der Tabelle das Kontrollkästchen in der Überschrift der Auswahlspalte, um alle Zeilen auszuwählen.

  Wenn Sie diese Option wählen und den Job so konfiguriert haben, dass er mehr als einmal ausgeführt wird, verwendet jeder Lauf nur die von Ihnen ausgewählten verwalteten Datenbezeichner. Mit anderen Worten, der Job verwendet bei jeder Ausführung dieselben verwalteten Datenbezeichner.

- Um keine verwalteten Datenkennungen und nur benutzerdefinierte Datenkennungen zu verwenden, wählen Sie Benutzerdefiniert und dann Keine verwalteten Datenkennungen verwenden aus. Wählen Sie dann im nächsten Schritt die zu verwendenden benutzerdefinierten Datenbezeichner aus.

2. Wenn Sie fertig sind, wählen Sie Next (Weiter) aus.

Schritt 5: Wählen Sie benutzerdefinierte Datenkennungen

Wählen Sie für diesen Schritt alle benutzerdefinierten Datenbezeichner aus, die der Job bei der Analyse von S3-Objekten verwenden soll. Der Job verwendet die ausgewählten Identifikatoren zusätzlich zu allen verwalteten Datenbezeichnern, für deren Verwendung Sie den Job konfiguriert haben. Weitere Informationen zu benutzerdefinierten Datenbezeichnern finden Sie unter. Erstellen von benutzerdefinierten Datenbezeichnern

Um benutzerdefinierte Datenbezeichner für den Job auszuwählen

1. Aktivieren Sie auf der Seite Benutzerdefinierte Datenbezeichner auswählen das Kontrollkästchen für jeden benutzerdefinierten Datenbezeichner, den der Job verwenden soll. Sie können bis zu 30 benutzerdefinierte Datenbezeichner auswählen.

   > **Tip**
   >
   > Um die Einstellungen für einen benutzerdefinierten Datenbezeichner zu überprüfen oder zu testen, bevor Sie ihn auswählen, wählen Sie das Linksymbol ( ) neben dem Namen des Identifikators. Macie öffnet eine Seite, auf der die Einstellungen der Kennung angezeigt werden.
   > Sie können diese Seite auch verwenden, um den Identifier anhand von Beispieldaten zu testen. Geben Sie dazu bis zu 1.000 Zeichen Text in das Feld Beispieldaten ein und wählen Sie dann Test aus. Macie wertet die Beispieldaten anhand der Kennung aus und meldet dann die Anzahl der Treffer.

2. Wenn Sie mit der Auswahl der benutzerdefinierten Datenbezeichner fertig sind, wählen Sie Weiter.

Schritt 6: Wählen Sie Zulassungslisten aus

Wählen Sie für diesen Schritt alle Zulassungslisten aus, die der Job bei der Analyse von S3-Objekten verwenden soll. Weitere Informationen zu Zulassungslisten finden Sie unterDefinition von Ausnahmen für sensible Daten mit Zulassungslisten.

So wählen Sie Zulassungslisten für den Job aus

1. Aktivieren Sie auf der Seite Zulassungslisten auswählen das Kontrollkästchen für jede Zulassungsliste, die der Job verwenden soll. Sie können bis zu 10 Listen auswählen.

   > **Tip**
   >
   > Wenn Sie die Einstellungen für eine Zulassungsliste überprüfen möchten, bevor Sie sie auswählen, klicken Sie auf das Linksymbol ( )

neben dem Namen der Liste. Macie öffnet eine Seite, auf der die Einstellungen der Liste angezeigt werden.
Wenn in der Liste ein regulärer Ausdruck (Regex) angegeben ist, können Sie diese Seite auch verwenden, um den regulären Ausdruck mit Beispieldaten zu testen. Geben Sie dazu bis zu 1.000 Zeichen Text in das Feld Beispieldaten ein, und wählen Sie dann Test aus. Macie wertet die Beispieldaten mithilfe der Regex aus und meldet dann die Anzahl der Treffer.

2. Wenn Sie mit der Auswahl der Zulassungslisten fertig sind, wählen Sie Weiter.

Schritt 7: Geben Sie die allgemeinen Einstellungen ein

Geben Sie für diesen Schritt einen Namen und optional eine Beschreibung des Jobs an.

Sie können dem Job auch Tags zuweisen. Ein Tag ist eine Bezeichnung, die Sie definieren und bestimmten Ressourcentypen AWS zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Mithilfe von Tags können Sie Ressourcen auf unterschiedliche Weise identifizieren, kategorisieren und verwalten, z. B. nach Zweck, Eigentümer, Umgebung oder anderen Kriterien. Weitere Informationen hierzu finden Sie unter Kennzeichnen von Amazon Macie-Ressourcen.

Um allgemeine Einstellungen für den Job einzugeben

1. Geben Sie auf der Seite Allgemeine Einstellungen eingeben einen Namen für den Job in das Feld Jobname ein. Der Name darf maximal 500 Zeichen enthalten.
2. (Optional) Geben Sie unter Stellenbeschreibung eine kurze Beschreibung der Stelle ein. Die Beschreibung darf maximal 200 Zeichen enthalten.
3. (Optional) Wählen Sie für Stichwörter die Option Tag hinzufügen aus und geben Sie dann bis zu 50 Stichwörter ein, die dem Job zugewiesen werden sollen.
4. Wenn Sie fertig sind, wählen Sie Next (Weiter) aus.

Schritt 8: Überprüfen und erstellen

Überprüfen Sie für diesen letzten Schritt die Konfigurationseinstellungen des Jobs und stellen Sie sicher, dass die Einstellungen korrekt sind. Dies ist ein wichtiger Schritt. Nachdem Sie einen Job erstellt haben, können Sie keine dieser Einstellungen ändern. Auf diese Weise können Sie

sicherstellen, dass Sie über einen unveränderlichen Verlauf der Ergebnisse sensibler Daten und der Ergebnisse der von Ihnen durchgeführten Datenschutzprüfungen oder Untersuchungen verfügen.

Abhängig von den Einstellungen des Jobs können Sie auch die geschätzten Gesamtkosten (in US-Dollar) für die einmalige Ausführung des Jobs überprüfen. Wenn Sie bestimmte S3-Buckets für den Job ausgewählt haben, basiert die Schätzung auf der Größe und den Typen der Objekte in den ausgewählten Buckets und darauf, wie viele dieser Daten der Job analysieren kann. Wenn Sie Bucket-Kriterien für den Job angegeben haben, basiert die Schätzung auf der Größe und den Typen von Objekten in bis zu 500 Buckets, die derzeit den Kriterien entsprechen, und darauf, wie viele dieser Daten der Job analysieren kann. Weitere Informationen zu dieser Schätzung finden Sie unterPrognose und Überwachung der Arbeitskosten.

Um den Job zu überprüfen und zu erstellen

1. Überprüfen Sie auf der Seite Überprüfen und erstellen jede Einstellung und stellen Sie sicher, dass sie korrekt sind. Um eine Einstellung zu ändern, wählen Sie in dem Abschnitt, der die Einstellung enthält, Bearbeiten aus und geben Sie dann die richtige Einstellung ein. Sie können auch die Navigationsregisterkarten verwenden, um zu der Seite zu gelangen, die eine Einstellung enthält.
2. Wenn Sie mit der Überprüfung der Einstellungen fertig sind, wählen Sie Senden aus, um den Job zu erstellen und zu speichern. Macie überprüft die Einstellungen und benachrichtigt Sie über alle Probleme, die behoben werden müssen.

> **Note**
>
> Wenn Sie kein Repository für die Ergebnisse der Erkennung sensibler Daten konfiguriert haben, zeigt Macie eine Warnung an und speichert den Job nicht. Um dieses Problem zu beheben, wählen Sie im Abschnitt Repository für die Ergebnisse der Erkennung sensibler Daten die Option Konfigurieren aus. Geben Sie dann die Konfigurationseinstellungen für das Repository ein. Um zu erfahren wie dies geht, vgl. Speicherung und Beibehaltung der Erkennungsergebnisse von vertraulichen Daten. Nachdem Sie die Einstellungen eingegeben haben, kehren Sie zur Seite Überprüfen und erstellen zurück und wählen Sie dann im Abschnitt Repository für Ergebnisse der Erkennung vertraulicher Daten die Option Aktualisieren ().
>
> Dies wird zwar nicht empfohlen, Sie können jedoch die Repository-Anforderung vorübergehend außer Kraft setzen und den Job speichern. Wenn Sie dies tun, riskieren

Sie den Verlust der Discovery-Ergebnisse aus dem Job — MacIE speichert die Ergebnisse nur 90 Tage lang. Um die Anforderung vorübergehend außer Kraft zu setzen, aktivieren Sie das Kontrollkästchen für die Option „Außerkraftsetzung“.

3. Wenn Macie Sie über Probleme informiert, die behoben werden müssen, gehen Sie auf die Probleme ein und klicken Sie dann erneut auf Absenden, um den Job zu erstellen und zu speichern.

Wenn Sie den Job so konfiguriert haben, dass er einmal, täglich oder am aktuellen Tag der Woche oder des Monats ausgeführt wird, startet Macie den Job sofort nach dem Speichern. Andernfalls bereitet sich Macie darauf vor, den Job am angegebenen Wochentag oder Monat auszuführen. Um den Job zu überwachen, können Sie den Status des Jobs überprüfen.

Überprüfung von Statistiken und Ergebnissen für Discovery-Jobs im Zusammenhang mit sensiblen Daten

Wenn Sie einen Discovery-Job für sensible Daten ausführen, berechnet Amazon Macie automatisch bestimmte statistische Daten für den Job und meldet diese. Macie meldet beispielsweise, wie oft der Job ausgeführt wurde, und die ungefähre Anzahl von Amazon Simple Storage Service (Amazon S3) -Objekten, die der Job während seiner aktuellen Ausführung noch nicht verarbeitet hat. Macie erzeugt außerdem verschiedene Arten von Ergebnissen für den Job: Protokollereignisse, Ergebnisse vertraulicher Daten und Ergebnisse der Erkennung sensibler Daten.

Themen

- Arten von Ergebnissen für Aufgaben zur Erkennung sensibler Daten
- Überprüfung von Statistiken und Ergebnissen für einen Job zur Erkennung sensibler Daten

Arten von Ergebnissen für Aufgaben zur Erkennung sensibler Daten

Während ein Job zur Erkennung sensibler Daten voranschreitet, erzeugt Amazon Macie die folgenden Arten von Ergebnissen für den Job.

Ereignis protokollieren

Dies ist eine Aufzeichnung eines Ereignisses, das während der Ausführung des Jobs aufgetreten ist. Macie protokolliert und veröffentlicht automatisch Daten für bestimmte Ereignisse in Amazon CloudWatch Logs. Die Daten in diesen Protokollen zeichnen Änderungen am Fortschritt oder

Status des Jobs auf, z. B. das genaue Datum und die Uhrzeit, an dem der Job gestartet oder beendet wurde. Die Daten enthalten auch Details zu allen Fehlern auf Konto- oder Bucket-Ebene, die während der Ausführung des Jobs aufgetreten sind.

Mithilfe von Protokollereignissen können Sie einen Job überwachen und alle Probleme beheben, die den Job daran gehindert haben, die gewünschten Daten zu analysieren. Wenn ein Job anhand von Laufzeitkriterien bestimmt, welche S3-Buckets analysiert werden sollen, können Sie anhand von Protokollereignissen auch feststellen, ob und welche S3-Buckets den Kriterien bei der Ausführung des Jobs entsprachen.

Sie können über die CloudWatch Amazon-Konsole oder die Amazon CloudWatch Logs-API auf Protokollereignisse zugreifen. Um Ihnen die Navigation zu den Protokollereignissen für einen Job zu erleichtern, stellt die Amazon Macie Macie-Konsole einen Link zu diesen Ereignissen bereit. Weitere Informationen finden Sie unter Überwachen von Aufträgen.

Suche nach sensiblen Daten

Dies ist ein Bericht über sensible Daten, die Macie in einem S3-Objekt gefunden hat. Jedes Ergebnis enthält eine Bewertung des Schweregrads und Einzelheiten wie:

- Datum und Uhrzeit, an dem Macie die sensiblen Daten gefunden hat.
- Die Kategorie und die Arten sensibler Daten, die Macie gefunden hat.
- Die Anzahl der Vorkommen der einzelnen Arten vertraulicher Daten, die Macie gefunden hat.
- Die eindeutige Kennung für den Job, der zu dem Ergebnis geführt hat.
- Der Name, die Einstellungen für den öffentlichen Zugriff, der Verschlüsselungstyp und andere Informationen zum betroffenen S3-Bucket und Objekt.

Je nach Dateityp oder Speicherformat des betroffenen S3-Objekts können die Details auch den Speicherort von bis zu 15 Vorkommen der sensiblen Daten beinhalten, die Macie gefunden hat. Um Standortdaten zu melden, verwenden die Ergebnisse sensibler Daten ein standardisiertes JSON-Schema.

Ein Ergebnis vertraulicher Daten beinhaltet nicht die sensiblen Daten, die Macie gefunden hat. Stattdessen enthält es Informationen, die Sie bei Bedarf für weitere Untersuchungen und Problembehebungen verwenden können.

Macie speichert Ergebnisse sensibler Daten 90 Tage lang. Sie können über die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API darauf zugreifen. Sie können sie auch mithilfe anderer Anwendungen, Dienste und Systeme überwachen und verarbeiten. Weitere Informationen finden Sie unter Analyse der Ergebnisse.

Ergebnis der Entdeckung sensibler Daten

Dies ist ein Datensatz, der Details zur Analyse eines S3-Objekts protokolliert. Macie erstellt automatisch ein Erkennungsergebnis vertraulicher Daten für jedes Objekt, für dessen Analyse Sie einen Job konfigurieren. Dazu gehören Objekte, in denen Macie keine sensiblen Daten findet und daher keine Ergebnisse für sensible Daten liefert, sowie Objekte, die Macie aufgrund von Fehlern oder Problemen nicht analysieren kann, z. B. aufgrund von Berechtigungseinstellungen oder der Verwendung eines nicht unterstützten Datei- oder Speicherformats.

Wenn Macie sensible Daten in einem S3-Objekt findet, umfasst das Ergebnis der Erkennung sensibler Daten auch Daten aus dem entsprechenden Fund vertraulicher Daten. Es bietet auch zusätzliche Informationen, z. B. den Standort von bis zu 1.000 Vorkommen jedes Typs vertraulicher Daten, die Macie in dem Objekt gefunden hat. Beispiel:

- Die Spalten- und Zeilennummer für eine Zelle oder ein Feld in einer Microsoft Excel-Arbeitsmappe, CSV-Datei oder TSV-Datei
- Der Pfad zu einem Feld oder Array in einer JSON- oder JSON Lines-Datei
- Die Zeilennummer für eine Zeile in einer nicht-binären Textdatei, bei der es sich nicht um eine CSV-, JSON-, JSON-Zeilen- oder TSV-Datei handelt, z. B. eine HTML-, TXT- oder XML-Datei
- Die Seitennummer für eine Seite in einer PDF-Datei (Adobe Portable Document Format)
- Der Datensatzindex und der Pfad zu einem Feld in einem Datensatz in einem Apache Avro-Objektcontainer oder einer Apache Parquet-Datei

Handelt es sich bei dem betroffenen S3-Objekt um eine Archivdatei, z. B. eine .tar- oder .zip-Datei, liefert das Ergebnis der Erkennung sensibler Daten auch detaillierte Standortdaten für das Vorkommen sensibler Daten in einzelnen Dateien, die Macie aus dem Archiv extrahiert. Macie nimmt diese Informationen nicht in die Ergebnisse sensibler Daten für Archivdateien auf. Um Standortdaten zu melden, verwenden die Ergebnisse der Erkennung sensibler Daten ein standardisiertes JSON-Schema.

Ein Ermittlungsergebnis für sensible Daten beinhaltet nicht die sensiblen Daten, die Macie gefunden hat. Stattdessen erhalten Sie einen Analysedatensatz, der für Prüfungen oder Untersuchungen zum Datenschutz hilfreich sein kann.

Macie speichert Ihre Ergebnisse der Entdeckung sensibler Daten 90 Tage lang. Sie können nicht direkt über die Amazon Macie Macie-Konsole oder mit der Amazon Macie Macie-API darauf zugreifen. Stattdessen konfigurieren Sie Macie so, dass sie verschlüsselt und in einem S3-Bucket gespeichert werden. Der Bucket kann als definitives, langfristiges Repository für all Ihre Erkennungsergebnisse sensibler Daten dienen. Anschließend können Sie optional auf die

Ergebnisse in diesem Repository zugreifen und diese abfragen. Informationen zur Konfiguration dieser Einstellungen finden Sie unterSpeicherung und Beibehaltung der Erkennungsergebnisse von vertraulichen Daten.

Nachdem Sie die Einstellungen konfiguriert haben, schreibt Macie Ihre Ergebnisse der Erkennung sensibler Daten in JSON Lines (.jsonl) -Dateien, verschlüsselt diese Dateien und fügt sie dem S3-Bucket als GNU-Zip-Dateien (.gz) hinzu. Um Ihnen die Navigation zu den Ergebnissen zu erleichtern, enthält die Amazon Macie Macie-Konsole Links zu diesen.

Sowohl die Ergebnisse sensibler Daten als auch die Ergebnisse der Entdeckung sensibler Daten entsprechen standardisierten Schemata. Auf diese Weise können Sie diese Daten optional mithilfe anderer Anwendungen, Dienste und Systeme abfragen, überwachen und verarbeiten.

> **Tip**
>
> Ein detailliertes, anschauliches Beispiel dafür, wie Sie die Ergebnisse der Erkennung sensibler Daten abfragen und verwenden können, um potenzielle Datensicherheitsrisiken zu analysieren und zu melden, finden Sie im QuickSight Blogbeitrag So fragen Sie die Ergebnisse der Erkennung sensibler Daten von Macie mit Amazon Athena und Amazon ab und visualisieren Sie sie im Security Blog. AWS
> Beispiele für Amazon Athena Athena-Abfragen, mit denen Sie Erkennungsergebnisse sensibler Daten analysieren können, finden Sie im Amazon Macie Results Analytics-Repository unter. GitHub Dieses Repository enthält auch Anweisungen zur Konfiguration von Athena zum Abrufen und Entschlüsseln Ihrer Ergebnisse sowie Skripten zum Erstellen von Tabellen für die Ergebnisse.

Überprüfung von Statistiken und Ergebnissen für einen Job zur Erkennung sensibler Daten

Um die Verarbeitungsstatistiken und Ergebnisse für einzelne Discovery-Jobs für sensible Daten zu überprüfen, können Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden. Gehen Sie wie folgt vor, um die Statistiken und Ergebnisse eines Jobs mithilfe der Konsole zu überprüfen.

Um programmgesteuert auf die Verarbeitungsstatistiken eines Jobs zuzugreifen, verwenden Sie den DescribeClassificationJobBetrieb der Amazon Macie Macie-API. Verwenden Sie für den programmatischen Zugriff auf die Ergebnisse, die ein Job generiert hat, den ListFindingsBetrieb der

Amazon Macie Macie-API und geben Sie die eindeutige Kennung des Jobs in einer Filterbedingung für das `classificationDetails.jobId` Feld an. Um zu erfahren wie dies geht, vgl. Filter erstellen und auf Ergebnisse anwenden. Anschließend können Sie den GetFindingsVorgang verwenden, um die Details der Ergebnisse abzurufen.

Um Statistiken und Ergebnisse für einen Job zu überprüfen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich die Option Jobs (Aufträge) aus.
3. Wählen Sie auf der Seite Jobs den Namen des Jobs aus, dessen Statistiken und Ergebnisse Sie überprüfen möchten. Im Detailbereich werden Statistiken, Einstellungen und andere Informationen über den Job angezeigt.
4. Führen Sie im Detailbereich einen der folgenden Schritte aus:

   - Informationen zur Überprüfung der Verarbeitungsstatistiken für den Job finden Sie im Bereich Statistiken des Fensters. In diesem Abschnitt werden Statistiken angezeigt, z. B. die Häufigkeit, mit der der Job ausgeführt wurde, und die ungefähre Anzahl der Objekte, die der Job während seiner aktuellen Ausführung noch verarbeiten muss.
   - Um die Protokollereignisse für den Job zu überprüfen, wählen Sie oben im Bereich „Ergebnisse anzeigen“ und anschließend „ CloudWatch Protokolle anzeigen“. Macie öffnet die CloudWatch Amazon-Konsole und zeigt eine Tabelle mit den Protokollereignissen an, die Macie für den Job veröffentlicht hat.
   - Um alle Ergebnisse zu sensiblen Daten zu überprüfen, die der Job hervorgebracht hat, wählen Sie oben im Fenster Ergebnisse anzeigen und dann Ergebnisse anzeigen aus. Macie öffnet die Ergebnisseite und zeigt alle Ergebnisse des Jobs an. Um die Details eines bestimmten Ergebnisses zu überprüfen, wählen Sie das Ergebnis aus und rufen Sie dann das Detailfenster auf.

     Tip

     Im Bereich mit den Befunddetails können Sie den Link im Feld Detaillierter Ergebnisort verwenden, um zum entsprechenden Ergebnis der Erkennung sensibler Daten in Amazon S3 zu navigieren:

     - Wenn sich das Ergebnis auf ein großes Archiv oder eine komprimierte Datei bezieht, zeigt der Link den Ordner an, der die Erkennungsergebnisse für die Datei enthält. Ein Archiv oder eine komprimierte Datei ist groß, wenn sie mehr als 100 Ermittlungsergebnisse generiert.

  - Wenn sich das Ergebnis auf ein kleines Archiv oder eine komprimierte Datei bezieht, zeigt der Link die Datei an, die die Ermittlungsergebnisse für die Datei enthält. Ein Archiv oder eine komprimierte Datei ist klein, wenn sie 100 oder weniger Ermittlungsergebnisse generiert.
  - Wenn der Befund auf einen anderen Dateityp zutrifft, zeigt der Link die Datei an, die die Ermittlungsergebnisse für die Datei enthält.

- Wählen Sie im oberen Bereich des Fensters die Option Ergebnisse anzeigen und anschließend Klassifizierungen anzeigen aus, um alle Ergebnisse der Suche nach vertraulichen Daten zu überprüfen. Macie öffnet die Amazon S3 S3-Konsole und zeigt den Ordner an, der alle Ermittlungsergebnisse für den Job enthält. Diese Option ist erst verfügbar, nachdem Sie Macie so konfiguriert haben, dass Ihre Erkennungsergebnisse vertraulicher Daten in einem S3-Bucket gespeichert werden.

Überwachung von Aufträgen zur Erkennung sensibler Daten mit Amazon CloudWatch Logs

Sie können nicht nur den Gesamtstatus eines Discovery-Jobs für sensible Daten überwachen und analysieren, sondern auch bestimmte Ereignisse überwachen und analysieren, die im Verlauf eines Auftrags auftreten. Sie können dies tun, indem Sie Protokolldaten nahezu in Echtzeit verwenden, die Amazon Macie automatisch in Amazon CloudWatch Logs veröffentlicht. Die Daten in diesen Protokollen zeichnen Änderungen am Fortschritt oder Status eines Jobs auf, z. B. das genaue Datum und die Uhrzeit, an dem ein Job gestartet, angehalten oder beendet wurde.

Die Protokolldaten enthalten auch Details zu Fehlern auf Konto- oder Bucket-Ebene, die während der Ausführung eines Jobs auftreten. Wenn beispielsweise die Berechtigungseinstellungen für einen S3-Bucket verhindern, dass ein Job Objekte im Bucket analysiert, protokolliert Macie ein Ereignis. Das Ereignis gibt an, wann der Fehler aufgetreten ist, und identifiziert sowohl den betroffenen Bucket als auch das Konto, dem der Bucket gehört. Die Daten für diese Ereignistypen können Ihnen helfen, Fehler zu identifizieren, zu untersuchen und zu beheben, die Macie daran hindern, die gewünschten Daten zu analysieren.

Mit Amazon CloudWatch Logs können Sie Protokolldateien von mehreren Systemen, Anwendungen und, einschließlich Macie, überwachen, speichern und AWS-Services darauf zugreifen. Sie können auch Protokolldaten abfragen und analysieren und CloudWatch Protokolle so konfigurieren, dass Sie benachrichtigt werden, wenn bestimmte Ereignisse eintreten oder Schwellenwerte erreicht werden. CloudWatch Logs bietet auch Funktionen zum Archivieren von Protokolldaten und zum Exportieren

der Daten nach Amazon S3. Weitere Informationen zu CloudWatch Logs finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch.

Themen

- So funktioniert die Protokollierung bei Aufträgen zur Erkennung sensibler Daten
- Überprüfung der Protokolle bei Aufträgen zur Erkennung sensibler Daten
- Protokollereignisschema für Aufgaben zur Erkennung sensibler Daten
- Arten von Protokollereignissen für Aufgaben zur Erkennung sensibler Daten

So funktioniert die Protokollierung bei Aufträgen zur Erkennung sensibler Daten

Wenn Sie mit der Ausführung von Aufträgen zur Erkennung sensibler Daten beginnen, erstellt und konfiguriert Macie automatisch die entsprechenden Ressourcen in Amazon CloudWatch Logs, um Ereignisse für alle Ihre aktuellen Jobs zu protokollieren. AWS-Region Macie veröffentlicht dann automatisch Ereignisdaten auf diesen Ressourcen, wenn Ihre Jobs ausgeführt werden. Die Berechtigungsrichtlinie für die dienstbezogene Macie-Rolle für Ihr Konto ermöglicht es Macie, diese Aufgaben in Ihrem Namen auszuführen. Sie müssen keine Schritte unternehmen, um Ressourcen in CloudWatch Logs zu erstellen oder zu konfigurieren oder um Ereignisdaten für Ihre Jobs zu protokollieren.

In CloudWatch Logs sind Logs in Protokollgruppen organisiert. Jede Protokollgruppe enthält Protokollstreams. Jeder Protokollstream enthält Protokollereignisse. Der allgemeine Zweck jeder dieser Ressourcen ist wie folgt:

- Eine Protokollgruppe ist eine Sammlung von Protokollströmen, die dieselben Einstellungen für Aufbewahrung, Überwachung und Zugriffskontrolle verwenden, z. B. die Sammlung von Protokollen für all Ihre Aufgaben zur Erkennung vertraulicher Daten.
- Ein Protokollstream ist eine Abfolge von Protokollereignissen, die dieselbe Quelle verwenden, z. B. eine einzelne Aufgabe zur Erkennung vertraulicher Daten.
- Ein Protokollereignis ist eine Aufzeichnung einer Aktivität, die von einer Anwendung oder Ressource aufgezeichnet wurde, z. B. ein einzelnes Ereignis, das Macie für einen bestimmten Discovery-Job für sensible Daten aufgezeichnet und veröffentlicht hat.

Macie veröffentlicht Ereignisse für alle Ihre Discovery-Jobs für sensible Daten in einer Protokollgruppe, und jeder Job hat einen eigenen Protokollstream in dieser Protokollgruppe. Die Protokollgruppe hat das folgende Präfix und den folgenden Namen:

```
/aws/macie/classificationjobs
```

Wenn diese Protokollgruppe bereits existiert, verwendet Macie sie, um Protokollereignisse für Ihre Jobs zu speichern. Dies kann hilfreich sein, wenn Ihr Unternehmen automatisierte Konfigurationen verwendet, z. B. AWS CloudFormationum Protokollgruppen mit vordefinierten Aufbewahrungsfristen für Protokolle, Verschlüsselungseinstellungen, Tags, Metrikfiltern usw. für Jobereignisse zu erstellen.

Wenn diese Protokollgruppe nicht existiert, erstellt Macie sie mit den Standardeinstellungen, die CloudWatch Logs für neue Protokollgruppen verwendet. Die Einstellungen beinhalten eine Aufbewahrungsfrist von Never Expire, was bedeutet, dass CloudWatch Logs die Protokolle auf unbestimmte Zeit speichert. Um den Aufbewahrungszeitraum für die Protokollgruppe zu ändern, können Sie die CloudWatch Amazon-Konsole oder die Amazon CloudWatch Logs-API verwenden. Wie das geht, erfahren Sie unter Arbeiten mit Protokollgruppen und Protokollstreams im Amazon CloudWatch Logs-Benutzerhandbuch.

Innerhalb dieser Protokollgruppe erstellt Macie einen eindeutigen Protokollstream für jeden Job, den Sie ausführen, wenn der Job zum ersten Mal ausgeführt wird. Der Name des Protokollstreams ist die eindeutige Kennung für den Job, z. B. `85a55dc0fa6ed0be5939d0408example` im folgenden Format.

```
/aws/macie/classificationjobs/85a55dc0fa6ed0be5939d0408example
```

Jeder Protokollstream enthält alle Protokollereignisse, die Macie für den entsprechenden Job aufgezeichnet und veröffentlicht hat. Bei periodischen Jobs umfasst dies Ereignisse für alle Jobausführungen. Wenn Sie den Protokollstream für einen periodischen Job löschen, erstellt Macie den Stream erneut, wenn der Job das nächste Mal ausgeführt wird. Wenn Sie den Protokollstream für einen einmaligen Job löschen, können Sie ihn nicht wiederherstellen.

Beachten Sie, dass die Protokollierung standardmäßig für alle Ihre Jobs aktiviert ist. Sie können es nicht deaktivieren oder Macie auf andere Weise daran hindern, Job-Ereignisse in CloudWatch Logs zu veröffentlichen. Wenn Sie die Protokolle nicht speichern möchten, können Sie die Aufbewahrungsfrist für die Protokollgruppe auf nur einen Tag reduzieren. Am Ende des Aufbewahrungszeitraums löscht CloudWatch Logs automatisch abgelaufene Ereignisdaten aus der Protokollgruppe.

Überprüfung der Protokolle bei Aufträgen zur Erkennung sensibler Daten

Sie können die Protokolle Ihrer Aufträge zur Erkennung sensibler Daten mithilfe der CloudWatch Amazon-Konsole oder der Amazon CloudWatch Logs-API überprüfen. Sowohl die Konsole als auch die API bieten Funktionen, mit denen Sie Protokolldaten überprüfen und analysieren können. Sie können diese Funktionen verwenden, um mit Protokollstreams und Ereignissen für Ihre Jobs zu arbeiten, genauso wie Sie mit jeder anderen Art von Protokolldaten in CloudWatch Logs arbeiten würden.

Sie können beispielsweise aggregierte Daten durchsuchen und filtern, um bestimmte Arten von Ereignissen zu identifizieren, die für alle Ihre Jobs in einem bestimmten Zeitraum aufgetreten sind. Oder Sie können eine gezielte Überprüfung aller Ereignisse durchführen, die für einen bestimmten Job eingetreten sind. CloudWatch Logs bietet auch Optionen für die Überwachung von Protokolldaten, die Definition von Metrikfiltern und die Erstellung benutzerdefinierter Alarme.

> **Tip**
>
> Gehen Sie wie folgt vor, um mithilfe der Amazon Macie Macie-Konsole zu den Protokollereignissen für einen bestimmten Job zu navigieren: Wählen Sie auf der Seite Jobs den Namen des Jobs aus. Wählen Sie oben im Detailbereich die Option Ergebnisse anzeigen und dann CloudWatch Protokolle anzeigen aus. Macie öffnet die CloudWatch Amazon-Konsole und zeigt eine Tabelle mit Protokollereignissen für den Job an.

Um die Protokolle für Ihre Jobs zu überprüfen (CloudWatch Amazon-Konsole)

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie Jobs ausgeführt haben, für die Sie Logs überprüfen möchten.
3. Wählen Sie im Navigationsbereich Logs (Protokolle) und dann Log groups (Protokollgruppen) aus.
4. Wählen Sie auf der Seite Protokollgruppen die Protokollgruppe /aws/macie/classificationjobs aus. CloudWatch Logs zeigt eine Tabelle mit Protokollstreams für die Jobs an, die Sie ausgeführt haben. Für jeden Job gibt es einen eigenen Stream. Der Name jedes Streams entspricht der eindeutigen Kennung für einen Job.
5. Führen Sie unter Streams protokollieren einen der folgenden Schritte aus:

- Um die Protokollereignisse für einen bestimmten Job zu überprüfen, wählen Sie den Log-Stream für den Job aus. Um den Stream leichter zu finden, geben Sie die eindeutige Kennung des Jobs in das Filterfeld über der Tabelle ein. Nachdem Sie den Protokollstream ausgewählt haben, zeigt CloudWatch Logs eine Tabelle mit Protokollereignissen für den Job an.
- Um die Protokollereignisse für alle Ihre Jobs zu überprüfen, wählen Sie Alle Protokollstreams durchsuchen aus. CloudWatch Logs zeigt eine Tabelle mit Protokollereignissen für all Ihre Jobs an.

6. (Optional) Geben Sie in das Filterfeld über der Tabelle Begriffe, Ausdrücke oder Werte ein, die die Merkmale bestimmter Ereignisse angeben, die überprüft werden sollen. Weitere Informationen finden Sie unter Durchsuchen von Protokolldaten mithilfe von Filtermustern im Amazon CloudWatch Logs-Benutzerhandbuch.
7. Um die Details eines bestimmten Protokollereignisses zu überprüfen, wählen Sie den Rechtspfeil ( ) in der Zeile für das Ereignis. CloudWatch Logs zeigt die Details des Ereignisses im JSON-Format an.

Wenn Sie sich mit den Daten in den Protokollereignissen vertraut machen, können Sie auch Aufgaben wie das Erstellen von Metrikfiltern ausführen, die Protokolldaten in numerische CloudWatch Messwerte umwandeln, und das Erstellen benutzerdefinierter Alarme, mit denen Sie bestimmte Protokollereignisse leichter identifizieren und darauf reagieren können. Weitere Informationen finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch.

Protokollereignisschema für Aufgaben zur Erkennung sensibler Daten

Jedes Protokollereignis für einen Discovery-Job für sensible Daten ist ein JSON-Objekt, das dem Amazon CloudWatch Logs-Ereignisschema entspricht und einen Standardsatz von Feldern enthält. Einige Ereignistypen verfügen über zusätzliche Felder, die Informationen enthalten, die für diesen Ereignistyp besonders nützlich sind. Ereignisse für Fehler auf Kontoebene beinhalten beispielsweise die Konto-ID der betroffenen Person. AWS-Konto Zu den Ereignissen für Fehler auf Bucket-Ebene gehört der Name des betroffenen S3-Buckets. Eine ausführliche Liste der Job-Ereignisse, die Macie in CloudWatch Logs veröffentlicht, finden Sie unter. Arten von Protokollereignissen für Jobs

Das folgende Beispiel zeigt das Protokollereignisschema für Aufträge zur Erkennung sensibler Daten. In diesem Beispiel meldet das Ereignis, dass Macie keine Objekte in einem S3-Bucket analysieren konnte, weil Amazon S3 den Zugriff auf den Bucket verweigert hat.

```
{
    "adminAccountId": "123456789012",
    "jobId": "85a55dc0fa6ed0be5939d0408example",
    "eventType": "BUCKET_ACCESS_DENIED",
    "occurredAt": "2021-04-14T17:11:30.574809Z",
    "description": "Macie doesn't have permission to access the affected S3 bucket.",
    "jobName": "My_Macie_Job",
    "operation": "ListObjectsV2",
    "runDate": "2021-04-14T17:08:30.345809Z",
    "affectedAccount": "111122223333",
    "affectedResource": {
        "type": "S3_BUCKET_NAME",
        "value": "DOC-EXAMPLE-BUCKET"
    }
}
```


Im vorherigen Beispiel hat Macie versucht, die Objekte im Bucket mithilfe der ListObjectsV2-Operation der Amazon S3 S3-API aufzulisten. Als Macie die Anfrage an Amazon S3 sendete, verweigerte Amazon S3 den Zugriff auf den Bucket.

Die folgenden Felder sind allen Protokollereignissen für Aufgaben zur Erkennung sensibler Daten gemeinsam:

- `adminAccountId`— Die eindeutige Kennung für denAWS-Konto, der den Job erstellt hat.
- `jobId`— Die eindeutige Kennung für den Job.
- `eventType`— Die Art des Ereignisses, das eingetreten ist. Eine vollständige Liste der möglichen Werte und eine Beschreibung der einzelnen Werte finden Sie unterArten von Protokollereignissen für Jobs.
- `occurredAt`— Datum und Uhrzeit in koordinierter Weltzeit (UTC) und erweitertem ISO 8601-Format, an dem das Ereignis eingetreten ist.
- `description`— Eine kurze Beschreibung des Ereignisses.
- `jobName`— Der benutzerdefinierte Name des Jobs.

Je nach Art und Art eines Ereignisses kann ein Protokollereignis auch die folgenden Felder enthalten:

- `affectedAccount`— Die eindeutige Kennung für denAWS-Konto, dem die betroffene Ressource gehört.

- `affectedResource`— Ein Objekt, das Details über die betroffene Ressource bereitstellt. Im Objekt gibt das `type` Feld ein Feld an, das Metadaten zu einer Ressource speichert. Das `value` Feld gibt den Wert für das Feld an (`type`).
- `operation`— Der Vorgang, den Macie durchzuführen versucht hat und der den Fehler verursacht hat.
- `runDate`— Datum und Uhrzeit in koordinierter Weltzeit (UTC) und erweitertem ISO 8601-Format, an dem der entsprechende Job oder die Ausführung des Jobs gestartet wurde.

Arten von Protokollereignissen für Aufgaben zur Erkennung sensibler Daten

Macie veröffentlicht Protokollereignisse für drei Kategorien von Ereignissen:

- Jobstatusereignisse, die Änderungen am Status oder Fortschritt eines Jobs oder einer Jobausführung aufzeichnen.
- Fehlerereignisse auf Kontoebene, bei denen Fehler aufgezeichnet werden, die Macie daran gehindert haben, Amazon S3 S3-Daten auf bestimmte Weise zu analysieren. AWS-Konto
- Fehlerereignisse auf Bucket-Ebene, bei denen Fehler aufgezeichnet werden, die Macie daran gehindert haben, Daten in einem bestimmten S3-Bucket zu analysieren.

In den Themen dieses Abschnitts sind die Ereignistypen aufgeführt und beschrieben, die Macie für jede Kategorie veröffentlicht.

Themen

- Ereignisse zum Jobstatus
- Fehlerereignisse auf Kontoebene
- Fehlerereignisse auf Bucket-Ebene

Ereignisse zum Jobstatus

Ein Jobstatusereignis zeichnet eine Änderung des Status oder des Fortschritts eines Auftrags oder einer Auftragsausführung auf. Bei periodischen Jobs protokolliert und veröffentlicht Macie diese Ereignisse sowohl für den gesamten Job als auch für einzelne Jobläufe. Hinweise zur Bestimmung des Gesamtstatus eines Jobs finden Sie unterÜberprüfen Sie den Status von Aufträgen zur Erkennung sensibler Daten.

Im folgenden Beispiel werden anhand von Beispieldaten die Struktur und Art der Felder in einem Jobstatusereignis veranschaulicht. In diesem Beispiel weist ein `SCHEDULED_RUN_COMPLETED` Ereignis darauf hin, dass eine geplante Ausführung eines periodischen Jobs beendet wurde. Der Lauf begann am 14. April 2021 um 17:09:30 UTC, wie aus dem Feld hervorgeht. `runDate` Der Lauf endete am 14. April 2021 um 17:16:30 UTC, wie aus dem Feld hervorgeht. `occurredAt`

```
{
    "adminAccountId": "123456789012",
    "jobId": "ffad0e71455f38a4c7c220f3cexample",
    "eventType": "SCHEDULED_RUN_COMPLETED",
    "occurredAt": "2021-04-14T17:16:30.574809Z",
    "description": "The scheduled job run finished running.",
    "jobName": "My_Daily_Macie_Job",
    "runDate": "2021-04-14T17:09:30.574809Z"
}
```

In der folgenden Tabelle sind die Typen von Jobstatusereignissen aufgeführt und beschrieben, die Macie protokolliert und in Logs veröffentlicht. CloudWatch In der Spalte Ereignistyp wird der Name jedes Ereignisses so angegeben, wie er im `eventType` Feld eines Ereignisses erscheint. Die Spalte Beschreibung enthält eine kurze Beschreibung des Ereignisses, wie es im `description` Feld eines Ereignisses angezeigt wird. Die zusätzlichen Informationen enthalten Informationen über die Art des Jobs, für den sich das Ereignis bezieht. Die Tabelle ist zuerst nach der allgemeinen chronologischen Reihenfolge sortiert, in der Ereignisse auftreten können, und dann in aufsteigender alphabetischer Reihenfolge nach Ereignistyp.

Ereignistyp	Beschreibung	Zusätzliche Informationen
JOB_CREATED	Der Job wurde erstellt.	Gilt für einmalige und regelmäßige Jobs.
ONE_TIME_JOB_STARTED	Der Job wurde gestartet.	Gilt nur für einmalige Jobs.
SCHEDULED_RUN_STARTED	Der geplante Joblauf wurde gestartet.	Gilt nur für periodische Jobs. Um den Start eines einmaligen Jobs zu protokollieren, veröffentlicht Macie ein

Ereignistyp	Beschreibung	Zusätzliche Informationen
		ONE_TIME_JOB_STARTED-Ereignis, nicht dieses Ereignis.
BUCKET_MATCHED_THE_CRITERIA	Der betroffene Bucket entsprach den für den Job angegebenen Bucket-Kriterien.	Gilt für einmalige und regelmäßige Jobs, bei denen anhand von Runtime-Bucket-Kriterien bestimmt wird, welche S3-Buckets analysiert werden sollen. Das `affectedResource` Objekt gibt den Namen des Buckets an, der den Kriterien entsprach und in die Analyse des Jobs aufgenommen wurde.
NO_BUCKETS_MATCHED_THE_CRITERIA	Der Job wurde gestartet, aber derzeit entsprechen keine Buckets den für den Job angegebenen Bucket-Kriterien. Der Job hat keine Daten analysiert.	Gilt für einmalige und regelmäßige Jobs, bei denen anhand von Runtime-Bucket-Kriterien bestimmt wird, welche S3-Buckets analysiert werden sollen.
SCHEDULED_RUN_COMPLETED	Die Ausführung des geplanten Auftrags wurde abgeschlossen.	Gilt nur für periodische Jobs. Um den Abschluss eines einmaligen Jobs zu protokollieren, veröffentlicht Macie ein JOB_COMPLETED-Ereignis, nicht dieses Ereignis.

Ereignistyp	Beschreibung	Zusätzliche Informationen
JOB_PAUSED_BY_USER	Der Job wurde von einem Benutzer angehalten.	Gilt für einmalige und regelmäßige Jobs, die Sie vorübergehend beendet (angehalten) haben.
JOB_RESUMED_BY_USER	Der Job wurde von einem Benutzer wieder aufgenommen.	Gilt für einmalige und regelmäßige Aufträge, die Sie vorübergehend beendet (angehalten) und anschließend wieder aufgenommen haben.
JOB_PAUSED_BY_MACIE_SERVICE_QUOTA_MET	Der Job wurde von Macie unterbrochen. Die Fertigstellung des Auftrags würde ein monatliches Kontingent für das betroffene Konto überschreiten.	Gilt für einmalige und regelmäßige Aufträge, die Macie vorübergehend beendet (angehalten) hat. Macie unterbricht einen Job automatisch, wenn die zusätzliche Verarbeitung durch den Job oder eine Auftragsausführung das monatliche Kontingent für die Erkennung sensibler Daten für ein oder mehrere Konten, für die der Job Daten analysiert, überschreiten würde. Um dieses Problem zu vermeiden, sollten Sie erwägen, das Kontingent für die betroffenen Konten zu erhöhen.

Ereignistyp	Beschreibung	Zusätzliche Informationen
JOB_RESUMED_BY_MACIE_SERVICE_QUOTA_LIFTED	Der Job wurde von Macie wieder aufgenommen. Das monatliche Servicekontingent für das betroffene Konto wurde aufgehoben.	Gilt für einmalige und regelmäßige Aufträge, die Macie vorübergehend beendet (angehalten) und anschließend wieder aufgenommen hat. Wenn Macie einen einmaligen Job automatisch angehalten hat, nimmt Macie den Job automatisch wieder auf, wenn der Folgemonat beginnt oder die monatliche Quote für die Erkennung sensibler Daten für alle betroffenen Konten erhöht wird, je nachdem, was zuerst eintritt. Wenn Macie einen regelmäßigen Job automatisch angehalten hat, nimmt Macie den Job automatisch wieder auf, wenn der nächste Lauf geplant ist oder der darauffolgende Monat beginnt, je nachdem, was zuerst eintritt.

Ereignistyp	Beschreibung	Zusätzliche Informationen
JOB_CANCELLED	Der Job wurde storniert.	Gilt für einmalige und regelmäßige Jobs, die Sie dauerhaft beendet (stornier t) oder, bei einmaligen Aufträgen, pausiert und nicht innerhalb von 30 Tagen wieder aufgenommen haben. Wenn Sie Macie aussetzen oder deaktivieren, gilt diese Art von Ereignis auch für Jobs, die aktiv oder pausiert waren, als Sie Macie gesperrt oder deaktiviert haben. Macie storniert deine Jobs automatis ch, AWS-Region wenn du Macie in der Region sperrst oder deaktivierst.
JOB_COMPLETED	Die Ausführung des Jobs wurde abgeschlossen.	Gilt nur für einmalige Jobs. Um den Abschluss eines Auftrags zu protokollieren, der für einen periodischen Job ausgeführt wird, veröffent licht Macie ein SCHEDULED _RUN_COMPLETED-Ereignis, nicht diesen Ereignistyp.

Fehlerereignisse auf Kontoebene

Ein Fehlerereignis auf Kontoebene zeichnet einen Fehler auf, der Macie daran hinderte, Objekte in S3-Buckets zu analysieren, die einer bestimmten Person gehören. AWS-Konto Das `affectedAccount` Feld in jedem Ereignis gibt die Konto-ID für dieses Konto an.

Im folgenden Beispiel werden anhand von Beispieldaten die Struktur und Art der Felder in einem Fehlerereignis auf Kontoebene veranschaulicht. In diesem Beispiel weist ein `ACCOUNT_ACCESS_DENIED` Ereignis darauf hin, dass Macie keine Objekte in S3-Buckets analysieren konnte, die einem Konto gehören. `444455556666`

```
{
    "adminAccountId": "123456789012",
    "jobId": "85a55dc0fa6ed0be5939d0408example",
    "eventType": "ACCOUNT_ACCESS_DENIED",
    "occurredAt": "2021-04-14T17:08:30.585709Z",
    "description": "Macie doesn't have permission to access S3 bucket data for the
 affected account.",
    "jobName": "My_Macie_Job",
    "operation": "ListBuckets",
    "runDate": "2021-04-14T17:05:27.574809Z",
    "affectedAccount": "444455556666"
}
```

In der folgenden Tabelle sind die Arten von Fehlerereignissen auf Kontoebene aufgeführt und beschrieben, die Macie protokolliert und in Logs veröffentlicht. CloudWatch In der Spalte Ereignistyp wird der Name jedes Ereignisses so angegeben, wie er im `eventType` Feld eines Ereignisses erscheint. Die Spalte Beschreibung enthält eine kurze Beschreibung des Ereignisses, wie es im `description` Feld eines Ereignisses angezeigt wird. Die Spalte Zusätzliche Informationen enthält alle anwendbaren Tipps zur Untersuchung oder Behebung des aufgetretenen Fehlers. Die Tabelle ist in aufsteigender alphabetischer Reihenfolge nach Ereignistyp sortiert.

Ereignistyp	Beschreibung	Zusätzliche Informationen
ACCOUNT_ACCESS_DENIED	Macie hat keine Berechtigung, auf S3-Bucket-Daten für das betroffene Konto zuzugreifen.	Dies liegt in der Regel daran, dass für die Buckets, die dem Konto gehören, restriktive Bucket-Richtlinien gelten. Informationen zur Behebung dieses Problems finden Sie unterMacie den Zugriff von S3-Buckets und -Objekten erlauben.

Ereignistyp	Beschreibung	Zusätzliche Informationen
		Anhand des Werts für das `operation` Feld im Ereignis können Sie ermitteln, welche Berechtigungseinstellungen Macie daran gehindert haben, auf S3-Daten für das Konto zuzugreifen. Dieses Feld gibt den Amazon S3 S3-Vorgang an, den Macie auszuführen versuchte, als der Fehler auftrat.
ACCOUNT_DISABLED	Der Job hat Ressourcen übersprungen, die dem betroffenen Konto gehören. Macie wurde für das Konto deaktiviert.	Um dieses Problem zu beheben, aktivieren Sie Macie erneut für das Konto in demselben. AWS-Region

Ereignistyp	Beschreibung	Zusätzliche Informationen
ACCOUNT_DISASSOCIATED	Der Job hat Ressourcen übersprungen, die dem betroffenen Konto gehören. Das Konto ist nicht mehr mit Ihrem Macie-Administratorkonto als Mitgliedskonto verknüpft.	Dies ist der Fall, wenn Sie als Macie-Administrator für eine Organisation einen Job zur Analyse von Daten für ein verknüpftes Mitgliedskonto konfigurieren und das Mitgliedskonto anschließend aus Ihrer Organisation entfernt wird. Um dieses Problem zu beheben, ordnen Sie das betroffene Konto erneut Ihrem Macie-Administratorkonto als Mitgliedskonto zu. Weitere Informationen finden Sie unter Verwalten mehrerer Konten.
ACCOUNT_ISOLATED	Der Job hat Ressourcen übersprungen, die dem betroffenen Konto gehören. Der AWS-Konto war isoliert.	–
ACCOUNT_REGION_DISABLED	Der Job hat Ressourcen übersprungen, die dem betroffenen Konto gehören. Der AWS-Konto ist derzeit AWS-Region nicht aktiv.	–

Ereignistyp	Beschreibung	Zusätzliche Informationen
ACCOUNT_SUSPENDIERT	Der Job wurde storniert oder es wurden Ressourcen übersprungen, die dem betroffenen Konto gehören. Macie wurde für das Konto gesperrt.	Wenn es sich bei dem angegebenen Konto um Ihr eigenes Konto handelt, hat Macie den Job automatisch storniert, als Sie Macie in derselben Region gesperrt haben. Um das Problem zu beheben, aktivieren Sie Macie in der Region erneut. Wenn es sich bei dem angegebenen Konto um ein Mitgliedskonto handelt, aktivieren Sie Macie erneut für dieses Konto in derselben Region.
ACCOUNT_TERMINATED	Der Job hat Ressourcen übersprungen, die dem betroffenen Konto gehören. Der AWS-Konto wurde beendet.	–

Fehlerereignisse auf Bucket-Ebene

Ein Fehlerereignis auf Bucket-Ebene zeichnet einen Fehler auf, der Macie daran hinderte, Objekte in einem bestimmten S3-Bucket zu analysieren. Das `affectedAccount` Feld in jedem Ereignis gibt die Konto-ID für denjenigen anAWS-Konto, dem der Bucket gehört. Das `affectedResource` Objekt in jedem Ereignis gibt den Namen des Buckets an.

Im folgenden Beispiel werden anhand von Beispieldaten die Struktur und Art der Felder in einem Fehlerereignis auf Bucket-Ebene veranschaulicht. In diesem Beispiel weist ein `BUCKET_ACCESS_DENIED` Ereignis darauf hin, dass Macie keine Objekte im genannten S3-Bucket analysieren konnte. `DOC-EXAMPLE-BUCKET` Als Macie versuchte, die Objekte im Bucket mithilfe der

ListObjectsV2-Operation der Amazon S3-API aufzulisten, verweigerte Amazon S3 den Zugriff auf den Bucket.

```
{
    "adminAccountId": "123456789012",
    "jobId": "85a55dc0fa6ed0be5939d0408example",
    "eventType": "BUCKET_ACCESS_DENIED",
    "occurredAt": "2021-04-14T17:11:30.574809Z",
    "description": "Macie doesn't have permission to access the affected S3 bucket.",
    "jobName": "My_Macie_Job",
    "operation": "ListObjectsV2",
    "runDate": "2021-04-14T17:09:30.685209Z",
    "affectedAccount": "111122223333",
    "affectedResource": {
        "type": "S3_BUCKET_NAME",
        "value": "DOC-EXAMPLE-BUCKET"
    }
}
```

In der folgenden Tabelle sind die Arten von Fehlerereignissen auf Bucket-Ebene aufgeführt und beschrieben, die Macie protokolliert und in Logs veröffentlicht. CloudWatch In der Spalte Ereignistyp wird der Name jedes Ereignisses so angegeben, wie er im `eventType` Feld eines Ereignisses erscheint. Die Spalte Beschreibung enthält eine kurze Beschreibung des Ereignisses, wie es im `description` Feld eines Ereignisses angezeigt wird. Die Spalte Zusätzliche Informationen enthält alle anwendbaren Tipps zur Untersuchung oder Behebung des aufgetretenen Fehlers. Die Tabelle ist in aufsteigender alphabetischer Reihenfolge nach Ereignistyp sortiert.

Ereignistyp	Beschreibung	Zusätzliche Informationen
BUCKET_ACCESS_DENIED	Macie hat keine Berechtigung, auf den betroffenen S3-Bucket zuzugreifen.	Dies ist in der Regel darauf zurückzuführen, dass für einen Bucket eine restrikti ve Bucket-Richtlinie gilt. Informationen zur Behebung dieses Problems finden Sie unterMacie den Zugriff von S3-Buckets und -Objekten erlauben.

Ereignistyp	Beschreibung	Zusätzliche Informationen
		Anhand des Werts für das `operation` Feld im Ereignis können Sie ermitteln, welche Berechtigungseinstellungen Macie daran gehindert haben, auf den Bucket zuzugreifen. Dieses Feld gibt den Amazon S3 S3-Vorgang an, den Macie auszuführen versuchte, als der Fehler auftrat.

Ereignistyp	Beschreibung	Zusätzliche Informationen
BUCKET_DETAILS_UNAVAILABLE	Ein vorübergehendes Problem hinderte Macie daran, Details über den Bucket und die Objekte des Buckets abzurufen.	Dieses Problem tritt auf, wenn Macie aufgrund eines vorübergehenden Problems die Bucket- und Objektmetadaten, die zur Analyse der Objekte eines Buckets benötigt werden, nicht abrufen konnte. Beispielsweise trat eine Amazon S3 S3-Ausnahme auf, als Macie versuchte zu überprüfen, ob er auf den Bucket zugreifen darf. Um das Problem für einen einmaligen Job zu beheben, sollten Sie erwägen, einen neuen einmaligen Job zur Analyse von Objekten im Bucket zu erstellen und auszuführen. Bei einem geplanten Job versucht Macie bei der nächsten Auftragsausführung erneut, die Metadaten abzurufen.
BUCKET_DOES_NOT_EXIST	Der betroffene S3-Bucket existiert nicht mehr.	Dies tritt normalerweise auf, weil ein Bucket gelöscht wurde.
BUCKET_IN_DIFFERENT_REGION	Der betroffene S3-Bucket wurde in einen anderen verschoben. AWS-Region	–

Ereignistyp	Beschreibung	Zusätzliche Informationen
BUCKET_OWNER_CHANGED	Der Besitzer des betroffenen S3-Buckets hat sich geändert. Macie hat keine Berechtigung mehr, auf den Bucket zuzugreifen.	Dies ist in der Regel der Fall, wenn der Besitz eines Buckets auf einen Bucket übertragen wurdeAWS-Konto, der nicht Teil Ihrer Organisation ist. Das `affectedAccount` Feld im Ereignis gibt die Konto-ID für das Konto an, dem der Bucket zuvor gehörte.

Verwaltung von Aufträgen zur Erkennung sensibler Daten

Um Sie bei der Verwaltung Ihrer Discovery-Jobs für sensible Daten zu unterstützen, bietet Amazon Macie für jeden AWS-Region Auftrag ein vollständiges Inventar Ihrer Aufträge. Mit diesem Inventar können Sie Ihre Jobs als eine einzige Sammlung verwalten und auf die Konfigurationseinstellungen, den Status und die Verarbeitungsstatistiken für einzelne Jobs zugreifen. Sie können auch auf die Ergebnisse sensibler Daten und andere Ergebnisse zugreifen, die bei jedem Auftrag erzielt wurden.

Zusätzlich zu diesen Aufgaben können Sie benutzerdefinierte Varianten einzelner Jobs erstellen: Kopieren Sie einen vorhandenen Job, passen Sie die Einstellungen für die Kopie an und speichern Sie die Kopie dann als neuen Job. Dies kann in Fällen hilfreich sein, in denen Sie verschiedene Datensätze auf dieselbe Weise oder denselben Datensatz auf unterschiedliche Weise analysieren möchten. Oder Sie möchten die Konfigurationseinstellungen für einen vorhandenen Job anpassen: Stornieren Sie den vorhandenen Job, kopieren Sie ihn und passen Sie die Kopie dann an und speichern Sie sie als neuen Job.

Themen

- Überprüfung Ihres Inventars an Aufträgen zur Erkennung sensibler Daten
- Überprüfung der Konfigurationseinstellungen für Discovery-Jobs für vertrauliche Daten
- Überprüfen Sie den Status von Aufträgen zur Erkennung sensibler Daten
- Unterbrechen, Wiederaufnehmen oder Abbrechen von Discovery-Aufträgen für sensible Daten
- Discovery-Jobs für vertrauliche Daten werden kopiert

Überprüfung Ihres Inventars an Aufträgen zur Erkennung sensibler Daten

Die Seite Jobs in der Amazon Macie Macie-Konsole enthält Informationen über alle aktuellen AWS-Region Discovery-Jobs für Ihr Konto. Für jeden Job enthält die Tabelle zusammenfassende Informationen, darunter: den aktuellen Status des Jobs, ob der Job nach einem Zeitplan und in regelmäßigen Abständen ausgeführt wird und ob der Job eine bestimmte Anzahl von S3-Buckets analysiert oder ob er S3-Buckets analysiert, die den Laufzeitkriterien entsprechen. Wenn Sie in der Tabelle einen Job auswählen, werden im Detailbereich die Konfigurationseinstellungen und andere Informationen zu dem Job angezeigt.

Um Ihr Jobinventar zu überprüfen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich die Option Jobs (Aufträge) aus. Die Seite „Jobs“ wird geöffnet und zeigt die Anzahl der Jobs in Ihrem Inventar sowie eine Tabelle dieser Jobs an.
3. Gehen Sie wie folgt vor, um einen bestimmten Job schneller zu finden:

   - Um die Tabelle nach einem bestimmten Feld zu sortieren, klicken Sie auf die Spaltenüberschrift für das Feld. Um die Sortierreihenfolge zu ändern, klicken Sie erneut auf die Spaltenüberschrift.
   - Um nur die Jobs anzuzeigen, die einen bestimmten Wert für ein Feld haben, platzieren Sie den Cursor in das Filterfeld. Wählen Sie im daraufhin angezeigten Menü das Feld aus, das für den Filter verwendet werden soll, und geben Sie den Wert für den Filter ein. Wählen Sie dann Apply (Anwenden).
   - Um Jobs auszublenden, die einen bestimmten Wert für ein Feld haben, platzieren Sie den Cursor in das Filterfeld. Wählen Sie im daraufhin angezeigten Menü das Feld aus, das für den Filter verwendet werden soll, und geben Sie den Wert für den Filter ein. Wählen Sie dann Apply (Anwenden). Wählen Sie im Filterfeld das Gleichheitssymbol (●) für den Filter aus. Dadurch wird der Operator des Filters von „gleich“ zu „ungleich“ () geändert. ⃠
   - Um einen Filter zu entfernen, wählen Sie das Symbol „Filter entfernen“ (⊗ für den Filter, den Sie entfernen möchten.
4. Um die Konfigurationseinstellungen und andere Details für einen bestimmten Job zu überprüfen, wählen Sie den Namen des Jobs in der Tabelle aus und gehen dann zum Detailbereich.

Überprüfung der Konfigurationseinstellungen für Discovery-Jobs für vertrauliche Daten

In der Amazon Macie Macie-Konsole können Sie den Detailbereich auf der Seite Jobs verwenden, um die Konfigurationseinstellungen und andere Informationen zu einzelnen Discovery-Jobs für sensible Daten zu überprüfen. Sie können beispielsweise eine Liste der S3-Buckets überprüfen, für deren Analyse ein Job konfiguriert ist, und welche verwalteten Datenkennungen ein Job verwendet, um Objekte in diesen Buckets zu analysieren.

> **Note**
>
> Sie können keine Konfigurationseinstellungen für einen vorhandenen Job ändern. Auf diese Weise können Sie sicherstellen, dass Sie über einen unveränderlichen Verlauf der Ergebnisse sensibler Daten und der Ergebnisse der von Ihnen durchgeführten Datenschutzprüfungen oder -untersuchungen verfügen. Wenn Sie einen bestehenden Job ändern möchten, stornieren Sie den Job. Kopieren Sie dann den Job, konfigurieren Sie die Kopie so, dass sie die gewünschten Einstellungen verwendet, und speichern Sie die Kopie als neuen Job.
>
> Wenn Sie dies tun, sollten Sie auch Maßnahmen ergreifen, um sicherzustellen, dass der neue Job vorhandene Daten nicht erneut auf dieselbe Weise analysiert. Notieren Sie sich dazu das Datum und die Uhrzeit, zu der Sie den vorhandenen Job stornieren. Konfigurieren Sie dann den Umfang des neuen Jobs so, dass er nur die Objekte umfasst, die erstellt oder geändert wurden, nachdem Sie den ursprünglichen Job storniert haben. Verwenden Sie beispielsweise Objektkriterien, um die Ausschlussbedingung Letzte Änderung hinzuzufügen, die das Datum und die Uhrzeit angibt, zu der Sie den ursprünglichen Auftrag storniert haben.

Um die Konfigurationseinstellungen eines Jobs zu überprüfen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich die Option Jobs (Aufträge) aus.
3. Wählen Sie auf der Seite Jobs den Namen des Jobs aus, dessen Einstellungen Sie überprüfen möchten. Im Detailbereich werden die Konfigurationseinstellungen und andere Informationen zum Job angezeigt. Je nach den Einstellungen des Jobs enthält das Fenster die folgenden Abschnitte.

Allgemeine Informationen

Dieser Abschnitt enthält allgemeine Informationen über den Job, z. B. den Amazon-Ressourcennamen (ARN) des Jobs, wann der Job zuletzt ausgeführt wurde und den aktuellen Status des Jobs. Wenn Sie den Job angehalten haben, gibt dieser Abschnitt auch an, wann Sie den Job angehalten haben und wann der Job oder die letzte Jobausführung entweder abgelaufen ist oder abläuft, wenn Sie ihn nicht fortsetzen.

Statistiken

In diesem Abschnitt werden Verarbeitungsstatistiken für den Job angezeigt, z. B. die Häufigkeit, mit der der Job ausgeführt wurde, und die ungefähre Anzahl von Objekten, die der Job während seiner aktuellen Ausführung noch verarbeiten muss.

Scope

In diesem Abschnitt wird angegeben, wie oft der Job ausgeführt wird. Außerdem werden Einstellungen angezeigt, mit denen der Umfang des Jobs verfeinert werden kann, z. B. die Stichprobentiefe und alle Objektkriterien, die S3-Objekte in die Analyse des Jobs einbeziehen oder ausschließen.

S3-Buckets

Dieser Abschnitt wird im Bereich angezeigt, wenn der Job für die Analyse von Buckets konfiguriert ist, die Sie bei der Erstellung des Jobs ausdrücklich ausgewählt haben. Er gibt die Nummer an, für AWS-Konten die der Job konfiguriert ist, um Daten zu analysieren. Es gibt auch die Anzahl der Buckets an, für deren Analyse der Job konfiguriert ist, sowie die Namen dieser Buckets (gruppiert nach Konto).

Um die vollständige Liste der Konten und Buckets im JSON-Format anzuzeigen, wählen Sie die Zahl im Feld Gesamtzahl der Buckets aus.

Kriterien für S3-Buckets

Dieser Abschnitt wird im Panel angezeigt, wenn der Job anhand von Laufzeitkriterien bestimmt, welche Buckets analysiert werden sollen. Er listet die Kriterien auf, für deren Verwendung der Job konfiguriert ist.

Um die Kriterien im JSON-Format anzuzeigen, wählen Sie Details und dann im daraufhin angezeigten Fenster die Registerkarte Kriterien aus.

Um eine Tabelle mit Buckets zu überprüfen, die derzeit den Kriterien entsprechen, wählen Sie „Details“ und dann im daraufhin angezeigten Fenster die Registerkarte „Passende Buckets“. Wählen Sie optional „Aktualisieren“ () um die neuesten Daten abzurufen.

> **Tip**
>
> Wenn der Job bereits ausgeführt wurde, können Sie auch feststellen, ob irgendwelche Buckets den Kriterien bei der Ausführung des Jobs entsprachen, und, falls ja, die Namen dieser Buckets. Überprüfen Sie dazu die Protokollereignisse für den Job: Wählen Sie oben im Bereich „Ergebnisse anzeigen“ und anschließend „Protokolle anzeigen CloudWatch “. Macie öffnet die CloudWatch Amazon-Konsole und zeigt eine Tabelle mit Protokollereignissen für den Job an. Die Ereignisse beinhalten ein `BUCKET_MATCHED_THE_CRITERIA` Ereignis für jeden Bucket, der den Kriterien entsprach und in die Analyse des Jobs aufgenommen wurde. Weitere Informationen finden Sie unter Überwachen von Aufträgen.

Benutzerdefinierte Datenbezeichner

Dieser Abschnitt wird im Bereich angezeigt, wenn der Job für die Verwendung eines oder mehrerer benutzerdefinierter Datenbezeichner konfiguriert ist. Er gibt die Namen dieser benutzerdefinierten Datenbezeichner an.

Listen zulassen

Dieser Abschnitt wird im Fenster angezeigt, wenn der Job für die Verwendung einer oder mehrerer Zulassungslisten konfiguriert ist. Er gibt die Namen dieser Listen an. Um die Einstellungen und den Status einer Liste zu überprüfen, wählen Sie das Linksymbol ( ) neben dem Namen der Liste.

Verwaltete Datenkennungen

In diesem Abschnitt wird angegeben, für welche verwalteten Datenbezeichner der Job konfiguriert ist. Dies wird durch den Auswahltyp für verwaltete Datenbezeichner für den Job bestimmt:

- Empfohlen — Verwenden Sie bei der Ausführung des Jobs die verwalteten Datenbezeichner, die sich im empfohlenen Satz befinden.
- Ausgewählte einbeziehen — Verwenden Sie nur die verwalteten Datenbezeichner, die im Abschnitt „Auswahl“ aufgeführt sind.
- Alle einbeziehen — Verwenden Sie alle verwalteten Datenkennungen, die bei der Ausführung des Jobs verfügbar sind.
- Ausgewählte ausschließen — Verwenden Sie alle verwalteten Datenkennungen, die bei der Ausführung des Jobs verfügbar sind, mit Ausnahme der im Abschnitt „Auswahl“ aufgeführten.
- Alle ausschließen — Verwenden Sie keine verwalteten Datenkennungen. Verwenden Sie nur die angegebenen benutzerdefinierten Datenbezeichner.

Um diese Einstellungen im JSON-Format zu überprüfen, wählen Sie Details.

Tags

Dieser Abschnitt wird im Bereich angezeigt, wenn dem Job Tags zugeordnet sind. Er listet diese Tags auf.

Ein Tag ist eine Bezeichnung, die Sie definieren und bestimmten Ressourcentypen AWS zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Mithilfe von Tags können Sie Ressourcen auf unterschiedliche Weise identifizieren, kategorisieren und verwalten, z. B. nach Zweck, Eigentümer, Umgebung oder anderen Kriterien. Weitere Informationen hierzu finden Sie unter Kennzeichnen von Amazon Macie-Ressourcen.

4. Um die Einstellungen des Jobs zu überprüfen und im JSON-Format zu speichern, wählen Sie oben im Fenster die eindeutige Kennung für den Job (Job-ID) aus und wählen Sie dann Herunterladen.

Überprüfen Sie den Status von Aufträgen zur Erkennung sensibler Daten

Wenn Sie einen Discovery-Job für sensible Daten erstellen, lautet sein Anfangsstatus je nach Art und Zeitplan des Auftrags Aktiv (Wird ausgeführt) oder Aktiv (Inaktiv). Der Job durchläuft dann weitere Status, die Sie im Verlauf des Jobs überwachen können.

> **Tip**
>
> Sie können nicht nur den Gesamtstatus eines Auftrags überwachen, sondern auch bestimmte Ereignisse überwachen, die im Verlauf eines Auftrags auftreten. Sie können dies tun, indem Sie Protokolldaten verwenden, die Macie automatisch in Amazon CloudWatch Logs veröffentlicht. Die Daten in diesen Protokollen enthalten eine Aufzeichnung der Änderungen am Status eines Jobs sowie Einzelheiten zu Fehlern auf Konto- oder Bucket-Ebene, die während der Ausführung eines Jobs auftreten. Weitere Informationen finden Sie unter Überwachen von Aufträgen.

Um den Status eines Jobs zu überprüfen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich die Option Jobs (Aufträge) aus.
3. Suchen Sie auf der Seite Jobs den Job, dessen Status Sie überprüfen möchten. Das Feld Status gibt den aktuellen Status des Jobs an.

   Aktiv (Inaktiv)

   Bei einem periodischen Auftrag ist die vorherige Ausführung abgeschlossen und die nächste geplante Ausführung steht noch aus. Dieser Wert gilt nicht für einmalige Jobs.

   Aktiv (läuft)

   Bei einem einmaligen Job ist der Job gerade in Bearbeitung. Bei einem periodischen Auftrag wird gerade eine geplante Ausführung ausgeführt.

   Abgebrochen

   Bei jeder Art von Auftrag wurde der Auftrag dauerhaft gestoppt (storniert).

   Ein Job hat diesen Status, wenn Sie ihn ausdrücklich storniert haben oder, falls es sich um einen einmaligen Job handelt, Sie den Job pausiert und nicht innerhalb von 30 Tagen wieder aufgenommen haben. Ein Job kann diesen Status auch haben, wenn du Macie zuvor in der aktuellen Zeit suspendiert hast. AWS-Region

Vollständig

Bei einem einmaligen Job wurde der Job erfolgreich ausgeführt und ist jetzt abgeschlossen. Dieser Wert gilt nicht für periodische Jobs. Stattdessen ändert sich der Status eines periodischen Auftrags in Aktiv (Inaktiv), wenn jede Ausführung erfolgreich abgeschlossen wurde.

Angehalten (von Macie)

Bei jeder Art von Job wurde der Job vorübergehend von Macie gestoppt (pausiert).

Ein Auftrag hat diesen Status, wenn der Abschluss des Auftrags oder einer Auftragsausführung das monatliche Kontingent für die Entdeckung sensibler Daten für Ihr Konto überschreiten würde. In diesem Fall unterbricht Macie den Job automatisch. Macie nimmt den Job automatisch wieder auf, wenn der nächste Kalendermonat beginnt (und das monatliche Kontingent für Ihr Konto zurückgesetzt wird) oder wenn Sie das Kontingent für Ihr Konto erhöhen.

Wenn Sie der Macie-Administrator einer Organisation sind und den Job so konfiguriert haben, dass er Daten für Mitgliedskonten analysiert, kann der Job auch diesen Status haben, wenn der Abschluss des Jobs oder einer Jobausführung das monatliche Kontingent für die Erkennung sensibler Daten für ein Mitgliedskonto überschreiten würde.

Wenn ein Job ausgeführt wird und die Analyse geeigneter Objekte dieses Kontingent für ein Mitgliedskonto erreicht, beendet der Job die Analyse von Objekten, die dem Konto gehören. Wenn der Job die Analyse der Objekte für alle anderen Konten abgeschlossen hat, die das Kontingent nicht erfüllt haben, unterbricht Macie den Job automatisch. Handelt es sich um einen einmaligen Job, nimmt Macie den Job automatisch wieder auf, wenn der nächste Kalendermonat beginnt, oder das Kontingent wird für alle betroffenen Konten erhöht, je nachdem, was zuerst eintritt. Handelt es sich um einen periodischen Job, nimmt Macie den Job automatisch wieder auf, wenn der nächste Lauf geplant ist oder der nächste Kalendermonat beginnt, je nachdem, was zuerst eintritt. Wenn eine geplante Ausführung vor Beginn des nächsten Kalendermonats beginnt oder das Kontingent für ein betroffenes Konto erhöht wird, analysiert der Job keine Objekte, die dem Konto gehören.

Angehalten (vom Benutzer)

Bei jeder Art von Job wurde der Job vorübergehend von Ihnen gestoppt (pausiert).

Wenn Sie einen einmaligen Job pausieren und ihn nicht innerhalb von 30 Tagen wieder aufnehmen, läuft der Job ab und Macie storniert ihn. Wenn Sie einen regelmäßigen Job unterbrechen, während er aktiv ausgeführt wird, und Sie ihn nicht innerhalb von 30 Tagen wieder aufnehmen, läuft die Ausführung des Jobs ab und Macie bricht den Lauf ab. Um das Ablaufdatum eines unterbrochenen Auftrags oder einer Auftragsausführung zu überprüfen, wählen Sie den Namen des Auftrags in der Tabelle aus und suchen Sie dann im Bereich Statusdetails im Detailbereich nach dem Feld Läuft ab.

Wenn ein Auftrag storniert oder angehalten wurde, können Sie anhand der Auftragsdetails feststellen, ob die Ausführung des Jobs gestartet wurde oder, bei einem periodischen Job, mindestens einmal ausgeführt wurde, bevor er abgebrochen oder angehalten wurde. Wählen Sie dazu den Namen des Jobs in der Tabelle aus und schauen Sie dann im Detailbereich nach. Im Bereich gibt das Feld Anzahl der Durchläufe an, wie oft der Job ausgeführt wurde. Das Feld Letzte Laufzeit gibt das Datum und die Uhrzeit an, zu der der Job zuletzt gestartet wurde.

Je nach aktuellem Status des Jobs können Sie den Job optional anhalten, fortsetzen oder abbrechen.

Unterbrechen, Wiederaufnehmen oder Abbrechen von Discovery-Aufträgen für sensible Daten

Nachdem Sie einen Discovery-Job für sensible Daten erstellt haben, können Sie ihn vorübergehend unterbrechen oder dauerhaft stornieren. Wenn Sie einen Job unterbrechen, der aktiv ausgeführt wird, beginnt Macie sofort damit, alle Verarbeitungsaufgaben für den Job anzuhalten. Wenn Sie einen Job stornieren, der aktiv ausgeführt wird, beginnt Macie sofort, alle Verarbeitungsaufgaben für den Job zu beenden. Sie können einen Job nicht fortsetzen oder neu starten, nachdem er storniert wurde.

Wenn Sie einen einmaligen Auftrag pausieren, können Sie ihn innerhalb von 30 Tagen wieder aufnehmen. Wenn Sie den Job fortsetzen, nimmt Macie die Verarbeitung sofort an dem Punkt wieder auf, an dem Sie den Job unterbrochen haben — Macie startet den Job nicht von vorne neu. Wenn Sie einen einmaligen Auftrag nicht innerhalb von 30 Tagen nach der Unterbrechung wieder aufnehmen, läuft der Job ab und Macie storniert ihn.

Wenn Sie einen regelmäßigen Job unterbrechen, können Sie ihn jederzeit wieder aufnehmen. Wenn Sie einen periodischen Job wieder aufnehmen und der Job sich im Leerlauf befand, als Sie ihn angehalten haben, setzt Macie den Job gemäß dem Zeitplan und anderen Konfigurationseinstellungen fort, die Sie bei der Erstellung des Jobs ausgewählt haben. Wenn Sie einen periodischen Job wieder aufnehmen und der Job aktiv ausgeführt wurde, als Sie ihn

angehalten haben, hängt die Art und Weise, wie Macie den Job wieder aufnimmt, davon ab, wann Sie den Job wieder aufnehmen:

- Wenn Sie den Job innerhalb von 30 Tagen nach dem Unterbrechen wieder aufnehmen, nimmt Macie sofort den letzten geplanten Lauf an dem Punkt wieder auf, an dem Sie den Job unterbrochen haben — Macie startet den Lauf nicht von vorne neu.
- Wenn Sie den Job nicht innerhalb von 30 Tagen nach der Unterbrechung wieder aufnehmen, läuft der letzte geplante Lauf ab und Macie bricht alle verbleibenden Verarbeitungsaufgaben für den Lauf ab. Wenn Sie den Job anschließend wieder aufnehmen, setzt Macie den Job gemäß dem Zeitplan und anderen Konfigurationseinstellungen fort, die Sie bei der Erstellung des Jobs ausgewählt haben.

Damit Sie leichter bestimmen können, wann ein angehaltener Job oder eine Auftragsausführung abläuft, fügt Macie den Auftragsdetails ein Ablaufdatum hinzu, während der Job angehalten ist. Um dieses Datum zu überprüfen, wählen Sie den Namen des Auftrags in der Tabelle auf der Seite Jobs aus und schauen Sie dann im Detailbereich im Bereich Statusdetails im Feld Läuft ab. Darüber hinaus benachrichtigen wir Sie ungefähr sieben Tage vor Ablauf des Auftrags oder der Auftragsausführung. Wir benachrichtigen Sie erneut, wenn der Job oder die Auftragsausführung abläuft und storniert wird. Um Sie zu benachrichtigen, senden wir eine E-Mail an die Adresse, die mit Ihrer verknüpft istAWS-Konto. Wir erstellen auch AWS Health Veranstaltungen und CloudWatch Amazon-Events für Ihr Konto.

Um einen Job zu pausieren, fortzusetzen oder zu stornieren

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich die Option Jobs (Aufträge) aus.
3. Aktivieren Sie auf der Seite Jobs das Kontrollkästchen für den Job, den Sie anhalten, fortsetzen oder stornieren möchten, und führen Sie dann im Menü Aktionen eine der folgenden Aktionen aus:

    - Um den Job vorübergehend anzuhalten, wählen Sie Pause. Diese Option ist nur verfügbar, wenn der aktuelle Status des Jobs Aktiv (Inaktiv), Aktiv (Wird ausgeführt) oder Angehalten (Von Macie) lautet.
    - Um den Job fortzusetzen, wählen Sie Fortsetzen. Diese Option ist nur verfügbar, wenn der aktuelle Status des Jobs „Unterbrochen (vom Benutzer)“ lautet.

- Um den Job dauerhaft abzubrechen, wählen Sie Abbrechen. Wenn Sie diese Option wählen, können Sie den Job anschließend nicht fortsetzen oder neu starten.

Discovery-Jobs für vertrauliche Daten werden kopiert

Um schnell einen neuen Discovery-Job für sensible Daten zu erstellen, der einem vorhandenen Job ähnelt, können Sie eine Kopie des Jobs erstellen, die Einstellungen der Kopie bearbeiten und die Kopie dann als neuen Job speichern. Dies kann in Fällen hilfreich sein, in denen Sie eine benutzerdefinierte Variante eines vorhandenen Jobs erstellen möchten. Oder Sie möchten die Konfigurationseinstellungen für einen vorhandenen Job anpassen, indem Sie den Job stornieren und dann die Einstellungen kopieren, ändern und als neuen Job speichern.

Um einen Job zu kopieren

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich die Option Jobs (Aufträge) aus.
3. Aktivieren Sie das Kontrollkästchen für den Job, den Sie kopieren möchten.
4. Wählen Sie im Menü Aktionen die Option In neuen Ordner kopieren aus.
5. Führen Sie die Schritte auf der Konsole aus, um die Einstellungen für die Kopie des Jobs zu überprüfen und anzupassen. Erwägen Sie, für den Schritt „Umfang verfeinern“ Optionen auszuwählen, die verhindern, dass der Job vorhandene Daten erneut auf dieselbe Weise analysiert:

   - Verwenden Sie für einen einmaligen Job Objektkriterien, um nur die Objekte einzubeziehen, die nach einer bestimmten Zeit erstellt oder geändert wurden. Wenn Sie beispielsweise eine Kopie eines Auftrags erstellen, den Sie storniert haben, fügen Sie die Bedingung Letzte Änderung hinzu, die das Datum und die Uhrzeit angibt, zu der Sie den vorhandenen Job storniert haben.
   - Deaktivieren Sie für einen periodischen Auftrag das Kontrollkästchen Bestehende Objekte einbeziehen. In diesem Fall werden bei der ersten Ausführung des Jobs nur die Objekte analysiert, die nach der Erstellung des Jobs und vor der ersten Ausführung des Jobs erstellt oder geändert wurden. Sie können auch Objektkriterien verwenden, um Objekte auszuschließen, die vor einem bestimmten Datum und einer bestimmten Uhrzeit zuletzt geändert wurden.

Weitere Informationen zu diesem und anderen Schritten finden Sie unterErstellen einer Aufgabe zur Erkennung vertraulicher Daten.

6. Wenn Sie fertig sind, wählen Sie „Senden“, um die Kopie als neuen Job zu speichern.

Prognostizieren und Überwachen der Kosten für Erkennungsaufgaben bei vertraulichen Daten

Die Preise von Amazon Macie basieren teilweise auf der Datenmenge, die Sie analysieren, indem Sie sensible Datenermittlungsaufträge ausführen. Um Ihre geschätzten Kosten für die Ausführung von Aufträgen zur Erkennung vertraulicher Daten zu prognostizieren und zu überwachen, können Sie die Kostenschätzungen überprüfen, die Macie bei der Erstellung eines Auftrags und nach Beginn der Ausführung von Aufträgen bereitstellt.

Um Ihre tatsächlichen Kosten zu überprüfen und zu überwachen, können Sie Folgendes verwendenAWS Billing and Cost Management. AWS Billing and Cost Managementbietet Funktionen, mit denen Sie Ihre Kosten für AWS-Services Ihr Konto oder Ihre Organisation verfolgen und analysieren sowie Budgets verwalten können. Es bietet auch Funktionen, mit denen Sie die Nutzungskosten auf der Grundlage historischer Daten prognostizieren können. Weitere Informationen finden Sie im AWS Billing-Benutzerhandbuch.

Informationen zu den Macie-Preisen finden Sie unter Amazon Macie Macie-Preise.

Themen

- Prognostizieren der Kosten einer Aufgabe zur Erkennung sensibler Daten
- Überwachen der geschätzten Kosten für Erkennungsaufträge für sensible Daten

Prognostizieren der Kosten einer Aufgabe zur Erkennung sensibler Daten

Wenn Sie einen Job zur Erkennung vertraulicher Daten erstellen, kann Amazon Macie die geschätzten Kosten in zwei wichtigen Schritten der Auftragserstellung berechnen und anzeigen: wenn Sie die Tabelle der S3-Buckets überprüfen, die Sie für den Job ausgewählt haben (Schritt 2), und wenn Sie alle Einstellungen für den Job überprüfen (Schritt 8). Anhand dieser Schätzungen können Sie entscheiden, ob Sie die Einstellungen des Jobs anpassen müssen, bevor Sie den Job speichern. Die Verfügbarkeit und Art der Schätzungen hängen von den Einstellungen ab, die Sie für den Job wählen.

Überprüfung der geschätzten Kosten für einzelne Buckets (Schritt 2)

Wenn Sie explizit einzelne Buckets für einen zu analysierenden Job auswählen, können Sie die geschätzten Kosten für die Analyse von Objekten in jedem dieser Buckets überprüfen. Macie zeigt diese Schätzungen in Schritt 2 des Prozesses zur Stellenbeschaffung an, wenn Sie Ihre Auswahl an Buckets überprüfen. In der Tabelle für diesen Schritt gibt das Feld Estimated cost (Geschätzte Kosten) die geschätzten Gesamtkosten (in US-Dollar) für die einmalige Ausführung der Aufgabe zur Analyse von Objekten in einem Bucket an.

Jede Schätzung spiegelt die prognostizierte Menge an unkomprimierten Daten wider, die der Job in einem Bucket analysieren wird, basierend auf der Größe und den Typen der Objekte, die derzeit im Bucket gespeichert sind. Die Schätzung spiegelt auch die aktuellen AWS-Region Preise von Macie wider.

In der Kostenschätzung für einen Bucket sind nur klassifizierbare Objekte enthalten. Ein klassifizierbares Objekt ist ein S3-Objekt, das eine unterstützte Amazon S3 S3--Speicherklasse verwendet und eine Dateinamenerweiterung für ein unterstütztes Datei- oder Speicherformat hat. Handelt es sich bei klassifizierbaren Objekten um komprimierte oder archivierte Dateien, wird bei der Schätzung davon ausgegangen, dass die Dateien ein Kompressionsverhältnis von 3:1 haben und der Job alle extrahierten Dateien analysieren kann.

Überprüfung der geschätzten Gesamtkosten eines Auftrags (Schritt 8)

Wenn Sie einen einmaligen Auftrag erstellen oder einen regelmäßigen Job erstellen und konfigurieren, der vorhandene S3-Objekte einschließt, berechnet Macie im letzten Schritt der Auftragserstellung die geschätzten Gesamtkosten des Jobs und zeigt sie an. Sie können diese Schätzung überprüfen, während Sie alle Einstellungen, die Sie für den Job ausgewählt haben, überprüfen und verifizieren.

Diese Schätzung gibt die geschätzten Gesamtkosten (in US-Dollar) für die einmalige Ausführung der Aufgabe in der aktuellen -Region an. Die Schätzung spiegelt die prognostizierte Menge an unkomprimierten Daten wider, die der Job analysieren wird. Es basiert auf der Größe und den Typen der Objekte, die derzeit in Buckets gespeichert sind, die Sie explizit für den Job ausgewählt haben, oder auf bis zu 500 Buckets, die derzeit den Bucket-Kriterien entsprechen, die Sie für den Job angegeben haben, je nach den Einstellungen des Jobs.

Beachten Sie, dass diese Schätzung keine Optionen berücksichtigt, die Sie ausgewählt haben, um den Umfang des Jobs zu verfeinern und zu reduzieren, z. B. eine geringere Stichprobentiefe oder Kriterien, die bestimmte S3-Objekte vom Job ausschließen. Es spiegelt auch nicht Ihre

monatliche Quote für die Entdeckung vertraulicher Daten wider, die den Umfang und die Kosten der Analyse des Jobs einschränken könnte, oder etwaige Rabatte, die für Ihr Konto gelten könnten.

Zusätzlich zu den geschätzten Gesamtkosten des Auftrags enthält die Schätzung aggregierte Daten, die Aufschluss über den prognostizierten Umfang und die Kosten des Auftrags geben:

- Größenwerte geben die Gesamtspeichergröße der Objekte an, die der Job analysieren kann und die nicht.
- Die Werte für die Objektanzahl geben die Gesamtzahl der Objekte an, die der Job analysieren kann und die nicht.

In diesen Werten ist ein klassifizierbares Objekt ein S3-Objekt, das eine unterstützte Amazon S3 S3-Speicherklasse verwendet und eine Dateinamenerweiterung für eine unterstützte Datei oder ein unterstütztes Speicherformat hat. Nur klassifizierbare Objekte sind in der Kostenschätzung enthalten. Ein nicht klassifizierbares Objekt ist ein Objekt, das keine unterstützte -Speicherklasse verwendet oder keine Dateinamenerweiterung für ein unterstütztes Datei- oder Speicherformat hat. Diese Objekte sind nicht im Kostenvoranschlag enthalten.

Die Schätzung liefert zusätzliche aggregierte Daten für S3-Objekte, bei denen es sich um komprimierte oder archivierte Dateien handelt. Der Wert Compressed gibt die Gesamtspeichergröße von Objekten an, die eine unterstützte -Speicherklasse von Amazon S3 verwenden und eine Dateinamenerweiterung für ein unterstütztes komprimiertes Datei- oder Archivdateityp haben. Der Wert Unkomprimiert gibt die ungefähre Größe dieser Objekte an, wenn sie dekomprimiert werden, basierend auf einem bestimmten Komprimierungsverhältnis. Diese Daten sind relevant, da Macie komprimierte Dateien und Archivdateien analysiert.

Wenn Macie eine komprimierte oder archivierte Datei analysiert, überprüft sie sowohl die vollständige Datei als auch den Inhalt der Datei. Um den Inhalt der Datei zu überprüfen, dekomprimiert Macie die Datei und überprüft dann jede extrahierte Datei, die ein unterstütztes Format verwendet. Die tatsächliche Datenmenge, die ein Job analysiert, hängt daher ab von:

- Ob eine Datei komprimiert wird und, falls ja, welche Kompressionsrate sie verwendet.
- Die Anzahl, Größe und das Format der extrahierten Dateien.

Standardmäßig geht Macie bei der Berechnung von Kostenschätzungen für einen Auftrag von Folgendem aus:

- Alle komprimierten und archivierten Dateien verwenden ein Kompressionsverhältnis von 3:1.
- Alle extrahierten Dateien verwenden ein unterstütztes Datei- oder Speicherformat.

Diese Annahmen können zu einer größeren Schätzung des Umfangs der zu analysierenden Daten und folglich zu einer höheren Kostenschätzung für den Auftrag führen.

Sie können die geschätzten Gesamtkosten des Jobs auf der Grundlage eines anderen Komprimierungsverhältnisses neu berechnen. Wählen Sie dazu das Verhältnis aus der Liste Wählen Sie ein geschätztes Kompressionsverhältnis im Abschnitt Geschätzte Kosten aus. Macie aktualisiert dann die Schätzung, sodass sie Ihrer Auswahl entspricht.

Weitere Informationen dazu, wie Macie die geschätzten Kosten berechnet, finden Sie unter. Verstehen, wie die geschätzten Nutzungskosten berechnet werden

Überwachen der geschätzten Kosten für Erkennungsaufträge für sensible Daten

Wenn Sie bereits Aufträge zur Erkennung vertraulicher Daten ausführen, können Sie auf der Seite „Verwendung“ auf der Amazon Macie Macie-Konsole die geschätzten Kosten dieser Jobs überwachen. Die Seite zeigt Ihre geschätzten Kosten (in US-Dollar) für die aktuelle Nutzung von Macie AWS-Region im aktuellen Kalendermonat. Hinweise dazu, wie Macie diese Schätzungen berechnet, finden Sie unter. Verstehen, wie die geschätzten Nutzungskosten berechnet werden

Um Ihre geschätzten Kosten für laufende Jobs zu überprüfen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. AWS-RegionWählen Sie mithilfe der Auswahl in der oberen rechten Ecke der Seite die -Region aus, in der Sie Ihre geschätzten Kosten überprüfen möchten.
3. Wählen Sie im Navigationsbereich Verwendung aus.
4. Auf der Seite Nutzung findest du die Aufschlüsselung der geschätzten Kosten für dein Konto. Das Element „Aufträge zur Erkennung vertraulicher Daten“ gibt die geschätzten Gesamtkosten der Jobs an, die Sie bisher im aktuellen Monat in der aktuellen Region ausgeführt haben.

   Wenn Sie der Macie-Administrator für eine Organisation sind, werden im Abschnitt Geschätzte Kosten die geschätzten Kosten für Ihre Organisation insgesamt für den aktuellen Monat in der aktuellen Region angezeigt. Um die geschätzten Gesamtkosten der Jobs anzuzeigen, die für ein bestimmtes Konto ausgeführt wurden, wählen Sie das Konto in der Tabelle aus. Im Abschnitt Geschätzte Kosten wird dann eine Aufschlüsselung der geschätzten Kosten für das Konto angezeigt, einschließlich der geschätzten Kosten der ausgeführten Jobs. Um diese Daten für ein anderes Konto anzuzeigen, wählen Sie das Konto in der Tabelle aus. Um Ihre Kontoauswahl zu löschen, wählen Sie das X neben der Konto-ID aus.

Um Ihre tatsächlichen Kosten zu überprüfen und zu überwachen, verwenden Sie AWS Billing and Cost Management.

Verwaltete Datenkennungen, die für die Erkennung vertraulicher Daten empfohlen werden

Um die Ergebnisse Ihrer Aufgaben zur Erkennung vertraulicher Daten zu optimieren, können Sie einzelne Jobs so konfigurieren, dass sie automatisch die von uns für Jobs empfohlenen verwalteten Datenkennungen verwenden. EINIdentifier für verwaltete Datenist eine Reihe integrierter Kriterien und Techniken, die darauf ausgelegt sind, einen bestimmten Typ sensibler Daten zu erkennen — zum BeispielAWSgeheime Zugangsschlüssel, Kreditkartennummern oder Passnummern für ein bestimmtes Land oder eine bestimmte Region.

Der empfohlene Satz verwalteter Datenkennungen dient der Erkennung gängiger Kategorien und Typen vertraulicher Daten. Basierend auf unseren Recherchen kann es allgemeine Kategorien und Arten sensibler Daten erkennen und gleichzeitig Ihre Arbeitsergebnisse optimieren, indem es den Lärm reduziert. Sobald wir neue Identifikatoren für verwaltete Daten veröffentlichen, fügen wir sie zu diesem Set hinzu, sofern sie Ihre Arbeitsergebnisse weiter optimieren könnten. Im Laufe der Zeit können wir dem Set auch bestehende Identifikatoren für verwaltete Daten hinzufügen oder daraus entfernen. Wenn wir dem empfohlenen Set eine verwaltete Daten-ID hinzufügen oder daraus entfernen, aktualisieren wir diese Seite, um die Art und den Zeitpunkt der Änderung anzugeben. Um automatische Benachrichtigungen über diese Änderungen zu erhalten, können Sie den RSS-Feed auf derGeschichte des Macie-DokumentsSeite.

Wenn Sie einen Job zur Erkennung vertraulicher Daten erstellen, geben Sie an, welche verwalteten Datenkennungen der Job zur Analyse von Objekten in Amazon Simple Storage Service (Amazon S3) -Buckets verwenden soll. Um einen Job so zu konfigurieren, dass er den empfohlenen Satz von verwalteten Datenkennungen verwendet, wählen SieEmpfohlenOption, wenn Sie den Job erstellen. Der Job verwendet dann automatisch alle verwalteten Datenkennungen, die im empfohlenen Satz enthalten sind, wenn der Job ausgeführt wird. Wenn Sie einen Job so konfigurieren, dass er mehr als einmal ausgeführt wird, verwendet jeder Lauf automatisch alle verwalteten Datenkennungen, die zu Beginn des Laufs im empfohlenen Satz enthalten sind.

In den folgenden Themen sind die verwalteten Datenkennungen aufgeführt, die derzeit im empfohlenen Satz enthalten sind, geordnet nach Kategorie und Typ vertraulicher Daten. Sie geben den eindeutigen Identifier (ID) für jeden verwalteten Datenbezeichner im Satz an. Diese ID beschreibt die Art sensibler Daten, die ein verwalteter Datenbezeichner erkennen soll, zum

Beispiel:`PGP_PRIVATE_KEY`für private PGP-Schlüssel und`USA_PASSPORT_NUMBER`für US-Passnummern.

Themen

- Anmeldeinformationen
- Finanzinformationen
- Persönlich Identifizierbare Informationen (PII)
- Aktualisierungen des empfohlenen Sets

Einzelheiten zu bestimmten Identifikatoren für verwaltete Daten oder eine vollständige Liste aller Identifikatoren für verwaltete Daten, die Macie derzeit bereitstellt, finden Sie unterVerwenden von verwalteten Datenbezeichnern.

Anmeldeinformationen

Um das Vorkommen von Anmeldeinformationsdaten in S3-Objekten zu erkennen, verwendet der empfohlene Satz die folgenden verwalteten Datenkennungen.

Sensibler Datentyp	ID der verwalteten Datenkennung
Geheimer AWS-Zugriffsschlüssel	`AWS_CREDENTIALS`
Header für die HTTP-Standardautorisierung	`HTTP_BASIC_AUTH_HEADER`
Privater OpenSSH-Schlüssel	`OPENSSH_PRIVATE_KEY`
Privater PGP-Schlüssel	`PGP_PRIVATE_KEY`
Privater Schlüssel des Public Key Cryptography Standard (PKCS)	`PKCS`
Privater PuTTY-Schlüssel	`PUTTY_PRIVATE_KEY`

Finanzinformationen

Um das Vorkommen von Finanzinformationen in S3-Objekten zu erkennen, verwendet das empfohlene Set die folgenden verwalteten Datenkennungen.

Sensibler Datentyp	ID der verwalteten Datenkennung
Kreditkarten-Magnetstreifendaten	`CREDIT_CARD_MAGNETIC_STRIPE`
Kreditkartennummer	`CREDIT_CARD_NUMBER` (für Kreditkartennummern in der Nähe eines Schlüsselworts)

Persönlich Identifizierbare Informationen (PII)

Um das Vorkommen personenbezogener Daten (PII) in S3-Objekten zu erkennen, verwendet das empfohlene Set die folgenden verwalteten Datenkennungen.

Sensibler Datentyp	ID der verwalteten Datenkennung
Identifikationsnummer des Führerscheins	`CANADA_DRIVERS_LICENSE`, `DRIVERS_LICENSE` (für die USA),`UK_DRIVERS_LICENSE`
Nummer der Wählerliste	`UK_ELECTORAL_ROLL_NUMBER`
Nationale Identifikationsnummern	`FRANCE_NATIONAL_IDENTIFICATION_NUMBER`, `GERMANY_NATIONAL_IDENTIFICATION_NUMBER`, `ITALY_NATIONAL_IDENTIFICATION_NUMBER`, `SPAIN_DNI_NUMBER`
Landesversicherungsnummer (NINO)	`UK_NATIONAL_INSURANCE_NUMBER`
Passnummer	`CANADA_PASSPORT_NUMBER`, `FRANCE_PASSPORT_NUMBER`, `GERMANY_PASSPORT_NUMBER`, `ITALY_PASSPORT_NUMBER`, `SPAIN_PASSPORT_NUMBER`, `UK_PASSPORT_NUMBER`, `USA_PASSPORT_NUMBER`
Sozialversicherungsnummer (SIN)	`CANADA_SOCIAL_INSURANCE_NUMBER`

Sensibler Datentyp	ID der verwalteten Datenkennung
Sozialversicherungsnummer (SSN)	`SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER`
Steuerpflichtigen-Identifikationsnummer oder Referenznummer	`AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER`

Aktualisierungen des empfohlenen Sets

In der folgenden Tabelle werden die Änderungen an der Gruppe der verwalteten Datenkennungen beschrieben, die wir für Aufgaben zur Erkennung vertraulicher Daten empfehlen. Um automatische Benachrichtigungen über diese Änderungen zu erhalten, abonnieren Sie den RSS-Feed auf derGeschichte des Macie-DokumentsSeite.

Änderung	Beschreibung	Datum
Allgemeine Verfügbarkeit	Erstveröffentlichung des empfohlenen Sets.	27. Juni 2023

Analysieren verschlüsselter Amazon S3-Objekte mit Amazon Macie

Wenn Sie Amazon Macie für Ihr aktivierenAWS-Konto, erstellt Macie eine serviceverknüpfte Rolle, die Macie die Berechtigungen erteilt, die es zum Aufrufen von Amazon Simple Storage Service (Amazon S3) und anderen AWS-Services in Ihrem Namen benötigt. Eine serviceverknüpfte Rolle vereinfacht das Einrichten eines , AWS-Service da Sie dem Service keine Berechtigungen manuell hinzufügen müssen, um Aktionen in Ihrem Namen durchzuführen. Weitere Informationen zu dieser Art von Rolle finden Sie unter Verwenden von serviceverknüpften Rollen im AWS Identity and Access Management -Benutzerhandbuch.

Die Berechtigungsrichtlinie für die serviceverknüpfte Macie-Rolle (`AWSServiceRoleForAmazonMacie`) ermöglicht es Macie, Aktionen auszuführen, die das Abrufen von Informationen zu Ihren S3-Buckets und Objekten sowie das Abrufen und Analysieren von Objekten in Ihren S3-Buckets beinhalten. Wenn Ihr Konto das Macie-Administratorkonto für eine Organisation ist, erlaubt die Richtlinie Macie auch, diese Aktionen in Ihrem Namen für Mitgliedskonten in Ihrer Organisation auszuführen.

Wenn ein S3-Objekt verschlüsselt ist, gewährt die Berechtigungsrichtlinie für die serviceverknüpfte Macie-Rolle Macie in der Regel die Berechtigungen, die es zum Entschlüsseln des Objekts benötigt. Dies hängt jedoch von der Art der verwendeten Verschlüsselung ab. Sie kann auch davon abhängen, ob Macie den entsprechenden Verschlüsselungsschlüssel verwenden darf.

Themen

- Verschlüsselungsoptionen für Amazon S3-Objekte
- Amazon Macie erlauben, einen vom Kunden verwalteten zu verwenden AWS KMS key

Verschlüsselungsoptionen für Amazon S3-Objekte

Amazon S3 unterstützt mehrere Verschlüsselungsoptionen für S3-Objekte. Für die meisten dieser Optionen kann Amazon Macie ein Objekt mithilfe der serviceverknüpften Macie-Rolle für Ihr Konto entschlüsseln. Dies hängt jedoch von der Art der Verschlüsselung ab, die zum Verschlüsseln eines Objekts verwendet wurde.

Serverseitige Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3)

Wenn ein Objekt mit serverseitiger Verschlüsselung mit einem von Amazon S3 verwalteten Schlüssel (SSE-S3) verschlüsselt wird, kann Macie das Objekt entschlüsseln.

Weitere Informationen zu dieser Art der Verschlüsselung finden Sie unter Verwenden der serverseitigen Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln im Benutzerhandbuch für Amazon Simple Storage Service.

Serverseitige Verschlüsselung mit AWS KMS keys (DSSE-KMS und SSE-KMS)

Wenn ein Objekt mit serverseitiger Dual-Layer-Verschlüsselung oder serverseitiger Verschlüsselung mit einem -AWSverwalteten AWS KMS key (DSSE-KMS oder SSE-KMS) verschlüsselt wird, kann Macie das Objekt entschlüsseln.

Wenn ein Objekt mit serverseitiger Dual-Layer-Verschlüsselung oder serverseitiger Verschlüsselung mit einem vom Kunden verwalteten AWS KMS key (DSSE-KMS oder

SSE-KMS) verschlüsselt wird, kann Macie das Objekt nur entschlüsseln, wenn Sie Macie erlauben, den Schlüssel zu verwenden. Dies ist bei Objekten der Fall, die mit KMS-Schlüsseln verschlüsselt sind, die vollständig innerhalb von AWS KMS und KMS-Schlüsseln in einem externen Schlüsselspeicher verwaltet werden. Wenn Macie den entsprechenden KMS-Schlüssel nicht verwenden darf, kann Macie nur Metadaten für das Objekt speichern und melden.

Weitere Informationen zu diesen Verschlüsselungstypen finden Sie unter Verwenden der serverseitigen Dual-Layer-Verschlüsselung mit AWS KMS keys und Verwenden der serverseitigen Verschlüsselung mit AWS KMS keys im Benutzerhandbuch für Amazon Simple Storage Service.

> **Tip**
>
> Sie können automatisch eine Liste aller vom Kunden verwalteten generierenAWS KMS keys, auf die Macie zugreifen muss, um Objekte in den S3-Buckets für Ihr Konto zu analysieren. Führen Sie dazu das AWS KMS Permission Analyzer-Skript aus, das im Amazon Macie Scripts-Repository auf verfügbar ist GitHub. Das Skript kann auch ein zusätzliches Skript von AWS Command Line Interface (AWS CLI)-Befehlen generieren. Sie können diese Befehle optional ausführen, um die erforderlichen Konfigurationseinstellungen und Richtlinien für von Ihnen angegebene KMS-Schlüssel zu aktualisieren.

Serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln (SSE-C)

Wenn ein Objekt mit serverseitiger Verschlüsselung mit einem vom Kunden bereitgestellten Schlüssel (SSE-C) verschlüsselt wird, kann Macie das Objekt nicht entschlüsseln. Macie kann nur Metadaten für das Objekt speichern und melden.

Weitere Informationen zu dieser Art der Verschlüsselung finden Sie unter Verwenden der serverseitigen Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln im Benutzerhandbuch für Amazon Simple Storage Service.

Clientseitige Verschlüsselung

Wenn ein Objekt mit clientseitiger Verschlüsselung verschlüsselt wird, kann Macie das Objekt nicht entschlüsseln. Macie kann nur Metadaten für das Objekt speichern und melden. Macie kann beispielsweise die Größe des Objekts und die Tags melden, die dem Objekt zugeordnet sind.

Informationen zu dieser Art der Verschlüsselung im Kontext von Amazon S3 finden Sie unter Schützen von Daten mithilfe der clientseitigen Verschlüsselung im Benutzerhandbuch für Amazon Simple Storage Service.

Sie können Ihren Bucket-Bestand in Macie filtern, um festzustellen, welche S3-Buckets Objekte speichern, die bestimmte Verschlüsselungstypen verwenden. Sie können auch bestimmen, welche Buckets standardmäßig bestimmte Arten der serverseitigen Verschlüsselung beim Speichern neuer Objekte verwenden. Die folgende Tabelle enthält Beispiele für Filter, die Sie auf Ihren Bucket-Bestand anwenden können, um diese Informationen zu finden.

So zeigen Sie Buckets an, die ...	Wenden Sie diesen Filter an...
Speichern von Objekten, die SSE-C-Verschlüsselung verwenden	Die Anzahl der Objekte nach Verschlüsselung ist Vom Kunden bereitgestellt und Von = 1
Speichern von Objekten, die DSSE-KMS- oder SSE-KMS-Verschlüsselung verwenden	Die Anzahl der Objekte nach Verschlüsselung wird AWS KMS verwaltet und von = 1
Speichern von Objekten, die SSE-S3-Verschlüsselung verwenden	Die Anzahl der Objekte nach Verschlüsselung wird von Amazon S3 verwaltet und von = 1
Speichern von Objekten, die clientseitige Verschlüsselung verwenden (oder nicht verschlüsselt sind)	Die Anzahl der Objekte nach Verschlüsselung ist Keine Verschlüsselung und Von = 1
Standardmäßige Verschlüsselung neuer Objekte mit DSSE-KMS-Verschlüsselung	Standardverschlüsselung = aws:kms:dsse
Standardmäßiges Verschlüsseln neuer Objekte mit SSE-KMS-Verschlüsselung	Standardverschlüsselung = aws:kms
Standardmäßiges Verschlüsseln neuer Objekte mit SSE-S3-Verschlüsselung	Standardverschlüsselung = AES256

Wenn ein Bucket so konfiguriert ist, dass neue Objekte standardmäßig mit DSSE-KMS- oder SSE-KMS-Verschlüsselung verschlüsselt werden, können Sie auch ermitteln, welche verwendet AWS KMS key wird. Wählen Sie dazu den Bucket auf der Seite S3-Buckets aus. Verweisen Sie im Bereich

mit den Bucket-Details unter Serverseitige Verschlüsselung auf das Feld . AWS KMS key Dieses Feld zeigt den Amazon-Ressourcennamen (ARN) oder die eindeutige Kennung (Schlüssel-ID) für den Schlüssel an.

Amazon Macie erlauben, einen vom Kunden verwalteten zu verwenden AWS KMS key

Wenn ein Amazon S3-Objekt mit serverseitiger Dual-Layer-Verschlüsselung oder serverseitiger Verschlüsselung mit einem vom Kunden verwalteten AWS KMS key (DSSE-KMS oder SSE-KMS) verschlüsselt wird, kann Amazon Macie das Objekt nur entschlüsseln, wenn es den Schlüssel verwenden darf. Wie Sie diesen Zugriff gewähren, hängt davon ab, ob das Konto, das den Schlüssel besitzt, auch Eigentümer des S3-Buckets ist, in dem das Objekt gespeichert ist:

- Wenn dasselbe Konto Eigentümer des AWS KMS key und des Buckets ist, muss ein Benutzer des Kontos die Richtlinie des Schlüssels aktualisieren.
- Wenn ein Konto Eigentümer des AWS KMS key und ein anderes Konto Eigentümer des Buckets ist, muss ein Benutzer des Kontos, dem der Schlüssel gehört, den kontoübergreifenden Zugriff auf den Schlüssel erlauben.

In diesem Thema wird beschrieben, wie diese Aufgaben ausgeführt werden, und es werden Beispiele für beide Szenarien bereitgestellt. Weitere Informationen zum Zulassen des Zugriffs auf vom Kunden AWS KMS keysverwaltete finden Sie unter Authentifizierung und Zugriffskontrolle für AWS KMS im AWS Key Management Service Entwicklerhandbuch für .

Erlauben des kontointernen Zugriffs auf einen vom Kunden verwalteten Schlüssel

Wenn dasselbe Konto sowohl den AWS KMS key als auch den S3-Bucket besitzt, muss ein Benutzer des Kontos der Richtlinie für den Schlüssel eine Anweisung hinzufügen. Die zusätzliche Anweisung muss es der serviceverknüpften Macie-Rolle für das Konto ermöglichen, Daten mithilfe des Schlüssels zu entschlüsseln. Ausführliche Informationen zum Aktualisieren einer Schlüsselrichtlinie finden Sie unter Ändern einer Schlüsselrichtlinie im AWS Key Management Service -Entwicklerhandbuch.

In der -Anweisung:

- Das -`Principal`Element muss den Amazon-Ressourcennamen (ARN) der serviceverknüpften Macie-Rolle für das Konto angeben, das Eigentümer des AWS KMS key und des S3-Buckets ist.

Wenn sich das Konto in einer Opt-in- befindetAWS-Region, muss der ARN auch den entsprechenden Regionscode für die Region enthalten. Wenn sich das Konto beispielsweise in der Region Naher Osten (Bahrain) befindet, die den Regionscode me-south-1 hat, muss das -PrincipalElement angeben`arn:aws:iam::123456789012:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie`, wobei *123456789012* die Konto-ID für das Konto ist. Eine Liste der Regionscodes für die Regionen, in denen Macie derzeit verfügbar ist, finden Sie unter Endpunkte und Kontingente von Amazon Macie im Allgemeine AWS-Referenz.

- Das `Action`Array muss die `kms:Decrypt` Aktion angeben. Dies ist die einzige AWS KMS Aktion, die Macie ausführen muss, um ein S3-Objekt zu entschlüsseln, das mit dem Schlüssel verschlüsselt ist.

Im Folgenden finden Sie ein Beispiel für die Anweisung, die der Richtlinie für eine hinzugefügt werden sollAWS KMS key.

```
{
    "Sid": "Allow the Macie service-linked role to use the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie"
    },
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

Für das obige Beispiel gilt:

- Das `AWS` Feld im -`Principal`Element gibt den ARN der serviceverknüpften Macie-Rolle (`AWSServiceRoleForAmazonMacie`) für das Konto an. Es ermöglicht der serviceverknüpften Macie-Rolle, die in der Richtlinienanweisung angegebene Aktion auszuführen. *123456789012* ist ein Beispiel für eine Konto-ID. Ersetzen Sie diesen Wert durch die Konto-ID für das Konto, das den KMS-Schlüssel und den S3-Bucket besitzt.
- Das `Action`Array gibt die Aktion an, die die serviceverknüpfte Macie-Rolle mit dem KMS-Schlüssel ausführen darf – entschlüsseln Sie Geheimtext, der mit dem Schlüssel verschlüsselt ist.

Wo Sie diese Anweisung zu einer Schlüsselrichtlinie hinzufügen, hängt von der Struktur und den Elementen ab, die die Richtlinie derzeit enthält. Wenn Sie die Anweisung hinzufügen, stellen Sie sicher, dass die Syntax gültig ist. Schlüsselrichtlinien verwenden das JSON-Format. Dies bedeutet, dass Sie auch ein Komma vor oder nach der Anweisung hinzufügen müssen, je nachdem, wo Sie die Anweisung zur Richtlinie hinzufügen.

Kontoübergreifenden Zugriff auf einen vom Kunden verwalteten Schlüssel erlauben

Wenn ein Konto Eigentümer des AWS KMS key (Schlüsselbesitzers) und ein anderes Konto Eigentümer des S3-Buckets (Bucket-Eigentümer) ist, muss der Schlüsselbesitzer dem Bucket-Eigentümer kontoübergreifenden Zugriff auf den KMS-Schlüssel gewähren. Dazu stellt der Schlüsseleigentümer zunächst sicher, dass die Richtlinie des Schlüssels dem Bucket-Eigentümer erlaubt, sowohl den Schlüssel zu verwenden als auch eine Erteilung für den Schlüssel zu erstellen. Der Bucket-Eigentümer erstellt dann eine Erteilung für den Schlüssel. Eine Erteilung ist ein Richtlinieninstrument, das es AWSPrinzipalen ermöglicht, KMS-Schlüssel in kryptografischen Operationen zu verwenden, wenn die in der Erteilung angegebenen Bedingungen erfüllt sind. In diesem Fall delegiert die Erteilung die relevanten Berechtigungen an die serviceverknüpfte Macie-Rolle für das Konto des Bucket-Eigentümers.

Ausführliche Informationen zum Aktualisieren einer Schlüsselrichtlinie finden Sie unter Ändern einer Schlüsselrichtlinie im AWS Key Management Service -Entwicklerhandbuch. Weitere Informationen zu Erteilungen finden Sie unter Erteilungen in AWS KMS im AWS Key Management Service -Entwicklerhandbuch.

Schritt 1: Aktualisieren der Schlüsselrichtlinie

In der Schlüsselrichtlinie sollte der Schlüsseleigentümer sicherstellen, dass die Richtlinie zwei Anweisungen enthält:

- Die erste Anweisung ermöglicht es dem Bucket-Eigentümer, den Schlüssel zum Entschlüsseln von Daten zu verwenden.
- Die zweite Anweisung ermöglicht es dem Bucket-Eigentümer, eine Erteilung für die serviceverknüpfte Macie-Rolle für sein Konto (das des Bucket-Eigentümers) zu erstellen.

In der ersten Anweisung muss das -`Principal`Element den ARN des Kontos des Bucket-Eigentümers angeben. Das `Action`Array muss die `kms:Decrypt` Aktion angeben. Dies ist die einzige AWS KMS Aktion, die Macie ausführen darf, um ein mit dem Schlüssel verschlüsseltes Objekt

zu entschlüsseln. Im Folgenden finden Sie ein Beispiel für diese Anweisung in der Richtlinie für einen AWS KMS key.

```
{
    "Sid": "Allow account 111122223333 to use the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

Für das obige Beispiel gilt:

- Das `AWS` Feld im -`Principal`Element gibt den ARN des Kontos des Bucket-Eigentümers (*111122223333*) an. Es ermöglicht dem Bucket-Eigentümer, die in der Richtlinienanweisung angegebene Aktion auszuführen. *111122223333* ist ein Beispiel für eine Konto-ID. Ersetzen Sie diesen Wert durch die Konto-ID für das Konto des Bucket-Eigentümers.
- Das `Action`Array gibt die Aktion an, die der Bucket-Eigentümer mit dem KMS-Schlüssel ausführen darf – Entschlüsseln von Geheimtext, der mit dem Schlüssel verschlüsselt ist.

Die zweite Anweisung in der Schlüsselrichtlinie ermöglicht es dem Bucket-Eigentümer, eine Erteilung für die Macie-serviceverknüpfte Rolle für sein Konto zu erstellen. In dieser Anweisung muss das -`Principal`Element den ARN des Kontos des Bucket-Eigentümers angeben. Das `Action`Array muss die `kms:CreateGrant` Aktion angeben. Ein -`Condition`Element kann den Zugriff auf die in der Anweisung angegebene `kms:CreateGrant` Aktion filtern. Im Folgenden finden Sie ein Beispiel für diese Anweisung in der Richtlinie für einen AWS KMS key.

```
{
    "Sid": "Allow account 111122223333 to create a grant",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "kms:CreateGrant"
    ],
```

```
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:GranteePrincipal": "arn:aws:iam::111122223333:role/aws-service-role/
macie.amazonaws.com/AWSServiceRoleForAmazonMacie"
        }
    }
}
```

Für das obige Beispiel gilt:

- Das `AWS` Feld im -`Principal`Element gibt den ARN des Kontos des Bucket-Eigentümers (*111122223333*) an. Es ermöglicht dem Bucket-Eigentümer, die in der Richtlinienanweisung angegebene Aktion auszuführen. *111122223333* ist ein Beispiel für eine Konto-ID. Ersetzen Sie diesen Wert durch die Konto-ID für das Konto des Bucket-Eigentümers.
- Das `Action`Array gibt die Aktion an, die der Bucket-Eigentümer für den KMS-Schlüssel ausführen darf – Erstellen Sie eine Erteilung für den Schlüssel.
- Das -`Condition`Element verwendet den `StringEquals` Bedingungsoperator und den `kms:GranteePrincipal` Bedingungsschlüssel, um den Zugriff auf die in der Richtlinienanweisung angegebene Aktion zu filtern. In diesem Fall kann der Bucket-Eigentümer eine Erteilung nur für das angegebene erstellen`GranteePrincipal`, bei dem es sich um den ARN der serviceverknüpften Macie-Rolle für sein Konto handelt. In diesem ARN ist *111122223333* ein Beispiel für eine Konto-ID. Ersetzen Sie diesen Wert durch die Konto-ID für das Konto des Bucket-Eigentümers.

  Wenn sich das Konto des Bucket-Eigentümers in einem Opt-in befindetAWS-Region, fügen Sie auch den entsprechenden Regionscode in den ARN der serviceverknüpften Macie-Rolle ein. Wenn sich das Konto beispielsweise in der Region Naher Osten (Bahrain) befindet, in der der Regionscode me-south-1 enthalten ist, ersetzen Sie `macie.me-south-1.amazonaws.com` im ARN `macie.amazonaws.com` durch . Eine Liste der Regionscodes für die Regionen, in denen Macie derzeit verfügbar ist, finden Sie unter Endpunkte und Kontingente von Amazon Macie im Allgemeine AWS-Referenz.

Wo der Schlüsseleigentümer diese Anweisungen zur Schlüsselrichtlinie hinzufügt, hängt von der Struktur und den Elementen ab, die die Richtlinie derzeit enthält. Wenn der Schlüsseleigentümer die Anweisungen hinzufügt, sollte er sicherstellen, dass die Syntax gültig ist. Schlüsselrichtlinien verwenden das JSON-Format. Das bedeutet, dass der Schlüsseleigentümer vor oder nach jeder

Anweisung auch ein Komma hinzufügen muss, je nachdem, wo er die Anweisung zur Richtlinie hinzufügt.

Schritt 2: Erstellen einer Erteilung

Nachdem der Schlüsseleigentümer die Schlüsselrichtlinie nach Bedarf aktualisiert hat, muss der Bucket-Eigentümer eine Berechtigung für den Schlüssel erstellen. Die Erteilung delegiert die relevanten Berechtigungen an die serviceverknüpfte Macie-Rolle für ihr Konto (das Konto des Bucket-Eigentümers). Bevor der Bucket-Eigentümer die Erteilung erstellt, sollte er überprüfen, ob er die `kms:CreateGrant` Aktion für sein Konto ausführen darf. Diese Aktion ermöglicht es ihnen, einem vorhandenen, vom Kunden verwalteten eine Erteilung hinzuzufügenAWS KMS key.

Um die Erteilung zu erstellen, kann der Bucket-Eigentümer die -CreateGrantOperation der AWS Key Management Service-API verwenden. Wenn der Bucket-Eigentümer die Erteilung erstellt, sollte er die folgenden Werte für die erforderlichen Parameter angeben:

- `KeyId` – Der ARN des KMS-Schlüssels. Für den kontoübergreifenden Zugriff auf einen KMS-Schlüssel muss dieser Wert ein ARN sein. Es darf keine Schlüssel-ID sein.
- `GranteePrincipal` – Der ARN der serviceverknüpften Macie-Rolle (`AWSServiceRoleForAmazonMacie`) für ihr Konto. Dieser Wert sollte sein`arn:aws:iam::`*`111122223333`*`:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`, wobei *`111122223333`* die Konto-ID für das Konto des Bucket-Eigentümers ist.

  Wenn sich ihr Konto in einer Opt-in-Region befindet, muss der ARN den entsprechenden Regionscode enthalten. Wenn sich ihr Konto beispielsweise in der Region Naher Osten (Bahrain) befindet, die den Regionscode me-south-1 hat, sollte der ARN lauten`arn:aws:iam::`*`111122223333`*`:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie`, wobei *`111122223333`* die Konto-ID für das Konto des Bucket-Eigentümers ist.
- `Operations` – Die AWS KMS Entschlüsselungsaktion (`Decrypt`). Dies ist die einzige AWS KMS Aktion, die Macie ausführen darf, um ein mit dem KMS-Schlüssel verschlüsseltes Objekt zu entschlüsseln.

Um eine Erteilung für einen vom Kunden verwalteten KMS-Schlüssel mithilfe der AWS Command Line Interface (AWS CLI) zu erstellen, führen Sie den Befehl create-grant aus. Im folgenden Beispiel wird gezeigt, wie dies geschieht. Das Beispiel ist für Microsoft Windows formatiert und verwendet das Zeilenkontinuierungszeichen caret (^), um die Lesbarkeit zu verbessern.

```
C:\> aws kms create-grant ^
--key-id arn:aws:kms:us-east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab ^
--grantee-principal arn:aws:iam::111122223333:role/aws-service-role/
macie.amazonaws.com/AWSServiceRoleForAmazonMacie ^
--operations "Decrypt"
```

Wobei gilt:

- `key-id` gibt den ARN des KMS-Schlüssels an, auf den die Erteilung angewendet werden soll.
- `grantee-principal` gibt den ARN der serviceverknüpften Macie-Rolle für das Konto an, das die durch die Erteilung angegebene Aktion ausführen darf. Dieser Wert sollte mit dem ARN übereinstimmen, der durch die `kms:GranteePrincipal` Bedingung der zweiten Anweisung in der Schlüsselrichtlinie angegeben wird.
- `operations` gibt die Aktion an, die die Erteilung dem angegebenen Prinzipal ermöglicht, d. h. entschlüsseln Sie Geheimtext, der mit dem KMS-Schlüssel verschlüsselt ist.

Wird der Befehl erfolgreich ausgeführt, erhalten Sie eine Ausgabe ähnlich der folgenden:

```
{
    "GrantToken": "<grant token>",
    "GrantId": "1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2"
}
```

Dabei `GrantToken` ist eine eindeutige, nicht geheime, base64-kodierte Zeichenfolge mit variabler Länge, die die erstellte Erteilung darstellt und die eindeutige Kennung für die Erteilung `GrantId` ist.

Speichern und Aufbewahren von Erkennungsergebnissen sensibler Daten mit Amazon Macie

Wenn Sie einen Discovery-Job für sensible Daten ausführen oder Amazon Macie eine automatische Erkennung sensibler Daten durchführt, erstellt Macie einen Analysedatensatz für jedes Amazon Simple Storage Service (Amazon S3) -Objekt, das im Umfang der Analyse enthalten ist. Diese Datensätze, die als Erkennungsergebnisse sensibler Daten bezeichnet werden, protokollieren Details zu der Analyse, die Macie an einzelnen S3-Objekten durchführt. Dazu gehören Objekte, in denen Macie keine sensiblen Daten erkennt und die daher keine Ergebnisse liefern, sowie Objekte, die Macie aufgrund von Fehlern oder Problemen nicht analysieren kann. Wenn Macie sensible

Daten in einem Objekt entdeckt, enthält der Datensatz Daten aus dem entsprechenden Ergebnis sowie zusätzliche Informationen. Die Ergebnisse der Entdeckung sensibler Daten liefern Ihnen Analyseaufzeichnungen, die für Prüfungen oder Untersuchungen zum Datenschutz hilfreich sein können.

Macie speichert Ihre Ergebnisse der Entdeckung sensibler Daten nur 90 Tage lang. Um auf Ihre Ergebnisse zuzugreifen und sie langfristig zu speichern und aufzubewahren, konfigurieren Sie Macie so, dass die Ergebnisse mit einem AWS Key Management Service (AWS KMS) -Schlüssel verschlüsselt und in einem S3-Bucket gespeichert werden. Der Bucket kann als definitives, langfristiges Repository für all Ihre Erkennungsergebnisse sensibler Daten dienen. Anschließend können Sie optional auf die Ergebnisse in diesem Repository zugreifen und diese abfragen.

In diesem Thema erfahren Sie, wie Sie mithilfe von ein Repository für Ihre Discovery-Ergebnisse für sensible Daten konfigurieren. AWS Management Console Die Konfiguration ist eine Kombination aus einem, der AWS KMS key die Ergebnisse verschlüsselt, einem S3-Bucket, in dem die Ergebnisse gespeichert werden, und Macie-Einstellungen, die angeben, welcher Schlüssel und welcher Bucket verwendet werden sollen. Wenn Sie es vorziehen, die Macie-Einstellungen programmgesteuert zu konfigurieren, können Sie den PutClassificationExportConfigurationBetrieb der Amazon Macie Macie-API verwenden.

Wenn Sie die Einstellungen in Macie konfigurieren, gelten Ihre Auswahlmöglichkeiten nur für die aktuelle Version. AWS-Region Wenn Sie der Macie-Administrator einer Organisation sind, gelten Ihre Auswahlmöglichkeiten nur für Ihr Konto. Sie gelten nicht für verknüpfte Mitgliedskonten.

Wenn Sie Macie in mehreren Fällen verwenden AWS-Regionen, konfigurieren Sie die Repository-Einstellungen für jede Region, in der Sie Macie verwenden. Sie können optional die Ergebnisse der Erkennung sensibler Daten für mehrere Regionen im selben S3-Bucket speichern. Beachten Sie jedoch die folgenden Anforderungen:

- Um die Ergebnisse für eine Region zu speichern, die standardmäßig AWS aktiviert ist AWS-Konten, z. B. die Region USA Ost (Nord-Virginia), müssen Sie einen Bucket in einer Region auswählen, die standardmäßig aktiviert ist. Die Ergebnisse können nicht in einem Bucket in einer Opt-in-Region gespeichert werden (Region, die standardmäßig deaktiviert ist).
- Um die Ergebnisse für eine Opt-in-Region zu speichern, z. B. die Region Naher Osten (Bahrain), müssen Sie einen Bucket in derselben Region oder eine Region auswählen, die standardmäßig aktiviert ist. Die Ergebnisse können nicht in einem Bucket in einer anderen Opt-in-Region gespeichert werden.

Informationen darüber, ob eine Region standardmäßig aktiviert ist, finden Sie im AWS Identity and Access Management Benutzerhandbuch unter Regionen und Endpunkte. Überlegen Sie sich zusätzlich zu den oben genannten Anforderungen auch, ob Sie Stichproben sensibler Daten abrufen möchten, die Macie als Einzelbefunde ausgibt. Um Stichproben vertraulicher Daten von einem betroffenen S3-Objekt abzurufen, müssen alle folgenden Ressourcen und Daten in derselben Region gespeichert sein: das betroffene Objekt, der entsprechende Befund und das entsprechende Ergebnis der Erkennung sensibler Daten.

Aufgaben

- Übersicht
- Schritt 1: Überprüfen Sie Ihre Berechtigungen
- Schritt 2: Konfigurieren Sie ein AWS KMS key
- Schritt 3: Wählen Sie einen S3-Bucket

Übersicht

Amazon Macie erstellt automatisch ein Erkennungsergebnis vertraulicher Daten für jedes Amazon S3 S3-Objekt, das analysiert wird oder zu analysieren versucht, wenn Sie einen Discovery-Job für sensible Daten ausführen oder wenn es eine automatische Erkennung sensibler Daten für Ihr Konto oder Ihre Organisation durchführt. Dies umfasst:

- Objekte, in denen Macie sensible Daten erkennt und die daher auch zu Ergebnissen sensibler Daten führen.
- Objekte, in denen Macie keine sensiblen Daten erkennt und daher keine Ergebnisse zu sensiblen Daten liefert.
- Objekte, die Macie aufgrund von Fehlern oder Problemen nicht analysieren kann, z. B. aufgrund von Berechtigungseinstellungen oder der Verwendung eines nicht unterstützten Datei- oder Speicherformats.

Wenn Macie sensible Daten in einem S3-Objekt entdeckt, umfasst das Ergebnis der Erkennung sensibler Daten auch Daten aus der entsprechenden Entdeckung vertraulicher Daten. Es bietet auch zusätzliche Informationen, z. B. den Standort von bis zu 1.000 Vorkommen jedes Typs vertraulicher Daten, die Macie in dem Objekt gefunden hat. Beispielsweise:

- Die Spalten- und Zeilennummer für eine Zelle oder ein Feld in einer Microsoft Excel-Arbeitsmappe, CSV-Datei oder TSV-Datei

- Der Pfad zu einem Feld oder Array in einer JSON- oder JSON Lines-Datei
- Die Zeilennummer für eine Zeile in einer nicht-binären Textdatei, bei der es sich nicht um eine CSV-, JSON-, JSON-Zeilen- oder TSV-Datei handelt, z. B. eine HTML-, TXT- oder XML-Datei
- Die Seitennummer für eine Seite in einer PDF-Datei (Adobe Portable Document Format)
- Der Datensatzindex und der Pfad zu einem Feld in einem Datensatz in einem Apache Avro-Objektcontainer oder einer Apache Parquet-Datei

Handelt es sich bei dem betroffenen S3-Objekt um eine Archivdatei, z. B. eine .tar- oder .zip-Datei, liefert das Ergebnis der Erkennung sensibler Daten auch detaillierte Standortdaten für das Vorkommen sensibler Daten in einzelnen Dateien, die Macie aus dem Archiv extrahiert. Macie nimmt diese Informationen nicht in die Ergebnisse sensibler Daten für Archivdateien auf. Um Standortdaten zu melden, verwenden die Ergebnisse der Erkennung sensibler Daten ein standardisiertes JSON-Schema.

Ein Ermittlungsergebnis für sensible Daten beinhaltet nicht die sensiblen Daten, die Macie gefunden hat. Stattdessen erhalten Sie einen Analysedatensatz, der für Audits oder Ermittlungen hilfreich sein kann.

Macie speichert Ihre Ergebnisse der Entdeckung sensibler Daten 90 Tage lang. Sie können nicht direkt über die Amazon Macie Macie-Konsole oder mit der Amazon Macie Macie-API darauf zugreifen. Folgen Sie stattdessen den Schritten in diesem Thema, um Macie so zu konfigurieren, AWS KMS key dass Ihre Ergebnisse mit einem von Ihnen angegebenen verschlüsselt werden, und speichern Sie die Ergebnisse in einem S3-Bucket, den Sie ebenfalls angeben. Macie schreibt dann die Ergebnisse in JSON-Lines-Dateien (.jsonl), fügt die Dateien dem Bucket als GNU-Zip-Dateien (.gz) hinzu und verschlüsselt die Daten mithilfe der SSE-KMS-Verschlüsselung. Seit dem 8. November 2023 signiert Macie die resultierenden S3-Objekte auch mit einem Hash-basierten Message Authentication Code (HMAC). AWS KMS key

Nachdem Sie Macie so konfiguriert haben, dass Ihre Erkennungsergebnisse vertraulicher Daten in einem S3-Bucket gespeichert werden, kann der Bucket als definitives, langfristiges Repository für die Ergebnisse dienen. Anschließend können Sie optional auf die Ergebnisse in diesem Repository zugreifen und diese abfragen.

> **Tip**
>
> Ein detailliertes, anschauliches Beispiel dafür, wie Sie die Ergebnisse der Erkennung sensibler Daten abfragen und verwenden können, um potenzielle Datensicherheitsrisiken

zu analysieren und zu melden, finden Sie im QuickSight Blogbeitrag So fragen Sie die Ergebnisse der Erkennung sensibler Daten von Macie mit Amazon Athena und Amazon ab und visualisieren Sie sie im Security Blog.AWS
Beispiele für Amazon Athena Athena-Abfragen, mit denen Sie Erkennungsergebnisse sensibler Daten analysieren können, finden Sie im Amazon Macie Results Analytics-Repository unter. GitHub Dieses Repository enthält auch Anweisungen zur Konfiguration von Athena zum Abrufen und Entschlüsseln Ihrer Ergebnisse sowie Skripten zum Erstellen von Tabellen für die Ergebnisse.

Schritt 1: Überprüfen Sie Ihre Berechtigungen

Bevor Sie ein Repository für Ihre Discovery-Ergebnisse vertraulicher Daten konfigurieren, stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen zum Verschlüsseln und Speichern der Ergebnisse verfügen. Um Ihre Berechtigungen zu überprüfen, verwenden Sie AWS Identity and Access Management (IAM), um die IAM-Richtlinien zu überprüfen, die mit Ihrer IAM-Identität verknüpft sind. Vergleichen Sie dann die Informationen in diesen Richtlinien mit der folgenden Liste von Aktionen, die Sie ausführen dürfen müssen, um das Repository zu konfigurieren.

Amazon Macie

Stellen Sie für Macie sicher, dass Sie die folgende Aktion ausführen dürfen:

`macie2:PutClassificationExportConfiguration`

Mit dieser Aktion können Sie die Repository-Einstellungen in Macie hinzufügen oder ändern.

Amazon S3

Stellen Sie für Amazon S3 sicher, dass Sie die folgenden Aktionen ausführen dürfen:

- `s3:CreateBucket`
- `s3:GetBucketLocation`
- `s3:ListAllMyBuckets`
- `s3:PutBucketAcl`
- `s3:PutBucketPolicy`
- `s3:PutBucketPublicAccessBlock`
- `s3:PutObject`

Mit diesen Aktionen können Sie auf einen S3-Bucket zugreifen und ihn konfigurieren, der als Repository dienen kann.

AWS KMS

Um die Amazon Macie Macie-Konsole zum Hinzufügen oder Ändern der Repository-Einstellungen zu verwenden, stellen Sie außerdem sicher, dass Sie die folgenden AWS KMS Aktionen ausführen dürfen:

- `kms:DescribeKey`
- `kms:ListAliases`

Diese Aktionen ermöglichen es Ihnen, Informationen über das AWS KMS keys für Ihr Konto abzurufen und anzuzeigen. Sie können dann einen dieser Schlüssel auswählen, um Ihre Erkennungsergebnisse vertraulicher Daten zu verschlüsseln.

Wenn Sie vorhaben, einen neuen AWS KMS key zu erstellen, um die Daten zu verschlüsseln, müssen Sie auch die folgenden Aktionen ausführen dürfen: `kms:CreateKeykms:GetKeyPolicy`, und. `kms:PutKeyPolicy`

Wenn Sie die erforderlichen Aktionen nicht ausführen dürfen, bitten Sie Ihren AWS Administrator um Unterstützung, bevor Sie mit dem nächsten Schritt fortfahren.

Schritt 2: Konfigurieren Sie ein AWS KMS key

Nachdem Sie Ihre Berechtigungen überprüft haben, legen AWS KMS key Sie fest, welche Methode Macie zur Verschlüsselung Ihrer Erkennungsergebnisse vertraulicher Daten verwenden soll. Bei dem Schlüssel muss es sich um einen vom Kunden verwalteten KMS-Schlüssel mit symmetrischer Verschlüsselung handeln, der in demselben AWS-Region S3-Bucket aktiviert ist, in dem Sie die Ergebnisse speichern möchten.

Der Schlüssel kann ein vorhandener Schlüssel AWS KMS key aus Ihrem eigenen Konto oder ein vorhandener AWS KMS key Schlüssel sein, den ein anderes Konto besitzt. Wenn Sie einen neuen KMS-Schlüssel verwenden möchten, erstellen Sie den Schlüssel, bevor Sie fortfahren. Wenn Sie einen vorhandenen Schlüssel verwenden möchten, der einem anderen Konto gehört, rufen Sie den Amazon-Ressourcennamen (ARN) des Schlüssels ab. Sie müssen diesen ARN eingeben, wenn Sie die Repository-Einstellungen in Macie konfigurieren. Informationen zum Erstellen und Überprüfen der Einstellungen für KMS-Schlüssel finden Sie unter Schlüssel verwalten im AWS Key Management Service Entwicklerhandbuch.

> **Note**
>
> Der Schlüssel kann sich AWS KMS key in einem externen Schlüsselspeicher befinden. Der Schlüssel ist dann jedoch möglicherweise langsamer und weniger zuverlässig als ein Schlüssel, der vollständig intern verwaltet wird AWS KMS. Sie können dieses Risiko verringern, indem Sie Ihre Ermittlungsergebnisse für sensible Daten in einem S3-Bucket speichern, der so konfiguriert ist, dass der Schlüssel als S3-Bucket-Key verwendet wird. Dadurch wird die Anzahl der AWS KMS Anfragen reduziert, die gestellt werden müssen, um Ihre Erkennungsergebnisse vertraulicher Daten zu verschlüsseln.
> Informationen zur Verwendung von KMS-Schlüsseln in externen Schlüsselspeichern finden Sie im AWS Key Management Service Entwicklerhandbuch unter Externe Schlüsselspeicher. Informationen zur Verwendung von S3-Bucket Keys finden Sie unter Reduzierung der Kosten für SSE-KMS mit Amazon S3 S3-Bucket Keys im Amazon Simple Storage Service-Benutzerhandbuch.

Nachdem Sie festgelegt haben, welchen KMS-Schlüssel Macie verwenden soll, erteilen Sie Macie die Erlaubnis, den Schlüssel zu verwenden. Andernfalls kann Macie Ihre Ergebnisse nicht verschlüsseln oder im Repository speichern. Um Macie die Erlaubnis zur Verwendung des Schlüssels zu erteilen, aktualisieren Sie die Schlüsselrichtlinie für den Schlüssel. Ausführliche Informationen zu wichtigen Richtlinien und zur Verwaltung des Zugriffs auf KMS-Schlüssel finden Sie unter Wichtige Richtlinien AWS KMS im AWS Key Management Service Entwicklerhandbuch.

So aktualisieren Sie die Schlüsselrichtlinie

1. Öffnen Sie die AWS KMS Konsole unter https://console.aws.amazon.com/kms.
2. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie den Schlüssel aus, den Macie zur Verschlüsselung Ihrer Erkennungsergebnisse vertraulicher Daten verwenden soll.
4. Wählen Sie auf der Registerkarte Schlüsselrichtlinie die Option Bearbeiten aus.
5. Kopieren Sie die folgende Anweisung in Ihre Zwischenablage und fügen Sie sie dann der Richtlinie hinzu:

```
{
    "Sid": "Allow Macie to use the key",
    "Effect": "Allow",
```

```
    "Principal": {
        "Service": "macie.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey",
        "kms:Encrypt"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
         },
         "ArnLike": {
             "aws:SourceArn": [
                 "arn:aws:macie2:Region:111122223333:export-configuration:*",
                 "arn:aws:macie2:Region:111122223333:classification-job/*"
             ]
         }
    }
}
```

Wenn Sie die Anweisung hinzufügen, stellen Sie sicher, dass die Syntax gültig ist. Richtlinien verwenden das JSON-Format. Das bedeutet, dass Sie vor oder nach der Anweisung auch ein Komma hinzufügen müssen, je nachdem, wo Sie die Anweisung zur Richtlinie hinzufügen. Wenn Sie die Anweisung als letzte Anweisung hinzufügen, fügen Sie hinter der schließenden geschweiften Klammer für die vorherige Anweisung ein Komma hinzu. Wenn Sie sie als erste Anweisung oder zwischen zwei vorhandenen Anweisungen hinzufügen, fügen Sie hinter der schließenden geschweiften Klammer für die Anweisung ein Komma ein.

6. Aktualisieren Sie die Anweisung mit den richtigen Werten für Ihre Umgebung:

   - Ersetzen Sie in den `Condition` Feldern die Platzhalterwerte, wobei:
     - *111122223333* ist die Konto-ID für Sie. AWS-Konto
     - *Region* ist die Region, AWS-Region in der Sie Macie verwenden und Sie möchten, dass Macie den Schlüssel verwendet.

       Wenn Sie Macie in mehreren Regionen verwenden und Macie erlauben möchten, den Schlüssel in weiteren Regionen zu verwenden, fügen Sie `aws:SourceArn` Bedingungen für jede weitere Region hinzu. Beispielsweise:

       ```
       "aws:SourceArn": [
       ```

```
    "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
    "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
    "arn:aws:macie2:us-west-2:111122223333:export-configuration:*",
    "arn:aws:macie2:us-west-2:111122223333:classification-job/*"
]
```

Alternativ können Sie Macie erlauben, den Schlüssel in allen Regionen zu verwenden. Ersetzen Sie dazu den Platzhalterwert durch das Platzhalterzeichen (*). Beispielsweise:

```
"aws:SourceArn": [
    "arn:aws:macie2:*:111122223333:export-configuration:*",
    "arn:aws:macie2:*:111122223333:classification-job/*"
]
```

- Wenn Sie Macie in einer Opt-in-Region verwenden, fügen Sie dem Wert für das Feld den entsprechenden Regionalcode hinzu. `Service` Wenn Sie Macie beispielsweise in der Region Naher Osten (Bahrain) verwenden, die den Regionalcode me-south-1 hat, ersetzen Sie ihn durch. `macie.amazonaws.com` `macie.me-south-1.amazonaws.com` Eine Liste der Regionen, in denen Macie derzeit verfügbar ist, sowie den jeweiligen Regionalcode finden Sie unter Amazon Macie Macie-Endpunkte und Kontingente in der. Allgemeine AWS-Referenz

Beachten Sie, dass die `Condition` Felder zwei globale IAM-Bedingungsschlüssel verwenden:

- aws: SourceAccount — Diese Bedingung ermöglicht es Macie, die angegebenen Aktionen nur für Ihr Konto auszuführen. Insbesondere bestimmt sie, welches Konto die angegebenen Aktionen für die in der `aws:SourceArn` Bedingung angegebenen Ressourcen und Aktionen ausführen kann.

  Damit Macie die angegebenen Aktionen für weitere Konten ausführen kann, fügen Sie dieser Bedingung die Konto-ID für jedes weitere Konto hinzu. Beispielsweise:

  ```
  "aws:SourceAccount": [111122223333,444455556666]
  ```

- aws: SourceArn — Diese Bedingung verhindert, dass andere AWS-Services die angegebenen Aktionen ausführen. Es verhindert auch, dass Macie den Schlüssel verwendet, während sie andere Aktionen für Ihr Konto ausführt. Mit anderen Worten, es ermöglicht Macie, S3-Objekte nur dann mit dem Schlüssel zu verschlüsseln, wenn es sich bei den Objekten um Erkennungsergebnisse vertraulicher Daten handelt, und nur, wenn es sich bei diesen

Ergebnissen um automatisierte Erkennungsaufträge oder Aufträge zur Erkennung sensibler Daten handelt, die vom angegebenen Konto in der angegebenen Region erstellt wurden.

Damit Macie die angegebenen Aktionen für weitere Konten ausführen kann, fügen Sie dieser Bedingung ARNs für jedes weitere Konto hinzu. Beispielsweise:

```
"aws:SourceArn": [
    "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
    "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
    "arn:aws:macie2:us-east-1:444455556666:export-configuration:*",
    "arn:aws:macie2:us-east-1:444455556666:classification-job/*"
]
```

Die in den `aws:SourceArn` Bedingungen `aws:SourceAccount` und angegebenen Konten müssen übereinstimmen.

Diese Bedingungen verhindern, dass Macie bei Transaktionen mit AWS KMS Macie als verwirrter Stellvertreter eingesetzt wird. Wir empfehlen es zwar nicht, aber Sie können diese Bedingungen aus der Erklärung entfernen.

7. Wenn Sie mit dem Hinzufügen und Aktualisieren der Erklärung fertig sind, wählen Sie Änderungen speichern.

Schritt 3: Wählen Sie einen S3-Bucket

Nachdem Sie Ihre Berechtigungen überprüft und konfiguriert haben AWS KMS key, können Sie angeben, welchen S3-Bucket Sie als Repository für Ihre Discovery-Ergebnisse für sensible Daten verwenden möchten. Sie haben hierfür zwei Möglichkeiten:

- Verwenden Sie einen neuen S3-Bucket, den Macie erstellt — Wenn Sie diese Option wählen, erstellt Macie automatisch einen neuen S3-Bucket im aktuellen Bucket AWS-Region für Ihre Discovery-Ergebnisse. Macie wendet auch eine Bucket-Richtlinie auf den Bucket an. Die Richtlinie ermöglicht es Macie, Objekte zum Bucket hinzuzufügen. Außerdem müssen die Objekte mit dem, was Sie angeben AWS KMS key , unter Verwendung der SSE-KMS-Verschlüsselung verschlüsselt werden. Um die Richtlinie zu überprüfen, wählen Sie in der Amazon Macie Macie-Konsole die Option Richtlinie anzeigen, nachdem Sie einen Namen für den Bucket und den zu verwendenden KMS-Schlüssel angegeben haben.

- Verwenden Sie einen vorhandenen S3-Bucket, den Sie erstellen — Wenn Sie Ihre Discovery-Ergebnisse lieber in einem bestimmten von Ihnen erstellten S3-Bucket speichern möchten, erstellen Sie den Bucket, bevor Sie fortfahren. Überprüfen Sie anschließend die Einstellungen des Buckets und aktualisieren Sie die Richtlinie des Buckets, um sicherzustellen, dass Macie dem Bucket Objekte hinzufügen kann. In diesem Thema wird erklärt, welche Einstellungen überprüft werden müssen und wie die Richtlinie aktualisiert wird. Es enthält auch Beispiele für die Anweisungen, die der Richtlinie hinzugefügt werden können.

Die folgenden Abschnitte enthalten Anweisungen für jede Option. Wählen Sie den Abschnitt für die gewünschte Option aus.

Verwenden Sie einen neuen S3-Bucket, den Macie erstellt

Wenn Sie lieber einen neuen S3-Bucket verwenden möchten, den Macie für Sie erstellt, besteht der letzte Schritt darin, die Repository-Einstellungen in Macie zu konfigurieren.

Um die Repository-Einstellungen in Macie zu konfigurieren

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Discovery-Ergebnisse aus.
3. Wählen Sie unter Repository für Erkennungsergebnisse vertraulicher Daten die Option Bucket erstellen aus.
4. Geben Sie im Feld Bucket erstellen einen Namen für den Bucket ein.

   Der Name muss über alle S3-Buckets eindeutig sein. Darüber hinaus darf der Name nur aus Kleinbuchstaben, Zahlen, Punkten (.) und Bindestrichen (-) bestehen. Weitere Benennungsanforderungen finden Sie unter Regeln zur Benennung von Buckets im Amazon Simple Storage Service-Benutzerhandbuch.
5. Erweitern Sie den Abschnitt Advanced (Erweitert).
6. (Optional) Um ein Präfix anzugeben, das im Pfad zu einem Speicherort im Bucket verwendet werden soll, geben Sie das Präfix in das Feld Datenermittlungsergebnispräfix ein.

   Wenn Sie einen Wert eingeben, aktualisiert Macie das Beispiel unter dem Feld, sodass der Pfad zum Bucket-Speicherort angezeigt wird, an dem Ihre Discovery-Ergebnisse gespeichert werden.
7. Wählen Sie für Gesamten öffentlichen Zugriff blockieren die Option Ja aus, um alle Einstellungen zum Sperren des öffentlichen Zugriffs für den Bucket zu aktivieren.

Informationen zu diesen Einstellungen finden Sie unter Sperren des öffentlichen Zugriffs auf Ihren Amazon S3 S3-Speicher im Amazon Simple Storage Service-Benutzerhandbuch.

8. Geben Sie unter Verschlüsselungseinstellungen AWS KMS key die Einstellungen an, die Macie zur Verschlüsselung der Ergebnisse verwenden soll:

   - Um einen Schlüssel aus Ihrem eigenen Konto zu verwenden, wählen Sie Wählen Sie einen Schlüssel aus Ihrem Konto aus. Wählen Sie dann in der AWS KMS keyListe den Schlüssel aus, den Sie verwenden möchten. In der Liste werden vom Kunden verwaltete KMS-Schlüssel mit symmetrischer Verschlüsselung für Ihr Konto angezeigt.
   - Um einen Schlüssel zu verwenden, der einem anderen Konto gehört, wählen Sie Geben Sie den ARN eines Schlüssels von einem anderen Konto ein. Geben Sie dann in das Feld AWS KMS key ARN den Amazon-Ressourcennamen (ARN) des zu verwendenden Schlüssels ein, z. B. **`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**

9. Wenn Sie mit der Eingabe der Einstellungen fertig sind, wählen Sie Speichern.

   Macie testet die Einstellungen, um sicherzustellen, dass sie korrekt sind. Wenn Einstellungen falsch sind, zeigt Macie eine Fehlermeldung an, um Ihnen bei der Behebung des Problems zu helfen.

Nachdem Sie die Repository-Einstellungen gespeichert haben, fügt Macie dem Repository vorhandene Ermittlungsergebnisse der letzten 90 Tage hinzu. Macie beginnt auch, dem Repository neue Ermittlungsergebnisse hinzuzufügen.

Verwenden Sie einen vorhandenen S3-Bucket, den Sie erstellen

Wenn Sie es vorziehen, Ihre Discovery-Ergebnisse vertraulicher Daten in einem bestimmten S3-Bucket zu speichern, den Sie erstellen, erstellen und konfigurieren Sie den Bucket, bevor Sie die Repository-Einstellungen in Macie konfigurieren. Beachten Sie beim Erstellen des Buckets die folgenden Anforderungen:

- Wenn Sie die Objektsperre für den Bucket aktivieren, müssen Sie die standardmäßige Aufbewahrungseinstellung für diese Funktion deaktivieren. Andernfalls kann Macie Ihre Discovery-Ergebnisse nicht zum Bucket hinzufügen. Informationen zu dieser Einstellung finden Sie unter Verwenden von S3 Object Lock im Amazon Simple Storage Service-Benutzerhandbuch.
- Um Ihre Ermittlungsergebnisse für eine Region zu speichern, für die standardmäßig aktiviert ist AWS-Konten, z. B. die Region USA Ost (Nord-Virginia), muss sich der Bucket in einer Region

befinden, die standardmäßig aktiviert ist. Die Ergebnisse können nicht in einem Bucket in einer Opt-in-Region gespeichert werden (Region, die standardmäßig deaktiviert ist).

- Um Ihre Discovery-Ergebnisse für eine Opt-in-Region wie die Region Naher Osten (Bahrain) zu speichern, muss sich der Bucket in derselben Region oder in einer Region befinden, die standardmäßig aktiviert ist. Die Ergebnisse können nicht in einem Bucket in einer anderen Opt-in-Region gespeichert werden.

Informationen darüber, ob eine Region standardmäßig aktiviert ist, finden Sie im AWS Identity and Access Management Benutzerhandbuch unter Regionen und Endpunkte.

Nachdem Sie den Bucket erstellt haben, aktualisieren Sie die Richtlinie des Buckets, sodass Macie Informationen über den Bucket abrufen und Objekte zum Bucket hinzufügen kann. Anschließend können Sie die Repository-Einstellungen in Macie konfigurieren.

Um die Bucket-Richtlinie für den Bucket zu aktualisieren

1. Öffnen Sie die Amazon-S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie den Bucket aus, in dem Sie Ihre Discovery-Ergebnisse speichern möchten.
3. Wählen Sie die Registerkarte Berechtigungen.
4. Wählen Sie im Abschnitt Bucket-Richtlinie die Option Bearbeiten aus.
5. Kopieren Sie die folgende Beispielrichtlinie in Ihre Zwischenablage:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Macie to use the GetBucketLocation operation",
            "Effect": "Allow",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:GetBucketLocation",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": [
```

```
                        "arn:aws:macie2:Region:111122223333:export-
configuration:*",
                        "arn:aws:macie2:Region:111122223333:classification-job/*"
                    ]
                }
            }
        },
        {
            "Sid": "Allow Macie to add objects to the bucket",
            "Effect": "Allow",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myBucketName/[optional prefix/]*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:macie2:Region:111122223333:export-
configuration:*",
                        "arn:aws:macie2:Region:111122223333:classification-job/*"
                    ]
                }
            }
        },
        {
            "Sid": "Deny unencrypted object uploads. This is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myBucketName/[optional prefix/]*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption": "aws:kms"
                }
            }
        },
        {
            "Sid": "Deny incorrect encryption headers. This is optional",
```

```
            "Effect": "Deny",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myBucketName/[optional prefix/]*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption-aws-kms-key-id":
 "arn:aws:kms:Region:111122223333:key/KMSKeyId"
                }
            }
        },
        {
            "Sid": "Deny non-HTTPS access",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::myBucketName/*",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

6. Fügen Sie die Beispielrichtlinie in den Bucket-Policy-Editor auf der Amazon S3 S3-Konsole ein.
7. Aktualisieren Sie die Beispielrichtlinie mit den richtigen Werten für Ihre Umgebung:

   - In der optionalen Anweisung, die falsche Verschlüsselungsheader ablehnt:
     - Ersetzen Sie es *myBucketName*durch den Namen des Buckets.
     - Ersetzen Sie in der `StringNotEquals` Bedingung *arn:aws:kms:region:111122223333:key/KMS KeyId* durch den Amazon-Ressourcennamen (ARN) der, der für die Verschlüsselung Ihrer Ermittlungsergebnisse verwendet werden soll. AWS KMS key
   - Ersetzen Sie in allen anderen Anweisungen die Platzhalterwerte, wobei:
     - *myBucketName*ist der Name des Buckets.
     - *111122223333* ist die Konto-ID für Sie. AWS-Konto

- *Region* ist die Region, AWS-Region in der Sie Macie verwenden und möchten, dass Macie Discovery-Ergebnisse zum Bucket hinzufügt.

  Wenn Sie Macie in mehreren Regionen verwenden und Macie erlauben möchten, Ergebnisse für weitere Regionen zum Bucket hinzuzufügen, fügen Sie `aws:SourceArn` Bedingungen für jede weitere Region hinzu. Beispielsweise:

  ```
  "aws:SourceArn": [
      "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
      "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
      "arn:aws:macie2:us-west-2:111122223333:export-configuration:*",
      "arn:aws:macie2:us-west-2:111122223333:classification-job/*"
  ]
  ```

  Alternativ können Sie Macie erlauben, dem Bucket Ergebnisse für alle Regionen hinzuzufügen, in denen Sie Macie verwenden. Ersetzen Sie dazu den Platzhalterwert durch das Platzhalterzeichen (*). Beispielsweise:

  ```
  "aws:SourceArn": [
      "arn:aws:macie2:*:111122223333:export-configuration:*",
      "arn:aws:macie2:*:111122223333:classification-job/*"
  ]
  ```

- Wenn Sie Macie in einer Opt-in-Region verwenden, fügen Sie dem Wert für das `Service` Feld in jeder Anweisung, die den Macie-Service Principal angibt, den entsprechenden Regionalcode hinzu. Wenn Sie beispielsweise Macie in der Region Naher Osten (Bahrain) verwenden, die den Regionalcode me-south-1 hat, ersetzen Sie ihn `macie.amazonaws.com` in jeder zutreffenden Anweisung durch. `macie.me-south-1.amazonaws.com` Eine Liste der Regionen, in denen Macie derzeit verfügbar ist, sowie den jeweiligen Regionalcode finden Sie unter Amazon Macie Macie-Endpunkte und Kontingente in der. Allgemeine AWS-Referenz

Beachten Sie, dass die Beispielrichtlinie Anweisungen enthält, die es Macie ermöglichen, festzustellen, in welcher Region sich der Bucket befindet (`GetBucketLocation`), und Objekte zum Bucket hinzuzufügen (). `PutObject` Diese Anweisungen definieren Bedingungen, die zwei globale IAM-Bedingungsschlüssel verwenden:

- aws: SourceAccount — Diese Bedingung ermöglicht es Macie, nur für Ihr Konto Ergebnisse der Erkennung sensibler Daten zum Bucket hinzuzufügen. Dadurch wird Macie daran

gehindert, Erkennungsergebnisse für andere Konten zum Bucket hinzuzufügen. Genauer gesagt gibt die Bedingung an, welches Konto den Bucket für die in der `aws:SourceArn` Bedingung angegebenen Ressourcen und Aktionen verwenden kann.

Um Ergebnisse für zusätzliche Konten im Bucket zu speichern, fügen Sie dieser Bedingung die Konto-ID für jedes weitere Konto hinzu. Beispielsweise:

```
"aws:SourceAccount": [111122223333,444455556666]
```

- aws: SourceArn — Diese Bedingung schränkt den Zugriff auf den Bucket basierend auf der Quelle der Objekte ein, die dem Bucket hinzugefügt werden. Sie verhindert, dass andere AWS-Services Objekte zum Bucket hinzufügen. Es verhindert auch, dass Macie Objekte zum Bucket hinzufügt und gleichzeitig andere Aktionen für Ihr Konto ausführt. Insbesondere erlaubt die Bedingung Macie, Objekte nur dann zum Bucket hinzuzufügen, wenn es sich bei den Objekten um Erkennungsergebnisse vertraulicher Daten handelt, und nur, wenn es sich bei diesen Ergebnissen um automatisierte Erkennungsaufträge oder Aufträge zur Erkennung sensibler Daten handelt, die vom angegebenen Konto in der angegebenen Region erstellt wurden.

  Damit Macie die angegebenen Aktionen für weitere Konten ausführen kann, fügen Sie dieser Bedingung ARNs für jedes weitere Konto hinzu. Beispielsweise:

```
"aws:SourceArn": [
    "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
    "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
    "arn:aws:macie2:us-east-1:444455556666:export-configuration:*",
    "arn:aws:macie2:us-east-1:444455556666:classification-job/*"
]
```

Die in den `aws:SourceArn` Bedingungen `aws:SourceAccount` und angegebenen Konten müssen übereinstimmen.

Beide Bedingungen verhindern, dass Macie bei Transaktionen mit Amazon S3 als verwirrter Stellvertreter eingesetzt wird. Wir raten zwar davon ab, aber Sie können diese Bedingungen aus der Bucket-Richtlinie entfernen.

8. Wenn Sie mit der Aktualisierung der Bucket-Richtlinie fertig sind, wählen Sie Änderungen speichern aus.

Sie können jetzt die Repository-Einstellungen in Macie konfigurieren.

Um die Repository-Einstellungen in Macie zu konfigurieren

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Discovery-Ergebnisse aus.
3. Wählen Sie unter Repository für Erkennungsergebnisse vertraulicher Daten die Option Existing Bucket aus.
4. Wählen Sie unter Wählen Sie einen Bucket aus den Bucket aus, in dem Sie Ihre Discovery-Ergebnisse speichern möchten.
5. (Optional) Um ein Präfix anzugeben, das im Pfad zu einem Speicherort im Bucket verwendet werden soll, erweitern Sie den Abschnitt Erweitert. Geben Sie dann unter Präfix für das Ergebnis der Datenermittlung das zu verwendende Präfix ein.

   Wenn Sie einen Wert eingeben, aktualisiert Macie das Beispiel unter dem Feld und zeigt den Pfad zum Bucket-Speicherort an, an dem Ihre Discovery-Ergebnisse gespeichert werden.
6. Geben Sie unter Verschlüsselungseinstellungen die Einstellungen an AWS KMS key , die Macie zum Verschlüsseln der Ergebnisse verwenden soll:

   - Um einen Schlüssel aus Ihrem eigenen Konto zu verwenden, wählen Sie Wählen Sie einen Schlüssel aus Ihrem Konto aus. Wählen Sie dann in der AWS KMS keyListe den Schlüssel aus, den Sie verwenden möchten. In der Liste werden vom Kunden verwaltete KMS-Schlüssel mit symmetrischer Verschlüsselung für Ihr Konto angezeigt.
   - Um einen Schlüssel zu verwenden, der einem anderen Konto gehört, wählen Sie Geben Sie den ARN eines Schlüssels von einem anderen Konto ein. Geben Sie dann in das Feld AWS KMS key ARN den ARN des zu verwendenden Schlüssels ein, z. B. **`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**
7. Wenn Sie mit der Eingabe der Einstellungen fertig sind, wählen Sie Speichern.

   Macie testet die Einstellungen, um sicherzustellen, dass sie korrekt sind. Wenn Einstellungen falsch sind, zeigt Macie eine Fehlermeldung an, um Ihnen bei der Behebung des Problems zu helfen.

Nachdem Sie die Repository-Einstellungen gespeichert haben, fügt Macie dem Repository vorhandene Ermittlungsergebnisse der letzten 90 Tage hinzu. Macie beginnt auch, dem Repository neue Ermittlungsergebnisse hinzuzufügen.

> **Note**
>
> Wenn Sie anschließend die Präfixeinstellung für das Datenermittlungsergebnis ändern, aktualisieren Sie auch die Bucket-Richtlinie in Amazon S3. Richtlinienanweisungen, die den vorherigen Pfad angeben, müssen den neuen Pfad angeben. Andernfalls darf Macie Ihre Discovery-Ergebnisse nicht zum Bucket hinzufügen.

> **Tip**
>
> Um die Kosten für serverseitige Verschlüsselung zu reduzieren, konfigurieren Sie den S3-Bucket auch so, AWS KMS key dass er einen S3-Bucket-Key verwendet, und geben Sie den an, den Sie für die Verschlüsselung Ihrer Erkennungsergebnisse sensibler Daten konfiguriert haben. Durch die Verwendung eines S3-Bucket-Keys wird die Anzahl der Aufrufe reduziert AWS KMS, wodurch die AWS KMS Anforderungskosten gesenkt werden können. Wenn sich der KMS-Schlüssel in einem externen Schlüsselspeicher befindet, kann die Verwendung eines S3-Bucket-Keys auch die Leistungseinbußen bei der Verwendung des Schlüssels minimieren. Weitere Informationen finden Sie unter Senkung der Kosten für SSE-KMS mit Amazon S3 S3-Bucket Keys im Amazon Simple Storage Service-Benutzerhandbuch.

Von Amazon Macie unterstützte Speicherklassen und -formate

Um Ihnen zu helfen, sensible Daten in Ihrem Amazon Simple Storage Service (Amazon S3) -Datenbestand zu finden, unterstützt Amazon Macie die meisten Amazon S3-Speicherklassen und eine Vielzahl von Datei- und Speicherformaten. Diese Unterstützung gilt für die Verwendung verwalteter Datenkennungen und die Verwendung von benutzerdefinierten Datenkennungen zur Analyse von S3-Objekten.

Damit Macie ein S3-Objekt analysieren kann, muss das Objekt in einem Amazon S3 S3-Allzweck-Bucket unter Verwendung einer unterstützten Speicherklasse gespeichert werden. Das Objekt muss außerdem ein unterstütztes Datei- oder Speicherformat verwenden. In den Themen in diesem Abschnitt sind die Speicherklassen sowie die Datei- und Speicherformate aufgeführt, die Macie derzeit unterstützt.

> **Tip**
>
> Obwohl Macie für Amazon S3 optimiert ist, können Sie damit sensible Daten in Ressourcen entdecken, die Sie derzeit woanders speichern. Sie können dies tun, indem Sie die Daten vorübergehend oder dauerhaft nach Amazon S3 verschieben. Exportieren Sie beispielsweise Amazon Relational Database Service- oder Amazon Aurora Aurora-Snapshots im Apache Parquet-Format nach Amazon S3. Oder exportieren Sie eine Amazon DynamoDB-Tabelle nach Amazon S3. Anschließend können Sie einen Discovery-Job für sensible Daten erstellen, um die Daten in Amazon S3 zu analysieren.

Themen

- Unterstützte Amazon S3 S3-Speicherklassen
- Unterstützte Datei- und Speicherformate

Unterstützte Amazon S3 S3-Speicherklassen

Für die Erkennung sensibler Daten unterstützt Amazon Macie die folgenden Amazon S3 S3-Speicherklassen:

- Reduzierte Redundanz (RRS)
- S3 Glacier Instant Retrieval
- S3 Intelligent-Tiering
- S3 One Zone-Seltener Zugriff (S3 One Zone-IA)
- S3 Standard
- S3 Standard-Seltener Zugriff (S3 Standard-IA)

Macie analysiert keine S3-Objekte, die andere Amazon S3 S3-Speicherklassen wie S3 Glacier Deep Archive oder S3 Express One Zone verwenden. Darüber hinaus analysiert Macie keine Objekte, die in Amazon S3 S3-Verzeichnis-Buckets gespeichert sind.

Wenn Sie einen Discovery-Job für sensible Daten konfigurieren, um S3-Objekte zu analysieren, die keine unterstützte Amazon S3 S3-Speicherklasse verwenden, überspringt Macie diese Objekte, wenn der Job ausgeführt wird. Macie versucht nicht, Daten in den Objekten abzurufen oder zu analysieren — die Objekte werden als nicht klassifizierbare Objekte behandelt. Ein nicht klassifizierbares

Objekt ist ein Objekt, das keine unterstützte Speicherklasse oder ein unterstütztes Datei- oder Speicherformat verwendet. Macie analysiert nur die Objekte, die eine unterstützte Speicherklasse und ein unterstütztes Datei- oder Speicherformat verwenden.

Wenn Sie Macie für die automatische Erkennung sensibler Daten konfigurieren, kommen nicht klassifizierbare Objekte ebenfalls nicht für die Auswahl und Analyse in Frage. Macie wählt nur die Objekte aus, die eine unterstützte Amazon S3 S3-Speicherklasse und ein unterstütztes Datei- oder Speicherformat verwenden.

Um S3-Buckets zu identifizieren, die nicht klassifizierbare Objekte enthalten, können Sie Ihr S3-Bucket-Inventar filtern. Für jeden Bucket in Ihrem Inventar gibt es Felder, die die Anzahl und die Gesamtspeichergröße der nicht klassifizierbaren Objekte im Bucket angeben.

Ausführliche Informationen zu den von Amazon S3 bereitgestellten Speicherklassen finden Sie unter Verwenden von Amazon S3 S3-Speicherklassen im Amazon Simple Storage Service-Benutzerhandbuch.

Unterstützte Datei- und Speicherformate

Wenn Amazon Macie ein S3-Objekt analysiert, ruft Macie die neueste Version des Objekts von Amazon S3 ab und führt dann eine gründliche Inspektion des Objektinhalts durch. Bei dieser Prüfung wird das Datei- oder Speicherformat der Daten berücksichtigt. Macie kann Daten in vielen verschiedenen Formaten analysieren, einschließlich häufig verwendeter Komprimierungs- und Archivformate.

Wenn Macie Daten in einer komprimierten Datei oder Archivdatei analysiert, überprüft Macie sowohl die gesamte Datei als auch den Inhalt der Datei. Um den Inhalt der Datei zu überprüfen, dekomprimiert Macie die Datei und überprüft dann jede extrahierte Datei, die ein unterstütztes Format verwendet. Macie kann dies für bis zu 1.000.000 Dateien und bis zu einer Verschachtelungstiefe von 10 Ebenen tun. Informationen zu zusätzlichen Kontingenten, die für die Erkennung vertraulicher Daten gelten, finden Sie unter. Amazon Macie Macie-Kontingente

In der folgenden Tabelle sind die Typen von Datei- und Speicherformaten aufgeführt und beschrieben, die Macie analysieren kann, um sensible Daten zu erkennen. Für jeden unterstützten Typ sind in der Tabelle auch die entsprechenden Dateinamenerweiterungen aufgeführt.

Datei- oder Speichertyp	Beschreibung	Dateinamenerweiterungen
Big Data	Apache Avro-Objektcontainer und Apache Parquet-Dateien	.avro, .parquet
Komprimierung oder Archivieren	GNU-Zip-komprimierte Archive, TAR-Archive und ZIP-komprimierte Archive	.gz, .gzip, .tar, .zip
Dokument	Dateien im Adobe Portable Document Format, Microsoft Excel-Arbeitsmappen und Microsoft Word-Dokumente	.doc, .docx, .pdf, .xls, .xlsx
E-Mail-Nachricht	E-Mail-Dateien, deren Inhalt den in einem IETF-RFC für E-Mail-Nachrichten festgelegten Anforderungen entspricht, z. B. RFC 2822	.eml
Text	Nicht-binäre Textdateien wie Dateien mit kommagetrennten Werten (CSV), Hypertext Markup Language (HTML) -Dateien, JavaScript Object Notation (JSON) -Dateien, JSON Lines-Dateien, Klartext-Dokumente, Dateien mit tabulatorgetrennten Werten (TSV) und Extensible Markup Language (XML) -Dateien	.csv, .htm, .html, .json, .jsonl, .tsv, .txt, . und andere (abhängig vom Typ der nicht-binären Textdatei)

Macie analysiert keine Daten in Bildern oder Audio-, Video- und anderen Arten von Multimedia-Inhalten.

Wenn Sie einen Discovery-Job für sensible Daten so konfigurieren, dass S3-Objekte analysiert werden, die kein unterstütztes Datei- oder Speicherformat verwenden, überspringt Macie diese

Objekte, wenn der Job ausgeführt wird. Macie versucht nicht, Daten in den Objekten abzurufen oder zu analysieren — die Objekte werden als nicht klassifizierbare Objekte behandelt. Ein nicht klassifizierbares Objekt ist ein Objekt, das keine unterstützte Amazon S3 S3-Speicherklasse oder ein unterstütztes Datei- oder Speicherformat verwendet. Macie analysiert nur die Objekte, die eine unterstützte Speicherklasse und ein unterstütztes Datei- oder Speicherformat verwenden.

Wenn Sie Macie für die automatische Erkennung sensibler Daten konfigurieren, kommen nicht klassifizierbare Objekte ebenfalls nicht für die Auswahl und Analyse in Frage. Macie wählt nur die Objekte aus, die eine unterstützte Amazon S3 S3-Speicherklasse und ein unterstütztes Datei- oder Speicherformat verwenden.

Um S3-Buckets zu identifizieren, die nicht klassifizierbare Objekte enthalten, können Sie Ihr S3-Bucket-Inventar filtern. Für jeden Bucket in Ihrem Inventar gibt es Felder, die die Anzahl und die Gesamtspeichergröße der nicht klassifizierbaren Objekte im Bucket angeben.

Analyse Amazon Macie von

Amazon Macie generiert Ergebnisse, wenn es potenzielle Richtlinienverstöße oder Probleme mit der Sicherheit oder dem Datenschutz Ihrer Amazon Simple Storage Service (Amazon S3) -Buckets feststellt oder vertrauliche Daten in S3-Objekten erkennt. Ein Ergebnis ist ein detaillierter Bericht über ein potenzielles Problem oder bei vertraulichen Daten, die Jedes Ergebnis enthält einen Schweregrad, Informationen über die betroffene Ressource und zusätzliche Details, z. B. wann und wie Macie das Problem oder die Daten gefunden hat. Macie speichert Ihre Richtlinie und die Ergebnisse vertraulicher Daten 90 Tage lang.

Sie können Ergebnisse wie folgt überprüfen, analysieren und verwalten.

Amazon Macie Macie-Konsole

Auf den Ergebnisseiten der Amazon Macie Macie-Konsole werden Ihre Ergebnisse aufgeführt und detaillierte Informationen zu den einzelnen Ergebnissen bereitgestellt. Diese Seiten bieten auch Optionen zum Gruppieren, Filtern und Sortieren von Ergebnissen sowie zum Erstellen und Verwalten von Unterdrückungsregeln. Mithilfe von Unterdrückungsregeln können Sie Ihre Analyse der Ergebnisse optimieren.

Amazon Macie

Mit der Amazon Macie Macie-API können Sie Ergebnisdaten abfragen und abrufen, indem Sie ein AWS Befehlszeilentool oder ein AWS SDK verwenden oder HTTPS-Anfragen direkt an Macie senden. Um die Daten abzufragen, senden Sie eine Anfrage an die Amazon Macie Macie-API und verwenden unterstützte Parameter, um anzugeben, welche Ergebnisse Sie abrufen möchten. Nachdem Sie Ihre Anfrage eingereicht haben, gibt Macie die Ergebnisse in einer JSON-Antwort zurück. Anschließend können Sie die Ergebnisse zur eingehenderen Analyse, Langzeitspeicherung oder Berichterstattung an einen anderen Dienst oder eine andere Anwendung weitergeben. Weitere Informationen finden Sie in der Amazon

Amazon EventBridge

Um die Integration mit anderen Diensten und Systemen wie Überwachungs- oder Eventmanagementsystemen weiter zu unterstützen, veröffentlicht Macie die Ergebnisse EventBridge als Ereignisse bei Amazon. EventBridge, ehemals Amazon CloudWatch Events, ist ein serverloser Event-Bus-Service, der einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, Software as a Service (SaaS) -Anwendungen und AWS-Services wie Es kann diese Daten zur zusätzlichen, automatisierten Verarbeitung an Ziele wie AWS Lambda

Funktionen, Amazon Simple Notification Service-Themen und Amazon Kinesis Kinesis-Streams weiterleiten. Die Verwendung von trägt EventBridge auch dazu bei, eine längerfristige Aufbewahrung der Ergebnisdaten sicherzustellen. Weitere Informationen EventBridge finden Sie im EventBridgeAmazon-Benutzerhandbuch.

Macie veröffentlicht automatisch Ereignisse, um neue Erkenntnisse EventBridge zu erhalten. Außerdem werden Ereignisse automatisch veröffentlicht, wenn bestehende politische Erkenntnisse später erneut auftreten. Da die Ergebnisdaten als EventBridge Ereignisse strukturiert sind, können Sie die Ergebnisse mithilfe anderer Dienste und Tools einfacher überwachen, analysieren und entsprechend handeln. Sie könnten beispielsweise bestimmte Arten neuer Erkenntnisse automatisch EventBridge an eine AWS Lambda Funktion senden, die wiederum die Daten verarbeitet und an Ihr SIEM-System (Security Incident and Event Management) sendet. Wenn Sie AWS-Benutzerbenachrichtigungen in Macie integrieren, können Sie die Ereignisse auch verwenden, um automatisch über die von Ihnen angegebenen Lieferkanäle über Ergebnisse informiert zu werden. Weitere Informationen zur Verwendung von EventBridge Ereignissen zur Überwachung und Verarbeitung von Ergebnissen finden Sie unterIntegration von Amazon Macie mit Amazon EventBridge.

AWS Security Hub

Für eine zusätzliche, umfassendere Analyse der Sicherheitslage Ihres Unternehmens können Sie die Ergebnisse auch unter veröffentlichenAWS Security Hub. Security Hub ist ein Dienst, der Sicherheitsdaten von AWS Partner Network Sicherheitslösungen sammelt AWS-Services und unterstützt, um Ihnen einen umfassenden Überblick über Ihren Sicherheitsstatus in Ihrer gesamten AWS Umgebung zu bieten. Security Hub hilft Ihnen außerdem dabei, Ihre Umgebung anhand von Sicherheitsstandards und bewährten Methoden der Sicherheitsbranche zu überprüfen. Weitere Informationen über Security Hub finden Sie im AWS Security Hub-Benutzerhandbuch. Weitere Informationen zur Verwendung von Security Hub zur Überwachung und Verarbeitung von Ergebnissen finden Sie unterAmazon MacieIntegration mit AWS Security Hub.

Zusätzlich zu den Ergebnissen erstellt Macie Ergebnisse zur Erkennung vertraulicher Daten für S3-Objekte, die es analysiert, um sensible Daten zu erkennen. Ein Erkennungsergebnis für vertrauliche Daten ist ein Datensatz, der Details zur Analyse eines Objekts protokolliert. Dazu gehören Objekte, in denen Die Ergebnisse der Erkennung sensibler Daten liefern Ihnen Analyseaufzeichnungen, die für Prüfungen oder Untersuchungen zu Datenschutz und Datenschutz hilfreich sein können. Sie können nicht direkt über die Amazon Macie-Konsole oder über die Amazon Macie Macie-API auf die Ergebnisse der Erkennung vertraulicher Daten zugreifen. Stattdessen konfigurieren Sie Sie können

dann optional auf die Ergebnisse in diesem Bucket zugreifen und diese abfragen. Informationen zum Speichern der Ergebnisse finden Sie unterSpeicherung und Beibehaltung der Erkennungsergebnisse von vertraulichen Daten.

Themen

- Arten von Amazon Macie-Ergebnissen
- Arbeiten mit Probenergebnissen in Amazon Macie
- Überprüfung der Ergebnisse auf der Amazon Macie Macie-Konsole
- Amazon Macie Macie-Ergebnisse finden
- Untersuchung sensibler Daten anhand der Ergebnisse von Amazon Macie
- Unterdrückung von Amazon Macie Macie-Ergebnissen
- Bewertung des Schweregrads der Amazon Macie Macie-Ergebnisse

Arten von Amazon Macie-Ergebnissen

Amazon Macie generiert zwei Kategorien von Erkenntnissen: Richtlinienergebnisse und Ergebnisse für sensible Daten. Eine Richtlinienerkenntnis ist ein detaillierter Bericht über einen potenziellen Richtlinienverstoß oder ein potenzielles Problem mit der Sicherheit oder dem Datenschutz eines Amazon Simple Storage Service (Amazon S3)-Buckets. Macie generiert Richtlinienergebnisse im Rahmen seiner laufenden Aktivitäten, um Ihre S3-Buckets auf Sicherheit und Zugriffskontrolle zu bewerten und zu überwachen. Eine Erkenntnis zu sensiblen Daten ist ein detaillierter Bericht über sensible Daten, die Macie in einem S3-Objekt erkannt hat. Macie generiert Ergebnisse zu sensiblen Daten im Rahmen der Aktivitäten, die es ausführt, wenn Sie Aufträge zur Erkennung vertraulicher Daten ausführen oder die es automatisch für Ihr Konto erkennt.

Innerhalb jeder Kategorie gibt es bestimmte Typen. Der Typ einer Erkenntnis gibt Aufschluss über die Art des Problems oder der sensiblen Daten, die Macie gefunden hat. Die Details einer Erkenntnis bieten eine Schweregradbewertung , Informationen über die betroffene Ressource und zusätzliche Informationen, z. B. wann und wie Macie das Problem oder die sensiblen Daten gefunden hat. Der Schweregrad und die Details der einzelnen Erkenntnisse variieren je nach Art und Art der Erkenntnisse.

Themen

- Arten von Richtlinienergebnissen
- Arten von Erkenntnissen zu sensiblen Daten

> **Tip**
>
> Um die verschiedenen Kategorien und Arten von Erkenntnissen zu erkunden und zu erfahren, die Macie generieren kann, erstellen Sie Beispielergebnisse. Beispielerkenntnisse verwenden Beispieldaten und Platzhalterwerte, um die Arten von Informationen zu demonstrieren, die jede Art von Erkenntnissen enthalten könnte.

Arten von Richtlinienergebnissen

Amazon Macie generiert ein Richtlinienergebnis, wenn die Richtlinien oder Einstellungen für einen S3-Bucket so geändert werden, dass die Sicherheit oder der Datenschutz des Buckets und der Objekte des Buckets reduziert werden. Informationen darüber, wie Macie diese Änderungen erkennt, finden Sie unter So überwacht Macie die Amazon S3 S3-Datensicherheit.

Macie generiert eine Richtlinienerkenntnis nur, wenn die Änderung auftritt, nachdem Sie Macie für Ihr aktiviert habenAWS-Konto. Wenn beispielsweise die Block Public Access-Einstellungen für einen S3-Bucket deaktiviert sind, nachdem Sie Macie aktiviert haben, generiert Macie eine Policy:IAMUser/S3BlockPublicAccessDisabled-Erkenntnis für den Bucket. Wenn jedoch die Block Public Access-Einstellungen für einen Bucket deaktiviert wurden, als Sie Macie aktiviert haben, und diese weiterhin deaktiviert sind, generiert Macie keine Policy:IAMUser/S3BlockPublicAccessDisabled-Erkenntnis für den Bucket.

Wenn Macie ein nachfolgendes Auftreten einer vorhandenen Richtlinienerkenntnis erkennt, aktualisiert Macie die vorhandene Erkenntnis, indem es Details zum nachfolgenden Auftreten hinzufügt und die Anzahl der Vorkommen erhöht. Macie speichert Richtlinienergebnisse 90 Tage lang.

Macie kann die folgenden Arten von Richtlinienergebnissen für einen S3-Bucket generieren.

Policy:IAMUser/S3BlockPublicAccessDisabled

Alle Einstellungen zum Blockieren des öffentlichen Zugriffs auf Bucket-Ebene wurden für den Bucket deaktiviert. Der Zugriff auf den Bucket wird durch die Block Public Access-Einstellungen für das Konto, Zugriffskontrolllisten (ACLs) und die Bucket-Richtlinie für den Bucket gesteuert.

Weitere Informationen zu den Einstellungen zum Blockieren des öffentlichen Zugriffs für S3-Buckets finden Sie unter Blockieren des öffentlichen Zugriffs auf Ihren Amazon S3-Speicher im Benutzerhandbuch für Amazon Simple Storage Service.

Policy:IAMUser/S3BucketEncryptionDisabled

Die Standardverschlüsselungseinstellungen für den Bucket wurden auf das standardmäßige Amazon S3-Verschlüsselungsverhalten zurückgesetzt, bei dem neue Objekte automatisch mit einem von Amazon S3 verwalteten Schlüssel verschlüsselt werden.

Ab dem 5. Januar 2023 wendet Amazon S3 automatisch serverseitige Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3) als Basisverschlüsselungsstufe für Objekte an, die Buckets hinzugefügt werden. Sie können optional die Standardverschlüsselungseinstellungen eines Buckets so konfigurieren, dass stattdessen die serverseitige Verschlüsselung mit einem -AWS KMSSchlüssel (SSE-KMS) oder die serverseitige Dual-Layer-Verschlüsselung mit einem -AWS KMSSchlüssel (DSSE-KMS) verwendet wird. Weitere Informationen zu den Standardverschlüsselungseinstellungen und -optionen für S3-Buckets finden Sie unter Festlegen des serverseitigen Standardverschlüsselungsverhaltens für S3-Buckets im Benutzerhandbuch für Amazon Simple Storage Service.

Wenn Macie diese Art von Erkenntnissen vor dem 5. Januar 2023 generiert hat, weist die Erkenntnis darauf hin, dass die Standardverschlüsselungseinstellungen für den betroffenen Bucket deaktiviert wurden. Dies bedeutete, dass die Einstellungen des Buckets kein standardmäßiges serverseitiges Verschlüsselungsverhalten für neue Objekte angeben. Die Möglichkeit, Standardverschlüsselungseinstellungen für einen Bucket zu deaktivieren, wird von Amazon S3 nicht mehr unterstützt.

Policy:IAMUser/S3BucketPublic

Eine ACL oder Bucket-Richtlinie für den Bucket wurde geändert, um anonymen Benutzern oder allen authentifizierten AWS Identity and Access Management (IAM)-Identitäten Zugriff zu gewähren.

Weitere Informationen zu ACLs und Bucket-Richtlinien für S3-Buckets finden Sie unter Identity and Access Management in Amazon S3 im Benutzerhandbuch für Amazon Simple Storage Service.

Policy:IAMUser/S3BucketReplicatedExternally

Die Replikation wurde aktiviert und so konfiguriert, AWS-Konto dass Objekte aus dem Bucket in einen Bucket für ein repliziert werden, das außerhalb (nicht Teil) Ihrer Organisation liegt. Eine Organisation besteht aus einer Reihe von Macie-Konten, die zentral als Gruppe verwandter Konten über AWS Organizations oder durch Macie-Einladung verwaltet werden.

Unter bestimmten Bedingungen generiert Macie diese Art von Erkenntnissen für einen Bucket, der nicht für die Replikation von Objekten in einen Bucket für einen externen konfiguriert istAWS-Konto. Dies kann der Fall sein, wenn der Ziel-Bucket AWS-Region in den letzten 24 Stunden in einer anderen erstellt wurde, nachdem Macie im Rahmen des täglichen Aktualisierungszyklus Bucket- und Objektmetadaten von Amazon S3 abgerufen hat. Um die Erkenntnis zu untersuchen, aktualisieren Sie zunächst Ihre Bestandsdaten. Überprüfen Sie dann die Details des Buckets. Die Details geben an, ob der Bucket so konfiguriert ist, dass Objekte in andere Buckets repliziert werden. Wenn der Bucket dafür konfiguriert ist, enthalten die Details die Konto-ID für jedes Konto, das einen Ziel-Bucket besitzt.

Weitere Informationen zu Replikationseinstellungen für S3-Buckets finden Sie unter Replizieren von Objekten im Amazon Simple Storage Service-Benutzerhandbuch.

Policy:IAMUser/S3BucketSharedExternally

Eine ACL- oder Bucket-Richtlinie für den Bucket wurde geändert, damit der Bucket mit einem geteilt werden kannAWS-Konto, der außerhalb (nicht Teil) Ihrer Organisation ist. Eine Organisation besteht aus einer Reihe von Macie-Konten, die zentral als Gruppe verwandter Konten über AWS Organizations oder durch Macie-Einladung verwaltet werden.

In bestimmten Fällen generiert Macie diese Art von Erkenntnis für einen Bucket, der nicht für ein externes AWS-Konto freigegeben ist. Dies kann passieren, wenn Macie die Beziehung zwischen dem -`Principal`Element in der Richtlinie des Buckets und bestimmten AWS globalen Bedingungskontextschlüsseln oder Amazon S3-Bedingungsschlüsseln im -`Condition`Element der Richtlinie nicht vollständig auswerten kann. Die entsprechenden Bedingungsschlüssel sind: `aws:PrincipalAccount`, `aws:PrincipalArn`, `aws:PrincipalOrgID`, `aws:PrincipalOrgPathsaws:PrincipalTag`, `aws:PrincipalType`, `aws:SourceAccount`, `aws:SourceArn`, , `aws:userid`, `s3:DataAccessPointAccount`, und `s3:DataAccessPointArn`. Wir empfehlen Ihnen, die Richtlinie des Buckets zu überprüfen, um festzustellen, ob dieser Zugriff beabsichtigt und sicher ist.

Weitere Informationen zu ACLs und Bucket-Richtlinien für S3-Buckets finden Sie unter Identity and Access Management in Amazon S3 im Benutzerhandbuch für Amazon Simple Storage Service.

Policy:IAMUser/S3BucketSharedWithCloudFront

Die Bucket-Richtlinie für den Bucket wurde geändert, damit der Bucket mit einer Amazon-CloudFront Ursprungszugriffsidentität (Origin Access Identity, OAI), einer CloudFront Ursprungszugriffssteuerung (Origin Access Control, OAC) oder sowohl einer CloudFront OAI als

auch einer CloudFront OAC geteilt werden kann. Eine CloudFront OAI oder OAC ermöglicht es Benutzern, über eine oder mehrere angegebene CloudFront Verteilungen auf die Objekte eines Buckets zuzugreifen.

Weitere Informationen zu CloudFront OAIs und OACs finden Sie unter Beschränken des Zugriffs auf einen Amazon S3-Ursprung im Amazon CloudFront-Entwicklerhandbuch.

> **Note**
>
> In bestimmten Fällen generiert Macie eine Policy:IAMUser /S3BucketSharedExternally-Erkenntnis anstelle einer Policy:IAMUser /S3BucketSharedWithCloudFront-Erkenntnis für einen Bucket. Diese Fälle sind:
>
> - Der Bucket wird zusätzlich zu einer CloudFront OAI oder OAC für einen freigegeben, der AWS-Konto außerhalb Ihrer Organisation liegt.
> - Die Richtlinie des Buckets gibt eine kanonische Benutzer-ID anstelle des Amazon-Ressourcennamens (ARN) einer CloudFront OAI an.
>
> Dies führt zu einem höheren Schweregrad für den Bucket.

Arten von Erkenntnissen zu sensiblen Daten

Macie generiert eine Erkenntnis zu sensiblen Daten, wenn es sensible Daten in einem S3-Objekt erkennt, das es analysiert, um sensible Daten zu erkennen. Dazu gehören Analysen, die Macie durchführt, wenn Sie einen Auftrag zur Erkennung sensibler Daten und eine automatisierte Erkennung sensibler Daten ausführen.

Wenn Sie beispielsweise einen Auftrag zur Erkennung vertraulicher Daten erstellen und ausführen und Macie Bankkontonummern in einem S3-Objekt erkennt, generiert Macie eine SensitiveData:S3Object/Financial-Erkenntnis für das Objekt. Wenn Macie Bankkontonummern in einem S3-Objekt erkennt, das es während eines automatisierten Erkennungszyklus für sensible Daten analysiert, generiert Macie ein SensitiveData:S3Object/Financial-Ergebnis für das Objekt.

Wenn Macie sensible Daten im selben S3-Objekt während einer nachfolgenden Auftragsausführung oder eines automatisierten Erkennungszyklus für sensible Daten erkennt, generiert Macie ein neues Ergebnis für sensible Daten für das Objekt. Im Gegensatz zu Richtlinienergebnissen werden alle

Erkenntnisse zu sensiblen Daten als neu (eindeutig) behandelt. Macie speichert Ergebnisse sensibler Daten 90 Tage lang.

Macie kann die folgenden Arten von Ergebnissen zu sensiblen Daten für ein S3-Objekt generieren.

SensitiveData:S3Object/Credentials

Das Objekt enthält sensible Anmeldeinformationen wie AWS geheime Zugriffsschlüssel oder private Schlüssel.

SensitiveData:S3Object/CustomIdentifier

Das Objekt enthält Text, der den Erkennungskriterien einer oder mehrerer benutzerdefinierter Datenkennungen entspricht. Das Objekt kann mehr als einen Typ sensibler Daten enthalten.

SensitiveData:S3Object/Financial

Das Objekt enthält sensible Finanzinformationen wie Bankkontonummern oder Kreditkartennummern.

SensitiveData:S3Object/Multiple

Das Objekt enthält mehr als eine Kategorie sensibler Daten – eine beliebige Kombination aus Anmeldeinformationen, Finanzinformationen, persönlichen Informationen oder Text, die den Erkennungskriterien einer oder mehrerer benutzerdefinierter Datenkennungen entspricht.

SensitiveData:S3Object/Personal

Das Objekt enthält sensible personenbezogene Daten – persönlich identifizierbare Informationen (PII) wie Reisepassnummern oder Führerscheinidentifikationsnummern, persönliche Gesundheitsdaten (PHI) wie Krankenversicherungs- oder medizinische Identifikationsnummern oder eine Kombination aus PII und PHI.

Informationen zu den Arten sensibler Daten, die Macie mithilfe integrierter Kriterien und Techniken erkennen kann, finden Sie unter Verwenden von verwalteten Datenbezeichnern. Informationen zu den Arten von S3-Objekten, die Macie analysieren kann, finden Sie unter Unterstützte Speicherklassen und -formate.

Arbeiten mit Probenergebnissen in Amazon Macie

Um die verschiedenen Arten von Ergebnissen, die Amazon Macie generieren kann, zu untersuchen und mehr über sie zu erfahren, können Sie Beispielergebnisse erstellen. Beispielergebnisse zeigen

anhand von Beispieldaten und Platzhalterwerten, welche Arten von Informationen die einzelnen Befunde enthalten können.

Das Beispielergebnis Policy:IAMuser/S3 BucketPublic enthält beispielsweise Details zu einem fiktiven Amazon Simple Storage Service (Amazon S3) -Bucket. Zu den Details des Ergebnisses gehören Beispieldaten über einen Akteur und eine Aktion, durch die die Zugriffskontrollliste (ACL) für den Bucket geändert und der Bucket öffentlich zugänglich gemacht wurde. In ähnlicher Weise enthält das SensitiveDataBeispielbefund:S3Object/Multiple Details zu einer fiktiven Microsoft Excel-Arbeitsmappe. Zu den Einzelheiten des Ergebnisses gehören Beispieldaten über die Typen und den Speicherort vertraulicher Daten in der Arbeitsmappe.

Sie können sich nicht nur mit den Informationen vertraut machen, die verschiedene Arten von Ergebnissen enthalten können, sondern auch die Integration mit anderen Anwendungen, Diensten und Systemen anhand von Beispielergebnissen testen. Abhängig von den Unterdrückungsregeln für Ihr Konto kann Macie Beispielergebnisse EventBridge als Ereignisse auf Amazon veröffentlichen. Mithilfe der Beispieldaten in den Stichprobenergebnissen können Sie automatisierte Lösungen für die Überwachung und Verarbeitung dieser Ereignisse entwickeln und testen. Abhängig von den Veröffentlichungseinstellungen für Ihr Konto kann Macie auch Beispielergebnisse veröffentlichen. AWS Security Hub Das bedeutet, dass Sie anhand von Beispielergebnissen auch Lösungen für die Überwachung und Verarbeitung von Macie-Ergebnissen in Security Hub entwickeln und testen können. Informationen zur Veröffentlichung von Ergebnissen in diesen Diensten finden Sie unterÜberwachung und Verarbeitung von Ergebnissen.

Themen

- Beispielergebnisse erstellen
- Überprüfung der Stichprobenergebnisse
- Unterdrücken von Stichprobenergebnissen

Beispielergebnisse erstellen

Sie können Beispielergebnisse mithilfe der Amazon Macie Macie-Konsole oder der Amazon Macie Macie-API erstellen. Wenn Sie die Konsole verwenden, generiert Macie automatisch einen Stichprobenbefund für jeden Befundtyp, den Macie unterstützt. Wenn Sie die API verwenden, können Sie für jeden Typ oder nur für bestimmte Typen, die Sie angeben, ein Beispiel erstellen.

Console

Gehen Sie wie folgt vor, um mithilfe der Amazon Macie Macie-Konsole Probenergebnisse zu erstellen.

Um Beispielergebnisse zu erstellen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie unter Sample findings (Beispielergebnisse) Generate sample findings (Beispielergebnisse generieren).

API

Verwenden Sie den CreateSampleFindingsBetrieb der Amazon Macie Macie-API, um Beispielergebnisse programmgesteuert zu erstellen. Wenn Sie Ihre Anfrage einreichen, können Sie optional den `findingTypes` Parameter verwenden, um nur bestimmte Arten von Probenergebnissen anzugeben, die erstellt werden sollen. Um automatisch Stichproben aller Art zu erstellen, nehmen Sie diesen Parameter nicht in Ihre Anfrage auf.

Führen Sie den create-sample-findingsBefehl aus, um Beispielergebnisse mithilfe von AWS Command Line Interface(AWS CLI) zu erstellen. Um automatisch Stichproben aller Arten von Ergebnissen zu erstellen, geben Sie den `finding-types` Parameter nicht an. Wenn Sie Stichproben nur für bestimmte Arten von Ergebnissen erstellen möchten, fügen Sie diesen Parameter hinzu und geben Sie an, welche Arten von Stichprobenergebnissen erstellt werden sollen. Beispiel:

```
C:\> aws macie2 create-sample-findings --finding-types "SensitiveData:S3Object/
Multiple" "Policy:IAMUser/S3BucketPublic"
```

Wobei: S3Object/Multiple eine Art von zu SensitiveDataerstellender Findungstyp für sensible Daten und Policy:IAMuser/S3 eine Art von zu erstellender Richtlinienermittlung ist. BucketPublic

Wenn der Befehl erfolgreich ausgeführt wird, gibt Macie eine leere Antwort zurück.

Überprüfung der Stichprobenergebnisse

Um Ihnen die Identifizierung der von Ihnen erstellten Stichprobenergebnisse zu erleichtern, setzt Macie den Wert für das Feld Stichprobe jedes Stichprobenergebnisses auf Wahr. Darüber hinaus ist der Name des betroffenen S3-Buckets für alle Stichprobenergebnisse derselbe: macie-sample-finding-bucket. Wenn Sie die Probenergebnisse mithilfe der Ergebnisseiten auf der Amazon Macie Macie-Konsole überprüfen, zeigt Macie für jedes Probenergebnis auch das Präfix [SAMPLE] im Feld Befundtyp an.

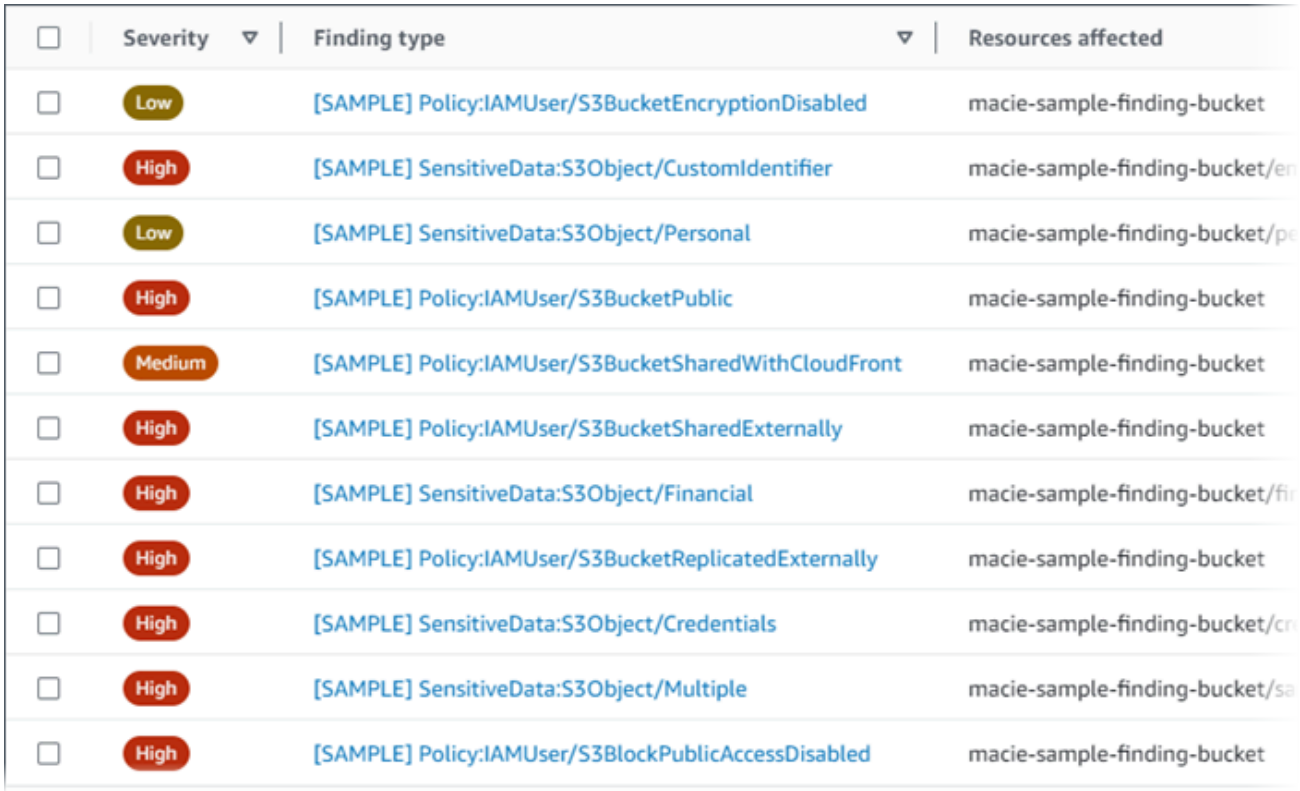
Console

Gehen Sie wie folgt vor, um die Probenergebnisse mithilfe der Amazon Macie Macie-Konsole zu überprüfen.

Um die Ergebnisse der Stichprobe zu überprüfen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich Findings aus.
3. Führen Sie auf der Seite mit den Ergebnissen einen der folgenden Schritte aus:

   - Suchen Sie in der Spalte Befundtyp nach Ergebnissen, deren Typ mit [SAMPLE] beginnt, wie in der folgenden Abbildung dargestellt.



Severity	Finding type	Resources affected
Low	[SAMPLE] Policy:IAMUser/S3BucketEncryptionDisabled	macie-sample-finding-bucket
High	[SAMPLE] SensitiveData:S3Object/CustomIdentifier	macie-sample-finding-bucket/
Low	[SAMPLE] SensitiveData:S3Object/Personal	macie-sample-finding-bucket/
High	[SAMPLE] Policy:IAMUser/S3BucketPublic	macie-sample-finding-bucket
Medium	[SAMPLE] Policy:IAMUser/S3BucketSharedWithCloudFront	macie-sample-finding-bucket
High	[SAMPLE] Policy:IAMUser/S3BucketSharedExternally	macie-sample-finding-bucket
High	[SAMPLE] SensitiveData:S3Object/Financial	macie-sample-finding-bucket/
High	[SAMPLE] Policy:IAMUser/S3BucketReplicatedExternally	macie-sample-finding-bucket
High	[SAMPLE] SensitiveData:S3Object/Credentials	macie-sample-finding-bucket/
High	[SAMPLE] SensitiveData:S3Object/Multiple	macie-sample-finding-bucket/
High	[SAMPLE] Policy:IAMUser/S3BlockPublicAccessDisabled	macie-sample-finding-bucket

- Mithilfe des Felds Filterkriterien über der Tabelle können Sie die Tabelle so filtern, dass nur Stichprobenergebnisse angezeigt werden. Platzieren Sie dazu den Cursor in dem Feld. Wählen Sie in der Liste der Felder, die angezeigt wird, die Option Beispiel aus. Wählen Sie dann True und anschließend Apply aus. Dadurch wird der Tabelle die folgende Filterbedingung hinzugefügt:

4. Um die Details eines bestimmten Stichprobenergebnisses zu überprüfen, wählen Sie das Ergebnis aus. Im Detailbereich werden Informationen zu dem Ergebnis angezeigt.

Sie können auch die Details eines oder mehrerer Beispielergebnisse herunterladen und als JSON-Datei speichern. Aktivieren Sie dazu das Kontrollkästchen für jedes Beispielergebnis, das Sie herunterladen und speichern möchten. Wählen Sie dann im Aktionsmenü oben auf der Ergebnisseite die Option Exportieren (JSON) aus. Wählen Sie im daraufhin angezeigten Fenster die Option Herunterladen aus. Eine ausführliche Beschreibung der JSON-Felder, die ein Ergebnis enthalten kann, finden Sie unter Ergebnisse in der Amazon Macie API-Referenz.

API

Um Stichprobenergebnisse programmgesteuert zu überprüfen, verwenden Sie zunächst die ListFindingsAmazon Macie Macie-API, um die eindeutige Kennung (`findingId`) für jedes von Ihnen erstellte Probenergebnis abzurufen. Verwenden Sie dann den GetFindingsVorgang, um die Details dieser Ergebnisse abzurufen.

Wenn Sie die ListFindings Anfrage einreichen, können Sie Filterkriterien angeben, um nur Stichprobenergebnisse in die Ergebnisse aufzunehmen. Fügen Sie dazu eine Filterbedingung hinzu, in der sich der Wert für das `sample` Feld befindet`true`. Wenn Sie den verwendenAWS CLI, führen Sie den Befehl list-findings aus und geben Sie mit dem `finding-criteria` Parameter die Filterbedingung an. Beispiel:

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"sample\":{\"eq\":
[\"true\"]}}}
```

Wenn Ihre Anfrage erfolgreich ist, gibt Macie ein Array zurück. `findingIds` Das Array listet die eindeutige Kennung für jedes Stichprobenergebnis für Ihr Konto in der aktuellen Version auf. AWS-Region

Um anschließend die Details der Stichprobenergebnisse abzurufen, geben Sie diese eindeutigen Kennungen in einer GetFindings Anfrage oderAWS CLI, falls Sie den Befehl get-findings ausführen, an.

Unterdrücken von Stichprobenergebnissen

Wie bei anderen Ergebnissen speichert Macie die Probenergebnisse 90 Tage lang. Nachdem Sie die Proben überprüft und mit ihnen experimentiert haben, können Sie sie optional archivieren, indem Sie eine Unterdrückungsregel erstellen. Wenn Sie dies tun, werden die Ergebnisse der Stichprobe standardmäßig nicht mehr auf der Konsole angezeigt und ihr Status ändert sich in archiviert.

Um Probenergebnisse mithilfe der Amazon Macie Macie-Konsole zu archivieren, konfigurieren Sie die Regel so, dass Ergebnisse archiviert werden, bei denen der Wert für das Probenfeld True ist. Um Probenergebnisse mithilfe der Amazon Macie Macie-API zu archivieren, konfigurieren Sie die Regel so, dass Ergebnisse dort archiviert werden, wo sich der Wert für das `sample` Feld befindet`true`.

Überprüfung der Ergebnisse auf der Amazon Macie Macie-Konsole

Amazon Macie überwacht Ihre AWS Umgebung und generiert Richtlinienergebnisse, wenn potenzielle Richtlinienverstöße oder Probleme mit der Sicherheit oder dem Datenschutz Ihrer Amazon Simple Storage Service (Amazon S3) -Buckets festgestellt werden. Macie generiert Ergebnisse zu sensiblen Daten, wenn es sensible Daten in S3-Objekten erkennt. Macie speichert Ihre Richtlinien und Ergebnisse zu sensiblen Daten 90 Tage lang.

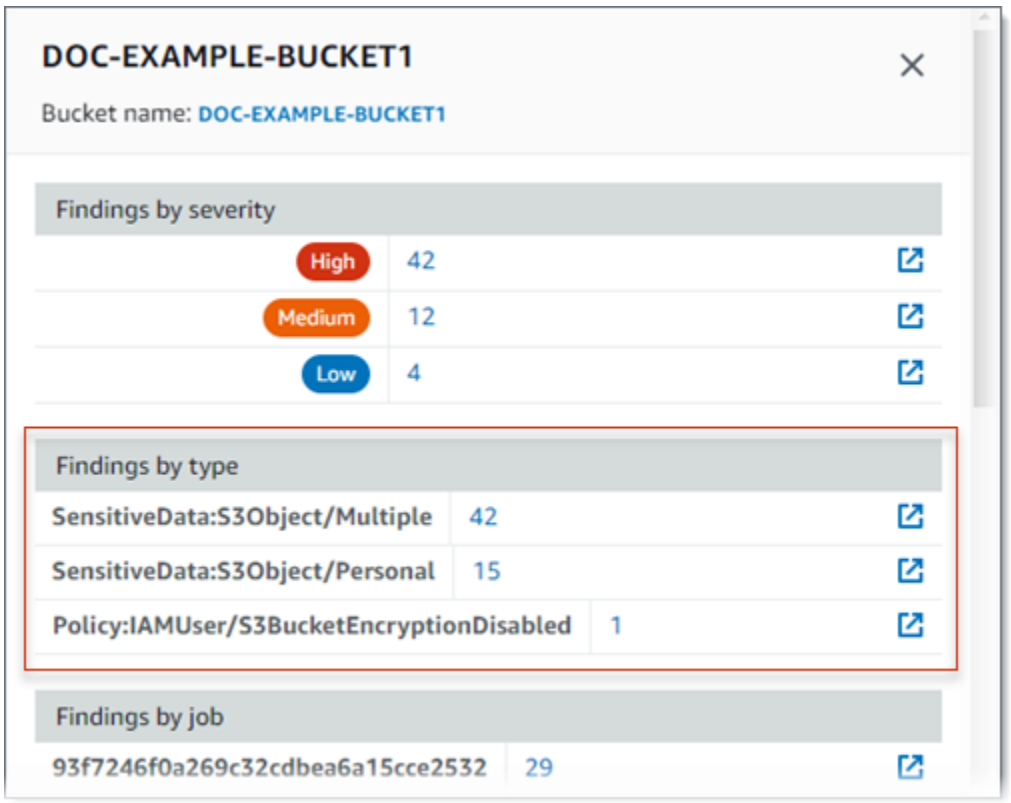
Jedes Ergebnis gibt einen Befundtyp und einen Schweregrad an. Zu den weiteren Informationen gehören Informationen über die betroffene Ressource und darüber, wann und wie Macie das Problem gefunden hat, oder über sensible Daten, die im Zusammenhang mit dem Befund gemeldet wurden. Der Schweregrad und die Einzelheiten der einzelnen Ergebnisse variieren je nach Art und Art des Befundes.

Mithilfe der Amazon Macie Macie-Konsole können Sie Ergebnisse überprüfen und analysieren und auf die Details einzelner Ergebnisse zugreifen. Sie können auch ein oder mehrere Ergebnisse in eine JSON-Datei exportieren. Um Ihnen bei der Optimierung Ihrer Analyse zu helfen, bietet die Konsole mehrere Optionen zum Erstellen benutzerdefinierter Ergebnisansichten.

Verwenden Sie vordefinierte Gruppierungen

Verwenden Sie spezielle Seiten, um Ergebnisse zu überprüfen, die nach Kriterien wie dem betroffenen S3-Bucket, dem Befundtyp oder dem Discovery-Job für sensible Daten gruppiert sind. Auf diesen Seiten können Sie aggregierte Statistiken für jede Gruppe überprüfen, z. B. die Anzahl der Ergebnisse nach Schweregrad. Sie können sich auch die Details einzelner Ergebnisse in einer Gruppe ansehen und Filter anwenden, um Ihre Analyse zu verfeinern.

Wenn Sie beispielsweise alle Ergebnisse nach S3-Bucket gruppieren und feststellen, dass in einem bestimmten Bucket eine Richtlinienverletzung vorliegt, können Sie schnell feststellen, ob es auch Ergebnisse mit sensiblen Daten für den Bucket gibt. Wählen Sie dazu im Navigationsbereich (unter Ergebnisse) die Option Nach Bucket und dann den Bucket aus. Im daraufhin angezeigten Detailbereich werden im Abschnitt Ergebnisse nach Typ die Arten von Ergebnissen aufgeführt, die für den Bucket gelten, wie in der folgenden Abbildung dargestellt.

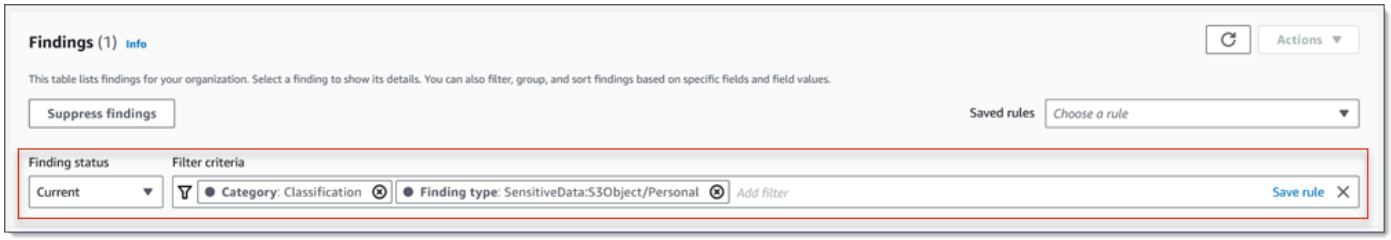


Um einen bestimmten Typ zu untersuchen, wählen Sie die Zahl für den Typ aus. Macie zeigt eine Tabelle mit allen Ergebnissen an, die dem ausgewählten Typ entsprechen und für den Bucket gelten. Um die Ergebnisse zu verfeinern, filtern Sie die Tabelle.

Filter erstellen und anwenden

Verwenden Sie bestimmte Ergebnisattribute, um bestimmte Ergebnisse in eine Ergebnistabelle ein- oder auszuschließen. Ein Ergebnisattribut ist ein Feld, in dem spezifische Daten für ein Ergebnis gespeichert werden, z. B. die Art der Ergebnisse, der Schweregrad oder der Name des betroffenen S3-Buckets. Wenn Sie eine Tabelle filtern, können Sie Ergebnisse mit bestimmten Merkmalen leichter identifizieren. Anschließend können Sie sich die Details dieser Ergebnisse genauer ansehen.

Um beispielsweise alle Ergebnisse Ihrer vertraulichen Daten zu überprüfen, fügen Sie Filterkriterien für das Feld Kategorie hinzu. Um die Ergebnisse zu verfeinern und nur einen bestimmten Typ der Suche nach vertraulichen Daten einzubeziehen, fügen Sie Filterkriterien für das Feld Suchtyp hinzu. Beispiel:



Um anschließend die Details eines bestimmten Ergebnisses zu überprüfen, wählen Sie das Ergebnis aus. Im Detailbereich werden Informationen zu dem Ergebnis angezeigt.

Sie können die Ergebnisse auch in aufsteigender oder absteigender Reihenfolge nach bestimmten Feldern sortieren. Klicken Sie dazu auf die Spaltenüberschrift für das Feld. Um die Sortierreihenfolge zu ändern, klicken Sie erneut auf die Spaltenüberschrift.

Um die Ergebnisse auf der Konsole zu überprüfen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich Findings aus. Auf der Seite mit den Ergebnissen werden Ergebnisse angezeigt, die Macie in den letzten 90 Tagen für Ihr Konto erstellt oder aktualisiert hat. AWS-Region Standardmäßig sind hier keine Ergebnisse enthalten, die durch eine Unterdrückungsregel unterdrückt wurden.
3. Um die Ergebnisse anhand einer vordefinierten logischen Gruppe zu überprüfen, wählen Sie im Navigationsbereich (unter Ergebnisse) die Option Nach Bucket, Nach Typ oder Nach Job aus. Wählen Sie dann ein Element in der Tabelle aus. Wählen Sie im Detailbereich den Link für das Feld aus, auf das Sie sich konzentrieren möchten.
4. Verwenden Sie die Filteroptionen über der Tabelle, um die Ergebnisse nach bestimmten Kriterien zu filtern:

   - Um Ergebnisse anzuzeigen, die durch eine Unterdrückungsregel unterdrückt wurden, verwenden Sie das Menü Suchstatus. Wählen Sie Alle, um sowohl unterdrückte als auch nicht unterdrückte Ergebnisse anzuzeigen, oder wählen Sie Archiviert, um nur unterdrückte Ergebnisse anzuzeigen. Um die unterdrückten Ergebnisse anschließend wieder auszublenden, wählen Sie „Aktuell“.
   - Verwenden Sie das Feld Filterkriterien, um nur die Ergebnisse anzuzeigen, die über ein bestimmtes Attribut verfügen. Platzieren Sie den Cursor in dem Feld und fügen Sie eine Filterbedingung für das Attribut hinzu. Um die Ergebnisse weiter zu verfeinern, fügen Sie Bedingungen für zusätzliche Attribute hinzu. Um

anschließend eine Bedingung zu entfernen, wählen Sie das Symbol „Bedingung entfernen“ (
für die zu entfernende Bedingung.

Weitere Informationen zum Filtern von Ergebnissen finden Sie unterFilter erstellen und auf Ergebnisse anwenden.

5. Um die Ergebnisse nach einem bestimmten Feld zu sortieren, klicken Sie auf die Spaltenüberschrift für das Feld. Um die Sortierreihenfolge zu ändern, klicken Sie erneut auf die Spaltenüberschrift.
6. Um die Details eines bestimmten Ergebnisses zu überprüfen, wählen Sie das Ergebnis aus. Im Detailbereich werden Informationen zu dem Ergebnis angezeigt.

> **Tip**
>
> Sie können den Bereich „Details“ verwenden, um bestimmte Felder genauer zu betrachten und genauer zu untersuchen. Um Ergebnisse anzuzeigen, die denselben Wert für ein Feld haben, wählen Sie
> in dem Feld die Option. Oder wählen
> Sie
> ob Ergebnisse angezeigt werden sollen, die andere Werte für das Feld haben.
> Wenn Sie nach vertraulichen Daten suchen, können Sie auch den Bereich „Details“ verwenden, um sensible Daten zu untersuchen, die Macie im betroffenen S3-Objekt gefunden hat:
>
> - Um nach Vorkommen eines bestimmten Typs vertraulicher Daten zu suchen, wählen Sie den numerischen Link im Feld für diesen Datentyp aus. Macie zeigt Informationen (im JSON-Format) darüber an, wo Macie die Daten gefunden hat. Weitere Informationen finden Sie unter Erkennen sensibler Daten.
> - Um Stichproben der sensiblen Daten abzurufen, die Macie gefunden hat, wählen Sie im Feld Beispiele anzeigen die Option Überprüfen aus. Weitere Informationen finden Sie unter Stichproben sensibler Daten werden abgerufen.
> - Um zum entsprechenden Ergebnis der Entdeckung sensibler Daten zu gelangen, klicken Sie auf den Link im Feld „Detaillierter Speicherort“. Macie öffnet die Amazon S3 S3-Konsole und zeigt die Datei oder den Ordner an, die das Erkennungsergebnis

enthält. Weitere Informationen finden Sie unter Speicherung und Beibehaltung der Erkennungsergebnisse von vertraulichen Daten.

Sie können auch die Details eines oder mehrerer Ergebnisse als JSON-Datei herunterladen und speichern. Aktivieren Sie dazu das Kontrollkästchen für jedes Ergebnis, das Sie herunterladen und speichern möchten. Wählen Sie dann im Aktionsmenü oben auf der Ergebnisseite die Option Exportieren (JSON) aus. Wählen Sie im daraufhin angezeigten Fenster die Option Herunterladen aus. Eine ausführliche Beschreibung der JSON-Felder, die ein Ergebnis enthalten kann, finden Sie unter Ergebnisse in der Amazon Macie API-Referenz.

Amazon Macie Macie-Ergebnisse finden

Um gezielte Analysen durchzuführen und Ergebnisse effizienter zu analysieren, können Sie die Ergebnisse von Amazon Macie filtern. Die Filter können benutzerdefinierte Ansichten und Abfragen für Ergebnisse enthalten. Die Ergebnisse können Ihnen helfen, Ergebnisse zu finden, die bestimmte Merkmale enthalten. Verwenden Sie die Amazon Macie Macie-Konsole, um Ergebnisse zu filtern, oder senden Sie Abfragen programmgesteuert über die Amazon Macie Macie-API.

Wenn Sie einen Filter erstellen, verwenden Sie bestimmte Ergebnisattribute, um Kriterien für das Ein- oder Ausschließen von Ergebnissen aus einer Ansicht oder aus Abfrageergebnissen zu definieren. Ein Finding-Attribut ist ein Feld, in dem bestimmte Daten für ein Ergebnis gespeichert werden, z. B. Schweregrad, Typ oder der Name des S3-Buckets, für den sich ein Ergebnis bezieht.

In Macie besteht ein Filter aus mindestens einer -Bedingung. Jede Bedingung, auch als Kriterium bezeichnet, besteht aus drei Teilen:

- Ein attributbasiertes Feld, z. B. Schweregrad oder Findungstyp.
- Ein Operator, z. B. ist gleich oder nicht gleich.
- Ein oder mehrere Werte. Der Typ und die Anzahl der Werte hängen vom ausgewählten Feld und Operator ab.

Wenn Sie einen Filter erstellen, den Sie erneut verwenden möchten, können Sie ihn als Filterregel speichern. Eine Filterregel ist eine Reihe von Filterkriterien, die Sie erstellen und speichern, um sie erneut anzuwenden, wenn Sie die Ergebnisse auf der Amazon Macie Macie-Konsole überprüfen.

Sie können einen Filter auch als Unterdrückungsregel speichern. Eine Unterdrückungsregel besteht aus einer Reihe von Filterkriterien, die Sie erstellen und speichern, um Ergebnisse, die den Kriterien

der Regel entsprechen, automatisch zu archivieren. Weitere Informationen zu Unterdrückungsregeln finden Sie unterUnterdrücken von Ergebnissen.

Themen

- Grundlagen der Filterung von Ergebnissen
- Filter erstellen und auf Ergebnisse anwenden
- Filterregeln für Ergebnisse erstellen und verwalten
- Felder zum Filtern von Ergebnissen

Grundlagen der Filterung von Ergebnissen

Beachten Sie beim Erstellen eines Filters die folgenden Funktionen und Richtlinien. Beachten Sie außerdem, dass gefilterte Ergebnisse auf die letzten 90 Tage und die aktuellen Tage beschränkt sindAWS-Region. Amazon Macie speichert Ihre Ergebnisse jeweils AWS-Region nur 90 Tage lang.

Themen

- Verwenden mehrerer Bedingungen in einem Filter
- Werte für Felder angeben
- Angeben mehrerer Werte für ein Feld
- Verwenden von Operatoren unter bestimmten Bedingungen

Verwenden mehrerer Bedingungen in einem Filter

Ein Filter kann eine oder mehrere Bedingungen enthalten. Jede Bedingung, auch als Kriterium bezeichnet, besteht aus drei Teilen:

- Ein auf Attributen basierendes Feld, z. B. Schweregrad oder Befundtyp. Eine Liste der Felder, die Sie verwenden können, finden Sie unter. Felder zum Filtern von Ergebnissen
- Ein Operator, z. B. ist gleich oder ungleich. Eine Liste der Operatoren, die Sie verwenden können, finden Sie unter. Verwenden von Operatoren unter bestimmten Bedingungen
- Ein oder mehrere Werte. Der Typ und die Anzahl der Werte hängen vom ausgewählten Feld und Operator ab.

Wenn ein Filter mehrere Bedingungen enthält, verwendet Macie die UND-Logik, um die Bedingungen zu verknüpfen und die Filterkriterien auszuwerten. Das bedeutet, dass ein Ergebnis nur dann den Filterkriterien entspricht, wenn es allen Bedingungen im Filter entspricht.

Wenn Sie beispielsweise eine Bedingung hinzufügen, die nur Ergebnisse mit hohem Schweregrad berücksichtigt, und eine weitere Bedingung hinzufügen, die nur Ergebnisse vertraulicher Daten einbezieht, gibt Macie alle Ergebnisse mit hohem Schweregrad und vertraulichen Daten zurück. Mit anderen Worten, Macie schließt alle politischen Ergebnisse sowie alle Ergebnisse sensibler Daten mit mittlerem und niedrigem Schweregrad aus.

Sie können ein Feld in einem Filter nur einmal verwenden. Sie können jedoch mehrere Werte für viele Felder angeben.

Wenn eine Bedingung beispielsweise das Feld Schweregrad verwendet, um nur Ergebnisse mit hohem Schweregrad aufzunehmen, können Sie das Feld Schweregrad nicht in einer anderen Bedingung verwenden, um Ergebnisse mit mittlerem oder niedrigem Schweregrad einzubeziehen. Geben Sie stattdessen mehrere Werte für die bestehende Bedingung an, oder verwenden Sie einen anderen Operator für die bestehende Bedingung. Um beispielsweise alle Ergebnisse mit mittlerem und hohem Schweregrad einzubeziehen, fügen Sie einen Schweregrad gleich Mittel, Hoch oder einen Schweregrad ungleich Niedrig hinzu.

Werte für Felder angeben

Wenn Sie einen Wert für ein Feld angeben, muss der Wert dem zugrunde liegenden Datentyp für das Feld entsprechen. Je nach Feld können Sie einen der folgenden Wertetypen angeben.

Textarray (Zeichenketten)

Gibt eine Liste von Textwerten (Zeichenfolge) für ein Feld an. Jede Zeichenfolge entspricht einem vordefinierten oder vorhandenen Wert für ein Feld, z. B. Hoch für das Feld Schweregrad, :S3Object/Financial für das Feld Finding type oder dem Namen eines S3-Buckets SensitiveDatafür das Feld S3-Bucket-Name.

Wenn Sie ein Array verwenden, beachten Sie Folgendes:

- Bei Werten wird zwischen Groß- und Kleinschreibung unterschieden.
- Sie können keine Teilwerte angeben oder Platzhalterzeichen in Werten verwenden. Sie müssen einen vollständigen, gültigen Wert für das Feld angeben.

Um beispielsweise Ergebnisse für einen S3-Bucket mit dem Namen my-S3-Bucket zu filtern, geben Sie ***`my-S3-bucket`*** als Wert für das Feld S3-Bucket-Name ein. Wenn Sie einen anderen

Wert eingeben, z. B. **`my-s3-bucket`** oder**`my-S3`**, gibt Macie keine Ergebnisse für den Bucket zurück.

Eine Liste der gültigen Werte für jedes Feld finden Sie unterFelder zum Filtern von Ergebnissen.

Sie können bis zu 50 Werte in einem Array angeben. Wie Sie die Werte angeben, hängt davon ab, ob Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden, wie unter beschrieben. Angeben mehrerer Werte für ein Feld

Boolesch

Gibt einen von zwei sich gegenseitig ausschließenden Werten für ein Feld an.

Wenn Sie die Amazon Macie Macie-Konsole verwenden, um diesen Wertetyp anzugeben, stellt die Konsole eine Liste mit Werten zur Auswahl bereit. Wenn Sie die Amazon Macie Macie-API verwenden, geben Sie `true` oder `false` für den Wert an.

Datum/Uhrzeit (und Zeitbereiche)

Gibt ein absolutes Datum und eine absolute Uhrzeit für ein Feld an. Wenn Sie diesen Wertetyp angeben, müssen Sie sowohl ein Datum als auch eine Uhrzeit angeben.

Auf der Amazon Macie Macie-Konsole entsprechen Datums- und Uhrzeitwerte Ihrer lokalen Zeitzone und verwenden die 24-Stunden-Notation. In allen anderen Kontexten sind diese Werte in der koordinierten Weltzeit (UTC) und im erweiterten ISO 8601-Format angegeben — zum Beispiel `2020-09-01T14:31:13Z` für 14:31:13 Uhr UTC am 1. September 2020.

Wenn ein Feld einen Datums-/Uhrzeitwert speichert, können Sie das Feld verwenden, um einen festen oder relativen Zeitraum zu definieren. Sie können beispielsweise nur die Ergebnisse einbeziehen, die zwischen zwei bestimmten Daten und Uhrzeiten erstellt wurden, oder nur die Ergebnisse, die vor oder nach einem bestimmten Datum und einer bestimmten Uhrzeit erstellt wurden. Wie Sie einen Zeitraum definieren, hängt davon ab, ob Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden:

- Verwenden Sie auf der Konsole eine Datumsauswahl oder geben Sie Text direkt in die Felder Von und Bis ein.
- Definieren Sie mit der API einen festen Zeitraum, indem Sie eine Bedingung hinzufügen, die das erste Datum und die erste Uhrzeit im Bereich angibt, und fügen Sie eine weitere Bedingung hinzu, die das letzte Datum und die letzte Uhrzeit im Bereich angibt. Wenn Sie dies tun, verwendet Macie die UND-Logik, um die Bedingungen zu verknüpfen. Um einen relativen Zeitraum zu definieren, fügen Sie eine Bedingung hinzu, die das erste oder letzte Datum und

die Uhrzeit im Bereich angibt. Geben Sie die Werte als Unix-Zeitstempel in Millisekunden an, z. B. `1604616572653` für 22:49:32 UTC am 5. November 2020.

Auf der Konsole sind Zeitbereiche inklusive. Bei der API können Zeitbereiche inklusiv oder exklusiv sein, je nachdem, welchen Betreiber Sie wählen.

Zahl (und numerische Bereiche)

Gibt eine lange Ganzzahl für ein Feld an.

Wenn ein Feld einen numerischen Wert speichert, können Sie das Feld verwenden, um einen festen oder relativen numerischen Bereich zu definieren. Sie können beispielsweise nur die Ergebnisse in ein S3-Objekt aufnehmen, die 50 bis 90 Fälle vertraulicher Daten melden. Wie Sie einen numerischen Bereich definieren, hängt davon ab, ob Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden:

- Verwenden Sie auf der Konsole die Felder Von und Bis, um die niedrigsten bzw. höchsten Zahlen im Bereich einzugeben.
- Definieren Sie mit der API einen festen numerischen Bereich, indem Sie eine Bedingung hinzufügen, die die niedrigste Zahl im Bereich angibt, und fügen Sie eine weitere Bedingung hinzu, die die höchste Zahl im Bereich angibt. Wenn Sie dies tun, verwendet Macie die UND-Logik, um die Bedingungen zu verknüpfen. Um einen relativen numerischen Bereich zu definieren, fügen Sie eine Bedingung hinzu, die die niedrigste oder höchste Zahl im Bereich angibt.

Auf der Konsole sind numerische Bereiche inklusiv. Mit der API können numerische Bereiche inklusiv oder exklusiv sein, je nachdem, welchen Operator Sie wählen.

Text (Zeichenfolge)

Gibt einen einzelnen Textwert (Zeichenfolge) für ein Feld an. Die Zeichenfolge korreliert mit einem vordefinierten oder vorhandenen Wert für ein Feld, z. B. High für das Schweregradfeld, dem Namen eines S3-Buckets für das S3-Bucket-Namensfeld oder der eindeutige Bezeichner für einen Discovery-Job vertraulicher Daten für das Job-ID-Feld.

Wenn Sie eine einzelne Textzeichenfolge angeben, beachten Sie Folgendes:

- Bei Werten wird zwischen Groß- und Kleinschreibung unterschieden.
- Sie können keine Teilwerte oder Platzhalterzeichen in Werten verwenden. Sie müssen einen vollständigen, gültigen Wert für das Feld angeben.

Um beispielsweise Ergebnisse für einen S3-Bucket mit dem Namen my-S3-Bucket zu filtern, geben Sie ***`my-S3-bucket`*** als Wert für das Feld S3-Bucket-Name ein. Wenn Sie einen anderen

Wert eingeben, z. B. **`my-s3-bucket`** oder**`my-S3`**, gibt Macie keine Ergebnisse für den Bucket zurück.

Eine Liste der gültigen Werte für jedes Feld finden Sie unterFelder zum Filtern von Ergebnissen.

Angeben mehrerer Werte für ein Feld

Bei bestimmten Feldern und Operatoren können Sie mehrere Werte für ein Feld angeben. Wenn Sie dies tun, verwendet Macie die OR-Logik, um die Werte zu verknüpfen und die Filterkriterien auszuwerten. Das bedeutet, dass ein Ergebnis den Kriterien entspricht, wenn es einen der Werte für das Feld enthält.

Wenn Sie beispielsweise eine Bedingung hinzufügen, um Ergebnisse einzubeziehen, bei denen der Wert für das Feld Finding-Typ:S3Object/Financial SensitiveData ,:S3Object/Personal entspricht, gibt SensitiveData Macie Ergebnisse vertraulicher Daten für S3-Objekte zurück, die nur Finanzinformationen enthalten, und S3-Objekte, die nur persönliche Informationen enthalten. Mit anderen Worten, Macie schließt alle politischen Ergebnisse aus. Macie schließt auch alle Ergebnisse sensibler Daten für Objekte aus, die andere Arten sensibler Daten oder mehrere Arten sensibler Daten enthalten.

Die Ausnahme bilden Bedingungen, die den eqExactMatchOperator verwenden. Für diesen Operator verwendet Macie die UND-Logik, um die Werte zu verknüpfen und die Filterkriterien auszuwerten. Das bedeutet, dass ein Ergebnis nur dann den Kriterien entspricht, wenn es alle Werte für das Feld und nur diese Werte für das Feld enthält. Weitere Informationen zu diesem Operator finden Sie unterVerwenden von Operatoren unter bestimmten Bedingungen.

Wie Sie mehrere Werte für ein Feld angeben, hängt davon ab, ob Sie die Amazon Macie Macie-API oder die Amazon Macie Macie-Konsole verwenden. Bei der API verwenden Sie ein Array, das die Werte auflistet.

Auf der Konsole wählen Sie die Werte normalerweise aus einer Liste aus. Bei einigen Feldern müssen Sie jedoch für jeden Wert eine eigene Bedingung hinzufügen. Gehen Sie beispielsweise wie folgt vor, um Ergebnisse für Daten einzubeziehen, die Macie anhand bestimmter benutzerdefinierter Datenkennungen erkannt hat:

1. Platzieren Sie den Cursor in dem Feld „Filterkriterien“ und wählen Sie dann das Feld „Name der benutzerdefinierten Daten-ID“ aus. Geben Sie den Namen einer benutzerdefinierten Daten-ID ein und wählen Sie dann Anwenden aus.

2. Wiederholen Sie den vorherigen Schritt für jeden weiteren benutzerdefinierten Datenbezeichner, den Sie für den Filter angeben möchten.

Eine Liste der Felder, für die Sie dies tun müssen, finden Sie unterFelder zum Filtern von Ergebnissen.

Verwenden von Operatoren unter bestimmten Bedingungen

Sie können die folgenden Typen von Operatoren unter individuellen Bedingungen verwenden.

Entspricht () eq

Entspricht (=) einem beliebigen Wert, der für das Feld angegeben wurde. Sie können den Gleichheitsoperator für die folgenden Wertetypen verwenden: Textarray (Zeichenketten), Boolean, Datum/Uhrzeit, Zahl und Text (Zeichenfolge).

Für viele Felder können Sie diesen Operator verwenden und bis zu 50 Werte für das Feld angeben. Wenn Sie dies tun, verwendet Macie die OR-Logik, um die Werte zu verknüpfen. Das bedeutet, dass ein Ergebnis den Kriterien entspricht, wenn es einen der für das Feld angegebenen Werte enthält.

Beispiele:

- Um Ergebnisse einzubeziehen, die das Vorkommen von Finanzinformationen, persönlichen Informationen oder sowohl finanziellen als auch persönlichen Informationen melden, fügen Sie eine Bedingung hinzu, die das Feld „Vertrauliche Daten“ und diesen Operator verwendet, und geben Sie Finanzinformationen und Persönliche Informationen als Werte für das Feld an.
- Um Ergebnisse einzubeziehen, die das Vorkommen von Kreditkartennummern, Postanschriften oder sowohl Kreditkartennummern als auch Postanschriften melden, fügen Sie eine Bedingung für das Feld Erkennungstyp vertraulicher Daten hinzu, verwenden Sie diesen Operator und geben Sie CREDIT_CARD_NUMBERund ADDRESSals Werte für das Feld an.

Wenn Sie die Amazon Macie Macie-API verwenden, um eine Bedingung zu definieren, die diesen Operator mit einem Datums-/Uhrzeitwert verwendet, geben Sie den Wert als Unix-Zeitstempel in Millisekunden an, `1604616572653` z. B. für 22:49:32 UTC am 5. November 2020.

eqExactMatchEntspricht exakter Übereinstimmung ()

Entspricht ausschließlich allen für das Feld angegebenen Werten. Sie können den Operator „Gleichheit und genaue Übereinstimmung“ mit einer ausgewählten Gruppe von Feldern verwenden.

Wenn Sie diesen Operator verwenden und mehrere Werte für ein Feld angeben, verwendet Macie die UND-Logik, um die Werte zu verknüpfen. Das bedeutet, dass ein Ergebnis nur dann den Kriterien entspricht, wenn es alle für das Feld angegebenen Werte und nur diese Werte für das Feld enthält. Sie können bis zu 50 Werte für das Feld angeben.

Beispiele:

- Um Ergebnisse einzubeziehen, die das Vorkommen von Kreditkartennummern und anderen Arten vertraulicher Daten melden, fügen Sie eine Bedingung für das Feld Erkennungstyp vertraulicher Daten hinzu, verwenden Sie diesen Operator und geben Sie ihn CREDIT_CARD_NUMBERals einzigen Wert für das Feld an.
- Um Ergebnisse einzubeziehen, bei denen sowohl Kreditkartennummern als auch Postanschriften (und keine anderen Arten vertraulicher Daten) gemeldet werden, fügen Sie eine Bedingung für das Feld Erkennungstyp vertraulicher Daten hinzu, verwenden Sie diesen Operator und geben Sie CREDIT_CARD_NUMBERund ADDRESSals Werte für das Feld an.

Da Macie die UND-Logik verwendet, um die Werte für ein Feld zu verknüpfen, können Sie diesen Operator nicht in Kombination mit anderen Operatoren für dasselbe Feld verwenden. Mit anderen Worten, wenn Sie den Gleichheitsoperator für exakte Übereinstimmung mit einem Feld in einer Bedingung verwenden, müssen Sie ihn in allen anderen Bedingungen verwenden, die dasselbe Feld verwenden.

Wie bei anderen Operatoren können Sie den Gleichheitsoperator für exakte Übereinstimmung in mehr als einer Bedingung in einem Filter verwenden. In diesem Fall verwendet Macie die UND-Logik, um die Bedingungen zu verknüpfen und den Filter auszuwerten. Das bedeutet, dass ein Ergebnis nur dann den Filterkriterien entspricht, wenn es alle Werte enthält, die durch alle Bedingungen im Filter angegeben wurden.

Gehen Sie beispielsweise wie folgt vor, um Ergebnisse einzubeziehen, die nach einer bestimmten Zeit erstellt wurden, das Vorkommen von Kreditkartennummern zu melden und keine anderen Arten vertraulicher Daten zu melden:

1. Fügen Sie eine Bedingung hinzu, die das Feld Erstellt am und den Operator Größer als verwendet und das Startdatum und die Startzeit für den Filter angibt.
2. Fügen Sie eine weitere Bedingung hinzu, die das Feld Typ für die Erkennung sensibler Daten verwendet, den Gleichheitsoperator „Exakte Übereinstimmung“ verwendet und CREDIT_CARD_NUMBERals einzigen Wert für das Feld angibt.

Sie können den Operator „Gleich“ und „Exakte Übereinstimmung“ für die folgenden Felder verwenden:

- ID () `customDataIdentifiers.detections.arn` Benutzerdefinierter Datenbezeichner
- Name der benutzerdefinierten Daten-ID (`customDataIdentifiers.detections.name`)
- S3-Bucket-Tag-Schlüssel (`resourcesAffected.s3Bucket.tags.key`)
- Wert des S3-Bucket-Tags (`resourcesAffected.s3Bucket.tags.value`)
- S3-Objekt-Tag-Schlüssel (`resourcesAffected.s3Object.tags.key`)
- Wert des S3-Objekt-Tags (`resourcesAffected.s3Object.tags.value`)
- Typ der Erkennung sensibler Daten (`sensitiveData.detections.type`)
- Kategorie sensibler Daten (`sensitiveData.category`)

In der obigen Liste verwendet der Name in Klammern die Punktnotation, um den Namen des Felds in JSON-Repräsentationen von Ergebnissen und der Amazon Macie Macie-API anzugeben.

Größer als () gt

Ist größer als (**>**) der für das Feld angegebene Wert. Sie können den Operator „Größer als“ für Zahlen- und Datums-/Uhrzeitwerte verwenden.

Um beispielsweise nur die Ergebnisse einzubeziehen, die mehr als 90 Vorkommen vertraulicher Daten in ein S3-Objekt melden, fügen Sie eine Bedingung hinzu, die das Feld Gesamtzahl sensibler Daten und diesen Operator verwendet, und geben Sie 90 als Wert für das Feld an. Geben Sie dazu in der Amazon Macie Macie-Konsole **91** in das Feld Von ein, geben Sie keinen Wert in das Feld An ein und wählen Sie dann Anwenden. Numerische und zeitbasierte Vergleiche sind auf der Konsole inkludiert.

Wenn Sie die Amazon Macie Macie-API verwenden, um einen Zeitbereich zu definieren, der diesen Operator verwendet, müssen Sie die Datums-/Uhrzeitwerte als Unix-Zeitstempel in Millisekunden angeben — zum Beispiel für 22:49:32 UTC am 5. November 2020. `1604616572653`

gteGrößer als oder gleich ()

Ist größer oder gleich (**> =**) dem für das Feld angegebenen Wert. Sie können den Operator „Größer als“ oder „Gleich“ mit Zahlen- und Datums-/Uhrzeitwerten verwenden.

Um beispielsweise nur die Ergebnisse einzubeziehen, die 90 oder mehr Vorkommen vertraulicher Daten in ein S3-Objekt melden, fügen Sie eine Bedingung hinzu, die das Feld Gesamtzahl sensibler Daten und diesen Operator verwendet, und geben Sie 90 als Wert für das Feld an. Geben Sie dazu in der Amazon Macie Macie-Konsole **90** in das Feld Von ein, geben Sie keinen Wert in das Feld An ein und wählen Sie dann Anwenden.

Wenn Sie die Amazon Macie Macie-API verwenden, um einen Zeitbereich zu definieren, der diesen Operator verwendet, müssen Sie die Datums-/Uhrzeitwerte als Unix-Zeitstempel in Millisekunden angeben — zum Beispiel für 22:49:32 UTC am 5. November 2020. `1604616572653`

Weniger als () lt

Ist kleiner als (**<**) der für das Feld angegebene Wert. Sie können den Operator „Weniger als“ für Zahlen- und Datums-/Uhrzeitwerte verwenden.

Um beispielsweise nur die Ergebnisse einzubeziehen, die weniger als 90 Vorkommen vertraulicher Daten in ein S3-Objekt melden, fügen Sie eine Bedingung hinzu, die das Feld Gesamtzahl sensibler Daten und diesen Operator verwendet, und geben Sie 90 als Wert für das Feld an. Geben Sie dazu in der Amazon Macie Macie-Konsole **89** in das Feld An ein, geben Sie keinen Wert in das Feld Von ein und wählen Sie dann Anwenden. Numerische und zeitbasierte Vergleiche sind auf der Konsole inkludiert.

Wenn Sie die Amazon Macie Macie-API verwenden, um einen Zeitbereich zu definieren, der diesen Operator verwendet, müssen Sie die Datums-/Uhrzeitwerte als Unix-Zeitstempel in Millisekunden angeben — zum Beispiel für 22:49:32 UTC am 5. November 2020. `1604616572653`

Weniger als oder gleich () lte

Ist kleiner oder gleich (**< =**) dem für das Feld angegebenen Wert. Sie können den Operator „Kleiner als“ oder „Gleich“ für Zahlen- und Datums-/Uhrzeitwerte verwenden.

Um beispielsweise nur die Ergebnisse einzubeziehen, die 90 oder weniger Vorkommen vertraulicher Daten in ein S3-Objekt melden, fügen Sie eine Bedingung hinzu, die das Feld Gesamtzahl sensibler Daten und diesen Operator verwendet, und geben Sie 90 als Wert für das Feld an. Geben Sie dazu in der Amazon Macie Macie-Konsole **90** in das Feld An ein, geben Sie keinen Wert in das Feld Von ein und wählen Sie dann Anwenden.

Wenn Sie die Amazon Macie Macie-API verwenden, um einen Zeitbereich zu definieren, der diesen Operator verwendet, müssen Sie die Datums-/Uhrzeitwerte als Unix-Zeitstempel in Millisekunden angeben — zum Beispiel für 22:49:32 UTC am 5. November 2020. `1604616572653`

Ist ungleich () neq

Stimmt mit keinem Wert überein, der für das Feld angegeben wurde. Sie können den Ungleichheitsoperator für die folgenden Wertetypen verwenden: Textarray (Zeichenketten), Boolean, Datum/Uhrzeit, Zahl und Text (Zeichenfolge).

Für viele Felder können Sie diesen Operator verwenden und bis zu 50 Werte für das Feld angeben. Wenn Sie dies tun, verwendet Macie die OR-Logik, um die Werte zu verknüpfen. Das bedeutet, dass ein Ergebnis den Kriterien entspricht, wenn es keinen der für das Feld angegebenen Werte enthält.

Beispiele:

- Um Ergebnisse auszuschließen, die das Vorkommen von Finanzinformationen, persönlichen Informationen oder sowohl finanziellen als auch persönlichen Informationen melden, fügen Sie eine Bedingung hinzu, die das Feld „Vertrauliche Daten“ und diesen Operator verwendet, und geben Sie Finanzinformationen und Persönliche Informationen als Werte für das Feld an.
- Um Ergebnisse auszuschließen, die das Vorkommen von Kreditkartennummern melden, fügen Sie eine Bedingung für das Feld Erkennungstyp vertraulicher Daten hinzu, verwenden Sie diesen Operator und geben Sie CREDIT_CARD_NUMBERals Wert für das Feld an.
- Um Ergebnisse auszuschließen, die das Vorkommen von Kreditkartennummern, Postanschriften oder sowohl Kreditkartennummern als auch Postanschriften melden, fügen Sie eine Bedingung für das Feld Erkennungstyp vertraulicher Daten hinzu, verwenden Sie diesen Operator und geben Sie CREDIT_CARD_NUMBERund ADDRESSals Wert für das Feld an.

Wenn Sie die Amazon Macie Macie-API verwenden, um eine Bedingung zu definieren, die diesen Operator mit einem Datums-/Uhrzeitwert verwendet, geben Sie den Wert als Unix-Zeitstempel in Millisekunden an, `1604616572653` z. B. für 22:49:32 UTC am 5. November 2020.

Filter erstellen und auf Ergebnisse anwenden

Um Ergebnisse mit bestimmten Merkmalen zu identifizieren und sich darauf zu konzentrieren, können Sie Ergebnisse in der Amazon Macie Macie-Konsole und in Abfragen filtern, die Sie programmgesteuert mithilfe der Amazon Macie Macie-API einreichen. Wenn Sie einen Filter erstellen, verwenden Sie bestimmte Ergebnisattribute, um Kriterien für das Ein- oder Ausschließen von Ergebnissen aus einer Ansicht oder aus Abfrageergebnissen zu definieren. Ein Suchattribut ist ein Feld, in dem bestimmte Daten für ein Ergebnis gespeichert werden, z. B. Schweregrad, Typ oder der Name des S3-Buckets, für den ein Ergebnis gilt.

In Macie besteht ein Filter aus einer oder mehreren Bedingungen. Jede Bedingung, auch als Kriterium bezeichnet, besteht aus drei Teilen:

- Ein auf Attributen basierendes Feld, z. B. Schweregrad oder Befundtyp.
- Ein Operator, z. B. ist gleich oder ungleich.
- Ein oder mehrere Werte. Der Typ und die Anzahl der Werte hängen vom ausgewählten Feld und Operator ab.

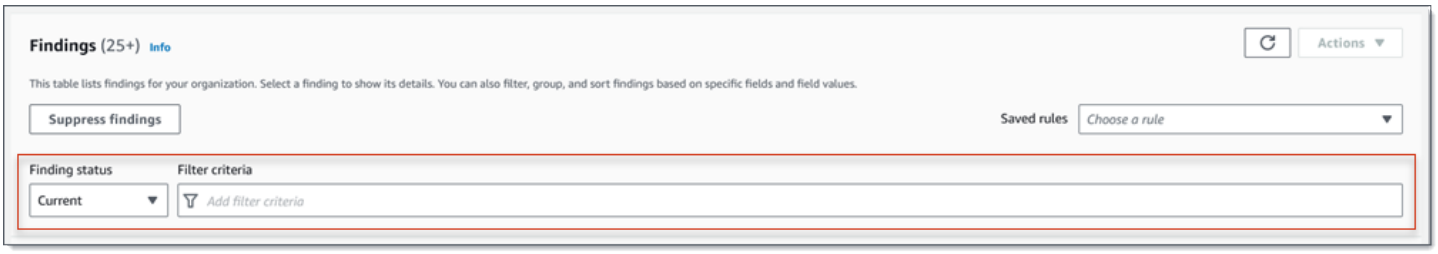
Wie Sie Filterbedingungen definieren und anwenden, hängt davon ab, ob Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden.

Themen

- Ergebnisse auf der Amazon Macie Macie-Konsole filtern
- Programmgesteuertes Filtern von Ergebnissen mit der Amazon Macie API

Ergebnisse auf der Amazon Macie Macie-Konsole filtern

Wenn Sie die Amazon Macie Macie-Konsole zum Filtern von Ergebnissen verwenden, bietet Macie Optionen, mit denen Sie Felder, Operatoren und Werte für einzelne Bedingungen auswählen können. Sie greifen auf diese Optionen zu, indem Sie die Filtereinstellungen auf den Ergebnisseiten verwenden, wie in der folgenden Abbildung dargestellt.



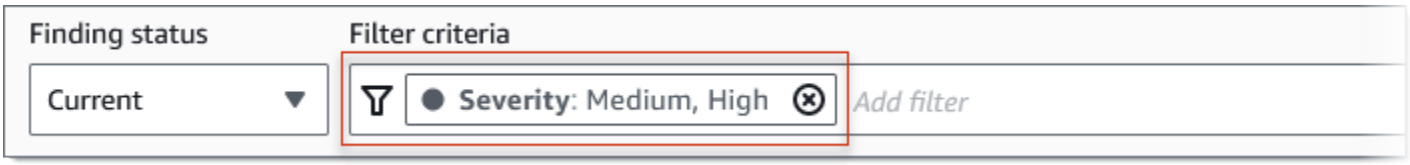
Mithilfe des Menüs „Suchstatus“ können Sie angeben, ob Ergebnisse berücksichtigt werden sollen, die durch eine Unterdrückungsregel unterdrückt (automatisch archiviert) wurden. Mithilfe des Felds Filterkriterien können Sie Filterbedingungen eingeben.

Wenn Sie den Cursor in das Feld Filterkriterien setzen, zeigt Macie eine Liste von Feldern an, die Sie für Filterbedingungen verwenden können. Die Felder sind nach logischen Kategorien geordnet. Beispielsweise umfasst die Kategorie Allgemeine Felder Felder, die für jede Art von Ergebnis gelten, und die Kategorie Klassifikationsfelder umfasst Felder, die nur für Ergebnisse mit vertraulichen Daten gelten. Die Felder sind innerhalb jeder Kategorie alphabetisch sortiert.

Um eine Bedingung hinzuzufügen, wählen Sie zunächst ein Feld aus der Liste aus. Um ein Feld zu finden, durchsuchen Sie die gesamte Liste oder geben Sie einen Teil des Feldnamens ein, um die Liste der Felder einzugrenzen.

Je nachdem, welches Feld Sie auswählen, zeigt Macie verschiedene Optionen an. Die Optionen spiegeln den Typ und die Art des von Ihnen ausgewählten Feldes wider. Wenn Sie beispielsweise das Feld Schweregrad auswählen, zeigt Macie eine Liste mit Werten an, aus denen Sie wählen können: Niedrig, Mittel und Hoch. Wenn Sie das Feld S3-Bucket-Name auswählen, zeigt Macie ein Textfeld an, in das Sie einen Bucket-Namen eingeben können. Welches Feld Sie auch wählen, Macie führt Sie durch die Schritte zum Hinzufügen einer Bedingung, die die erforderlichen Einstellungen für das Feld enthält.

Nachdem Sie eine Bedingung hinzugefügt haben, wendet Macie die Kriterien für die Bedingung an und fügt die Bedingung einem Filtertoken im Feld Filterkriterien hinzu, wie in der folgenden Abbildung gezeigt.



In diesem Beispiel ist die Bedingung so konfiguriert, dass sie alle Ergebnisse mit mittlerem und hohem Schweregrad einschließt und alle Ergebnisse mit niedrigem Schweregrad ausschließt. Es werden Ergebnisse zurückgegeben, bei denen der Wert für das Feld Schweregrad dem Wert Mittel oder Hoch entspricht.

> **Tip**
>
> Für viele Felder können Sie den Operator einer Bedingung von gleich in ungleich ändern, indem Sie das Gleichheitssymbol (●) im Filtertoken für die Bedingung auswählen. Wenn Sie dies tun, ändert Macie den Operator in „ungleich“ und zeigt das Symbol „ungleich“ () im Token an.
>
> Um wieder zum Gleichheitsoperator zu wechseln, wählen Sie das Symbol „Nicht gleich“.

Wenn Sie weitere Bedingungen hinzufügen, wendet Macie deren Kriterien an und fügt sie den Tokens im Feld Filterkriterien hinzu. Sie können das

Feld jederzeit aufrufen, um festzustellen, welche Kriterien Sie angewendet haben. Um eine Bedingung zu entfernen, wählen Sie das Symbol „Bedingung entfernen“ (

im Token für die Bedingung.

Um Ergebnisse mit der Konsole zu filtern

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich Findings aus.
3. (Optional) Wählen Sie im Navigationsbereich (unter Ergebnisse) die Option „Nach Bereich“, „Nach Typ“ oder „Nach Auftrag“ aus, um die Ergebnisse zunächst anhand einer vordefinierten logischen Gruppe zu überprüfen. Wählen Sie dann ein Element in der Tabelle aus. Wählen Sie im Detailbereich den Link für das Feld aus, auf das Sie sich konzentrieren möchten.
4. (Optional) Um Ergebnisse anzuzeigen, die durch eine Unterdrückungsregel unterdrückt wurden, ändern Sie die Einstellung Filterstatus. Wählen Sie Archiviert, um nur unterdrückte Ergebnisse anzuzeigen, oder wählen Sie Alle, um sowohl unterdrückte als auch nicht unterdrückte Ergebnisse anzuzeigen. Um unterdrückte Ergebnisse auszublenden, wählen Sie „Aktuell“.
5. Um eine Filterbedingung hinzuzufügen:

   a. Platzieren Sie den Cursor in dem Feld Filterkriterien und wählen Sie dann das Feld aus, das für die Bedingung verwendet werden soll. Informationen zu den Feldern, die Sie verwenden können, finden Sie unterFelder zum Filtern von Ergebnissen.

   b. Geben Sie den entsprechenden Wertetyp für das Feld ein. Ausführliche Informationen zu den verschiedenen Wertetypen finden Sie unterWerte für Felder angeben.

      Textarray (Zeichenketten)

      Für diesen Wertetyp stellt Macie häufig eine Werteliste zur Auswahl bereit. Wenn dies der Fall ist, wählen Sie jeden Wert aus, den Sie in der Bedingung verwenden möchten.

      Wenn Macie keine Werteliste bereitstellt, geben Sie einen vollständigen, gültigen Wert für das Feld ein. Um zusätzliche Werte für das Feld anzugeben, wählen Sie Anwenden und fügen Sie dann für jeden zusätzlichen Wert eine weitere Bedingung hinzu.

      Beachten Sie, dass bei Werten zwischen Groß- und Kleinschreibung unterschieden wird. Darüber hinaus können Sie in Werten keine Teilwerte oder Platzhalterzeichen verwenden. Um beispielsweise Ergebnisse für einen S3-Bucket mit dem Namen my-S3-

Bucket zu filtern, geben Sie ***my-S3-bucket*** als Wert für das Feld S3-Bucket-Name ein. Wenn Sie einen anderen Wert eingeben, z. B. **my-s3-bucket** oder**my-S3**, gibt Macie keine Ergebnisse für den Bucket zurück.

Boolesch

Für diesen Wertetyp stellt Macie eine Werteliste zur Auswahl bereit. Wählen Sie den Wert aus, den Sie in der Bedingung verwenden möchten.

Datum/Uhrzeit (Zeitbereiche)

Verwenden Sie für diesen Wertetyp die Felder Von und Bis, um einen inklusiven Zeitraum zu definieren:

- Um einen festen Zeitraum zu definieren, verwenden Sie die Felder Von und Bis, um das erste Datum und die erste Uhrzeit bzw. das letzte Datum und die letzte Uhrzeit im Bereich anzugeben.
- Um einen relativen Zeitraum zu definieren, der an einem bestimmten Datum und einer bestimmten Uhrzeit beginnt und zur aktuellen Uhrzeit endet, geben Sie das Startdatum und die Startzeit in die Felder Von ein und löschen Sie den gesamten Text in den Feldern Bis.
- Um einen relativen Zeitraum zu definieren, der an einem bestimmten Datum und einer bestimmten Uhrzeit endet, geben Sie das Enddatum und die Endzeit in die Felder Bis ein und löschen Sie den gesamten Text in den Feldern Von.

Beachten Sie, dass für Zeitwerte die 24-Stunden-Notation verwendet wird. Wenn Sie die Datumsauswahl verwenden, um Daten auszuwählen, können Sie die Werte verfeinern, indem Sie Text direkt in die Felder Von und Bis eingeben.

Zahl (numerische Bereiche)

Verwenden Sie für diesen Wertetyp die Felder Von und Bis, um eine oder mehrere ganze Zahlen einzugeben, die einen inklusiven, festen oder relativen numerischen Bereich definieren.

Textwerte (Zeichenfolge)

Geben Sie für diesen Wertetyp einen vollständigen, gültigen Wert für das Feld ein.

Beachten Sie, dass bei Werten zwischen Groß- und Kleinschreibung unterschieden wird. Darüber hinaus können Sie in Werten keine Teilwerte oder Platzhalterzeichen verwenden. Um beispielsweise Ergebnisse für einen S3-Bucket mit dem Namen my-S3-

Bucket zu filtern, geben Sie ***my-S3-bucket*** als Wert für das Feld S3-Bucket-Name ein. Wenn Sie einen anderen Wert eingeben, z. B. **my-s3-bucket** oder**my-S3**, gibt Macie keine Ergebnisse für den Bucket zurück.

c. Wenn Sie mit dem Hinzufügen von Werten für das Feld fertig sind, wählen Sie Anwenden. Macie wendet die Filterkriterien an und fügt die Bedingung einem Filtertoken im Feld Filterkriterien hinzu.

6. Wiederholen Sie Schritt 5 für jede weitere Bedingung, die Sie hinzufügen möchten.
7. Um eine Bedingung zu entfernen, wählen Sie das Symbol „Bedingung entfernen“ (⊗ im Filtertoken für die Bedingung aus.
8. Um eine Bedingung zu ändern, entfernen Sie die Bedingung, indem Sie das Symbol „Bedingung entfernen“ (⊗ im Filtertoken für die Bedingung auswählen. Wiederholen Sie dann Schritt 5, um eine Bedingung mit den richtigen Einstellungen hinzuzufügen.

Wenn Sie diesen Satz von Bedingungen später erneut verwenden möchten, können Sie den Satz als Filterregel speichern. Wählen Sie dazu im Feld Filterkriterien die Option Regel speichern aus. Geben Sie anschließend einen Namen und optional eine Beschreibung für die Regel ein. Wählen Sie Save (Speichern) aus, wenn Sie fertig sind.

Programmgesteuertes Filtern von Ergebnissen mit der Amazon Macie API

Um Ergebnisse programmgesteuert zu filtern, geben Sie Filterkriterien in Abfragen an, die Sie mithilfe der ListFindingsAmazon GetFindingStatisticsMacie Macie-API einreichen. Der ListFindings Vorgang gibt ein Array von Ergebnis-IDs zurück, eine ID für jedes Ergebnis, das den Filterkriterien entspricht. Der GetFindingStatistics Vorgang gibt aggregierte statistische Daten zu allen Ergebnissen zurück, die den Filterkriterien entsprechen, gruppiert nach einem Feld, das Sie in Ihrer Anfrage angeben.

Beachten Sie, dass sich die GetFindingStatistics Operationen ListFindings und von Vorgängen unterscheiden, mit denen Sie Ergebnisse unterdrücken. Im Gegensatz zu Unterdrückungsvorgängen, bei denen auch Filterkriterien angegeben werden, werden bei den GetFindingStatistics Operationen ListFindings und nur Ergebnisdaten abgefragt. Sie führen keine Aktion für Ergebnisse aus, die den Filterkriterien entsprechen. Verwenden Sie den CreateFindingsFilterBetrieb der Amazon Macie Macie-API, um Ergebnisse zu unterdrücken.

Um Filterkriterien in einer Abfrage anzugeben, fügen Sie Ihrer Anfrage eine Übersicht der Filterbedingungen bei. Geben Sie für jede Bedingung ein Feld, einen Operator und einen oder

mehrere Werte für das Feld an. Der Typ und die Anzahl der Werte hängen vom ausgewählten Feld und Operator ab. Informationen zu den Feldern, Operatoren und Wertetypen, die Sie in einer Bedingung verwenden können, finden Sie unter Felder zum Filtern von ErgebnissenVerwenden von Operatoren unter bestimmten Bedingungen, undWerte für Felder angeben.

In den folgenden Beispielen wird gezeigt, wie Sie Filterkriterien in Abfragen angeben, die Sie mit AWS Command Line Interface(AWS CLI) einreichen. Sie können dies auch tun, indem Sie eine aktuelle Version eines anderen AWS Befehlszeilentools oder eines AWS SDK verwenden oder HTTPS-Anfragen direkt an Macie senden. Informationen zu AWS Tools und SDKs finden Sie unter Tools, auf denen Sie aufbauen können. AWS

Beispiele

- Beispiel 1: Ergebnisse nach Schweregrad filtern
- Beispiel 2: Filtern Sie Ergebnisse auf der Grundlage der Kategorie sensibler Daten
- Beispiel 3: Filtern Sie Ergebnisse auf der Grundlage eines festen Zeitraums
- Beispiel 4: Filtert Ergebnisse auf der Grundlage des Unterdrückungsstatus
- Beispiel 5: Filtern Sie Ergebnisse auf der Grundlage mehrerer Felder und Wertetypen

In den Beispielen wird der Befehl list-findings verwendet. Wenn ein Beispiel erfolgreich ausgeführt wird, gibt Macie ein Array zurück. `findingIds` Das Array listet die eindeutige Kennung für jedes Ergebnis auf, das den Filterkriterien entspricht, wie im folgenden Beispiel gezeigt.

```
{
    "findingIds": [
        "1f1c2d74db5d8caa76859ec52example",
        "6cfa9ac820dd6d55cad30d851example",
        "702a6fd8750e567d1a3a63138example",
        "826e94e2a820312f9f964cf60example",
        "274511c3fdcd87010a19a3a42example"
    ]
}
```

Wenn keine Ergebnisse den Filterkriterien entsprechen, gibt Macie ein leeres `findingIds` Array zurück.

```
{
    "findingIds": []
```

```
}
```

Beispiel 1: Ergebnisse nach Schweregrad filtern

In diesem Beispiel wird der Befehl list-findings verwendet, um Suchkennungen für all Ihre aktuellen Ergebnisse mit hohem und mittlerem Schweregrad abzurufen. AWS-Region

Für Linux, macOS oder Unix:

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"severity.description":
{"eq":["High","Medium"]}}}'
```

Für Microsoft Windows:

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":
{\"severity.description\":{\"eq\":[\"High\",\"Medium\"]}}}
```

Wobei gilt:

- *severity.description* gibt den JSON-Namen des Felds Severity an.
- *eq* gibt den Gleichheitsoperator an.
- *Hoch* und ***Mittel*** sind eine Reihe von Aufzählungswerten für das Feld Schweregrad.

Beispiel 2: Filtern Sie Ergebnisse auf der Grundlage der Kategorie sensibler Daten

In diesem Beispiel wird der Befehl list-findings verwendet, um Such-IDs für all Ihre Ergebnisse mit vertraulichen Daten abzurufen, die sich in der aktuellen Region befinden, und um das Vorkommen von Finanzinformationen (und keine anderen Kategorien vertraulicher Daten) in S3-Objekten zu melden.

Verwenden Sie für Linux, macOS oder Unix den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit:

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.category":{"eqExactMatch":
["FINANCIAL_INFORMATION"]}}}'
```

Verwenden Sie für Microsoft Windows das Zeilenfortsetzungszeichen Caret (^), um die Lesbarkeit zu verbessern:

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.category\":{\"eqExactMatch\":
[\"FINANCIAL_INFORMATION\"]}}}
```

Wobei gilt:

- *ClassificationDetails.Result.SensitiveData.Category gibt den JSON-Namen des Felds für die Kategorie Sensitive* Daten an.
- *eqExactMatch*gibt den Gleichheitsoperator für exakte Übereinstimmung an.
- *FINANCIAL_INFORMATION* ist ein Aufzählungswert für das Kategoriefeld Vertrauliche Daten.

Beispiel 3: Filtern Sie Ergebnisse auf der Grundlage eines festen Zeitraums

In diesem Beispiel wird der Befehl list-findings verwendet, um Such-IDs für all Ihre Ergebnisse abzurufen, die sich in der aktuellen Region befinden und zwischen 07:00 Uhr UTC am 5. Oktober 2020 und 07:00 Uhr UTC am 5. November 2020 (einschließlich) erstellt wurden.

Für Linux, macOS oder Unix:

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"createdAt":
{"gte":1601881200000,"lte":1604559600000}}}'
```

Für Microsoft Windows:

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"createdAt\":
{\"gte\":1601881200000,\"lte\":1604559600000}}}
```

Wobei gilt:

- *CreatedAt* gibt den JSON-Namen des Felds Created at an.
- *gte* gibt den Operator größer als oder gleich an.
- *1601881200000* ist das erste Datum und die erste Uhrzeit (als Unix-Zeitstempel in Millisekunden) im Zeitbereich.

- *lte gibt den Operator* kleiner als oder gleich an.
- *1604559600000* ist das letzte Datum und die letzte Uhrzeit (als Unix-Zeitstempel in Millisekunden) im Zeitbereich.

Beispiel 4: Filtert Ergebnisse auf der Grundlage des Unterdrückungsstatus

In diesem Beispiel wird der Befehl list-findings verwendet, um Such-IDs für all Ihre Ergebnisse abzurufen, die sich in der aktuellen Region befinden und durch eine Unterdrückungsregel unterdrückt (automatisch archiviert) wurden.

Für Linux, macOS oder Unix:

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"archived":{"eq":
["true"]}}}'
```

Für Microsoft Windows:

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"archived\":{\"eq\":
[\"true\"]}}}
```

Wobei gilt:

- *archived* gibt den JSON-Namen des Felds Archived an.
- *eq* gibt den Gleichheitsoperator an.
- *true* ist ein boolescher Wert für das Feld Archiviert.

Beispiel 5: Filtern Sie Ergebnisse auf der Grundlage mehrerer Felder und Wertetypen

In diesem Beispiel wird der Befehl list-findings verwendet, um Such-IDs für all Ihre Ergebnisse mit vertraulichen Daten abzurufen, die sich in der aktuellen Region befinden und die folgenden Kriterien erfüllen: wurden zwischen 07:00 Uhr UTC am 5. Oktober 2020 und 07:00 Uhr UTC am 5. November 2020 (ausschließlich) erstellt, melden Vorkommen von Finanzdaten und keinen anderen Kategorien vertraulicher Daten in S3-Objekten und wurden nicht durch eine Unterdrückungsregel unterdrückt (automatisch archiviert).

Verwenden Sie für Linux, macOS oder Unix den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit:

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":{"createdAt":
{"gt":1601881200000,"lt":1604559600000},"classificationDetails.result.sensitiveData.category":
{"eqExactMatch":["FINANCIAL_INFORMATION"]},"archived":{"eq":["false"]}}}'
```

Verwenden Sie für Microsoft Windows das Zeilenfortsetzungszeichen Caret (^), um die Lesbarkeit zu verbessern:

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":{\"createdAt\":{\"gt\":1601881200000,
\"lt\":1604559600000},\"classificationDetails.result.sensitiveData.category\":
{\"eqExactMatch\":[\"FINANCIAL_INFORMATION\"]},\"archived\":{\"eq\":[\"false\"]}}}
```

Wobei gilt:

- *CreatedAt* gibt den JSON-Namen des Felds Created at an und:
  - *gt* gibt den Operator größer als oder gleich an.
  - *1601881200000* ist das erste Datum und die erste Uhrzeit (als Unix-Zeitstempel in Millisekunden) im Zeitbereich.
  - *Es gibt den Operator* „kleiner als“ oder „gleich“ an.
  - *1604559600000* ist das letzte Datum und die letzte Uhrzeit (als Unix-Zeitstempel in Millisekunden) im Zeitbereich.
- *ClassificationDetails.Result.SensitiveData.Category* gibt den JSON-Namen des Felds für die Kategorie Sensitive Daten an und:
  - *eqExactMatch*gibt den Gleichheitsoperator für exakte Übereinstimmung an.
  - *FINANCIAL_INFORMATION* ist ein Aufzählungswert für das Feld.
- *archived* gibt den JSON-Namen des archivierten Felds an und:
  - *eq* gibt den Gleichheitsoperator an.
  - *false* ist ein boolescher Wert für das Feld.

Filterregeln für Ergebnisse erstellen und verwalten

Eine Filterregel besteht aus einer Reihe von Filterkriterien, die Sie erstellen und speichern, um sie erneut zu verwenden, wenn Sie die Ergebnisse auf der Amazon Macie Macie-Konsole überprüfen. Filterregeln können Ihnen dabei helfen, Ergebnisse, die bestimmte Merkmale aufweisen, konsistent

zu analysieren. Sie könnten beispielsweise eine Filterregel für die Analyse aller Richtlinienergebnisse mit hohem Schweregrad für S3-Buckets erstellen, die unverschlüsselte Objekte enthalten, und eine weitere Filterregel für die Analyse aller Ergebnisse mit hohem Schweregrad für sensible Daten, die bestimmte Typen vertraulicher Daten melden.

Beachten Sie, dass sich Filterregeln von Unterdrückungsregeln unterscheiden. Eine Unterdrückungsregel besteht aus einer Reihe von Filterkriterien, die Sie erstellen und speichern, um Ergebnisse, die den Kriterien der Regel entsprechen, automatisch zu archivieren. Obwohl beide Regeltypen Filterkriterien speichern und anwenden, führt eine Filterregel keine Aktion für Ergebnisse aus, die den Kriterien der Regel entsprechen. Stattdessen bestimmt eine Filterregel nur, welche Ergebnisse auf der Konsole angezeigt werden, nachdem Sie die Regel angewendet haben. Informationen zu Unterdrückungsregeln finden Sie unterUnterdrücken von Ergebnissen.

Um Filterregeln zu erstellen und zu verwalten, können Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden. In den folgenden Themen wird erklärt, wie das geht. Für die API enthalten die Themen Beispiele dafür, wie diese Aufgaben mithilfe von AWS Command Line Interface(AWS CLI) ausgeführt werden können. Sie können diese Aufgaben auch ausführen, indem Sie eine aktuelle Version eines anderen AWS Befehlszeilentools oder eines AWS SDK verwenden oder indem Sie HTTPS-Anfragen direkt an Macie senden. Informationen zu AWS Tools und SDKs finden Sie unter Tools, auf denen Sie aufbauen können. AWS

Themen

- Filterregeln erstellen
- Anwenden von Filterregeln
- Filterregeln ändern
- Filterregeln löschen

Filterregeln erstellen

Wenn Sie eine Filterregel erstellen, geben Sie Filterkriterien, einen Namen und optional eine Beschreibung der Regel an. Sie können eine Filterregel mithilfe der Amazon Macie Macie-Konsole oder der Amazon Macie Macie-API erstellen.

Console

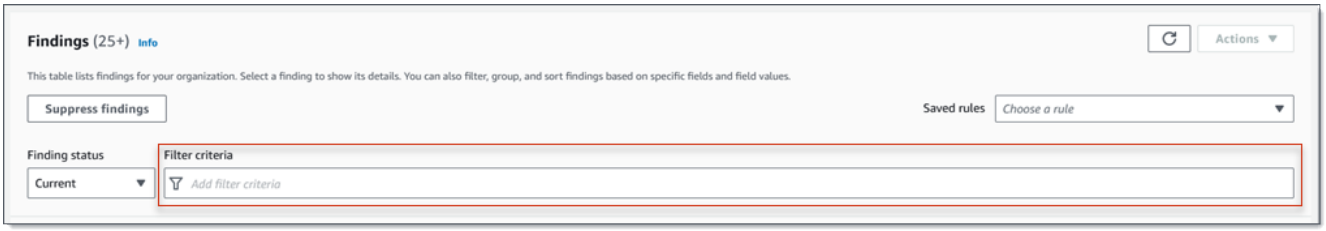
Gehen Sie wie folgt vor, um mithilfe der Amazon Macie Macie-Konsole eine Filterregel zu erstellen.

Um eine Filterregel zu erstellen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich Findings aus.

> **Tip**
>
> Um eine bestehende Filterregel als Ausgangspunkt zu verwenden, wählen Sie die Regel aus der Liste Gespeicherte Regeln aus.
> Sie können die Erstellung einer Regel auch vereinfachen, indem Sie die Ergebnisse zunächst anhand einer vordefinierten logischen Gruppe durchblättern und anschließend aufschlüsseln. In diesem Fall erstellt Macie automatisch die entsprechenden Filterbedingungen und wendet sie an. Dies kann ein hilfreicher Ausgangspunkt für die Erstellung einer Regel sein. Wählen Sie dazu im Navigationsbereich (unter Ergebnisse) die Option Nach Bereich, Nach Typ oder Nach Auftrag und wählen Sie dann ein Element in der Tabelle aus. Wählen Sie im Detailbereich den Link für das Feld aus, auf das Sie sich konzentrieren möchten.

3. Fügen Sie im Feld Filterkriterien Bedingungen hinzu, die die Filterkriterien für die Regel definieren.



Informationen zum Hinzufügen von Filterbedingungen finden Sie unterFilter erstellen und auf Ergebnisse anwenden.

4. Wenn Sie mit der Definition der Filterkriterien für die Regel fertig sind, wählen Sie im Feld Filterkriterien die Option Regel speichern aus.

5. Geben Sie unter Filterregel einen Namen und optional eine Beschreibung der Regel ein.

6. Wählen Sie Speichern aus.

API

Um eine Filterregel programmgesteuert zu erstellen, verwenden Sie den CreateFindingsFilterBetrieb der Amazon Macie Macie-API und geben Sie die entsprechenden Werte für die erforderlichen Parameter an:

- Geben Sie für den `action` Parameter Folgendes an, `NOOP` um sicherzustellen, dass Macie keine Ergebnisse unterdrückt (automatisch archiviert), die den Kriterien der Regel entsprechen.
- Geben Sie für den `criterion` Parameter eine Zuordnung von Bedingungen an, die die Filterkriterien für die Regel definieren.

  In der Map sollte jede Bedingung ein Feld, einen Operator und einen oder mehrere Werte für das Feld angeben. Der Typ und die Anzahl der Werte hängen vom ausgewählten Feld und Operator ab. Informationen zu den Feldern, Operatoren und Wertetypen, die Sie in einer Bedingung verwenden können, finden Sie unter Felder zum Filtern von ErgebnissenVerwenden von Operatoren unter bestimmten Bedingungen, undWerte für Felder angeben.

Um eine Filterregel mithilfe von zu erstellenAWS CLI, führen Sie den create-findings-filterBefehl aus und geben Sie die entsprechenden Werte für die erforderlichen Parameter an. In den folgenden Beispielen wird eine Filterregel erstellt, die alle aktuellen Ergebnisse mit vertraulichen Daten zurückgibt AWS-Region und das Vorkommen persönlicher Informationen (und keiner anderen Kategorien vertraulicher Daten) in S3-Objekten meldet.

Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\), um die Lesbarkeit zu verbessern.

```
$ aws macie2 create-findings-filter \
--action NOOP \
--name my_filter_rule \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.category":{"eqExactMatch":
["PERSONAL_INFORMATION"]}}}'
```

Dieses Beispiel ist für Microsoft Windows formatiert und verwendet das Zeilenfortsetzungszeichen Caret (^), um die Lesbarkeit zu verbessern.

```
C:\> aws macie2 create-findings-filter ^
```

```
--action NOOP ^
--name my_filter_rule ^
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.category\":{\"eqExactMatch\":
[\"PERSONAL_INFORMATION\"]}}}
```

Wobei gilt:

- *my_filter_rule ist der benutzerdefinierte Name für die Regel*.
- `criterion`ist eine Übersicht der Filterbedingungen für die Regel:
  - *ClassificationDetails.Result.SensitiveData.Category ist der JSON-Name des Felds „Vertrauliche Daten*“.
  - *eqExactMatch*gibt den Gleichheitsoperator für exakte Übereinstimmung an.
  - *PERSONAL_INFORMATION* ist ein Aufzählungswert für das Kategoriefeld Vertrauliche Daten.

Wird der Befehl erfolgreich ausgeführt, erhalten Sie eine Ausgabe ähnlich der folgenden:

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/9b2b4508-
aa2f-4940-b347-d1451example",
    "id": "9b2b4508-aa2f-4940-b347-d1451example"
}
```

Wo `arn` ist der Amazon-Ressourcenname (ARN) der Filterregel, die erstellt wurde, und `id` ist der eindeutige Bezeichner für die Regel.

Weitere Beispiele für Filterkriterien finden Sie unterProgrammgesteuertes Filtern von Ergebnissen mit der Amazon Macie API.

Anwenden von Filterregeln

Wenn Sie eine Filterregel anwenden, verwendet Amazon Macie die Kriterien der Regel, um zu bestimmen, welche Ergebnisse in Ihre Ergebnisansicht auf der Konsole aufgenommen oder daraus ausgeschlossen werden sollen. Macie zeigt auch die Kriterien an, damit Sie feststellen können, welche Kriterien Sie angewendet haben.

Beachten Sie, dass Filterregeln für die Verwendung mit der Amazon Macie Macie-Konsole konzipiert sind. Sie können sie nicht direkt in Abfragen verwenden, die Sie programmgesteuert

über die Amazon Macie Macie-API einreichen. Wenn Sie jedoch die API verwenden, um Ergebnisse abzufragen, können Sie die Filterkriterien für eine Regel mithilfe des Vorgangs abrufen. GetFindingsFilter Anschließend können Sie die Kriterien zu Ihrer Abfrage hinzufügen. Informationen zum Angeben von Filterkriterien in einer Abfrage finden Sie unterFilter erstellen und auf Ergebnisse anwenden.

Gehen Sie wie folgt vor, um Ergebnisse auf der Konsole zu filtern, indem Sie eine Filterregel anwenden.

Um eine Filterregel anzuwenden

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich Findings aus.
3. Wählen Sie in der Liste Gespeicherte Regeln die Filterregel aus, die Sie anwenden möchten. Macie wendet die Kriterien der Regel an und zeigt die Kriterien im Feld Filterkriterien an.
4. (Optional) Um die Kriterien zu verfeinern, verwenden Sie das Feld Filterkriterien, um Filterbedingungen hinzuzufügen oder zu entfernen. Wenn Sie dies tun, wirken sich Ihre Änderungen nicht auf die Einstellungen für die Regel aus. Macie speichert keine Ihrer Änderungen, es sei denn, Sie speichern sie ausdrücklich als neue Regel.
5. Um eine andere Filterregel anzuwenden, wiederholen Sie Schritt 3.

Nachdem Sie eine Filterregel angewendet haben, können Sie schnell alle zugehörigen Filterkriterien aus Ihrer Ansicht entfernen, indem Sie das X im Feld Filterkriterien auswählen.

Filterregeln ändern

Sie können die Einstellungen für eine Filterregel jederzeit mithilfe der Amazon Macie Macie-Konsole oder der Amazon Macie Macie-API ändern. Sie können der Regel auch Tags zuweisen und verwalten.

Ein Tag ist eine Bezeichnung, die Sie definieren und bestimmten Ressourcentypen AWS zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Mithilfe von Tags können Sie Ressourcen auf unterschiedliche Weise identifizieren, kategorisieren und verwalten, z. B. nach Zweck, Eigentümer, Umgebung oder anderen Kriterien. Weitere Informationen hierzu finden Sie unter Kennzeichnen von Amazon Macie-Ressourcen.

Console

Gehen Sie wie folgt vor, um die Einstellungen für eine bestehende Filterregel mithilfe der Amazon Macie Macie-Konsole zu ändern.

Um eine Filterregel zu ändern

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich Findings aus.
3. Wählen Sie in der Liste Gespeicherte Regeln das Bearbeitungssymbol () neben der Filterregel aus, die Sie ändern möchten.
4. Führen Sie eine der folgenden Aktionen aus:
   - Um die Filterkriterien der Regel zu ändern, geben Sie im Feld Filterkriterien Bedingungen für die gewünschten Kriterien ein. Um zu erfahren wie dies geht, vgl. Filter erstellen und auf Ergebnisse anwenden.
   - Um den Namen der Regel zu ändern, geben Sie im Feld Name unter Filterregel einen neuen Namen ein.
   - Um die Beschreibung der Regel zu ändern, geben Sie im Feld Beschreibung unter Filterregel eine neue Beschreibung ein.
   - Um der Regel Tags zuzuweisen, zu überprüfen oder zu bearbeiten, wählen Sie unter Filterregel die Option Tags verwalten aus. Überprüfen Sie dann die Tags und ändern Sie sie nach Bedarf. Eine Regel kann bis zu 50 Tags enthalten.
5. Wenn Sie die gewünschten Änderungen vorgenommen haben, wählen Sie Save (Speichern) aus.

API

Um eine Filterregel programmgesteuert zu ändern, verwenden Sie den UpdateFindingsFilterBetrieb der Amazon Macie Macie-API. Wenn Sie Ihre Anfrage einreichen, verwenden Sie die unterstützten Parameter, um für jede Einstellung, die Sie ändern möchten, einen neuen Wert anzugeben.

Geben Sie für den `id` Parameter den eindeutigen Bezeichner für die zu ändernde Regel an. Sie können diese Kennung abrufen, indem Sie den ListFindingsFilterVorgang verwenden,

um eine Liste von Filter- und Unterdrückungsregeln für Ihr Konto abzurufen. Wenn Sie den verwendenAWS CLI, führen Sie den list-findings-filtersBefehl aus, um diese Liste abzurufen.

Um eine Filterregel mithilfe von zu ändernAWS CLI, führen Sie den update-findings-filterBefehl aus und geben Sie mithilfe der unterstützten Parameter für jede Einstellung, die Sie ändern möchten, einen neuen Wert an. Mit dem folgenden Befehl wird beispielsweise der Name einer vorhandenen Filterregel geändert.

```
C:\> aws macie2 update-findings-filter --id 9b2b4508-aa2f-4940-b347-d1451example --
name personal_information_only
```

Wobei gilt:

- *9b2b4508-aa2f-4940-b347-d1451example* ist der eindeutige Bezeichner für die Regel.
- *personal_information_only ist der neue Name für die Regel*.

Wird der Befehl erfolgreich ausgeführt, erhalten Sie eine Ausgabe ähnlich der folgenden:

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/9b2b4508-
aa2f-4940-b347-d1451example",
    "id": "9b2b4508-aa2f-4940-b347-d1451example"
}
```

Wo `arn` ist der Amazon-Ressourcenname (ARN) der Regel, die geändert wurde, und `id` ist der eindeutige Bezeichner für die Regel.

In ähnlicher Weise konvertiert das folgende Beispiel eine Unterdrückungsregel in eine Filterregel, indem der Wert für den `action` Parameter von `ARCHIVE` bis geändert wird`NOOP`.

```
C:\> aws macie2 update-findings-filter --id 8a1c3508-aa2f-4940-b347-d1451example --
action NOOP
```

Wobei gilt:

- *8a1c3508-aa2f-4940-b347-d1451example* ist der eindeutige Bezeichner für die Regel.
- *NOOP* ist die neue Aktion, die Macie bei Ergebnissen durchführt, die den Kriterien der Regel entsprechen. Führen Sie keine Aktion aus (unterdrücken Sie die Ergebnisse nicht).

Wenn der Befehl erfolgreich ausgeführt wird, erhalten Sie eine Ausgabe, die der folgenden ähnelt:

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a1c3508-
aa2f-4940-b347-d1451example",
    "id": "8a1c3508-aa2f-4940-b347-d1451example"
}
```

Wo `arn` ist der Amazon-Ressourcenname (ARN) der Regel, die geändert wurde, und `id` ist der eindeutige Bezeichner für die Regel.

Filterregeln löschen

Sie können eine Filterregel jederzeit mithilfe der Amazon Macie Macie-Konsole oder der Amazon Macie Macie-API löschen.

Console

Gehen Sie wie folgt vor, um eine Filterregel mithilfe der Amazon Macie Macie-Konsole zu löschen.

Um eine Filterregel zu löschen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich Findings aus.
3. Wählen Sie in der Liste Gespeicherte Regeln das Bearbeitungssymbol () neben der Filterregel aus, die Sie löschen möchten.
4. Wählen Sie unter Filterregel die Option Löschen aus.

API

Um eine Filterregel programmgesteuert zu löschen, verwenden Sie den DeleteFindingsFilterBetrieb der Amazon Macie Macie-API. Geben Sie für den `id` Parameter die eindeutige Kennung für die zu löschende Filterregel an. Sie können diese Kennung abrufen, indem Sie den ListFindingsFilterVorgang zum Abrufen einer Liste von Filter- und Unterdrückungsregeln für Ihr Konto verwenden. Wenn Sie den verwendenAWS CLI, führen Sie den list-findings-filtersBefehl aus, um diese Liste abzurufen.

Um eine Filterregel mithilfe von zu löschenAWS CLI, führen Sie den delete-findings-filterBefehl aus. Beispiele:

```
C:\> aws macie2 delete-findings-filter --id 9b2b4508-aa2f-4940-b347-d1451example
```

Wobei *9b2b4508-aa2f-4940-b347-d1451example* der eindeutige Bezeichner für die zu löschende Filterregel ist.

Wenn der Befehl erfolgreich ausgeführt wird, gibt Macie eine leere HTTP 200-Antwort zurück. Andernfalls gibt Macie eine HTTP 4 xx - oder 500-Antwort zurück, die angibt, warum der Vorgang fehlgeschlagen ist.

Felder zum Filtern von Ergebnissen

Damit Sie Erkenntnisse effizienter analysieren können, bieten die Amazon Macie-Konsole und die Amazon Macie-API Zugriff auf mehrere Gruppen von Feldern zum Filtern von Ergebnissen:

- Häufige Felder – Diese Felder speichern Daten, die für jede Art von Erkenntnis gelten. Sie korrelieren mit gemeinsamen Attributen von Erkenntnissen wie Schweregrad, Erkenntnistyp und Erkenntnis-ID.
- Betroffene Ressourcenfelder – Diese Felder speichern Daten über die Ressourcen, für die ein Ergebnis gilt, z. B. Name, Tags und Verschlüsselungseinstellungen für einen betroffenen S3-Bucket oder ein Objekt.
- Richtlinienfelder – Diese Felder speichern Daten, die spezifisch für Richtlinienergebnisse sind, z. B. die Aktion, die ein Ergebnis erzeugt hat, und die Entität, die die Aktion ausgeführt hat.
- Felder zur Klassifizierung sensibler Daten – Diese Felder speichern Daten, die für Ergebnisse sensibler Daten spezifisch sind, z. B. die Kategorie und die Arten sensibler Daten, die Macie in einem betroffenen S3-Objekt gefunden hat.

Ein Filter kann eine Kombination von Feldern aus einem der vorhergehenden Sätze verwenden.

In den Themen in diesem Abschnitt werden die einzelnen Felder aufgelistet und beschrieben, mit denen Sie Ergebnisse filtern können. Weitere Informationen zu diesen Feldern, einschließlich Beziehungen zwischen den Feldern, finden Sie unter Erkenntnisse in der Amazon Macie-API-Referenz.

Themen

- Gemeinsame Felder
- Betroffene Ressourcenfelder
- Richtlinienfelder
- Klassifizierungsfelder für sensible Daten

Gemeinsame Felder

In der folgenden Tabelle werden Felder aufgeführt und beschrieben, mit denen Sie Ergebnisse basierend auf allgemeinen Ergebnisattributen filtern können. Diese Felder speichern Daten, die für jede Art von Erkenntnis gelten.

In der Tabelle gibt die Spalte Feld den Namen des Feldes in der Amazon MacieKonsole an. Die JSON-Feldspalte verwendet Punktnotation, um den Namen des Feldes in JSON-Darstellungen von Erkenntnissen und der Amazon Macie-API anzugeben. Die Spalte Beschreibung enthält eine kurze Beschreibung der Daten, die das Feld speichert, und gibt alle Anforderungen für Filterwerte an. Die Tabelle wird in aufsteigender alphabetischer Reihenfolge nach Feld und dann nach JSON-Feld sortiert.

Feld	JSON-Feld	Beschreibung
Konto-ID*	`accountId`	Die eindeutige Kennung für die AWS-Konto, für die die Erkenntnis gilt. Dies ist in der Regel das Konto, das Eigentümer der betroffenen Ressource ist.
—	`archived`	Ein boolescher Wert, der angibt, ob das Ergebnis durch eine Unterdrückungsrege l unterdrückt (automatisch archiviert) wurde. Um dieses Feld in einem Filter in der Konsole zu verwenden , wählen Sie eine Option im Menü Erkenntnisstatus aus:

Feld	JSON-Feld	Beschreibung
		Archiviert (nur unterdrückt), Aktuell (nur unterdrückt) oder All e(sowohl unterdrückt als auch nicht unterdrückt).
Kategorie	`category`	Die Kategorie der Erkenntnis. Die Konsole bietet eine Liste der Werte, aus denen Sie wählen können, wenn Sie dieses Feld zu einem Filter hinzufügen. In der API sind gültige Werte: `CLASSIFICATION` , für eine Erkenntnis zu sensiblen Daten und `POLICY`, für eine Richtlinienerkenntnis.
—	`count`	Die Gesamtzahl der Vorkommen der Erkenntnis. Bei Ergebnissen mit sensiblen Daten ist dieser Wert immer 1. Alle Erkenntnisse zu sensiblen Daten gelten als eindeutig. Dieses Feld ist in der Konsole nicht als Filteroption verfügbar. Mit der API können Sie dieses Feld verwenden, um einen numerischen Bereich für einen Filter zu definieren.

Feld	JSON-Feld	Beschreibung
Erstellt am	`createdAt`	Das Datum und die Uhrzeit, zu der Macie das Ergebnis erstellt hat. Sie können dieses Feld verwenden, um einen Zeitraum für einen Filter zu definieren.
ID der Suche*	`id`	Die eindeutige Kennung für die Erkenntnis. Dies ist eine zufällige Zeichenfolge, die Macie generiert und einem Ergebnis zuweist, wenn es das Ergebnis erstellt.
Erkenntnistyp*	`type`	Der Typ der Erkenntnis, z. B. `SensitiveData:S3Object/Personal` oder `Policy:IAMUser/S3BucketPublic`. Die Konsole bietet eine Liste der Werte, aus denen Sie wählen können, wenn Sie dieses Feld zu einem Filter hinzufügen. Eine Liste der gültigen Werte in der API finden Sie unter FindingType in der Amazon Macie-API-Referenz.
Region	`region`	Die AWS-Region, in der Macie die Erkenntnis erstellt hat, z. B. `us-east-1` oder `ca-central-1`.

Feld	JSON-Feld	Beschreibung
Beispiel	`sample`	Ein boolescher Wert, der angibt, ob es sich bei der Erkenntnis um eine Beispiele rkenntnis handelt. Ein Beispielergebnis ist ein Ergebnis, das Beispield aten und Platzhalterwerte verwendet, um zu demonstri eren, was ein Ergebnis enthalten könnte. Die Konsole bietet eine Liste der Werte, aus denen Sie wählen können, wenn Sie dieses Feld zu einem Filter hinzufügen.
Schweregrad	`severity.description`	Die qualitative Darstellung des Schweregrads der Erkenntnis. Die Konsole bietet eine Liste der Werte, aus denen Sie wählen können, wenn Sie dieses Feld zu einem Filter hinzufügen. In der API sind die gültigen Werte: `Low`, `Medium`, und `High`.

Feld	JSON-Feld	Beschreibung
Aktualisiert um	`updatedAt`	Das Datum und die Uhrzeit der letzten Aktualisierung der Erkenntnis. Bei Ergebnissen mit sensiblen Daten entsprich t dieser Wert dem Wert für das Feld Erstellt am. Alle Erkenntni sse zu sensiblen Daten werden als neu (eindeutig) angesehen. Sie können dieses Feld verwenden, um einen Zeitraum für einen Filter zu definieren.

* Um mehrere Werte für dieses Feld in der Konsole anzugeben, fügen Sie eine Bedingung hinzu, die das Feld verwendet und einen eindeutigen Wert für den Filter angibt, und wiederholen Sie diesen Schritt dann für jeden zusätzlichen Wert. Um dies mit der API zu tun, verwenden Sie ein Array, das die Werte auflistet, die für den Filter verwendet werden sollen.

Betroffene Ressourcenfelder

In den folgenden Themen werden die Felder aufgelistet und beschrieben, mit denen Sie Ergebnisse basierend auf der Ressource filtern können, für die ein Ergebnis gilt. Die Themen sind nach Ressourcentyp organisiert.

Themen

- S3-Bucket
- S3-Objekt

S3-Bucket

In der folgenden Tabelle werden Felder aufgeführt und beschrieben, mit denen Sie Ergebnisse basierend auf den Eigenschaften des S3-Buckets filtern können, für den ein Ergebnis gilt.

In der Tabelle gibt die Spalte Feld den Namen des Feldes in der Amazon MacieKonsole an. Die JSON-Feldspalte verwendet Punktnotation, um den Namen des Felds in JSON-Darstellungen von Ergebnissen und der Amazon Macie-API anzugeben. (Längere JSON-Feldnamen verwenden die Zeichenfolge für neue Zeilen (\n), um die Lesbarkeit zu verbessern.) Die Spalte Beschreibung enthält eine kurze Beschreibung der Daten, die das Feld speichert, und gibt alle Anforderungen für Filterwerte an. Die Tabelle wird in aufsteigender alphabetischer Reihenfolge nach Feld und dann nach JSON-Feld sortiert.

Feld	JSON-Feld	Beschreibung
—	`resourcesAffected.s3Bucket.createdAt`	Das Datum und die Uhrzeit, zu der der betroffene Bucket erstellt wurde, oder Änderungen wie Änderungen an der Bucket-Richtlinie wurden zuletzt am betroffenen Bucket vorgenommen. Dieses Feld ist in der Konsole nicht als Filteroption verfügbar. Mit der API können Sie dieses Feld verwenden, um einen Zeitraum für einen Filter zu definieren.
S3-Bucket-Standardverschlüsselung	`resourcesAffected.s3Bucket.defaultServerSideEncryption.encryptionType`	Der serverseitige Verschlüsselungsalgorithmus, der standardmäßig zum Verschlüsseln von Objekten verwendet wird, die dem betroffenen Bucket hinzugefügt werden. Die Konsole bietet eine Liste der Werte, aus denen Sie wählen können, wenn Sie dieses Feld zu einem Filter

Feld	JSON-Feld	Beschreibung
		hinzufügen. Eine Liste der gültigen Werte für die API finden Sie unter EncryptionType in der Amazon Macie-API-Referenz.
S3-Bucket-Verschlüsselung – KMS-Schlüssel-ID*	`resourcesAffected.s3Bucket.defaultServerSideEncryption.kmsMasterKeyId`	Der Amazon-Ressourcenname (ARN) oder die eindeutige Kennung (Schlüssel-ID) für die AWS KMS key, die standardmäßig zum Verschlüsseln von Objekten verwendet wird, die dem betroffenen Bucket hinzugefügt werden.
S3-Bucket-Verschlüsselung gemäß Bucket-Richtlinie erforderlich	`resourcesAffected.s3Bucket.allowsUnencryptedObjectUploads`	Gibt an, ob die Bucket-Richtlinie für den betroffenen Bucket eine serverseitige Verschlüsselung von Objekten erfordert, wenn Objekte zum Bucket hinzugefügt werden. Die Konsole bietet eine Liste der Werte, aus denen Sie wählen können, wenn Sie dieses Feld zu einem Filter hinzufügen. Eine Liste der gültigen Werte für die API finden Sie unter S3Bucket in der Amazon Macie-API-Referenz.
Name des S3-Buckets*	`resourcesAffected.s3Bucket.name`	Der vollständige Name des betroffenen Buckets.

Feld	JSON-Feld	Beschreibung
Anzeigename des S3-Bucket-Eigentümers*	`resourcesAffected.s3Bucket.owner.displayName`	Der Anzeigename des AWS Benutzers, dem der betroffene Bucket gehört.
Öffentliche Zugriffsberechtigung für S3-Buckets	`resourcesAffected.s3Bucket.publicAccess.effectivePermission`	Gibt an, ob der betroffene Bucket basierend auf einer Kombination von Berechtigungseinstellungen, die für den Bucket gelten, öffentlich zugänglich ist. Die Konsole bietet eine Liste der Werte, aus denen Sie wählen können, wenn Sie dieses Feld zu einem Filter hinzufügen. Eine Liste der gültigen Werte für die API finden Sie unter BucketPublicAccess in der Amazon Macie-API-Referenz.

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`accountLevelPermissions.blockPublicAccess.blockPublicAcls`
		Ein boolescher Wert, der angibt, ob Amazon S3 öffentliche Zugriffssteuerungslisten (ACLs) für den betroffenen Bucket und die Objekte im Bucket blockiert. Dies ist eine Einstellung zum Blockieren des öffentlichen Zugriffs auf Kontoebene für den Bucket.
		
		Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.

Feld	JSON-Feld	Beschreibung

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`accountLevelPermissions.blockPublicAccess.blockPublicPolicy`
		Ein boolescher Wert, der angibt, ob Amazon S3 öffentliche Bucket-Richtlinien für den betroffenen Bucket blockiert. Dies ist eine Einstellung zum Blockieren des öffentlichen Zugriffs auf Kontoebene für den Bucket.
		
		Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`accountLevelPermissions.blockPublicAccess.ignorePublicAcls`
		Ein boolescher Wert, der angibt, ob Amazon S3 öffentliche ACLs für den betroffenen Bucket und Objekte im Bucket ignoriert. Dies ist eine Einstellung zum Blockieren des öffentlichen Zugriffs auf Kontoebene für den Bucket.
		
		Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`accountLevelPermissions.blockPublicAccess.restrictPublicBuckets`
		Ein boolescher Wert, der angibt, ob Amazon S3 öffentliche Bucket-Richtlinien für den betroffenen Bucket einschränkt. Dies ist eine Einstellung zum Blockieren des öffentlichen Zugriffs auf Kontoebene für den Bucket.
		
		Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.

Feld	JSON-Feld	Beschreibung

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`bucketLevelPermissions.accessControlList.allowsPublicReadAccess`
		Ein boolescher Wert, der angibt, ob die ACL auf Bucket-Ebene für den betroffenen Bucket der allgemeinen Öffentlichkeit Lesezugriffsberechtigungen für den Bucket gewährt.
		
		Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`bucketLevelPermissions.accessControlList.allowsPublicWriteAccess`
		Ein boolescher Wert, der angibt, ob die ACL auf Bucket-Ebene für den betroffenen Bucket der allgemeinen Öffentlichkeit Schreibzugriffsberechtigungen für den Bucket gewährt.
		
		Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`bucketLevelPermissions.blockPublicAccess.blockPublicAcls`
		Ein boolescher Wert, der angibt, ob Amazon S3 öffentliche ACLs für den betroffenen Bucket und Objekte im Bucket blockiert. Dies ist eine Einstellung zum Blockieren des öffentlichen Zugriffs auf Bucket-Ebene für einen Bucket.
		
		Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.

Feld	JSON-Feld	Beschreibung

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`bucketLevelPermissions.blockPublicAccess.blockPublicPolicy`
		Ein boolescher Wert, der angibt, ob Amazon S3 öffentliche Bucket-Richtlinien für den betroffenen Bucket blockiert. Dies ist eine Einstellung zum Blockieren des öffentlichen Zugriffs auf Bucket-Ebene für den Bucket.
		
		Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`bucketLevelPermissions.blockPublicAccess.ignorePublicAcls`
		Ein boolescher Wert, der angibt, ob Amazon S3 öffentliche ACLs für den betroffenen Bucket und Objekte im Bucket ignoriert. Dies ist eine Einstellung zum Blockieren des öffentlichen Zugriffs auf Bucket-Ebene für den Bucket.
		
		Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`bucketLevelPermissions.blockPublicAccess.restrictPublicBuckets`
		Ein boolescher Wert, der angibt, ob Amazon S3 öffentliche Bucket-Richtlinien für den betroffenen Bucket einschränkt. Dies ist eine Einstellung zum Blockieren des öffentlichen Zugriffs auf Bucket-Ebene für den Bucket.
		
		Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.

Feld	JSON-Feld	Beschreibung

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`bucketLevelPermissions.bucketPolicy.allowsPublicReadAccess`
		Ein boolescher Wert, der angibt, ob die Richtlinie des betroffenen Buckets der allgemeinen Öffentlichkeit Lesezugriff auf den Bucket gewährt.
		
		Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`bucketLevelPermissions.bucketPolicy.allowsPublicWriteAccess`
		Ein boolescher Wert, der angibt, ob die Richtlinie des betroffenen Buckets der allgemeinen Öffentlichkeit Schreibzugriff auf den Bucket gewährt.
		
		Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.

S3-Bucket-Tag-Schlüssel*	`resourcesAffected.s3Bucket.tags.key`	Ein Tag-Schlüssel, der dem betroffenen Bucket zugeordnet ist.
S3-Bucket-Tag-Wert*	`resourcesAffected.s3Bucket.tags.value`	Ein Tag-Wert, der dem betroffenen Bucket zugeordnet ist.

* Um mehrere Werte für dieses Feld in der Konsole anzugeben, fügen Sie eine Bedingung hinzu, die das Feld verwendet und einen eindeutigen Wert für den Filter angibt, und wiederholen Sie diesen Schritt dann für jeden zusätzlichen Wert. Um dies mit der API zu tun, verwenden Sie ein Array, das die Werte auflistet, die für den Filter verwendet werden sollen.

S3-Objekt

In der folgenden Tabelle werden Felder aufgeführt und beschrieben, mit denen Sie Ergebnisse basierend auf den Eigenschaften des S3-Objekts filtern können, für das ein Ergebnis gilt.

In der Tabelle gibt die Spalte Feld den Namen des Feldes in der Amazon MacieKonsole an. Die JSON-Feldspalte verwendet Punktnotation, um den Namen des Feldes in JSON-Darstellungen von Erkenntnissen und der Amazon Macie-API anzugeben. Die Spalte Beschreibung enthält eine kurze Beschreibung der Daten, die das Feld speichert, und gibt alle Anforderungen für Filterwerte an. Die Tabelle wird in aufsteigender alphabetischer Reihenfolge nach Feld und dann nach JSON-Feld sortiert.

Feld	JSON-Feld	Beschreibung
KMS-Schlüssel-ID* der S3-Objektverschlüsselung	`resourcesAffected.s3Object.serverSideEncryption.kmsMasterKeyId`	Der Amazon-Ressourcenname (ARN) oder die eindeutige Kennung (Schlüssel-ID) für das AWS KMS key, das zum Verschlüsseln des betroffenen Objekts verwendet wurde.
S3-Objektverschlüsselungstyp	`resourcesAffected.s3Object.serverSideEncryption.encryptionType`	Der serverseitige Verschlüsselungsalgorithmus, der zur Verschlüsselung des betroffenen Objekts verwendet wurde. Die Konsole bietet eine Liste der Werte, aus denen Sie wählen können, wenn Sie dieses Feld zu einem Filter hinzufügen. Eine Liste der gültigen Werte für die API finden Sie unter EncryptionType in der Amazon Macie-API-Referenz.

Feld	JSON-Feld	Beschreibung
—	`resourcesAffected.s3Object.extension`	Die Dateinamenerweiterung des betroffenen Objekts. Geben Sie für Objekte, die keine Dateinamenerweiterung haben, `""` als Wert für den Filter an. Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.
—	`resourcesAffected.s3Object.lastModified`	Das Datum und die Uhrzeit, zu der das betroffene Objekt erstellt oder zuletzt geändert wurde, je nachdem, was zuletzt eintritt. Dieses Feld ist in der Konsole nicht als Filteroption verfügbar. Mit der API können Sie dieses Feld verwenden, um einen Zeitraum für einen Filter zu definieren.
S3-Objektschlüssel*	`resourcesAffected.s3Object.key`	Der vollständige Name (Schlüssel) des betroffenen Objekts, einschließlich des Präfixes des Objekts, falls zutreffend.

Feld	JSON-Feld	Beschreibung
—	`resourcesAffected.s3Object.path`	Der vollständige Pfad zum betroffenen Objekt, einschließlich des Namens des betroffenen Buckets und des Objektnamens (Schlüssel). Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.
Öffentlicher Zugriff auf S3-Objekte	`resourcesAffected.s3Object.publicAccess`	Ein boolescher Wert, der angibt, ob das betroffene Objekt öffentlich zugänglich ist, basierend auf einer Kombination von Berechtigungseinstellungen, die für das Objekt gelten. Die Konsole bietet eine Liste der Werte, aus denen Sie wählen können, wenn Sie dieses Feld zu einem Filter hinzufügen.
S3-Objekt-Tag-Schlüssel*	`resourcesAffected.s3Object.tags.key`	Ein Tag-Schlüssel, der dem betroffenen Objekt zugeordnet ist.
S3-Objekt-Tag-Wert*	`resourcesAffected.s3Object.tags.value`	Ein Tag-Wert, der dem betroffenen Objekt zugeordnet ist.

* Um mehrere Werte für dieses Feld in der Konsole anzugeben, fügen Sie eine Bedingung hinzu, die das Feld verwendet und einen eindeutigen Wert für den Filter angibt, und wiederholen Sie diesen

Schritt dann für jeden zusätzlichen Wert. Um dies mit der API zu tun, verwenden Sie ein Array, das die Werte auflistet, die für den Filter verwendet werden sollen.

Richtlinienfelder

In der folgenden Tabelle sind Felder aufgeführt und beschrieben, mit denen Sie Richtlinienergebnisse filtern können. Diese Felder speichern Daten, die für Richtlinienergebnisse spezifisch sind.

In der Tabelle gibt die Spalte Feld den Namen des Feldes in der Amazon MacieKonsole an. Die JSON-Feldspalte verwendet Punktnotation, um den Namen des Feldes in JSON-Darstellungen von Erkenntnissen und der Amazon Macie-API anzugeben. (Längere JSON-Feldnamen verwenden die Zeichenfolge für neue Zeilen (\n), um die Lesbarkeit zu verbessern.) Die Spalte Beschreibung enthält eine kurze Beschreibung der Daten, die das Feld speichert, und gibt alle Anforderungen für Filterwerte an. Die Tabelle wird in aufsteigender alphabetischer Reihenfolge nach Feld und dann nach JSON-Feld sortiert.

Feld	JSON-Feld	Beschreibung
Aktionstyp	`policyDetails.action.actionType`	Die Art der Aktion, die das Ergebnis erzeugt hat. Der einzige gültige Wert für dieses Feld ist `AWS_API_CALL` .
API-Aufrufname*	`policyDetails.action.apiCallDetails.api`	Der Name der Operation, die zuletzt aufgerufen und das Ergebnis erzeugt hat, z. B. `PutBucketPublicAccessBlock` .
API-Servicename*	`policyDetails.action.apiCallDetails.apiServiceName`	Die URL des AWS-Service, der die aufgerufene Operation bereitstellt und das Ergebnis erzeugt hat, z. B. `s3.amazonaws.com` .
—	`policyDetails.action.apiCallDetails.firstSeen`	Das erste Datum und die erste Uhrzeit, zu der eine Operation aufgerufen und das Ergebnis erzeugt wurde.

Feld	JSON-Feld	Beschreibung
		Dieses Feld ist in der Konsole nicht als Filteroption verfügbar. Mit der API können Sie dieses Feld verwenden, um einen Zeitraum für einen Filter zu definieren.
—	`policyDetails.action.apiCallDetails.lastSeen`	Das letzte Datum und die letzte Uhrzeit, zu der die angegebene Operation (API-Aufrufname oder `api`) aufgerufen und das Ergebnis erzeugt wurde. Dieses Feld ist in der Konsole nicht als Filteroption verfügbar. Mit der API können Sie dieses Feld verwenden, um einen Zeitraum für einen Filter zu definieren.
—	`policyDetails.actor.domainDetails.domainName`	Der Domänenname des Geräts, das zum Ausführen der Aktion verwendet wurde. Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.
IP-Stadt*	`policyDetails.actor.ipAddressDetails.ipCity.name`	Der Name der ursprünglichen Stadt für die IP-Adresse des Geräts, das zur Ausführung der Aktion verwendet wurde.

Feld	JSON-Feld	Beschreibung
IP-Land*	`policyDetails.actor.ipAddressDetails.ipCountry.name`	Der Name des Ursprungslandes für die IP-Adresse des Geräts, das zur Ausführung der Aktion verwendet wurde, z. B. `United States`.
—	`policyDetails.actor.ipAddressDetails.ipOwner.asn`	Die autonome Systemnummer (ASN) für das autonome System, das die IP-Adresse des Geräts enthielt, das zur Ausführung der Aktion verwendet wurde. Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.
ASN-Organisation des IP-Besitzers*	`policyDetails.actor.ipAddressDetails.ipOwner.asnOrg`	Die Organisations-ID, die der ASN für das autonome System zugeordnet ist, das die IP-Adresse des Geräts enthielt, das zur Ausführung der Aktion verwendet wurde.
IP-Besitzer-ISP*	`policyDetails.actor.ipAddressDetails.ipOwner.isp`	Der Name des Internetdienstanbieters (ISP), dem die IP-Adresse des Geräts gehörte, das zur Ausführung der Aktion verwendet wurde.
IP-V4-Adresse*	`policyDetails.actor.ipAddressDetails.ipAddressV4`	Die IPv4-Adresse (Internet Protocol Version 4) des Geräts, das zur Ausführung der Aktion verwendet wurde.

Feld	JSON-Feld	Beschreibung
—	`policyDetails.actor.userIdentity.assumedRole.accessKeyId`	Für eine Aktion, die mit temporären Sicherheitsanmeldeinformationen ausgeführt wurde, die mit der `AssumeRole` -Operation der AWS STSAPI abgerufen wurden, die AWS Zugriffsschlüssel-ID, die die Anmeldeinformationen identifiziert. Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.
Benutzeridentität hat Rolle übernommen Konto-ID*	`policyDetails.actor.userIdentity.assumedRole.accountId`	Bei einer Aktion, die mit temporären Sicherheitsanmeldeinformationen ausgeführt wurde, die mit der `AssumeRole` -Operation der AWS STS-API abgerufen wurden, die eindeutige Kennung für das AWS-Konto , das Eigentümer der Entität ist, die zum Abrufen der Anmeldeinformationen verwendet wurde.

Feld	JSON-Feld	Beschreibung
Benutzeridentität hat Rolle übernommen Prinzipal-ID*	`policyDetails.actor.userIdentity.assumedRole.principalId`	Für eine Aktion, die mit temporären Sicherheitsanmeldeinformationen ausgeführt wurde, die mit der AWS STS-`AssumeRole` Operation der API abgerufen wurden, die eindeutige Kennung für die Entität, die zum Abrufen der Anmeldeinformationen verwendet wurde.
ARN* für Sitzungen mit übernommener Benutzeridentität	`policyDetails.actor.userIdentity.assumedRole.arn`	Für eine Aktion, die mit temporären Sicherheitsanmeldeinformationen ausgeführt wurde, die mit der -`AssumeRole` Operation der AWS STS-API abgerufen wurden, der Amazon-Ressourcenname (ARN) des Quellkontos, des IAM-Benutzers oder der Rolle, die zum Abrufen der Anmeldeinformationen verwendet wurde.

Feld	JSON-Feld	Beschreibung
—	`policyDetails.actor.userIdentity.assumedRole.sessionContext.\n sessionIssuer.type`	Für eine Aktion, die mit temporären Sicherheitsanmeldeinformationen ausgeführt wurde, die mit der `-AssumeRole` Operation der AWS STS-API abgerufen wurden, die Quelle der temporären Sicherheitsanmeldeinformationen, z. B. `RootIAMUser`, oder `Role`. Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.
—	`policyDetails.actor.userIdentity.assumedRole.sessionContext.\n sessionIssuer.userName`	Bei einer Aktion, die mit temporären Sicherheitsanmeldeinformationen ausgeführt wurde, die mit der `-AssumeRole` Operation der AWS STS-API abgerufen wurden, der Name oder Alias des Benutzers oder der Rolle, der/die die Sitzung ausgegeben hat. Beachten Sie, dass dieser Wert null ist, wenn die Anmeldeinformationen von einem Stammkonto abgerufen wurden, das keinen Alias hat. Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.

Feld	JSON-Feld	Beschreibung
AWS Benutzeridentitätskonto-ID*	`policyDetails.actor.userIdentity.awsAccount.accountId`	Für eine Aktion, die mit den Anmeldeinformationen für ein anderes ausgeführt wirdAWS-Konto, die eindeutige Kennung für das Konto.
Prinzipal-ID des AWS Benutzeridentitätskontos*	`policyDetails.actor.userIdentity.awsAccount.principalId`	Für eine Aktion, die mit den Anmeldeinformationen für ein anderes ausgeführt wirdAWS-Konto, die eindeutige Kennung für die Entität, die die Aktion ausgeführt hat.
Vom aufgerufener AWS Benutzeridentitätsservice	`policyDetails.actor.userIdentity.awsService.invokedBy`	Bei einer Aktion, die von einem Konto ausgeführt wird, das zu einem gehörtAWS-Service, der Name des Services.
—	`policyDetails.actor.userIdentity.federatedUser.accessKeyId`	Für eine Aktion, die mit temporären Sicherheitsanmeldeinformationen ausgeführt wurde, die mit der `GetFederationToken`-Operation der AWS STSAPI abgerufen wurden, die AWS Zugriffsschlüssel-ID, die die Anmeldeinformationen identifiziert. Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.

Feld	JSON-Feld	Beschreibung
ARN* für Benutzeridentitäts verbundsitzungen	`policyDetails.actor.userIdentity.federatedUser.arn`	Bei einer Aktion, die mit temporären Sicherheitsanmeldeinformationen ausgeführt wurde, die mit der `GetFederationToken` -Operation der AWS STS-API abgerufen wurden, der ARN der Entität, die zum Abrufen der Anmeldeinformationen verwendet wurde.
Benutzeridentitätsverbundbenutzerkonto-ID*	`policyDetails.actor.userIdentity.federatedUser.accountId`	Bei einer Aktion, die mit temporären Sicherheitsanmeldeinformationen ausgeführt wurde, die mit der AWS STS-`GetFederationToken` Operation der API abgerufen wurden, die eindeutige Kennung für das AWS-Konto , das Eigentümer der Entität ist, die zum Abrufen der Anmeldeinformationen verwendet wurde.
Benutzeridentitätsverbundbenutzer-Prinzipal-ID*	`policyDetails.actor.userIdentity.federatedUser.principalId`	Für eine Aktion, die mit temporären Sicherheitsanmeldeinformationen ausgeführt wurde, die mithilfe der AWS STS-`GetFederationToken` Operation der API abgerufen wurden, die eindeutige Kennung für die Entität, die zum Abrufen der Anmeldeinformationen verwendet wurde.

Feld	JSON-Feld	Beschreibung
—	`policyDetails.actor.userIdentity.federatedUser.sessionContext.\n sessionIssuer.type`	Für eine Aktion, die mit temporären Sicherheitsanmeldeinformationen ausgeführt wurde, die mit der `GetFederationToken` Operation der AWS STS-API abgerufen wurden, die Quelle der temporären Sicherheitsanmeldeinformationen, z. B. `RootIAMUser`, oder `Role`. Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.
—	`policyDetails.actor.userIdentity.federatedUser.sessionContext.\n sessionIssuer.userName`	Bei einer Aktion, die mit temporären Sicherheitsanmeldeinformationen ausgeführt wurde, die mit der `GetFederationToken` Operation der AWS STS-API abgerufen wurden, der Name oder Alias des Benutzers oder der Rolle, der/die die Sitzung ausgegeben hat. Beachten Sie, dass dieser Wert null ist, wenn die Anmeldeinformationen von einem Stammkonto abgerufen wurden, das keinen Alias hat. Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.

Feld	JSON-Feld	Beschreibung
Benutzeridentität IAM-Konto-ID*	`policyDetails.actor.userIdentity.iamUser.accountId`	Für eine Aktion, die mit den Anmeldeinformationen eines IAM-Benutzers ausgeführt wird, die eindeutige Kennung für die AWS-Konto, die dem IAM-Benutzer zugeordnet ist, der die Aktion ausgeführt hat.
IAM-Prinzipal-ID der Benutzeridentität*	`policyDetails.actor.userIdentity.iamUser.principalId`	Für eine Aktion, die mit den Anmeldeinformationen eines IAM-Benutzers ausgeführt wird, die eindeutige Kennung für den IAM-Benutzer, der die Aktion ausgeführt hat.
IAM-Benutzername der Benutzeridentität*	`policyDetails.actor.userIdentity.iamUser.userName`	Bei einer Aktion, die mit den Anmeldeinformationen eines IAM-Benutzers ausgeführt wird, der Benutzername des IAM-Benutzers, der die Aktion ausgeführt hat.
Stammkonto-ID* der Benutzeridentität	`policyDetails.actor.userIdentity.root.accountId`	Für eine Aktion, die mit den Anmeldeinformationen für Ihr ausgeführt wirdAWS-Konto, die eindeutige Kennung für das Konto.
Stamm-Prinzipal-ID der Benutzeridentität*	`policyDetails.actor.userIdentity.root.principalId`	Für eine Aktion, die mit den Anmeldeinformationen für Ihr ausgeführt wirdAWS-Konto, die eindeutige Kennung für die Entität, die die Aktion ausgeführt hat.

Feld	JSON-Feld	Beschreibung
Benutzer-Identitätstyp	`policyDetails.actor.userIdentity.type`	Der Typ der Entität, die die Aktion ausgeführt hat, die das Ergebnis erzeugt hat. Die Konsole bietet eine Liste der Werte, aus denen Sie wählen können, wenn Sie dieses Feld zu einem Filter hinzufügen. Eine Liste der gültigen Werte für die API finden Sie unter UserIdentityType in der Amazon Macie-API-Referenz.

* Um mehrere Werte für dieses Feld in der Konsole anzugeben, fügen Sie eine Bedingung hinzu, die das Feld verwendet und einen eindeutigen Wert für den Filter angibt, und wiederholen Sie diesen Schritt dann für jeden zusätzlichen Wert. Um dies mit der API zu tun, verwenden Sie ein Array, das die Werte auflistet, die für den Filter verwendet werden sollen.

Klassifizierungsfelder für sensible Daten

In der folgenden Tabelle sind Felder aufgeführt und beschrieben, mit denen Sie Erkenntnisse zu sensiblen Daten filtern können. Diese Felder speichern Daten, die für Erkenntnisse zu sensiblen Daten spezifisch sind.

In der Tabelle gibt die Spalte Feld den Namen des Feldes in der Amazon MacieKonsole an. Die JSON-Feldspalte verwendet Punktnotation, um den Namen des Feldes in JSON-Darstellungen von Erkenntnissen und der Amazon Macie-API anzugeben. Die Spalte Beschreibung enthält eine kurze Beschreibung der Daten, die das Feld speichert, und gibt alle Anforderungen für Filterwerte an. Die Tabelle wird in aufsteigender alphabetischer Reihenfolge nach Feld und dann nach JSON-Feld sortiert.

Feld	JSON-Feld	Beschreibung
ID der benutzerdefinierten Datenkennung*	`classificationDetails.result.customDataIdentifiers.detections.arn`	Die eindeutige Kennung für die benutzerdefinierte Datenkennung, die die Daten erkannt und das Ergebnis erstellt hat.
Name der benutzerdefinierten Datenkennung*	`classificationDetails.result.customDataIdentifiers.detections.name`	Der Name der benutzerdefinierten Datenkennung, die die Daten erkannt und das Ergebnis erstellt hat.
Gesamtzahl der benutzerdefinierten Datenkennungen	`classificationDetails.result.customDataIdentifiers.detections.count`	Die Gesamtzahl der Vorkommen von Daten, die von benutzerdefinierten Datenkennungen erkannt und das Ergebnis erzeugt wurden. Sie können dieses Feld verwenden, um einen numerischen Bereich für einen Filter zu definieren.
Auftrags-ID*	`classificationDetails.jobId`	Die eindeutige Kennung für die Aufgabe zur Erkennung vertraulicher Daten, die das Ergebnis erzeugt hat.
Ursprungstyp	`classificationDetails.originType`	Wie Macie die sensiblen Daten gefunden hat, die das Ergebnis erzeugt haben: `AUTOMATED_SENSITIVE_DATA_DISCOVERY` oder `SENSITIVE_DATA_DISCOVERY_JOB` .

Feld	JSON-Feld	Beschreibung
—	`classificationDetails.result.mimeType`	Der Inhaltstyp als MIME-Typ, für den die Erkenntnis gilt, z. B. `text/csv` für eine CSV-Datei oder `application/pdf` für eine Adobe portable Document Format-Datei. Dieses Feld ist in der Konsole nicht als Filteroption verfügbar.
—	`classificationDetails.result.sizeClassified`	Die Gesamtspeichergröße des S3-Objekts in Byte, für das die Erkenntnis gilt. Dieses Feld ist in der Konsole nicht als Filteroption verfügbar. Mit der API können Sie dieses Feld verwenden, um einen numerischen Bereich für einen Filter zu definieren.

Feld	JSON-Feld	Beschreibung
Ergebnisstatuscode*	`classificationDetails.result.status.code`	Der Status der Erkenntnis. Gültige Werte für sind: • `COMPLETE` – Macie hat seine Analyse des Objekts abgeschlossen. • `PARTIAL` – Macie hat nur eine Teilmenge der Daten im Objekt analysiert. Das -Objekt ist beispielsweise eine Archivdatei, die Dateien in einem nicht unterstützten Format enthält. • `SKIPPED` – Macie konnte das Objekt nicht analysieren. Das -Objekt ist beispielsweise eine fehlerhafte Datei.
Kategorie sensibler Daten	`classificationDetails.result.sensitiveData.category`	Die Kategorie der sensiblen Daten, die erkannt und das Ergebnis erzeugt haben. Die Konsole bietet eine Liste der Werte, aus denen Sie wählen können, wenn Sie dieses Feld zu einem Filter hinzufügen. In der API sind die gültigen Werte: `CREDENTIALS` `FINANCIAL_INFORMATION` , und `PERSONAL_INFORMATION` .

Feld	JSON-Feld	Beschreibung
Erkennungstyp für sensible Daten	`classificationDetails.result.sensitiveData.detections.type`	Die Art der sensiblen Daten, die erkannt und das Ergebnis erzeugt haben. Die Konsole bietet eine Liste der Werte, aus denen Sie wählen können, wenn Sie dieses Feld zu einem Filter hinzufügen. Eine Liste der gültigen Werte sowohl für die Konsole als auch für die API finden Sie unter Erkennungstypen für sensible Daten.
Gesamtzahl sensibler Daten	`classificationDetails.result.sensitiveData.detections.count`	Die Gesamtzahl der Vorkommen der sensiblen Daten, die erkannt und das Ergebnis erzeugt haben. Sie können dieses Feld verwenden, um einen numerischen Bereich für einen Filter zu definieren.

* Um mehrere Werte für dieses Feld in der Konsole anzugeben, fügen Sie eine Bedingung hinzu, die das Feld verwendet und einen eindeutigen Wert für den Filter angibt, und wiederholen Sie diesen Schritt dann für jeden zusätzlichen Wert. Um dies mit der API zu tun, verwenden Sie ein Array, das die Werte auflistet, die für den Filter verwendet werden sollen.

Erkennungstypen für sensible Daten

In den folgenden Themen werden Werte aufgeführt, die Sie für das Feld Erkennungstyp sensibler Daten in einem Filter angeben können. (Der JSON-Name dieses Felds lautet `classificationDetails.result.sensitiveData.detections.type`.) Die Themen sind nach Kategorien sensibler Daten organisiert, die Macie mithilfe verwalteter Datenkennungen erkennen kann.

Kategorien

- Anmeldeinformationen
- Finanzinformationen
- Persönliche Informationen: Persönliche Gesundheitsinformationen (PHI)
- Persönliche Informationen: Persönlich identifizierbare Informationen (PII)

Weitere Informationen zur verwalteten Datenkennung für einen bestimmten Typ sensibler Daten finden Sie unter Ausführliche Referenz: Von Amazon Macie verwaltete Datenkennungen.

Anmeldeinformationen

Sie können die folgenden Werte angeben, um Ergebnisse zu filtern, die Vorkommen von Anmeldeinformationsdaten in S3-Objekten melden.

Sensibler Datentyp	Filterwert
Geheimer AWS-Zugriffsschlüssel	`AWS_CREDENTIALS`
Google-Cloud-API-Schlüssel	`GCP_API_KEY`
HTTP Basic Authorization-Header	`HTTP_BASIC_AUTH_HEADER`
JSON-Web-Token (JWT)	`JSON_WEB_TOKEN`
Privater OpenSSH-Schlüssel	`OPENSSH_PRIVATE_KEY`
Privater PGP-Schlüssel	`PGP_PRIVATE_KEY`
Privater Schlüssel des Public Key Cryptography Standard (PKCS)	`PKCS`
Privater PuTTY-Schlüssel	`PUTTY_PRIVATE_KEY`
Stripe-API-Schlüssel	`STRIPE_CREDENTIALS`

Finanzinformationen

Sie können die folgenden Werte angeben, um Erkenntnisse zu filtern, die Vorkommen von Finanzinformationen in S3-Objekten melden.

Sensibler Datentyp	Filterwert
Bankkontonummer	`BANK_ACCOUNT_NUMBER` (für Kanada und die USA)
Grundlegende Bankkontonummer (BBAN)	Je nach Land oder Region: `FRANCE_BANK_ACCOUNT_NUMBER`, `GERMANY_BANK_ACCOUNT_NUMBER`, `ITALY_BANK_ACCOUNT_NUMBER`, `SPAIN_BANK_ACCOUNT_NUMBER`, `UK_BANK_ACCOUNT_NUMBER`
Ablaufdatum der Kreditkarte	`CREDIT_CARD_EXPIRATION`
Daten zu Kreditkarten-Magnetstrips	`CREDIT_CARD_MAGNETIC_STRIPE`
Kreditkartennummer	`CREDIT_CARD_NUMBER` (für Kreditkartennummern in der Nähe eines Schlüsselworts), `CREDIT_CARD_NUMBER_(NO_KEYWORD)` (für Kreditkartennummern, die sich nicht in der Nähe eines Schlüsselworts befinden)
Bestätigungscode für die Kreditkarte	`CREDIT_CARD_SECURITY_CODE`
Internationale Bankkontonummer (IBAN)	Je nach Land oder Region: `ALBANIA_BANK_ACCOUNT_NUMBER`, `ANDORRA_BANK_ACCOUNT_NUMBER`, `BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER`, `BRAZIL_BANK_ACCOUNT_NUMBER`, `BULGARIA_BANK_ACCOUNT_NUMBER`, `COSTA_RICA_BANK_ACCOUNT_NUMBER`, `CROATIA_BANK_ACCOUNT_NUMBER`, `CYPRUS_BANK_ACCOUNT_NUMBER`, `CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER`, `DENMARK_BANK_ACCOUNT_NUMBER`, `DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER`, `EGYPT_BA`

Sensibler Datentyp	Filterwert
	NK_ACCOUNT_NUMBER, ESTONIA_B ANK_ACCOUNT_NUMBER, FAROE_IS LANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER , GREENLAND_BANK_ACCOUNT_NUMB ER, HUNGARY_BANK_ACCOUNT_NUMBE R, ICELAND_BANK_ACCOUNT_NUMBER , IRELAND_BANK_ACCOUNT_NUMBE R, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER , KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT _NUMBER, LITHUANIA_BANK_AC COUNT_NUMBER, MALTA_BANK_ACCOUNT _NUMBER, MAURITANIA_BANK_A CCOUNT_NUMBER, MAURITIU S_BANK_ACCOUNT_NUMBER, MONACO_BA NK_ACCOUNT_NUMBER, MONTENEG RO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_N UMBER, NORTH_MACEDONIA_B ANK_ACCOUNT_NUMBER, POLAND_B ANK_ACCOUNT_NUMBER, PORTUGAL_ BANK_ACCOUNT_NUMBER, SAN_MARI NO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER , SLOVAKIA_BANK_ACCOUNT_NUMBE R, SLOVENIA_BANK_ACCOUNT_NUMB ER, SPAIN_BANK_ACCOUNT_NUMBER,

Sensibler Datentyp	Filterwert
	SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER (für die Britischen Jungferninseln)

Persönliche Informationen: Persönliche Gesundheitsinformationen (PHI)

Sie können die folgenden Werte angeben, um Erkenntnisse zu filtern, die Vorkommen persönlicher Gesundheitsinformationen (PHI) in S3-Objekten melden.

Sensibler Datentyp	Filterwert
Registrierungsnummer der Telefoniebehörde (DEA)	US_DRUG_ENFORCEMENT_AGENCY_NUMBER
Health Insurance Claim Number (HICN)	USA_HEALTH_INSURANCE_CLAIM_NUMBER
Krankenversicherungs- oder medizinische Identifizierungsnummer	Je nach Land oder Region: CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER

Sensibler Datentyp	Filterwert
Code des Common Procedure Coding System (HCPCS) von Telefonie	`USA_HEALTHCARE_PROCEDURE_CODE`
Nationaler Nationaler Nationaler Jungferncode (NDC)	`USA_NATIONAL_DRUG_CODE`
National Provider Identifier (NPI)	`USA_NATIONAL_PROVIDER_IDENTIFIER`
Eindeutige Gerätekennung (UDI)	`MEDICAL_DEVICE_UDI`

Persönliche Informationen: Persönlich identifizierbare Informationen (PII)

Sie können die folgenden Werte angeben, um Erkenntnisse zu filtern, die Vorkommen von persönlich identifizierbaren Informationen (PII) in S3-Objekten melden.

Sensibler Datentyp	Filterwert
Geburtsdatum	`DATE_OF_BIRTH`
Identifikationsnummer des Führerscheins	Je nach Land oder Region: `AUSTRALIA_DRIVERS_LICENSE`, `AUSTRIA_DRIVERS_LICENSE`, `BELGIUM_DRIVERS_LICENSE`, `BULGARIA_DRIVERS_LICENSE`, `CANADA_DRIVERS_LICENSE`, `CROATIA_DRIVERS_LICENSE`, `CYPRUS_DRIVERS_LICENSE`, `CZECHIA_DRIVERS_LICENSE`, `DENMARK_DRIVERS_LICENSE`, `DRIVERS_LICENSE` (für die USA), `ESTONIA_DRIVERS_LICENSE`, `FINLAND_DRIVERS_LICENSE`, `FRANCE_DRIVERS_LICENSE`, `GERMANY_DRIVERS_LICENSE`, `GREECE_DRIVERS_LICENSE`, `HUNGARY_D`

Sensibler Datentyp	Filterwert
	RIVERS_LICENSE, INDIA_DR IVERS_LICENSE, IRELAND_D RIVERS_LICENSE, ITALY_DR IVERS_LICENSE, LATVIA_DR IVERS_LICENSE, LITHUANI A_DRIVERS_LICENSE, LUXEMBOUR G_DRIVERS_LICENSE, MALTA_DR IVERS_LICENSE, NETHERLAN DS_DRIVERS_LICENSE, POLAND_D RIVERS_LICENSE, PORTUGAL_ DRIVERS_LICENSE, ROMANIA_ DRIVERS_LICENSE, SLOVAKIA_ DRIVERS_LICENSE, SLOVENIA _DRIVERS_LICENSE, SPAIN_DRI VERS_LICENSE, SWEDEN_D RIVERS_LICENSE, UK_DRIVER S_LICENSE
Nummer der Wählerliste	UK_ELECTORAL_ROLL_NUMBER
Vollständiger Name	NAME
Globale Positionierungssystem (GPS)-Koo rdinaten	LATITUDE_LONGITUDE
HTTP-Cookie	HTTP_COOKIE
Postanschrift	ADDRESS, BRAZIL_CEP_CODE
Nationale Identifikationsnummern	Je nach Land oder Region: BRAZIL_RG _NUMBER, FRANCE_NATIONAL_I DENTIFICATION_NUMBER, GERMANY_ NATIONAL_IDENTIFICATION_NUM BER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATI ON_NUMBER, SPAIN_DNI_NUMBER

Sensibler Datentyp	Filterwert
Nationale Versicherungsnummer (NINO)	`UK_NATIONAL_INSURANCE_NUMBER`
Passnummer	Je nach Land oder Region: `CANADA_PASSPORT_NUMBER`, `FRANCE_PASSPORT_NUMBER`, `GERMANY_PASSPORT_NUMBER`, `ITALY_PASSPORT_NUMBER`, `SPAIN_PASSPORT_NUMBER`, `UK_PASSPORT_NUMBER`, `USA_PASSPORT_NUMBER`
Ständige Wohnsitznummer	`CANADA_NATIONAL_IDENTIFICATION_NUMBER`
Phone number (Telefonnummer)	Abhängig von Land oder Region: `BRAZIL_PHONE_NUMBER`, `FRANCE_PHONE_NUMBER`, `GERMANY_PHONE_NUMBER`, `ITALY_PHONE_NUMBER`, `PHONE_NUMBER` (für Kanada und die USA) `SPAIN_PHONE_NUMBER`, `UK_PHONE_NUMBER`
Sozialversicherungsnummer (SIN)	`CANADA_SOCIAL_INSURANCE_NUMBER`
Sozialversicherungsnummer (SSN)	Je nach Land oder Region: `SPAIN_SOCIAL_SECURITY_NUMBER`, `USA_SOCIAL_SECURITY_NUMBER`

Sensibler Datentyp	Filterwert
Steuerpflichtigen-Identifikationsnummer oder Referenznummer	Je nach Land oder Region: `AUSTRALIA_TAX_FILE_NUMBER`, `BRAZIL_CNPJ_NUMBER`, `BRAZIL_CPF_NUMBER`, `FRANCE_TAX_IDENTIFICATION_NUMBER`, `GERMANY_TAX_IDENTIFICATION_NUMBER`, `INDIA_PERMANENT_ACCOUNT_NUMBER`, `SPAIN_NIE_NUMBER`, `SPAIN_NIF_NUMBER`, `SPAIN_TAX_IDENTIFICATION_NUMBER`, `UK_TAX_IDENTIFICATION_NUMBER`, `USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER`
Fahrzeugidentifikationsnummer (VIN)	`VEHICLE_IDENTIFICATION_NUMBER`

Untersuchung sensibler Daten anhand der Ergebnisse von Amazon Macie

Wenn Sie Aufträge zur Erkennung vertraulicher Daten ausführen oder Amazon Macie eine automatische Erkennung sensibler Daten durchführt, erfasst Macie Details über den Standort jedes Vorkommens vertraulicher Daten, die es in Amazon Simple Storage Service (Amazon S3) -Objekten findet. Dazu gehören sensible Daten, die Macie anhand verwalteter Datenkennungen erkennt, und Daten, die den Kriterien von benutzerdefinierten Datenbezeichnern entsprechen, für deren Verwendung Sie einen Job oder Macie konfigurieren.

Bei Ergebnissen vertraulicher Daten können Sie diese Details auf bis zu 15 Vorkommen sensibler Daten überprüfen, die Macie in einzelnen S3-Objekten findet. Die Details geben Aufschluss über die Bandbreite der Kategorien und Typen sensibler Daten, die bestimmte S3-Buckets und -Objekte enthalten können. Sie können Ihnen dabei helfen, einzelne Vorkommen sensibler Daten in Objekten zu lokalisieren und zu entscheiden, ob bestimmte Buckets und Objekte eingehender untersucht werden sollten.

Für zusätzliche Einblicke können Sie Macie optional konfigurieren und verwenden, um Stichproben sensibler Daten abzurufen, die Macie als Einzelergebnisse meldet. Anhand der Beispiele können Sie die Art der sensiblen Daten überprüfen, die Macie gefunden hat. Sie können Ihnen auch dabei helfen, Ihre Untersuchung eines betroffenen S3-Buckets und -Objekts maßgeschneidert zu gestalten. Wenn Sie für einen Befund Stichproben sensibler Daten abrufen möchten, verwendet Macie die im Ergebnis enthaltenen Daten, um 1—10 Vorkommen jeder Art von sensiblen Daten zu lokalisieren, die durch den Befund gemeldet wurden. Macie extrahiert dann diese Vorkommen sensibler Daten aus dem betroffenen Objekt und zeigt die Daten zur Überprüfung an.

Wenn ein S3-Objekt viele Vorkommen vertraulicher Daten enthält, kann Ihnen ein Ergebnis auch dabei helfen, zum entsprechenden Erkennungsergebnis vertraulicher Daten zu gelangen. Im Gegensatz zu einer Entdeckung vertraulicher Daten liefert ein Erkennungsergebnis vertraulicher Daten detaillierte Standortdaten für bis zu 1.000 Vorkommen jedes Typs vertraulicher Daten, die Macie in einem Objekt findet. Macie verwendet dasselbe Schema für Standortdaten bei Ergebnissen sensibler Daten und bei der Entdeckung sensibler Daten. Weitere Informationen zu den Ergebnissen der Erkennung sensibler Daten finden Sie unterSpeicherung und Beibehaltung der Erkennungsergebnisse von vertraulichen Daten.

In den Themen dieses Abschnitts wird erläutert, wie Sie anhand von Ergebnissen vertraulicher Daten gemeldete Vorkommen sensibler Daten lokalisieren und optional abrufen können. Außerdem wird das Schema erklärt, das Macie verwendet, um den Standort einzelner Vorkommen vertraulicher Daten, die Macie findet, zu melden.

Themen

- Auffinden vertraulicher Daten mit den Ergebnissen von Amazon Macie
- Abrufen sensibler Datenproben mit Amazon Macie Macie-Ergebnissen
- JSON-Schema für sensible Datenspeicherorte

Auffinden vertraulicher Daten mit den Ergebnissen von Amazon Macie

Wenn Sie Aufträge zur Erkennung vertraulicher Daten ausführen oder Amazon Macie die automatische Erkennung vertraulicher Daten durchführt, führt Macie eine gründliche Inspektion der neuesten Version jedes Amazon Simple Storage Service (Amazon S3) -Objekts durch, das es analysiert. Für jede Auftragsausführung oder jeden Analysezyklus verwendet Macie außerdem einen Algorithmus zur Tiefensuche, um die resultierenden Ergebnisse mit Details über den Standort bestimmter Vorkommen vertraulicher Daten zu füllen, die Macie in S3-Objekten findet. Diese Vorkommen eines jeden Typs sensibler Daten, die ein betroffenes S3-Bucket und -Objekt enthalten

kann. Anhand dieser Informationen können Sie einzelne Vorkommen sensibler Daten in Objekten lokalisieren und entscheiden, ob Sie bestimmte Buckets und Objekte eingehender untersuchen sollten.

Anhand vertraulicher Daten können Sie den Standort von bis zu 15 Vorkommen vertraulicher Daten ermitteln, die Macie in einem betroffenen S3-Objekt gefunden hat. Dazu gehören vertrauliche Daten, die Macie mithilfe verwalteter Datenkennungen erkannt hat, und Daten, die den Kriterien benutzerdefinierter Datenkennungen entsprechen, die Sie für einen Job konfiguriert haben oder für deren Verwendung Macie konfiguriert hat.

Ein Fund sensibler Daten kann folgende Informationen liefern:

- Die Spalten- und Zeilennummer für eine Zelle oder ein Feld in einer Microsoft Excel-Arbeitsmappe, CSV-Datei oder TSV-Datei.
- Der Pfad zu einem Feld oder Array in einer JSON- oder JSON Lines-Datei.
- Die Zeilennummer für eine Zeile in einer nichtbinären Textdatei, bei der es sich nicht um eine CSV-, JSON-, JSON-Zeilen- oder TSV-Datei handelt, z. B. eine HTML-, TXT- oder XML-Datei.
- Die Seitenzahl für eine Seite in einer PDF-Datei (Adobe Portable Document Format).
- Der Datensatzindex und der Pfad zu einem Feld in einem Datensatz in einem Apache Avro-Objektcontainer oder einer Apache Parquet-Datei.

Sie können auf diese Details zugreifen, indem Sie die Amazon-Macie-Konsole oder die Amazon-Macie-API verwenden. Sie können auf diese Details auch in Ergebnissen zugreifen, die Macie bei anderen veröffentlichtAWS-Services, EventBridge sowohl AWS Security Hub bei Amazon als auch. Weitere Informationen zu den JSON-Strukturen, die Macie verwendet, um diese Details zu melden, finden Sie unterJSON-Schema für sensible Datenspeicherorte. Informationen zum Zugriff auf die Details in Ergebnissen, die Macie für andere veröffentlichtAWS-Services, finden Sie unterÜberwachung und Verarbeitung von Ergebnissen.

Wenn ein S3-Objekt viele Vorkommen vertraulicher Daten enthält, können Sie mithilfe eines Ergebnisses auch zum entsprechenden Ergebnis der Erkennung vertraulicher Daten navigieren. Im Gegensatz zu Ergebnissen der Erkennung sensibler Daten, die Macie erkennt und die in Ergebnissen der Erkennung sensibler Daten detaillierte Standortdaten bereitstellt. Wenn es sich bei einem S3-Objekt um eine Archivdatei handelt, z. B. eine .tar- oder .zip-Datei, schließt dies das Vorkommen vertraulicher Daten in einzelnen Dateien ein, die Macie aus dem Archiv extrahiert hat. (Macie bezieht diese Informationen nicht in die Ergebnisse vertraulicher Daten ein.) Weitere Informationen zu den Ergebnissen der Erkennung vertraulicher Daten finden Sie unterSpeicherung und Beibehaltung

der Erkennungsergebnisse von vertraulichen Daten. Macie verwendet dasselbe Schema für Standortdaten in vertraulichen Datenergebnissen und Ergebnissen der Erkennung vertraulicher Daten.

Auffinden von Vorkommen sensibler Daten

Um das Vorkommen vertraulicher Daten zu lokalisieren, können Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden. In den folgenden Schritten wird erläutert, wie Sie mithilfe der Konsole nach sensiblen Daten suchen können.

Verwenden Sie den GetFindingsBetrieb der Amazon Macie Macie-API, um sensible Daten programmgesteuert zu finden. Wenn ein Befund Details über den Ort eines oder mehrerer Vorkommen eines bestimmten Typs sensibler Daten enthält, liefern die `occurrences` Objekte im Befund diese Informationen. Weitere Informationen finden Sie unter JSON-Schema für sensible Datenspeicherorte.

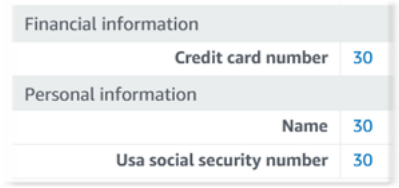
Um das Vorkommen sensibler Daten zu lokalisieren

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich Findings aus.

   > **Tip**
   >
   > Sie können die Seite Jobs verwenden, um alle Ergebnisse eines bestimmten Auftrags zur Erkennung vertraulicher Daten anzuzeigen. Wählen Sie dazu im Navigationsbereich die Option Jobs und dann den Namen des Jobs aus. Wählen Sie oben im Detailbereich Ergebnisse anzeigen und anschließend Ergebnisse anzeigen aus.

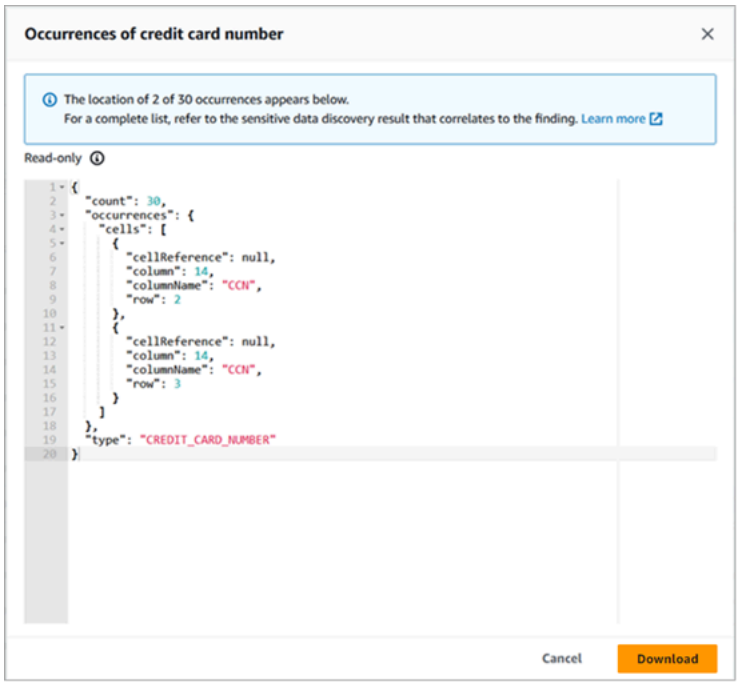
3. Wählen Sie auf der Seite Ergebnisse den Befund für die vertraulichen Daten aus, nach denen Sie suchen möchten. Im Detailfenster werden Informationen zum Ergebnisses angezeigt.
4. Scrollen Sie im Detailbereich zum Abschnitt Vertrauliche Daten. Dieser Abschnitt enthält Informationen zu den Kategorien und Arten von sensiblen Daten, die Macie im betroffenen S3-Objekt gefunden hat kann. Es zeigt auch die Anzahl von Vorkommen eines jeden Typs sensibler Daten, die Macie erkennt kann.

   Die folgende Abbildung zeigt beispielsweise einige Details eines Ergebnisses, das 30 Vorkommen von Kreditkartennummern, 30 Vorkommen von Namen und 30 Vorkommen von US-Sozialversicherungsnummern meldet.



Wenn das Ergebnis Details über den Standort eines oder mehrerer Vorkommen eines bestimmten Typs sensibler Daten enthält, ist die Anzahl der Vorkommen ein Zusammenhang. Wählen Sie den Link, um die Details anzuzeigen. Macie öffnet ein neues Fenster und zeigt die Details im JSON-Format an.

Die folgende Abbildung zeigt beispielsweise die Position von zwei Vorkommen von Kreditkartennummern in einem betroffenen S3-Objekt.



Um die Details als JSON-Datei zu speichern, wählen Sie Herunterladen und geben Sie dann einen Namen und Speicherort für die Datei an.

5. (Optional) Um alle Details des Ergebnisses als JSON-Datei zu speichern, wählen Sie oben im Detailbereich die Kennung des Ergebnisses (Finding-ID) aus. Macie öffnet ein neues Fenster und zeigt alle Details im JSON-Format an. Wählen Sie Herunterladen und geben Sie dann einen Namen und einen Speicherort für die Datei an.

Informationen zum Speicherort von bis zu 1.000 Vorkommen jeder Art von sensiblen Daten im betroffenen Objekt finden Sie im entsprechenden Ergebnis der Entdeckung vertraulicher Daten für

den Befund. Scrollen Sie dazu zum Anfang des Detailbereichs des Panels. Wählen Sie dann den Link im Feld Detaillierte Position des Ergebnisses aus. Macie öffnet die Amazon S3 S3-Konsole und zeigt die Datei oder den Ordner an, der das entsprechende Ermittlungsergebnis enthält.

Abrufen sensibler Datenproben mit Amazon Macie Macie-Ergebnissen

Um die Art der sensiblen Daten zu überprüfen, die Amazon Macie in Ergebnissen meldet, können Sie Macie optional so konfigurieren und verwenden, dass Stichproben sensibler Daten abgerufen und angezeigt werden, die von einzelnen Ergebnissen gemeldet wurden. Dazu gehören sensible Daten, die Macie anhand verwalteter Datenkennungen erkennt, sowie Daten, die den Kriterien von benutzerdefinierten Datenkennungen entsprechen. Die Beispiele können Ihnen helfen, Ihre Untersuchung eines betroffenen Amazon Simple Storage Service (Amazon S3) -Objekts und -Buckets auf Ihre Bedürfnisse zuzuschneiden.

Wenn Sie sensible Datenproben für einen Befund abrufen und offenlegen, führt Macie die folgenden allgemeinen Aufgaben aus:

1. Überprüft, ob der Befund den Standort einzelner Vorkommen vertraulicher Daten und den Ort eines entsprechenden Ergebnisses der Entdeckung sensibler Daten angibt.
2. Wertet das entsprechende Erkennungsergebnis vertraulicher Daten aus und überprüft die Gültigkeit der Metadaten für das betroffene S3-Objekt und der Standortdaten auf das Vorkommen sensibler Daten im Objekt.
3. Findet mithilfe von Daten im Ermittlungsergebnis vertraulicher Daten die ersten 1—10 Vorkommen sensibler Daten, die durch den Befund gemeldet wurden, und extrahiert die ersten 1—128 Zeichen jedes Vorkommens aus dem betroffenen S3-Objekt. Wenn das Ergebnis mehrere Typen vertraulicher Daten meldet, führt Macie dies für bis zu 100 Typen durch.
4. Verschlüsselt die extrahierten Daten mit einem von Ihnen AWS KMS angegebenen Schlüssel AWS Key Management Service ().
5. Speichert die verschlüsselten Daten vorübergehend in einem Cache und zeigt die Daten zur Überprüfung an. Die Daten sind jederzeit verschlüsselt, sowohl bei der Übertragung als auch bei der Speicherung.
6. Kurz nach dem Extrahieren und Verschlüsseln werden die Daten dauerhaft aus dem Cache gelöscht, es sei denn, eine zusätzliche Aufbewahrung ist vorübergehend erforderlich, um ein Betriebsproblem zu lösen.

Wenn Sie sich dafür entscheiden, sensible Datenproben für einen Fund erneut abzurufen und offenzulegen, wiederholt Macie diese Aufgaben, um die Proben zu finden, zu extrahieren, zu verschlüsseln, zu speichern und schließlich zu löschen.

Macie verwendet die mit dem Dienst verknüpfte Macie-Rolle für Ihr Konto nicht, um diese Aufgaben auszuführen. Stattdessen verwenden Sie Ihre AWS Identity and Access Management (IAM-) Identität oder erlauben Macie, eine IAM-Rolle in Ihrem Konto anzunehmen. Sie können Stichproben sensibler Daten abrufen und offenlegen, um festzustellen, ob Sie oder die Rolle auf die erforderlichen Ressourcen und Daten zugreifen und die erforderlichen Aktionen ausführen dürfen. Alle erforderlichen Aktionen sind angemeldet. AWS CloudTrail

> **Important**
>
> Wir empfehlen, den Zugriff auf diese Funktion mithilfe benutzerdefinierter IAM-Richtlinien einzuschränken. Für eine zusätzliche Zugriffskontrolle empfehlen wir, dass Sie auch eine spezielle Lösung AWS KMS key für die Verschlüsselung von Stichproben einrichten, die abgerufen werden, und die Verwendung des Schlüssels nur auf die Prinzipale beschränken, denen das Abrufen und Offenlegen vertraulicher Datenproben gestattet sein muss. Empfehlungen und Beispiele für Richtlinien, mit denen Sie den Zugriff auf diese Funktion kontrollieren können, finden Sie im Blogbeitrag How to use Amazon Macie to preview sensitive data in S3 Buckets im AWSSecurity Blog.

In den Themen dieses Abschnitts wird erklärt, wie Macie konfiguriert und verwendet wird, um Stichproben sensibler Daten abzurufen und für Ergebnisse offenzulegen. Sie können diese Aufgaben in allen Regionen ausführen, in AWS-Regionen denen Macie derzeit verfügbar ist, mit Ausnahme der Regionen Asien-Pazifik (Osaka) und Israel (Tel Aviv).

Themen

- Konfigurationsoptionen und Anforderungen für den Abruf sensibler Datenproben mit Ergebnissen
- Konfiguration von Amazon Macie für den Abruf und die Offenlegung sensibler Datenproben mit Ergebnissen
- Abrufen und Offenlegen sensibler Datenproben mit Befunden

Konfigurationsoptionen und Anforderungen für den Abruf sensibler Datenproben mit Ergebnissen

Sie können Amazon Macie optional konfigurieren und verwenden, um Stichproben vertraulicher Daten abzurufen und offenzulegen, die Macie in einzelnen Ergebnissen meldet. Wenn Sie Stichproben sensibler Daten für einen Befund abrufen und offenlegen, verwendet Macie die Daten im entsprechenden Ermittlungsergebnis für sensible Daten, um das Vorkommen sensibler Daten im betroffenen Amazon Simple Storage Service (Amazon S3) -Objekt zu lokalisieren. Macie extrahiert dann Proben dieser Vorkommnisse aus dem betroffenen Objekt. Macie verschlüsselt die extrahierten Daten mit einem von Ihnen angegebenen Schlüssel AWS Key Management Service (AWS KMS), speichert die verschlüsselten Daten vorübergehend in einem Cache und gibt die Daten in Ihren Ergebnissen für die Suche zurück. Kurz nach dem Extrahieren und Verschlüsseln löscht Macie die Daten dauerhaft aus dem Cache, es sei denn, eine zusätzliche Aufbewahrung ist vorübergehend erforderlich, um ein Betriebsproblem zu lösen.

Macie verwendet die mit dem Dienst verknüpfte Macie-Rolle für Ihr Konto nicht, um sensible Datenproben für betroffene S3-Objekte zu finden, abzurufen, zu verschlüsseln oder offenzulegen. Stattdessen verwendet Macie Einstellungen und Ressourcen, die Sie für Ihr Konto konfigurieren. Wenn Sie die Einstellungen in Macie konfigurieren, geben Sie an, wie auf die betroffenen S3-Objekte zugegriffen werden soll. Sie geben auch an, welches AWS KMS key zum Verschlüsseln der Samples verwendet werden soll. Sie können die Einstellungen in allen Regionen konfigurieren, in AWS-Regionen denen Macie derzeit verfügbar ist, mit Ausnahme der Regionen Asien-Pazifik (Osaka) und Israel (Tel Aviv).

Um auf betroffene S3-Objekte zuzugreifen und sensible Datenproben von ihnen abzurufen, haben Sie zwei Möglichkeiten. Sie können Macie so konfigurieren, dass es AWS Identity and Access Management (IAM-) Benutzeranmeldedaten verwendet oder eine IAM-Rolle übernimmt:

- IAM-Benutzeranmeldedaten verwenden — Bei dieser Option verwendet jeder Benutzer Ihres Kontos seine individuelle IAM-Identität, um die Beispiele zu finden, abzurufen, zu verschlüsseln und offenzulegen. Das bedeutet, dass ein Benutzer sensible Datenproben abrufen und offenlegen kann, um festzustellen, ob er auf die erforderlichen Ressourcen und Daten zugreifen und die erforderlichen Aktionen ausführen darf.
- Nehmen Sie eine IAM-Rolle an — Mit dieser Option erstellen Sie eine IAM-Rolle, die den Zugriff an Macie delegiert. Sie stellen außerdem sicher, dass die Vertrauens- und Berechtigungsrichtlinien für die Rolle alle Voraussetzungen erfüllen, damit Macie die Rolle übernehmen kann. Macie übernimmt dann die Rolle, wenn ein Benutzer Ihres Kontos entscheidet, sensible Datenproben zu finden, abzurufen, zu verschlüsseln und offenzulegen, um eine Entdeckung zu machen.

Sie können beide Konfigurationen mit jeder Art von Macie-Konto verwenden — dem delegierten Macie-Administratorkonto für eine Organisation, einem Macie-Mitgliedskonto in einer Organisation oder einem eigenständigen Macie-Konto.

In den folgenden Themen werden Optionen, Anforderungen und Überlegungen erläutert, anhand derer Sie festlegen können, wie Sie die Einstellungen und Ressourcen für Ihr Konto konfigurieren. Dazu gehören die Vertrauens- und Berechtigungsrichtlinien, die einer IAM-Rolle zugewiesen werden können. Weitere Empfehlungen und Beispiele für Richtlinien, die Sie zum Abrufen und Offenlegen vertraulicher Datenproben verwenden können, finden Sie im Blogbeitrag How to use Amazon Macie to preview sensitive data in S3 buckets im AWSSecurity Blog.

Themen

- Bestimmen Sie, welche Zugriffsmethode verwendet werden soll
- Verwenden von IAM-Benutzeranmeldedaten für den Zugriff auf betroffene S3-Objekte
- Annahme einer IAM-Rolle für den Zugriff auf betroffene S3-Objekte
- Konfiguration einer IAM-Rolle für den Zugriff auf betroffene S3-Objekte
- Betroffene S3-Objekte werden entschlüsselt

Bestimmen Sie, welche Zugriffsmethode verwendet werden soll

Bei der Entscheidung, welche Konfiguration für Ihre AWS Umgebung am besten geeignet ist, sollten Sie unbedingt berücksichtigen, ob Ihre Umgebung mehrere Amazon Macie Macie-Konten umfasst, die zentral als Organisation verwaltet werden. Wenn Sie der delegierte Macie-Administrator für eine Organisation sind, kann die Konfiguration von Macie für die Übernahme einer IAM-Rolle den Abruf sensibler Datenproben von betroffenen S3-Objekten für Konten in Ihrer Organisation rationalisieren. Mit diesem Ansatz erstellen Sie eine IAM-Rolle in Ihrem Administratorkonto. Sie erstellen auch eine IAM-Rolle in jedem entsprechenden Mitgliedskonto. Die Rolle in Ihrem Administratorkonto delegiert den Zugriff auf Macie. Die Rolle in einem Mitgliedskonto delegiert den kontoübergreifenden Zugriff auf die Rolle in Ihrem Administratorkonto. Falls implementiert, können Sie dann mithilfe der Rollenverkettung auf die betroffenen S3-Objekte für Ihre Mitgliedskonten zugreifen.

Überlegen Sie auch, wer standardmäßig direkten Zugriff auf einzelne Ergebnisse hat. Um sensible Datenproben für ein Ergebnis abzurufen und offenzulegen, muss ein Benutzer zunächst Zugriff auf das Ergebnis haben:

- Jobs zur Erkennung sensibler Daten — Nur das Konto, das einen Job erstellt, kann auf die Ergebnisse zugreifen, die der Job liefert. Wenn Sie über ein Macie-Administratorkonto

verfügen, können Sie einen Job zur Analyse von Objekten in S3-Buckets für jedes Konto in Ihrer Organisation konfigurieren. Daher können Ihre Jobs Ergebnisse für Objekte in Buckets liefern, die Ihren Mitgliedskonten gehören. Wenn Sie ein Mitgliedskonto oder ein eigenständiges Macie-Konto haben, können Sie einen Job so konfigurieren, dass nur Objekte in Buckets analysiert werden, die Ihrem Konto gehören.

- Automatisierte Erkennung sensibler Daten — Nur das Macie-Administratorkonto kann auf Ergebnisse zugreifen, die die automatische Erkennung für Konten in ihrem Unternehmen generiert. Mitgliedskonten können nicht auf diese Ergebnisse zugreifen. Wenn Sie ein eigenständiges Macie-Konto haben, können Sie nur für Ihr eigenes Konto auf Ergebnisse zugreifen, die durch automatische Erkennung generiert werden.

Wenn Sie planen, mithilfe einer IAM-Rolle auf betroffene S3-Objekte zuzugreifen, sollten Sie auch Folgendes berücksichtigen:

- Um das Vorkommen vertraulicher Daten in einem Objekt zu lokalisieren, muss das entsprechende Erkennungsergebnis vertraulicher Daten in einem S3-Objekt gespeichert werden, das Macie mit einem Hash-basierten Message Authentication Code (HMAC) signiert hat. AWS KMS key Macie muss in der Lage sein, die Integrität und Authentizität des Ermittlungsergebnisses vertraulicher Daten zu überprüfen. Andernfalls übernimmt Macie nicht die IAM-Rolle beim Abrufen sensibler Datenproben. Dies ist eine zusätzliche Schutzmaßnahme zur Beschränkung des Zugriffs auf Daten in S3-Objekten für ein Konto.
- Um sensible Datenproben von einem Objekt abzurufen, das verschlüsselt und von einem Kunden verwaltet wirdAWS KMS key, muss die IAM-Rolle berechtigt sein, Daten mit dem Schlüssel zu entschlüsseln. Insbesondere muss die Richtlinie des Schlüssels es der Rolle ermöglichen, die Aktion auszuführen. `kms:Decrypt` Bei anderen Arten der serverseitigen Verschlüsselung sind keine zusätzlichen Berechtigungen oder Ressourcen erforderlich, um ein betroffenes Objekt zu entschlüsseln. Weitere Informationen finden Sie unter Betroffene S3-Objekte werden entschlüsselt.
- Um sensible Datenproben von einem Objekt für ein anderes Konto abzurufen, müssen Sie derzeit der delegierte Macie-Administrator für das entsprechende Konto sein. AWS-Region Darüber hinaus gilt:
  - Macie muss derzeit für das Mitgliedskonto in der entsprechenden Region aktiviert sein.
  - Das Mitgliedskonto muss über eine IAM-Rolle verfügen, die den kontoübergreifenden Zugriff an eine IAM-Rolle in Ihrem Macie-Administratorkonto delegiert. Der Name der Rolle muss in Ihrem Macie-Administratorkonto und im Mitgliedskonto identisch sein.

- Die Vertrauensrichtlinie für die IAM-Rolle im Mitgliedskonto muss eine Bedingung enthalten, die die richtige externe ID für Ihre Konfiguration angibt. Diese ID ist eine eindeutige alphanumerische Zeichenfolge, die Macie automatisch generiert, nachdem Sie die Einstellungen für Ihr Macie-Administratorkonto konfiguriert haben. Informationen zur Verwendung externer IDs in Vertrauensrichtlinien finden Sie im Benutzerhandbuch unter So verwenden Sie eine externe ID, wenn Sie Dritten Zugriff auf Ihre AWS Ressourcen gewähren. AWS Identity and Access Management
- Wenn die IAM-Rolle im Mitgliedskonto alle Macie-Anforderungen erfüllt, muss das Mitgliedskonto keine Macie-Einstellungen konfigurieren und aktivieren, damit Sie sensible Datenproben von Objekten für das Konto abrufen können. Macie verwendet nur die Einstellungen und die IAM-Rolle in Ihrem Macie-Administratorkonto und die IAM-Rolle im Mitgliedskonto.

> **Tip**
>
> Wenn Ihr Konto Teil einer großen Organisation ist, sollten Sie erwägen, ein AWS CloudFormation Template- und Stack-Set zu verwenden, um die IAM-Rollen für Mitgliedskonten in Ihrer Organisation bereitzustellen und zu verwalten. Informationen zur Erstellung und Verwendung von Vorlagen und Stack-Sets finden Sie im AWS CloudFormationBenutzerhandbuch.
> Um eine CloudFormation Vorlage zu überprüfen und optional herunterzuladen, die als Ausgangspunkt dienen kann, können Sie die Amazon Macie Macie-Konsole verwenden. Wählen Sie im Navigationsbereich der Konsole unter Einstellungen die Option Beispiele anzeigen aus. Wählen Sie „Bearbeiten“ und anschließend „Rollenberechtigungen und CloudFormation Vorlage für Mitglieder anzeigen“.

Die nachfolgenden Themen in diesem Abschnitt enthalten zusätzliche Details und Überlegungen zu den einzelnen Konfigurationstypen. Bei IAM-Rollen umfasst dies die Vertrauens- und Berechtigungsrichtlinien, die einer Rolle zugewiesen werden sollen. Wenn Sie sich nicht sicher sind, welcher Konfigurationstyp für Ihre Umgebung am besten geeignet ist, bitten Sie Ihren AWS Administrator um Unterstützung.

Verwenden von IAM-Benutzeranmeldedaten für den Zugriff auf betroffene S3-Objekte

Wenn Sie Amazon Macie so konfigurieren, dass sensible Datenproben mithilfe von IAM-Benutzeranmeldedaten abgerufen werden, verwendet jeder Benutzer Ihres Macie-Kontos seine IAM-Identität, um Stichproben für einzelne Ergebnisse zu finden, abzurufen, zu verschlüsseln und

anzuzeigen. Dies bedeutet, dass ein Benutzer sensible Datenproben abrufen und offenlegen kann, um festzustellen, ob seine IAM-Identität auf die erforderlichen Ressourcen und Daten zugreifen darf, und die erforderlichen Aktionen ausführen kann. Alle erforderlichen Aktionen sind angemeldet. AWS CloudTrail

Um Stichproben sensibler Daten für ein bestimmtes Ergebnis abzurufen und aufzudecken, muss ein Benutzer Zugriff auf die folgenden Daten und Ressourcen haben: den Befund, das entsprechende Ermittlungsergebnis vertraulicher Daten, den betroffenen S3-Bucket und das betroffene S3-Objekt. Sie müssen auch das verwenden dürfenAWS KMS key, das, falls zutreffend, zum Verschlüsseln des betroffenen Objekts verwendet wurde, und das, für AWS KMS key das Sie Macie zum Verschlüsseln sensibler Datenproben konfiguriert haben. Wenn IAM-Richtlinien, Ressourcenrichtlinien oder andere Berechtigungseinstellungen den erforderlichen Zugriff verweigern, kann der Benutzer keine Stichproben für das Ergebnis abrufen und anzeigen.

Um diese Art von Konfiguration einzurichten, führen Sie die folgenden allgemeinen Aufgaben aus:

1. Stellen Sie sicher, dass Sie ein Repository für die Ergebnisse der Erkennung sensibler Daten konfiguriert haben.
2. Konfigurieren Sie denAWS KMS key, der für die Verschlüsselung sensibler Datenproben verwendet werden soll.
3. Überprüfen Sie Ihre Berechtigungen für die Konfiguration der Einstellungen in Macie.
4. Konfigurieren und aktivieren Sie die Einstellungen in Macie.

Informationen zur Ausführung dieser Aufgaben finden Sie unterKonfiguration von Amazon Macie für den Abruf und die Offenlegung sensibler Datenproben mit Ergebnissen.

Annahme einer IAM-Rolle für den Zugriff auf betroffene S3-Objekte

Um Amazon Macie so zu konfigurieren, dass sensible Datenproben abgerufen werden, indem eine IAM-Rolle übernommen wird, erstellen Sie zunächst eine IAM-Rolle, die den Zugriff an Macie delegiert. Stellen Sie sicher, dass die Vertrauens- und Berechtigungsrichtlinien für die Rolle alle Voraussetzungen erfüllen, damit Macie die Rolle übernehmen kann. Wenn ein Benutzer Ihres Macie-Kontos dann entscheidet, sensible Datenproben für einen Befund abzurufen und offenzulegen, übernimmt Macie die Rolle, die Proben aus dem betroffenen S3-Objekt abzurufen. Macie übernimmt die Rolle nur, wenn ein Benutzer sich dafür entscheidet, Proben für einen Befund abzurufen und offenzulegen. Um die Rolle zu übernehmen, verwendet Macie den AssumeRoleBetrieb der AWS Security Token Service (AWS STS) -API. Alle erforderlichen Aktionen sind angemeldet. AWS CloudTrail

Um Stichproben vertraulicher Daten für ein bestimmtes Ergebnis abzurufen und aufzudecken, muss ein Benutzer Zugriff auf den Befund, das entsprechende Ermittlungsergebnis vertraulicher Daten und das, für AWS KMS key das Sie Macie zur Verschlüsselung sensibler Datenproben konfiguriert haben, zugreifen dürfen. Die IAM-Rolle muss Macie den Zugriff auf den betroffenen S3-Bucket und das betroffene S3-Objekt ermöglichen. Die Rolle muss gegebenenfalls auch das verwenden dürfenAWS KMS key, mit dem das betroffene Objekt verschlüsselt wurde. Wenn IAM-Richtlinien, Ressourcenrichtlinien oder andere Berechtigungseinstellungen den erforderlichen Zugriff verweigern, kann der Benutzer keine Stichproben für das Ergebnis abrufen und anzeigen.

Führen Sie die folgenden allgemeinen Aufgaben aus, um diese Art von Konfiguration einzurichten. Wenn Sie ein Mitgliedskonto in einer Organisation haben, entscheiden Sie gemeinsam mit Ihrem Macie-Administrator, ob und wie Sie die Einstellungen und Ressourcen für Ihr Konto konfigurieren müssen.

1. Definieren Sie Folgendes:
   - Der Name der IAM-Rolle, die Macie annehmen soll. Wenn Ihr Konto Teil einer Organisation ist, muss dieser Name für das delegierte Macie-Administratorkonto und jedes entsprechende Mitgliedskonto in der Organisation identisch sein. Andernfalls kann der Macie-Administrator nicht auf die betroffenen S3-Objekte für ein entsprechendes Mitgliedskonto zugreifen.
   - Der Name der IAM-Berechtigungsrichtlinie, die der IAM-Rolle zugewiesen werden soll. Wenn Ihr Konto Teil einer Organisation ist, empfehlen wir, dass Sie für jedes entsprechende Mitgliedskonto in der Organisation denselben Richtliniennamen verwenden. Dies kann die Bereitstellung und Verwaltung der Rolle in Mitgliedskonten optimieren.
2. Stellen Sie sicher, dass Sie ein Repository für die Ergebnisse der Erkennung sensibler Daten konfiguriert haben.
3. Konfigurieren Sie denAWS KMS key, der für die Verschlüsselung sensibler Datenproben verwendet werden soll.
4. Überprüfen Sie Ihre Berechtigungen für die Erstellung von IAM-Rollen und die Konfiguration der Einstellungen in Macie.
5. Wenn Sie der delegierte Macie-Administrator für eine Organisation sind oder über ein eigenständiges Macie-Konto verfügen:
   a. Erstellen und konfigurieren Sie die IAM-Rolle für Ihr Konto. Stellen Sie sicher, dass die Vertrauens- und Berechtigungsrichtlinien für die Rolle alle Voraussetzungen erfüllen, damit Macie die Rolle übernehmen kann. Einzelheiten zu diesen Anforderungen finden Sie im nächsten Thema.

b. Konfigurieren und aktivieren Sie die Einstellungen in Macie. Macie generiert dann eine externe ID für die Konfiguration. Wenn Sie der Macie-Administrator einer Organisation sind, notieren Sie sich diese ID. In der Vertrauensrichtlinie für die IAM-Rolle in jedem Ihrer jeweiligen Mitgliedskonten muss diese ID angegeben sein.

6. Wenn Sie ein Mitgliedskonto in einer Organisation haben:

   a. Fragen Sie Ihren Macie-Administrator nach der externen ID, die Sie in der Vertrauensrichtlinie für die IAM-Rolle in Ihrem Konto angeben müssen. Überprüfen Sie außerdem den Namen der IAM-Rolle und die zu erstellende Berechtigungsrichtlinie.

   b. Erstellen und konfigurieren Sie die IAM-Rolle für Ihr Konto. Stellen Sie sicher, dass die Vertrauens- und Berechtigungsrichtlinien für die Rolle alle Anforderungen erfüllen, damit Ihr Macie-Administrator die Rolle übernehmen kann. Einzelheiten zu diesen Anforderungen finden Sie im nächsten Thema.

   c. (Optional) Wenn Sie sensible Datenproben von betroffenen S3-Objekten für Ihr eigenes Konto abrufen und offenlegen möchten, konfigurieren und aktivieren Sie die Einstellungen in Macie. Wenn Sie möchten, dass Macie beim Abrufen der Samples eine IAM-Rolle übernimmt, erstellen und konfigurieren Sie zunächst eine zusätzliche IAM-Rolle in Ihrem Konto. Stellen Sie sicher, dass die Vertrauens- und Berechtigungsrichtlinien für diese zusätzliche Rolle alle Voraussetzungen erfüllen, damit Macie die Rolle übernehmen kann. Konfigurieren Sie dann die Einstellungen in Macie und geben Sie den Namen dieser zusätzlichen Rolle an. Einzelheiten zu den Richtlinienanforderungen für die Rolle finden Sie im nächsten Thema.

Informationen zur Ausführung dieser Aufgaben finden Sie unterKonfiguration von Amazon Macie für den Abruf und die Offenlegung sensibler Datenproben mit Ergebnissen.

Konfiguration einer IAM-Rolle für den Zugriff auf betroffene S3-Objekte

Um mithilfe einer IAM-Rolle auf betroffene S3-Objekte zuzugreifen, erstellen und konfigurieren Sie zunächst eine Rolle, die den Zugriff an Amazon Macie delegiert. Stellen Sie sicher, dass die Vertrauens- und Berechtigungsrichtlinien für die Rolle alle Voraussetzungen erfüllen, damit Macie die Rolle übernehmen kann. Wie Sie dabei vorgehen, hängt von der Art Ihres Macie-Kontos ab.

In den folgenden Abschnitten finden Sie Einzelheiten zu den Vertrauens- und Berechtigungsrichtlinien, die der IAM-Rolle für jeden Macie-Kontotyp zugewiesen werden müssen. Wählen Sie den Abschnitt für den Kontotyp aus, den Sie haben.

> **Note**
>
> Wenn Sie ein Mitgliedskonto in einer Organisation haben, müssen Sie möglicherweise zwei IAM-Rollen für Ihr Konto erstellen und konfigurieren:
>
> - Damit Ihr Macie-Administrator sensible Datenproben von betroffenen S3-Objekten für Ihr Konto abrufen und offenlegen kann, erstellen und konfigurieren Sie eine Rolle, die Ihr Administratorkonto übernehmen kann. Wählen Sie für diese Informationen den Abschnitt Macie-Mitgliedskonto aus.
> - Um sensible Datenproben von betroffenen S3-Objekten für Ihr eigenes Konto abzurufen und offenzulegen, erstellen und konfigurieren Sie eine Rolle, die Macie übernehmen kann. Wählen Sie für diese Informationen den Abschnitt Eigenständiges Macie-Konto aus.
>
> Bevor Sie eine der IAM-Rollen erstellen und konfigurieren, sollten Sie mit Ihrem Macie-Administrator die passende Konfiguration für Ihr Konto ermitteln.

Ausführliche Informationen zur Verwendung von IAM zur Erstellung der Rolle finden Sie im Benutzerhandbuch unter Erstellen einer Rolle mithilfe benutzerdefinierter Vertrauensrichtlinien. AWS Identity and Access Management

Macie-Administratorkonto

Wenn Sie der delegierte Macie-Administrator für eine Organisation sind, verwenden Sie zunächst den IAM-Richtlinieneditor, um die Berechtigungsrichtlinie für die IAM-Rolle zu erstellen. Die Richtlinie sollte wie folgt lauten.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RetrieveS3Objects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "*"
            ]
        },
```

```
        {
            "Sid": "AssumeMacieRevealRoleForCrossAccountAccess",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": "arn:aws:iam::*:role/IAMRoleName"
        }
    ]
}
```

Dabei RoleName ist *IAM* der Name der IAM-Rolle, die Macie beim Abrufen sensibler Datenproben von betroffenen S3-Objekten für die Konten Ihrer Organisation übernehmen soll. Ersetzen Sie diesen Wert durch den Namen der Rolle, die Sie für Ihr Konto erstellen und die Erstellung für entsprechende Mitgliedskonten in Ihrer Organisation planen. Dieser Name muss für Ihr Macie-Administratorkonto und jedes entsprechende Mitgliedskonto identisch sein.

> **Note**
>
> In der vorherigen Berechtigungsrichtlinie verwendet das `Resource` Element in der ersten Anweisung ein Platzhalterzeichen (*). Dadurch kann eine angehängte IAM-Entität Objekte aus allen S3-Buckets abrufen, die Ihrem Unternehmen gehören. Um diesen Zugriff nur für bestimmte Buckets zu gewähren, ersetzen Sie das Platzhalterzeichen durch den Amazon-Ressourcennamen (ARN) jedes Buckets. Um beispielsweise nur den Zugriff auf Objekte in einem Bucket mit dem Namen zu ermöglichen DOC-EXAMPLE-BUCKET, ändern Sie das Element wie folgt:
> `"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"`
> Sie können den Zugriff auf Objekte in bestimmten S3-Buckets auch für einzelne Konten einschränken. Geben Sie dazu die Bucket-ARNs im `Resource` Element der Berechtigungsrichtlinie für die IAM-Rolle in jedem entsprechenden Konto an. Weitere Informationen und Beispiele finden Sie unter IAM-JSON-Richtlinienelemente: Ressource im AWS Identity and Access Management Benutzerhandbuch.

Nachdem Sie die Berechtigungsrichtlinie für die IAM-Rolle erstellt haben, erstellen und konfigurieren Sie die Rolle. Wenn Sie dazu die IAM-Konsole verwenden, wählen Sie Benutzerdefinierte Vertrauensrichtlinie als vertrauenswürdigen Entitätstyp für die Rolle aus. Geben Sie für die Vertrauensrichtlinie, die vertrauenswürdige Entitäten für die Rolle definiert, Folgendes an.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowMacieReveal",
            "Effect": "Allow",
            "Principal": {
                "Service": "reveal-samples.macie.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "accountID"
                }
            }
        }
    ]
}
```

Wobei *AccountID* die accountID für Sie AWS-Konto ist. Ersetzen Sie diesen Wert durch Ihre 12-stellige Konto-ID.

In der vorherigen Vertrauensrichtlinie:

- Das `Principal` Element gibt den Dienstprinzipal an, den Macie beim Abrufen sensibler Datenproben von betroffenen S3-Objekten verwendet,. `reveal-samples.macie.amazonaws.com`
- Das `Action` Element gibt die Aktion an, die der Dienstprinzipal ausführen darf, nämlich den AssumeRoleBetrieb der AWS Security Token Service (AWS STS) -API.
- Das `Condition` Element definiert eine Bedingung, die den Kontextschlüssel aws: SourceAccount global condition verwendet. Diese Bedingung bestimmt, welches Konto die angegebene Aktion ausführen kann. In diesem Fall kann Macie die Rolle nur für das angegebene Konto (*AccountID*) übernehmen. Diese Bedingung verhindert, dass Macie bei Transaktionen mit Macie als verwirrter Stellvertreter eingesetzt wird. AWS STS

Nachdem Sie die Vertrauensrichtlinie für die IAM-Rolle definiert haben, fügen Sie der Rolle die Berechtigungsrichtlinie hinzu. Dies sollte die Berechtigungsrichtlinie sein, die Sie erstellt haben, bevor Sie mit der Erstellung der Rolle begonnen haben. Führen Sie dann die verbleibenden Schritte in IAM

aus, um die Erstellung und Konfiguration der Rolle abzuschließen. Wenn Sie fertig sind, konfigurieren und aktivieren Sie die Einstellungen in Macie.

Macie-Mitgliedskonto

Wenn Sie ein Macie-Mitgliedskonto haben und Ihrem Macie-Administrator ermöglichen möchten, sensible Datenproben von betroffenen S3-Objekten für Ihr Konto abzurufen und offenzulegen, fragen Sie zunächst Ihren Macie-Administrator nach den folgenden Informationen:

- Der Name der zu erstellenden IAM-Rolle. Der Name muss für Ihr Konto und das Macie-Administratorkonto für Ihre Organisation identisch sein.
- Der Name der IAM-Berechtigungsrichtlinie, die der Rolle zugewiesen werden soll.
- Die externe ID, die in der Vertrauensrichtlinie für die Rolle angegeben werden soll. Diese ID muss die externe ID sein, die Macie für die Konfiguration Ihres Macie-Administrators generiert hat.

Nachdem Sie diese Informationen erhalten haben, verwenden Sie den IAM-Richtlinieneditor, um die Berechtigungsrichtlinie für die Rolle zu erstellen. Die Richtlinie sollte wie folgt lauten.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RetrieveS3Objects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Die oben genannte Berechtigungsrichtlinie ermöglicht es einer angehängten IAM-Entität, Objekte aus allen S3-Buckets für Ihr Konto abzurufen. Das liegt daran, dass das `Resource` Element in der Richtlinie ein Platzhalterzeichen (*) verwendet. Um diesen Zugriff nur für bestimmte Buckets zu gewähren, ersetzen Sie das Platzhalterzeichen durch den Amazon-Ressourcennamen (ARN) jedes Buckets. Um beispielsweise nur den Zugriff auf Objekte in einem Bucket mit dem Namen zu ermöglichen DOC-EXAMPLE-BUCKET2, ändern Sie das Element wie folgt:

```
"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2/*"
```

Weitere Informationen und Beispiele finden Sie unter IAM-JSON-Richtlinienelemente: Ressource im AWS Identity and Access ManagementBenutzerhandbuch.

Nachdem Sie die Berechtigungsrichtlinie für die IAM-Rolle erstellt haben, erstellen Sie die Rolle. Wenn Sie die Rolle mithilfe der IAM-Konsole erstellen, wählen Sie Benutzerdefinierte Vertrauensrichtlinie als vertrauenswürdigen Entitätstyp für die Rolle aus. Geben Sie für die Vertrauensrichtlinie, die vertrauenswürdige Entitäten für die Rolle definiert, Folgendes an.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowMacieAdminRevealRoleForCrossAccountAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::administratorAccountID:role/IAMRoleName"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "sts:ExternalId": "externalID",
                    "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
                }
            }
        }
    ]
}
```

Ersetzen Sie in der vorherigen Richtlinie die Platzhalterwerte durch die richtigen Werte für Ihre AWS Umgebung. Dabei gilt:

- *AdministratorAccountID* ist die 12-stellige Konto-ID für Ihr Macie-Administratorkonto.
- *IAM RoleName* ist der Name der IAM-Rolle in Ihrem Macie-Administratorkonto. Es sollte der Name sein, den Sie von Ihrem Macie-Administrator erhalten haben.
- *ExternalID* ist die externe ID, die Sie von Ihrem Macie-Administrator erhalten haben.

Im Allgemeinen ermöglicht die Vertrauensrichtlinie Ihrem Macie-Administrator, die Rolle des Abrufs und der Offenlegung sensibler Datenproben von betroffenen S3-Objekten für Ihr Konto

zu übernehmen. Das `Principal` Element gibt den ARN einer IAM-Rolle im Konto Ihres Macie-Administrators an. Dies ist die Rolle, die Ihr Macie-Administrator verwendet, um sensible Datenproben für die Konten Ihrer Organisation abzurufen und offenzulegen. Der `Condition` Block definiert zwei Bedingungen, die weiter bestimmen, wer die Rolle übernehmen kann:

- Die erste Bedingung gibt eine externe ID an, die für die Konfiguration Ihrer Organisation eindeutig ist. Weitere Informationen zu externen IDs finden Sie im AWS Identity and Access ManagementBenutzerhandbuch unter So verwenden Sie eine externe ID, wenn Sie Dritten Zugriff auf Ihre AWS Ressourcen gewähren.
- Die zweite Bedingung verwendet den globalen Bedingungskontextschlüssel aws: PrincipalOrg ID. Der Wert für den Schlüssel ist eine dynamische Variable, die den eindeutigen Bezeichner für eine Organisation in AWS Organizations (`${aws:ResourceOrgID}`) darstellt. Die Bedingung beschränkt den Zugriff nur auf die Konten, die Teil derselben Organisation in AWS Organizations sind. Wenn Sie Ihrer Organisation beigetreten sind, indem Sie eine Einladung in Macie angenommen haben, entfernen Sie diese Bedingung aus der Richtlinie.

Nachdem Sie die Vertrauensrichtlinie für die IAM-Rolle definiert haben, fügen Sie der Rolle die Berechtigungsrichtlinie hinzu. Dies sollte die Berechtigungsrichtlinie sein, die Sie erstellt haben, bevor Sie mit der Erstellung der Rolle begonnen haben. Führen Sie dann die verbleibenden Schritte in IAM aus, um die Erstellung und Konfiguration der Rolle abzuschließen. Konfigurieren und geben Sie keine Einstellungen für die Rolle in Macie ein.

Eigenständiges Macie-Konto

Wenn Sie ein eigenständiges Macie-Konto oder ein Macie-Mitgliedskonto haben und sensible Datenproben von betroffenen S3-Objekten für Ihr eigenes Konto abrufen und offenlegen möchten, verwenden Sie zunächst den IAM-Richtlinieneditor, um die Berechtigungsrichtlinie für die IAM-Rolle zu erstellen. Die Richtlinie sollte wie folgt lauten.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RetrieveS3Objects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
```

```
                "*"
            ]
        }
    ]
}
```

In der vorherigen Berechtigungsrichtlinie verwendet das `Resource` Element ein Platzhalterzeichen (*). Auf diese Weise kann eine angehängte IAM-Entität Objekte aus allen S3-Buckets für Ihr Konto abrufen. Um diesen Zugriff nur für bestimmte Buckets zu gewähren, ersetzen Sie das Platzhalterzeichen durch den Amazon-Ressourcennamen (ARN) jedes Buckets. Um beispielsweise nur den Zugriff auf Objekte in einem Bucket mit dem Namen zu ermöglichen DOC-EXAMPLE-BUCKET3, ändern Sie das Element wie folgt:

```
"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET3/*"
```

Weitere Informationen und Beispiele finden Sie unter IAM-JSON-Richtlinienelemente: Ressource im AWS Identity and Access ManagementBenutzerhandbuch.

Nachdem Sie die Berechtigungsrichtlinie für die IAM-Rolle erstellt haben, erstellen Sie die Rolle. Wenn Sie die Rolle mithilfe der IAM-Konsole erstellen, wählen Sie Benutzerdefinierte Vertrauensrichtlinie als vertrauenswürdigen Entitätstyp für die Rolle aus. Geben Sie für die Vertrauensrichtlinie, die vertrauenswürdige Entitäten für die Rolle definiert, Folgendes an.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowMacieReveal",
            "Effect": "Allow",
            "Principal": {
                "Service": "reveal-samples.macie.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "accountID"
                }
            }
        }
    ]
}
```

Wobei *AccountID* die accountID für Sie AWS-Konto ist. Ersetzen Sie diesen Wert durch Ihre 12-stellige Konto-ID.

In der vorherigen Vertrauensrichtlinie:

- Das `Principal` Element gibt den Dienstprinzipal an, den Macie beim Abrufen und Aufdecken sensibler Datenproben von betroffenen S3-Objekten verwendet,. `reveal-samples.macie.amazonaws.com`
- Das `Action` Element spezifiziert die Aktion, die der Dienstprinzipal ausführen darf, nämlich den AssumeRoleBetrieb der AWS Security Token Service (AWS STS) -API.
- Das `Condition` Element definiert eine Bedingung, die den Kontextschlüssel aws: SourceAccount global condition verwendet. Diese Bedingung bestimmt, welches Konto die angegebene Aktion ausführen kann. Es ermöglicht Macie, die Rolle nur für das angegebene Konto (*AccountID*) zu übernehmen. Diese Bedingung verhindert, dass Macie bei Transaktionen mit als verwirrter Stellvertreterin eingesetzt wird. AWS STS

Nachdem Sie die Vertrauensrichtlinie für die IAM-Rolle definiert haben, fügen Sie der Rolle die Berechtigungsrichtlinie hinzu. Dies sollte die Berechtigungsrichtlinie sein, die Sie erstellt haben, bevor Sie mit der Erstellung der Rolle begonnen haben. Führen Sie dann die verbleibenden Schritte in IAM aus, um die Erstellung und Konfiguration der Rolle abzuschließen. Wenn Sie fertig sind, konfigurieren und aktivieren Sie die Einstellungen in Macie.

Betroffene S3-Objekte werden entschlüsselt

Amazon S3 unterstützt mehrere Verschlüsselungsoptionen für S3-Objekte. Für die meisten dieser Optionen sind keine zusätzlichen Ressourcen oder Berechtigungen erforderlich, damit ein IAM-Benutzer oder eine IAM-Rolle sensible Datenproben von einem betroffenen Objekt entschlüsseln und abrufen kann. Dies ist der Fall bei einem Objekt, das mithilfe einer serverseitigen Verschlüsselung mit einem von Amazon S3 verwalteten Schlüssel oder einem AWS AWS KMS key verwalteten Schlüssel verschlüsselt wurde.

Wenn ein S3-Objekt jedoch verschlüsselt und von einem Kunden verwaltet wirdAWS KMS key, sind zusätzliche Berechtigungen erforderlich, um sensible Datenproben aus dem Objekt zu entschlüsseln und abzurufen. Genauer gesagt muss die Schlüsselrichtlinie für den KMS-Schlüssel es dem IAM-Benutzer oder der IAM-Rolle ermöglichen, die `kms:Decrypt` Aktion auszuführen. Andernfalls tritt ein Fehler auf und Macie ruft keine Samples aus dem Objekt ab. Informationen darüber, wie Sie einem IAM-Benutzer diesen Zugriff gewähren, finden Sie unter Authentifizierung und Zugriffskontrolle für AWS KMS im AWS Key Management ServiceEntwicklerhandbuch.

Wie dieser Zugriff für eine IAM-Rolle bereitgestellt wird, hängt davon ab, ob das Konto, dem die Rolle gehört, AWS KMS key auch Eigentümer der Rolle ist:

- Wenn dasselbe Konto den KMS-Schlüssel und die Rolle besitzt, muss ein Benutzer des Kontos die Richtlinie für den Schlüssel aktualisieren.
- Wenn ein Konto den KMS-Schlüssel und ein anderes Konto die Rolle besitzt, muss ein Benutzer des Kontos, dem der Schlüssel gehört, kontenübergreifenden Zugriff auf den Schlüssel gewähren.

In diesem Thema wird beschrieben, wie Sie diese Aufgaben für eine IAM-Rolle ausführen, die Sie zum Abrufen sensibler Datenproben aus S3-Objekten erstellt haben. Es enthält auch Beispiele für beide Szenarien. Informationen zur Gewährung des Zugriffs für vom Kunden verwaltete Systeme AWS KMS keys für andere Szenarien finden Sie unter Authentifizierung und Zugriffskontrolle für AWS KMS im AWS Key Management ServiceEntwicklerhandbuch.

Erlauben des Zugriffs auf einen vom Kunden verwalteten Schlüssel für dasselbe Konto

Wenn dasselbe Konto AWS KMS key sowohl die als auch die IAM-Rolle besitzt, muss ein Benutzer des Kontos der Richtlinie für den Schlüssel eine Erklärung hinzufügen. Die zusätzliche Anweisung muss es der IAM-Rolle ermöglichen, Daten mithilfe des Schlüssels zu entschlüsseln. Ausführliche Informationen zur Aktualisierung einer Schlüsselrichtlinie finden Sie unter Ändern einer Schlüsselrichtlinie im AWS Key Management ServiceEntwicklerhandbuch.

In der Erklärung:

- Das `Principal` Element muss den Amazon-Ressourcennamen (ARN) der IAM-Rolle angeben.
- Das `Action` Array muss die `kms:Decrypt` Aktion spezifizieren. Dies ist die einzige AWS KMS Aktion, die die IAM-Rolle ausführen darf, um ein mit dem Schlüssel verschlüsseltes Objekt zu entschlüsseln.

Im Folgenden finden Sie ein Beispiel für die Anweisung, die der Richtlinie für einen KMS-Schlüssel hinzugefügt werden soll.

```
{
    "Sid": "Allow the Macie reveal role to use the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/IAMRoleName"
    },
```

```
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

Für das obige Beispiel gilt:

- Das `AWS` Feld im `Principal` Element gibt den ARN der IAM-Rolle im Konto an. Es ermöglicht der Rolle, die in der Richtlinienerklärung angegebene Aktion auszuführen. *`123456789012`* ist ein Beispiel für eine Konto-ID. Ersetzen Sie diesen Wert durch die Konto-ID für das Konto, dem die Rolle gehört, und durch den KMS-Schlüssel. *`IAM RoleName`* ist ein Beispielname. Ersetzen Sie diesen Wert durch den Namen der IAM-Rolle im Konto.
- Das `Action` Array gibt die Aktion an, die die IAM-Rolle mithilfe des KMS-Schlüssels ausführen darf, d. h. den Chiffretext entschlüsseln, der mit dem Schlüssel verschlüsselt ist.

Wo Sie diese Anweisung zu einer wichtigen Richtlinie hinzufügen, hängt von der Struktur und den Elementen ab, die die Richtlinie derzeit enthält. Stellen Sie beim Hinzufügen der Anweisung sicher, dass die Syntax gültig ist. Wichtige Richtlinien verwenden das JSON-Format. Das bedeutet, dass Sie vor oder nach der Anweisung auch ein Komma hinzufügen müssen, je nachdem, wo Sie die Anweisung zur Richtlinie hinzufügen.

Ermöglicht den kontoübergreifenden Zugriff auf einen vom Kunden verwalteten Schlüssel

Wenn ein Konto den AWS KMS key (Schlüsselinhaber) besitzt und ein anderes Konto die IAM-Rolle (Rolleninhaber) besitzt, muss der Schlüsselinhaber dem Rolleninhaber kontoübergreifenden Zugriff auf den Schlüssel gewähren. Eine Möglichkeit, dies zu tun, ist die Verwendung eines Zuschusses. Ein Zuschuss ist ein politisches Instrument, das es AWS Prinzipalen ermöglicht, KMS-Schlüssel für kryptografische Operationen zu verwenden, sofern die im Zuschuss festgelegten Bedingungen erfüllt sind. Weitere Informationen zu Zuschüssen finden Sie unter Zuschüsse AWS KMS im AWS Key Management Service Entwicklerhandbuch.

Bei diesem Ansatz stellt der Schlüsselinhaber zunächst sicher, dass die Richtlinie des Schlüssels es dem Rolleninhaber ermöglicht, einen Zuschuss für den Schlüssel zu erstellen. Der Rolleninhaber erstellt dann einen Zuschuss für den Schlüssel. Durch die Gewährung werden die entsprechenden Berechtigungen an die IAM-Rolle in ihrem Konto delegiert. Sie ermöglicht der Rolle, S3-Objekte zu entschlüsseln, die mit dem Schlüssel verschlüsselt wurden.

Schritt 1: Aktualisieren Sie die Schlüsselrichtlinie

In der Schlüsselrichtlinie sollte der Schlüsselinhaber sicherstellen, dass die Richtlinie eine Erklärung enthält, die es dem Rolleninhaber ermöglicht, einen Zuschuss für die IAM-Rolle in seinem Konto (dem des Rollenbesitzers) zu erstellen. In dieser Anweisung muss das `Principal` Element den ARN des Kontos des Rollenbesitzers angeben. Das `Action` Array muss die `kms:CreateGrant` Aktion angeben. Ein `Condition` Block kann den Zugriff auf die angegebene Aktion filtern. Im Folgenden finden Sie ein Beispiel für diese Anweisung in der Richtlinie für einen KMS-Schlüssel.

```
{
    "Sid": "Allow a role in an account to create a grant",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:GranteePrincipal": "arn:aws:iam::111122223333:role/IAMRoleName"
        },
        "ForAllValues:StringEquals": {
            "kms:GrantOperations": "Decrypt"
        }
    }
}
```

Für das obige Beispiel gilt:

- Das `AWS` Feld im `Principal` Element gibt den ARN des Kontos des Rollenbesitzers an. Es ermöglicht dem Konto, die in der Richtlinienerklärung angegebene Aktion auszuführen. *111122223333* ist ein Beispiel für eine Konto-ID. Ersetzen Sie diesen Wert durch die Konto-ID für das Konto des Rollenbesitzers.
- Das `Action` Array gibt die Aktion an, die der Rolleninhaber mit dem KMS-Schlüssel ausführen darf — eine Zuweisung für den Schlüssel erstellen.
- Der `Condition` Block verwendet Bedingungsoperatoren und die folgenden Bedingungsschlüssel, um den Zugriff auf die Aktion zu filtern, die der Rolleninhaber mit dem KMS-Schlüssel ausführen darf:

- kms: GranteePrincipal — Diese Bedingung ermöglicht es dem Rolleninhaber, einen Grant nur für den angegebenen Principal des Empfängers zu erstellen, bei dem es sich um den ARN der IAM-Rolle in seinem Konto handelt. In diesem ARN ist *`111122223333 ein Beispiel für eine Konto-ID`*. Ersetzen Sie diesen Wert durch die Konto-ID für das Konto des Rollenbesitzers. *`IAM RoleName`* ist ein Beispielname. Ersetzen Sie diesen Wert durch den Namen der IAM-Rolle im Konto des Rollenbesitzers.
- kms: GrantOperations — Diese Bedingung ermöglicht es dem Rolleninhaber, eine Genehmigung nur zu erstellen, um die Erlaubnis zur Ausführung der AWS KMS `Decrypt` Aktion zu delegieren (Entschlüsselung des mit dem Schlüssel verschlüsselten Chiffretextes). Sie verhindert, dass der Rolleninhaber Genehmigungen erstellt, mit denen Berechtigungen zur Ausführung anderer Aktionen mit dem KMS-Schlüssel delegiert werden. Diese `Decrypt` Aktion ist die einzige AWS KMS Aktion, die die IAM-Rolle ausführen darf, um ein mit dem Schlüssel verschlüsseltes Objekt zu entschlüsseln.

Wo der Schlüsselinhaber diese Erklärung zur Schlüsselrichtlinie hinzufügt, hängt von der Struktur und den Elementen ab, die die Richtlinie derzeit enthält. Wenn der Schlüsselinhaber die Anweisung hinzufügt, sollte er sicherstellen, dass die Syntax gültig ist. Wichtige Richtlinien verwenden das JSON-Format. Das bedeutet, dass der Schlüsselinhaber vor oder nach der Anweisung auch ein Komma hinzufügen muss, je nachdem, wo er die Anweisung zur Richtlinie hinzufügt. Ausführliche Informationen zur Aktualisierung einer wichtigen Richtlinie finden Sie unter Ändern einer Schlüsselrichtlinie im AWS Key Management ServiceEntwicklerhandbuch.

Schritt 2: Einen Zuschuss erstellen

Nachdem der Schlüsselinhaber die Schlüsselrichtlinie nach Bedarf aktualisiert hat, erstellt der Rolleninhaber einen Grant für den Schlüssel. Durch die Erteilung werden die entsprechenden Berechtigungen an die IAM-Rolle in ihrem Konto (dem des Rollenbesitzers) delegiert. Bevor der Rolleninhaber den Zuschuss erstellt, sollte er überprüfen, ob er die `kms:CreateGrant` Aktion ausführen darf. Diese Aktion ermöglicht es ihnen, einem bestehenden, vom Kunden verwalteten Betrag einen Zuschuss hinzuzufügenAWS KMS key.

Um den Zuschuss zu erstellen, kann der Rolleninhaber den CreateGrantBetrieb der AWS Key Management Service API verwenden. Wenn der Rolleninhaber den Grant erstellt, sollte er die folgenden Werte für die erforderlichen Parameter angeben:

- `KeyId`— Der ARN des KMS-Schlüssels. Für den kontoübergreifenden Zugriff auf einen KMS-Schlüssel muss es sich bei diesem Wert um einen ARN handeln. Es kann keine Schlüssel-ID sein.

- `GranteePrincipal`— Der ARN der IAM-Rolle in ihrem Konto. Dieser Wert sollte lautenarn:aws:iam::*111122223333*:role/*IAMRoleName*, wobei *111122223333* die Konto-ID für das Konto des Rollenbesitzers und *IAM* der Name der Rolle RoleName ist.
- `Operations`— Die AWS KMS Entschlüsselungsaktion (). `Decrypt` Dies ist die einzige AWS KMS Aktion, die die IAM-Rolle ausführen darf, um ein Objekt zu entschlüsseln, das mit dem KMS-Schlüssel verschlüsselt ist.

Wenn der Rollenbesitzer AWS Command Line Interface (AWS CLI) verwendet, kann er den Befehl create-grant ausführen, um den Grant zu erstellen. Im folgenden Beispiel wird gezeigt, wie dies geschieht. Das Beispiel ist für Microsoft Windows formatiert und verwendet das Zeilenfortsetzungszeichen Caret (^), um die Lesbarkeit zu verbessern.

```
C:\> aws kms create-grant ^
--key-id arn:aws:kms:us-east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab ^
--grantee-principal arn:aws:iam::111122223333:role/IAMRoleName ^
--operations "Decrypt"
```

Wobei gilt:

- `key-id`gibt den ARN des KMS-Schlüssels an, auf den der Zuschuss angewendet werden soll.
- `grantee-principal`gibt den ARN der IAM-Rolle an, die die im Grant angegebene Aktion ausführen darf. Dieser Wert sollte dem ARN entsprechen, der in der `kms:GranteePrincipal` Bedingung in der Schlüsselrichtlinie angegeben ist.
- `operations`gibt die Aktion an, die der angegebene Prinzipal aufgrund des Grants ausführen kann — das Entschlüsseln von Chiffretext, der mit dem Schlüssel verschlüsselt ist.

Wird der Befehl erfolgreich ausgeführt, erhalten Sie eine Ausgabe ähnlich der folgenden:

```
{
    "GrantToken": "<grant token>",
    "GrantId": "1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2"
}
```

Dabei `GrantToken` handelt es sich um eine eindeutige, nicht geheime, Base64-kodierte Zeichenfolge mit variabler Länge, die den Grant darstellt, der erstellt wurde, und der eindeutige Bezeichner für den Grant ist. `GrantId`

Konfiguration von Amazon Macie für den Abruf und die Offenlegung sensibler Datenproben mit Ergebnissen

Sie können Amazon Macie optional konfigurieren und verwenden, um Stichproben vertraulicher Daten abzurufen und offenzulegen, die Macie als individuelle Ergebnisse sensibler Daten meldet. Anhand der Beispiele können Sie die Art der sensiblen Daten überprüfen, die Macie gefunden hat. Sie können Ihnen auch dabei helfen, Ihre Untersuchung eines betroffenen Amazon Simple Storage Service (Amazon S3) -Objekts und -Buckets maßgeschneidert zu gestalten. Sie können sensible Datenproben überall dort abrufen und offenlegen, AWS-Regionen wo Macie derzeit verfügbar ist, mit Ausnahme der Regionen Asien-Pazifik (Osaka) und Israel (Tel Aviv).

Wenn Sie Stichproben sensibler Daten für einen Befund abrufen und offenlegen, verwendet Macie die Daten aus dem entsprechenden Ermittlungsergebnis für sensible Daten, um das Vorkommen sensibler Daten im betroffenen S3-Objekt zu lokalisieren. Macie extrahiert dann Stichproben dieser Vorkommnisse aus dem betroffenen Objekt. Macie verschlüsselt die extrahierten Daten mit einem von Ihnen angegebenen Schlüssel AWS Key Management Service (AWS KMS), speichert die verschlüsselten Daten vorübergehend in einem Cache und gibt die Daten in Ihren Ergebnissen für die Suche zurück. Kurz nach dem Extrahieren und Verschlüsseln löscht Macie die Daten dauerhaft aus dem Cache, es sei denn, eine zusätzliche Aufbewahrung ist vorübergehend erforderlich, um ein Betriebsproblem zu lösen.

Um Stichproben vertraulicher Daten abzurufen und für Ergebnisse freizugeben, müssen Sie zunächst die Einstellungen für Ihr Macie-Konto konfigurieren und aktivieren. Außerdem müssen Sie unterstützende Ressourcen und Berechtigungen für Ihr Konto konfigurieren. Die Themen in diesem Abschnitt führen Sie durch die Konfiguration von Macie für den Abruf und die Offenlegung sensibler Datenproben sowie durch die Verwaltung des Status der Konfiguration für Ihr Konto.

Themen

- Bevor Sie beginnen
- Konfiguration und Aktivierung der Amazon Macie Macie-Einstellungen
- Amazon Macie Macie-Einstellungen deaktivieren

> **Tip**
>
> Empfehlungen und Beispiele für Richtlinien, mit denen Sie den Zugriff auf diese Funktion kontrollieren können, finden Sie im Blogbeitrag How to use Amazon Macie to preview sensitive data in S3 Buckets im AWSSecurity Blog.

Bevor Sie beginnen

Bevor Sie Amazon Macie so konfigurieren, dass Stichproben sensibler Daten für Ergebnisse abgerufen und offengelegt werden, führen Sie die folgenden Aufgaben durch, um sicherzustellen, dass Sie über die erforderlichen Ressourcen und Berechtigungen verfügen.

Aufgaben

- Schritt 1: Konfigurieren Sie ein Repository für die Ergebnisse der Erkennung sensibler Daten
- Schritt 2: Ermitteln Sie, wie auf die betroffenen S3-Objekte zugegriffen werden soll
- Schritt 3: Konfigurieren Sie ein AWS KMS key
- Schritt 4: Überprüfen Sie Ihre Berechtigungen

Diese Aufgaben sind optional, wenn Sie Macie bereits für den Abruf und die Offenlegung sensibler Datenproben konfiguriert haben und nur Ihre Konfigurationseinstellungen ändern möchten.

Schritt 1: Konfigurieren Sie ein Repository für die Ergebnisse der Erkennung sensibler Daten

Wenn Sie Stichproben sensibler Daten für einen Befund abrufen und offenlegen, verwendet Macie die Daten aus dem entsprechenden Ermittlungsergebnis für sensible Daten, um das Vorkommen sensibler Daten im betroffenen S3-Objekt zu lokalisieren. Daher ist es wichtig, zu überprüfen, ob Sie ein Repository für die Ergebnisse der Erkennung sensibler Daten konfiguriert haben. Andernfalls wird Macie nicht in der Lage sein, Stichproben sensibler Daten zu finden, die Sie abrufen und offenlegen möchten.

Um festzustellen, ob Sie dieses Repository für Ihr Konto konfiguriert haben, können Sie die Amazon Macie Macie-Konsole verwenden: Wählen Sie im Navigationsbereich Discovery-Ergebnisse (unter Einstellungen) aus. Um dies programmgesteuert zu tun, verwenden Sie den GetClassificationExportConfigurationBetrieb der Amazon Macie Macie-API. Weitere Informationen zu den Ergebnissen der Erkennung sensibler Daten und zur Konfiguration dieses Repositorys finden Sie unter. Speicherung und Beibehaltung der Erkennungsergebnisse von vertraulichen Daten

Schritt 2: Ermitteln Sie, wie auf die betroffenen S3-Objekte zugegriffen werden soll

Um auf betroffene S3-Objekte zuzugreifen und sensible Datenproben von ihnen abzurufen, haben Sie zwei Möglichkeiten. Sie können Macie so konfigurieren, dass es Ihre AWS Identity and Access Management (IAM-) Benutzeranmeldedaten verwendet. Oder Sie können Macie so konfigurieren, dass es eine IAM-Rolle annimmt, die den Zugriff an Macie delegiert. Sie können beide Konfigurationen mit einem beliebigen Macie-Konto verwenden — dem delegierten Macie-Administratorkonto für eine Organisation, einem Macie-Mitgliedskonto in einer Organisation oder einem eigenständigen Macie-Konto. Bevor Sie die Einstellungen in Macie konfigurieren, legen Sie fest, welche Zugriffsmethode Sie verwenden möchten. Einzelheiten zu den Optionen und Anforderungen für die einzelnen Methoden finden Sie unterKonfigurationsoptionen und Anforderungen für den Abruf sensibler Datenproben mit Ergebnissen.

Wenn Sie eine IAM-Rolle verwenden möchten, erstellen und konfigurieren Sie die Rolle, bevor Sie die Einstellungen in Macie konfigurieren. Stellen Sie außerdem sicher, dass die Vertrauens- und Berechtigungsrichtlinien für die Rolle alle Voraussetzungen erfüllen, damit Macie die Rolle übernehmen kann. Wenn Ihr Konto Teil einer Organisation ist, die mehrere Macie-Konten zentral verwaltet, entscheiden Sie zunächst mit Ihrem Macie-Administrator, ob und wie die Rolle für Ihr Konto konfiguriert werden soll.

Schritt 3: Konfigurieren Sie ein AWS KMS key

Wenn Sie sensible Datenproben für einen Befund abrufen und offenlegen, verschlüsselt Macie die Stichproben mit einem von Ihnen AWS KMS angegebenen Schlüssel AWS Key Management Service (). Daher müssen Sie festlegen, welchen AWS KMS key Sie zum Verschlüsseln der Stichproben verwenden möchten. Der Schlüssel kann ein vorhandener KMS-Schlüssel aus Ihrem eigenen Konto oder ein vorhandener KMS-Schlüssel sein, den ein anderes Konto besitzt. Wenn Sie einen Schlüssel verwenden möchten, den ein anderes Konto besitzt, rufen Sie den Amazon-Ressourcennamen (ARN) des Schlüssels ab. Sie müssen diesen ARN angeben, wenn Sie die Konfigurationseinstellungen in Macie eingeben.

Der KMS-Schlüssel muss ein vom Kunden verwalteter, symmetrischer Verschlüsselungsschlüssel sein. Es muss sich außerdem um einen Schlüssel für eine einzelne Region handeln, der genauso aktiviert ist AWS-Region wie Ihr Macie-Konto. Der KMS-Schlüssel kann sich in einem externen Schlüsselspeicher befinden. Der Schlüssel ist dann jedoch möglicherweise langsamer und weniger zuverlässig als ein Schlüssel, der vollständig innerhalb verwaltet wirdAWS KMS. Wenn Macie aufgrund von Latenz- oder Verfügbarkeitsproblemen daran gehindert wird, sensible Datenproben zu verschlüsseln, die Sie abrufen und offenlegen möchten, tritt ein Fehler auf und Macie sendet keine Stichproben für die Suche zurück.

Darüber hinaus muss die Schlüsselrichtlinie für den Schlüssel es den entsprechenden Prinzipalen (IAM-Rollen, IAM-Benutzern oderAWS-Konten) ermöglichen, die folgenden Aktionen auszuführen:

- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKey`

> **Important**
>
> Als zusätzliche Ebene der Zugriffskontrolle empfehlen wir, einen speziellen KMS-Schlüssel für die Verschlüsselung der abgerufenen vertraulichen Datenproben zu erstellen und die Verwendung des Schlüssels auf die Prinzipale zu beschränken, die sensible Datenproben abrufen und offenlegen dürfen. Wenn ein Benutzer die oben genannten Aktionen für den Schlüssel nicht ausführen darf, lehnt Macie seine Anfrage ab, sensible Datenproben abzurufen und offenzulegen. Macie sendet keine Proben für den Befund zurück.

Informationen zum Erstellen und Konfigurieren von KMS-Schlüsseln finden Sie unter Schlüssel verwalten im AWS Key Management ServiceEntwicklerhandbuch. Informationen zur Verwendung von Schlüsselrichtlinien zur Verwaltung des Zugriffs auf KMS-Schlüssel finden Sie unter Wichtige Richtlinien AWS KMS im AWS Key Management Service Entwicklerhandbuch.

Schritt 4: Überprüfen Sie Ihre Berechtigungen

Bevor Sie die Einstellungen in Macie konfigurieren, stellen Sie außerdem sicher, dass Sie über die erforderlichen Berechtigungen verfügen. Um Ihre Berechtigungen zu überprüfen, verwenden Sie AWS Identity and Access Management (IAM), um die IAM-Richtlinien zu überprüfen, die mit Ihrer IAM-Identität verknüpft sind. Vergleichen Sie dann die Informationen in diesen Richtlinien mit der folgenden Liste von Aktionen, die Sie ausführen dürfen müssen.

Amazon Macie

Stellen Sie für Macie sicher, dass Sie die folgenden Aktionen ausführen dürfen:

- `macie2:GetMacieSession`
- `macie2:UpdateRevealConfiguration`

Mit der ersten Aktion können Sie auf Ihr Macie-Konto zugreifen. Mit der zweiten Aktion können Sie Ihre Konfigurationseinstellungen für das Abrufen und Offenlegen sensibler Datenproben ändern. Dazu gehört das Aktivieren und Deaktivieren der Konfiguration für Ihr Konto.

Vergewissern Sie sich optional, dass Sie die `macie2:GetRevealConfiguration` Aktion auch ausführen dürfen. Mit dieser Aktion können Sie Ihre aktuellen Konfigurationseinstellungen und den aktuellen Status der Konfiguration für Ihr Konto abrufen.

AWS KMS

Wenn Sie die Amazon Macie Macie-Konsole verwenden möchten, um die Konfigurationseinstellungen einzugeben, stellen Sie außerdem sicher, dass Sie die folgenden AWS Key Management Service (AWS KMS) Aktionen ausführen dürfen:

- `kms:DescribeKey`
- `kms:ListAliases`

Diese Aktionen ermöglichen es Ihnen, Informationen über das AWS KMS keys für Ihr Konto abzurufen. Sie können dann bei der Eingabe der Einstellungen einen dieser Schlüssel auswählen.

IAM

Wenn Sie Macie so konfigurieren möchten, dass es eine IAM-Rolle zum Abrufen und Offenlegen vertraulicher Datenproben annimmt, stellen Sie außerdem sicher, dass Sie die folgende IAM-Aktion ausführen dürfen:. `iam:PassRole` Diese Aktion ermöglicht es Ihnen, die Rolle an Macie zu übergeben, wodurch Macie wiederum die Rolle übernehmen kann. Wenn Sie die Konfigurationseinstellungen für Ihr Konto eingeben, kann Macie dann auch überprüfen, ob die Rolle in Ihrem Konto vorhanden und korrekt konfiguriert ist.

Wenn Sie die erforderlichen Aktionen nicht ausführen dürfen, bitten Sie Ihren AWS Administrator um Unterstützung.

Konfiguration und Aktivierung der Amazon Macie Macie-Einstellungen

Nachdem Sie sich vergewissert haben, dass Sie über die benötigten Ressourcen und Berechtigungen verfügen, können Sie die Einstellungen in Amazon Macie konfigurieren und die Konfiguration für Ihr Konto aktivieren.

Wenn Ihr Konto Teil einer Organisation ist, die mehrere Macie-Konten zentral verwaltet, beachten Sie Folgendes, bevor Sie die Einstellungen für Ihr Konto konfigurieren oder anschließend ändern:

- Wenn Sie ein Mitgliedskonto haben, entscheiden Sie gemeinsam mit Ihrem Macie-Administrator, ob und wie Sie die Einstellungen für Ihr Konto konfigurieren müssen. Ihr Macie-Administrator kann Ihnen helfen, die richtigen Konfigurationseinstellungen für Ihr Konto zu ermitteln.
- Wenn Sie über ein Macie-Administratorkonto verfügen und Ihre Einstellungen für den Zugriff auf betroffene S3-Objekte ändern, können sich Ihre Änderungen auf andere Konten und Ressourcen Ihrer Organisation auswirken. Dies hängt davon ab, ob Macie derzeit so konfiguriert ist, dass es eine AWS Identity and Access Management (IAM-) Rolle beim Abrufen sensibler Datenproben übernimmt. Ist dies der Fall und Sie konfigurieren Macie für die Verwendung von IAM-Benutzeranmeldedaten neu, löscht Macie dauerhaft die vorhandenen Einstellungen für die IAM-Rolle — den Namen der Rolle und die externe ID für Ihre Konfiguration. Wenn sich Ihre Organisation später dafür entscheidet, wieder IAM-Rollen zu verwenden, müssen Sie in der Vertrauensrichtlinie für die Rolle in jedem entsprechenden Mitgliedskonto eine neue externe ID angeben.

Einzelheiten zu den Konfigurationsoptionen für beide Kontotypen finden Sie unterKonfigurationsoptionen und Anforderungen für den Abruf sensibler Datenproben mit Ergebnissen.

Um die Einstellungen in Macie zu konfigurieren und die Konfiguration für Ihr Konto zu aktivieren, können Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden.

Console

Gehen Sie wie folgt vor, um die Einstellungen mithilfe der Amazon Macie Macie-Konsole zu konfigurieren und zu aktivieren.

Um die Macie-Einstellungen zu konfigurieren und zu aktivieren

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie mithilfe des AWS-Region Auswahlfensters in der oberen rechten Ecke der Seite die Region aus, in der Sie Macie konfigurieren und aktivieren möchten, um sensible Datenproben abzurufen und anzuzeigen.
3. Wählen Sie im Navigationsbereich unter Einstellungen die Option Beispiele anzeigen aus.
4. Wählen Sie im Abschnitt Settings (Einstellungen) die Option Edit (Bearbeiten) aus.
5. Wählen Sie für Status die Option Aktiviert.
6. Geben Sie unter Zugriff die Zugriffsmethode und die Einstellungen an, die Sie beim Abrufen sensibler Datenproben von betroffenen S3-Objekten verwenden möchten:

- Um eine IAM-Rolle zu verwenden, die den Zugriff an Macie delegiert, wählen Sie Assume an IAM-Rolle. Wenn Sie diese Option wählen, ruft Macie die Beispiele ab, indem es die IAM-Rolle annimmt, die Sie in Ihrem erstellt und konfiguriert haben. AWS-Konto Geben Sie im Feld Rollenname den Namen der Rolle ein.
- Um die Anmeldeinformationen des IAM-Benutzers zu verwenden, der die Beispiele anfordert, wählen Sie „IAM-Benutzeranmeldedaten verwenden“. Wenn Sie diese Option wählen, verwendet jeder Benutzer Ihres Kontos seine individuelle IAM-Identität, um die Samples abzurufen.

7. Geben Sie unter Verschlüsselung die Daten anAWS KMS key, die Sie zum Verschlüsseln sensibler Datenproben verwenden möchten, die abgerufen werden:

   - Um einen KMS-Schlüssel von Ihrem eigenen Konto zu verwenden, wählen Sie Wählen Sie einen Schlüssel aus Ihrem Konto aus. Wählen Sie dann in der AWS KMS keyListe den Schlüssel aus, den Sie verwenden möchten. In der Liste werden die vorhandenen KMS-Schlüssel mit symmetrischer Verschlüsselung für Ihr Konto angezeigt.
   - Um einen KMS-Schlüssel zu verwenden, der einem anderen Konto gehört, wählen Sie Geben Sie den ARN eines Schlüssels von einem anderen Konto ein. Geben Sie dann in das Feld AWS KMS keyARN den Amazon-Ressourcennamen (ARN) des zu verwendenden Schlüssels ein, z. B. **`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**

8. Wenn Sie mit der Eingabe der Einstellungen fertig sind, wählen Sie Speichern.

Macie testet die Einstellungen und stellt sicher, dass sie korrekt sind. Wenn Sie Macie so konfiguriert haben, dass er eine IAM-Rolle annimmt, überprüft Macie auch, ob die Rolle in Ihrem Konto vorhanden ist und dass die Vertrauens- und Berechtigungsrichtlinien korrekt konfiguriert sind. Wenn es ein Problem gibt, zeigt Macie eine Meldung an, in der das Problem beschrieben wird.

Informationen zur Behebung eines Problems mit dem AWS KMS key finden Sie in den Anforderungen im vorherigen Thema und geben Sie einen KMS-Schlüssel an, der die Anforderungen erfüllt. Um ein Problem mit der IAM-Rolle zu beheben, überprüfen Sie zunächst, ob Sie den richtigen Rollennamen eingegeben haben. Wenn der Name korrekt ist, stellen Sie sicher, dass die Richtlinien der Rolle alle Voraussetzungen erfüllen, damit Macie die Rolle übernehmen kann. Diese Einzelheiten finden Sie unterKonfiguration einer IAM-Rolle für den

Zugriff auf betroffene S3-Objekte. Nachdem Sie alle Probleme behoben haben, können Sie die Einstellungen speichern und aktivieren.

> **Note**
>
> Wenn Sie der Macie-Administrator einer Organisation sind und Macie so konfiguriert haben, dass er eine IAM-Rolle annimmt, generiert Macie eine externe ID und zeigt sie an, nachdem Sie die Einstellungen für Ihr Konto gespeichert haben. Notieren Sie sich diese ID. In der Vertrauensrichtlinie für die IAM-Rolle in jedem Ihrer jeweiligen Mitgliedskonten muss diese ID angegeben sein. Andernfalls können Sie keine sensiblen Datenproben von S3-Objekten abrufen, die den Konten gehören.

API

Verwenden Sie den UpdateRevealConfigurationBetrieb der Amazon Macie Macie-API, um die Einstellungen programmgesteuert zu konfigurieren und zu aktivieren. Geben Sie in Ihrer Anfrage die entsprechenden Werte für die unterstützten Parameter an:

- Geben Sie für die `retrievalConfiguration` Parameter die Zugriffsmethode und die Einstellungen an, die Sie beim Abrufen sensibler Datenproben von betroffenen S3-Objekten verwenden möchten:
  - Um eine IAM-Rolle anzunehmen, die den Zugriff an Macie delegiert, geben Sie `ASSUME_ROLE` für den `retrievalMode` Parameter und den Namen der Rolle für den Parameter an. `roleName` Wenn Sie diese Einstellungen angeben, ruft Macie die Beispiele ab, indem es die IAM-Rolle annimmt, die Sie in Ihrem erstellt und konfiguriert haben. AWS-Konto
  - Um die Anmeldeinformationen des IAM-Benutzers zu verwenden, der die Beispiele anfordert, geben Sie `CALLER_CREDENTIALS` für den Parameter Folgendes an. `retrievalMode` Wenn Sie diese Einstellung angeben, verwendet jeder Benutzer Ihres Kontos seine individuelle IAM-Identität, um die Samples abzurufen.

> **Important**
>
> Wenn Sie keine Werte für diese Parameter angeben, setzt Macie die Zugriffsmethode (`retrievalMode`) auf. `CALLER_CREDENTIALS` Wenn Macie derzeit so konfiguriert ist, dass eine IAM-Rolle zum Abrufen der Beispiele verwendet wird, löscht Macie auch den aktuellen Rollennamen und die externe ID für Ihre Konfiguration dauerhaft.

> Um diese Einstellungen für eine bestehende Konfiguration beizubehalten, nehmen Sie die `retrievalConfiguration` Parameter in Ihre Anfrage auf und geben Sie Ihre aktuellen Einstellungen für diese Parameter an. Um Ihre aktuellen Einstellungen abzurufen, verwenden Sie die GetRevealConfigurationOperation oder, falls Sie die AWS Command Line Interface (AWS CLI) verwenden, führen Sie den get-reveal-configurationBefehl aus.

- Geben Sie für den `kmsKeyId` Parameter den AWS KMS key an, den Sie zum Verschlüsseln sensibler Datenproben verwenden möchten, die abgerufen werden:
  - Um einen KMS-Schlüssel aus Ihrem eigenen Konto zu verwenden, geben Sie den Amazon-Ressourcennamen (ARN), die ID oder den Alias für den Schlüssel an. Wenn Sie einen Alias angeben, geben Sie das `alias/` Präfix an, z. B. `alias/ExampleAlias`
  - Um einen KMS-Schlüssel zu verwenden, der einem anderen Konto gehört, geben Sie den ARN des Schlüssels an, z. B.. `arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` Oder geben Sie den ARN des Alias für den Schlüssel an, z. B. `arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias`
- Geben Sie für den `status` Parameter an, ob `ENABLED` die Konfiguration für Ihr Macie-Konto aktiviert werden soll.

Stellen Sie in Ihrer Anfrage außerdem sicher, dass Sie die Konfiguration angeben, AWS-Region in der Sie die Konfiguration aktivieren und verwenden möchten.

Um die Einstellungen mithilfe von zu konfigurieren und zu aktivierenAWS CLI, führen Sie den update-reveal-configurationBefehl aus und geben Sie die entsprechenden Werte für die unterstützten Parameter an. Wenn Sie beispielsweise den AWS CLI unter Microsoft Windows verwenden, führen Sie den folgenden Befehl aus:

```
C:\> aws macie2 update-reveal-configuration ^
--region us-east-1 ^
--configuration={\"kmsKeyId\":\"arn:aws:kms:us-east-1:111122223333:alias/
ExampleAlias\",\"status\":\"ENABLED\"} ^
--retrievalConfiguration={\"retrievalMode\":\"ASSUME_ROLE\",\"roleName\":
\"MacieRevealRole\"}
```

Wobei gilt:

- *us-east-1* ist die Region, in der die Konfiguration aktiviert und verwendet werden soll. In diesem Beispiel die Region USA Ost (Nord-Virginia).
- *arn:aws:kms:us-east- ExampleAlias 1:111122223333:alias/* ist der ARN des zu verwendenden Alias. AWS KMS key In diesem Beispiel gehört der Schlüssel einem anderen Konto.
- ENABLEDist der Status der Konfiguration.
- *ASSUME_ROLE* ist die zu verwendende Zugriffsmethode. Gehen Sie in diesem Beispiel von der angegebenen IAM-Rolle aus.
- *MacieRevealRole*ist der Name der IAM-Rolle, die Macie beim Abrufen sensibler Datenproben übernehmen soll.

Im vorherigen Beispiel wird das Zeilenfortsetzungszeichen Caret (^) verwendet, um die Lesbarkeit zu verbessern.

Wenn Sie Ihre Anfrage einreichen, testet Macie die Einstellungen. Wenn Sie Macie so konfiguriert haben, dass es eine IAM-Rolle annimmt, überprüft Macie auch, ob die Rolle in Ihrem Konto vorhanden ist und dass die Vertrauens- und Berechtigungsrichtlinien korrekt konfiguriert sind. Wenn es ein Problem gibt, schlägt Ihre Anfrage fehl und Macie gibt eine Nachricht zurück, in der das Problem beschrieben wird. Um ein Problem mit dem zu behebenAWS KMS key, lesen Sie die Anforderungen im vorherigen Thema und geben Sie einen KMS-Schlüssel an, der die Anforderungen erfüllt. Um ein Problem mit der IAM-Rolle zu beheben, überprüfen Sie zunächst, ob Sie den richtigen Rollennamen angegeben haben. Wenn der Name korrekt ist, stellen Sie sicher, dass die Richtlinien der Rolle alle Voraussetzungen erfüllen, damit Macie die Rolle übernehmen kann. Diese Einzelheiten finden Sie unterKonfiguration einer IAM-Rolle für den Zugriff auf betroffene S3-Objekte. Nachdem Sie das Problem behoben haben, reichen Sie Ihre Anfrage erneut ein.

Wenn Ihre Anfrage erfolgreich ist, aktiviert Macie die Konfiguration für Ihr Konto in der angegebenen Region und Sie erhalten eine Ausgabe, die der folgenden ähnelt.

```
{
  "configuration": {
    "kmsKeyId": "arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias",
    "status": "ENABLED"
  },
  "retrievalConfiguration": {
    "externalId": "o2vee30hs31642lexample",
```

```
    "retrievalMode": "ASSUME_ROLE",
    "roleName": "MacieRevealRole"
  }
}
```

Wo `kmsKeyId` gibt das anAWS KMS key, was zur Verschlüsselung sensibler Daten verwendet werden soll, die abgerufen werden, und `status` ist der Status der Konfiguration für Ihr Macie-Konto. Die `retrievalConfiguration` Werte geben die Zugriffsmethode und die Einstellungen an, die beim Abrufen der Samples verwendet werden sollen.

> **Note**
>
> Wenn Sie der Macie-Administrator einer Organisation sind und Macie so konfiguriert haben, dass er eine IAM-Rolle annimmt, notieren Sie sich die externe ID (`externalId`) in der Antwort. In der Vertrauensrichtlinie für die IAM-Rolle in jedem Ihrer jeweiligen Mitgliedskonten muss diese ID angegeben sein. Andernfalls können Sie keine sensiblen Datenproben von betroffenen S3-Objekten abrufen, die den Konten gehören.

Um anschließend die Einstellungen oder den Status der Konfiguration für Ihr Konto zu überprüfen, verwenden Sie den GetRevealConfigurationVorgang oder führen Sie für den den AWS CLI den get-reveal-configurationBefehl aus.

Amazon Macie Macie-Einstellungen deaktivieren

Sie können die Konfigurationseinstellungen für Ihr Amazon Macie Macie-Konto jederzeit deaktivieren. Wenn Sie die Konfiguration deaktivieren, behält Macie die Einstellung bei, die angibt, welche AWS KMS key für die Verschlüsselung sensibler Datenproben verwendet werden soll, die abgerufen werden. Macie löscht die Amazon S3 S3-Zugriffseinstellungen für die Konfiguration dauerhaft.

> **Warning**
>
> Wenn Sie die Konfigurationseinstellungen für Ihr Macie-Konto deaktivieren, löschen Sie auch dauerhaft die aktuellen Einstellungen, die angeben, wie auf die betroffenen S3-Objekte zugegriffen werden soll. Wenn Macie derzeit so konfiguriert ist, dass es auf betroffene Objekte zugreift, indem es eine AWS Identity and Access Management (IAM-) Rolle annimmt, beinhaltet dies: den Namen der Rolle und die externe ID, die Macie für die Konfiguration

generiert hat. Diese Einstellungen können nicht wiederhergestellt werden, nachdem sie gelöscht wurden.

Um die Konfigurationseinstellungen für Ihr Macie-Konto zu deaktivieren, können Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden.

Console

Gehen Sie wie folgt vor, um die Konfigurationseinstellungen für Ihr Konto mithilfe der Amazon Macie Macie-Konsole zu deaktivieren.

Um die Macie-Einstellungen zu deaktivieren

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie die Konfigurationseinstellungen für Ihr Macie-Konto deaktivieren möchten.
3. Wählen Sie im Navigationsbereich unter Einstellungen die Option Reveal samples aus.
4. Wählen Sie im Abschnitt Settings (Einstellungen) die Option Edit (Bearbeiten) aus.
5. Wählen Sie für Status die Option Deaktivieren aus.
6. Wählen Sie Speichern aus.

API

Um die Konfigurationseinstellungen programmgesteuert zu deaktivieren, verwenden Sie den UpdateRevealConfigurationBetrieb der Amazon Macie Macie-API. Stellen Sie in Ihrer Anfrage sicher, dass Sie angeben, AWS-Region in welcher Version Sie die Konfiguration deaktivieren möchten. Geben Sie für den Parameter `status` `DISABLED` an:

Um die Konfigurationseinstellungen mithilfe von AWS Command Line Interface (AWS CLI) zu deaktivieren, führen Sie den update-reveal-configurationBefehl aus. Verwenden Sie den `region` Parameter, um die Region anzugeben, in der Sie die Konfiguration deaktivieren möchten. Geben Sie für den Parameter `status` `DISABLED` an: Wenn Sie beispielsweise den AWS CLI unter Microsoft Windows verwenden, führen Sie den folgenden Befehl aus:

```
C:\> aws macie2 update-reveal-configuration --region us-east-1 --
configuration={\"status\":\"DISABLED\"}
```

Wobei gilt:

- *us-east-1* ist die Region, in der die Konfiguration deaktiviert werden soll. In diesem Beispiel die Region USA Ost (Nord-Virginia).
- DISABLEDist der neue Status der Konfiguration.

Wenn Ihre Anfrage erfolgreich ist, deaktiviert Macie die Konfiguration für Ihr Konto in der angegebenen Region und Sie erhalten eine Ausgabe, die der folgenden ähnelt.

```
{
    "configuration": {
        "status": "DISABLED"
    }
}
```

Wo `status` ist der neue Status der Konfiguration für Ihr Macie-Konto?

Wenn Macie so konfiguriert wurde, dass es eine IAM-Rolle zum Abrufen sensibler Datenproben annimmt, können Sie optional die Rolle und die Berechtigungsrichtlinie der Rolle löschen. Macie löscht diese Ressourcen nicht, wenn Sie die Konfigurationseinstellungen für Ihr Konto deaktivieren. Darüber hinaus verwendet Macie diese Ressourcen nicht, um andere Aufgaben für Ihr Konto auszuführen. Um die Rolle und ihre Berechtigungsrichtlinie zu löschen, können Sie die IAM-Konsole oder die IAM-API verwenden. Weitere Informationen finden Sie im AWS Identity and Access ManagementBenutzerhandbuch unter Löschen von Rollen.

Abrufen und Offenlegen sensibler Datenproben mit Befunden

Mithilfe von Amazon Macie können Sie Stichproben sensibler Daten abrufen und offenlegen, die Macie als individuelle Ergebnisse für sensible Daten meldet. Dazu gehören sensible Daten, die Macie anhand verwalteter Datenkennungen erkennt, sowie Daten, die den Kriterien von benutzerdefinierten Datenkennungen entsprechen. Anhand der Beispiele können Sie die Art der sensiblen Daten überprüfen, die Macie gefunden hat. Sie können Ihnen auch dabei helfen, Ihre Untersuchung eines betroffenen Amazon Simple Storage Service (Amazon S3) -Objekts und -Buckets maßgeschneidert zu gestalten. Sie können sensible Datenproben überall dort abrufen und offenlegen, AWS-Regionen wo Macie derzeit verfügbar ist, mit Ausnahme der Regionen Asien-Pazifik (Osaka) und Israel (Tel Aviv).

Wenn Sie Stichproben sensibler Daten für einen Befund abrufen und offenlegen, verwendet Macie die Daten aus dem entsprechenden Ergebnis der Entdeckung sensibler Daten, um die ersten 1—10 Vorkommen sensibler Daten zu lokalisieren, die im Rahmen des Befundes gemeldet wurden. Macie extrahiert dann die ersten 1—128 Zeichen jedes Vorkommens aus dem betroffenen S3-Objekt. Wenn ein Befund mehrere Typen sensibler Daten meldet, tut Macie dies für bis zu 100 Arten sensibler Daten, die durch den Befund gemeldet wurden.

Wenn Macie vertrauliche Daten aus einem betroffenen S3-Objekt extrahiert, verschlüsselt Macie die Daten mit einem von Ihnen angegebenen Schlüssel AWS Key Management Service (AWS KMS), speichert die verschlüsselten Daten vorübergehend in einem Cache und gibt die Daten in Ihren Ergebnissen für den Befund zurück. Kurz nach der Extraktion und Verschlüsselung löscht Macie die Daten dauerhaft aus dem Cache, es sei denn, eine zusätzliche Aufbewahrung ist vorübergehend erforderlich, um ein Betriebsproblem zu lösen.

Wenn Sie sich dafür entscheiden, sensible Datenproben für einen Fund erneut abzurufen und offenzulegen, wiederholt Macie den Vorgang zum Auffinden, Extrahieren, Verschlüsseln, Speichern und schließlich zum Löschen der Proben.

Eine Demonstration, wie Sie sensible Datenproben mithilfe der Amazon Macie-Konsole abrufen und offenlegen können, finden Sie im folgenden Video: Samples sensibler Daten mit Amazon Macie abrufen und offenlegen.

Themen

- Bevor Sie beginnen
- Feststellen, ob Stichproben sensibler Daten für einen Befund verfügbar sind
- Stichproben sensibler Daten für einen Befund abrufen und offenlegen

Bevor Sie beginnen

Bevor Sie sensible Datenproben abrufen und für Befunde offenlegen können, müssen Sie die Einstellungen für Ihr Amazon Macie Macie-Konto konfigurieren und aktivieren. Sie müssen auch mit Ihrem AWS Administrator zusammenarbeiten, um zu überprüfen, ob Sie über die erforderlichen Berechtigungen und Ressourcen verfügen.

Wenn Sie sensible Datenproben für einen Befund abrufen und offenlegen, führt Macie eine Reihe von Aufgaben aus, um die Proben zu lokalisieren, abzurufen, zu verschlüsseln und offenzulegen. Macie verwendet die mit dem Dienst verknüpfte Macie-Rolle für Ihr Konto nicht, um diese Aufgaben

auszuführen. Stattdessen verwenden Sie Ihre AWS Identity and Access Management (IAM-) Identität oder erlauben Macie, eine IAM-Rolle in Ihrem Konto anzunehmen.

Um Stichproben vertraulicher Daten für einen Befund abzurufen und offenzulegen, benötigen Sie Zugriff auf den Befund, das entsprechende Ermittlungsergebnis vertraulicher Daten und das, für AWS KMS key das Sie Macie zur Verschlüsselung sensibler Datenproben konfiguriert haben. Darüber hinaus müssen Sie oder die IAM-Rolle Zugriff auf den betroffenen S3-Bucket und das betroffene S3-Objekt haben. Sie oder die Rolle müssen gegebenenfalls auch AWS KMS key das verwenden dürfen, mit dem das betroffene Objekt verschlüsselt wurde. Wenn IAM-Richtlinien, Ressourcenrichtlinien oder andere Berechtigungseinstellungen den erforderlichen Zugriff verweigern, tritt ein Fehler auf und Macie sendet keine Stichproben für die Suche zurück.

Sie müssen außerdem berechtigt sein, die folgenden Macie-Aktionen auszuführen:

- `macie2:GetMacieSession`
- `macie2:GetFindings`
- `macie2:ListFindings`
- `macie2:GetSensitiveDataOccurrences`

Mit den ersten drei Aktionen können Sie auf Ihr Macie-Konto zugreifen und die Einzelheiten der Ergebnisse abrufen. Mit der letzten Aktion können Sie sensible Datenproben für Ergebnisse abrufen und offenlegen.

Um die Amazon Macie Macie-Konsole zum Abrufen und Offenlegen vertraulicher Datenproben zu verwenden, müssen Sie außerdem die folgende Aktion ausführen dürfen:`macie2:GetSensitiveDataOccurrencesAvailability`. Mit dieser Aktion können Sie feststellen, ob Proben für einzelne Ergebnisse verfügbar sind. Sie benötigen keine Genehmigung, um diese Aktion zum programmgesteuerten Abrufen und Anzeigen von Proben auszuführen. Mit dieser Berechtigung können Sie jedoch das Abrufen von Proben vereinfachen.

Wenn Sie der delegierte Macie-Administrator für eine Organisation sind und Macie so konfiguriert haben, dass er eine IAM-Rolle zum Abrufen sensibler Datenproben annimmt, müssen Sie auch die folgende Aktion ausführen dürfen:. `macie2:GetMember` Mit dieser Aktion können Sie Informationen über die Verknüpfung zwischen Ihrem Konto und einem betroffenen Konto abrufen. Dadurch kann Macie überprüfen, ob Sie derzeit der Macie-Administrator für das betroffene Konto sind.

Wenn Sie die erforderlichen Aktionen nicht ausführen oder nicht auf die erforderlichen Daten und Ressourcen zugreifen dürfen, bitten Sie Ihren AWS Administrator um Unterstützung.

Feststellen, ob Stichproben sensibler Daten für einen Befund verfügbar sind

Um Stichproben sensibler Daten für einen Befund abrufen und offenlegen zu können, muss der Befund bestimmte Kriterien erfüllen. Es muss Standortdaten für bestimmte Vorkommen sensibler Daten enthalten. Darüber hinaus muss der Speicherort eines gültigen, entsprechenden Ermittlungsergebnisses für sensible Daten angegeben werden. Das Ergebnis der Entdeckung sensibler Daten muss im selben Verzeichnis AWS-Region wie das Ergebnis gespeichert werden. Wenn Sie Amazon Macie für den Zugriff auf betroffene S3-Objekte konfiguriert haben, indem Sie eine AWS Identity and Access Management (IAM-) Rolle übernehmen, muss das Ergebnis der Erkennung sensibler Daten auch in einem S3-Objekt gespeichert werden, das Macie mit einem Hash-basierten Message Authentication Code (HMAC) signiert hat. AWS KMS key

Das betroffene S3-Objekt muss außerdem bestimmte Kriterien erfüllen. Der MIME-Typ des Objekts muss einer der folgenden sein:

- application/avro, für eine Apache Avro-Objektcontainerdatei (.avro)
- application/gzip, für eine komprimierte GNU Zip-Archivdatei (.gz oder .gzip)
- application/json, für eine JSON- oder JSON-Lines-Datei (.json oder .jsonl)
- application/parquet, für eine Apache Parquet-Datei (.parquet)
- application/vnd.openxmlformats-officedocument.spreadsheetml.sheet, für eine Microsoft Excel-Arbeitsmappendatei (.xlsx)
- application/zip, für eine komprimierte ZIP-Archivdatei (.zip)
- text/csv, für eine CSV-Datei (.csv)
- text/plain, für eine nicht-binäre Textdatei, bei der es sich nicht um eine CSV-, JSON-, JSON Lines- oder TSV-Datei handelt
- text/tab-separated-values, für eine TSV-Datei (.tsv)

Außerdem muss der Inhalt des S3-Objekts mit dem Inhalt identisch sein, zu dem der Befund erstellt wurde. Macie überprüft das Entity-Tag (ETag) des Objekts, um festzustellen, ob es mit dem durch den Befund angegebenen ETag übereinstimmt. Außerdem darf die Speichergröße des Objekts das für das Abrufen und Offenlegen sensibler Datenproben geltende Größenkontingent nicht überschreiten. Eine Liste der geltenden Kontingente finden Sie unterAmazon Macie Macie-Kontingente.

Wenn ein Ergebnis und das betroffene S3-Objekt die oben genannten Kriterien erfüllen, sind Stichproben sensibler Daten für den Befund verfügbar. Sie können optional feststellen, ob dies bei

einem bestimmten Befund der Fall ist, bevor Sie versuchen, Stichproben für den Befund abzurufen und aufzudecken.

Um festzustellen, ob Stichproben sensibler Daten für einen Befund verfügbar sind

Sie können die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden, um festzustellen, ob sensible Datenproben für einen Befund verfügbar sind.

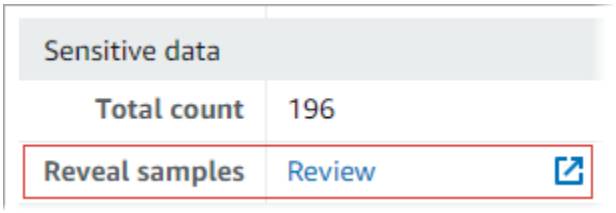
Console

Folgen Sie diesen Schritten auf der Amazon Macie Macie-Konsole, um festzustellen, ob sensible Datenproben für eine Suche verfügbar sind.

Um festzustellen, ob Stichproben für einen Befund verfügbar sind

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich Findings aus.
3. Wählen Sie auf der Seite Ergebnisse das Ergebnis aus. Im Detailbereich werden Informationen zum Ergebnis angezeigt.
4. Scrollen Sie im Detailbereich zum Abschnitt Vertrauliche Daten. Sehen Sie sich dann das Feld Reveal-Beispiele an.

   Wenn Stichproben sensibler Daten für den Befund verfügbar sind, wird in dem Feld der Link Überprüfen angezeigt, wie in der folgenden Abbildung dargestellt.



   Wenn für den Befund keine Stichproben vertraulicher Daten verfügbar sind, wird im Feld Stichproben anzeigen ein Text angezeigt, der angibt, warum:

   - Konto nicht in der Organisation — Sie sind nicht berechtigt, mit Macie auf das betroffene S3-Objekt zuzugreifen. Das betroffene Konto ist derzeit nicht Teil Ihrer Organisation. Oder das Konto ist Teil Ihrer Organisation, aber Macie ist derzeit nicht für das Konto aktiviert. AWS-Region
   - Ungültiges Klassifizierungsergebnis — Für den Befund gibt es kein entsprechendes Ermittlungsergebnis vertraulicher Daten. Oder das entsprechende Ermittlungsergebnis

für vertrauliche Daten ist aktuell nicht verfügbar AWS-Region, falsch formatiert oder beschädigt oder verwendet ein nicht unterstütztes Speicherformat. Macie kann den Speicherort der abzurufenden sensiblen Daten nicht überprüfen.

- Ungültige Ergebnissignatur — Das entsprechende Ergebnis der Erkennung sensibler Daten wird in einem S3-Objekt gespeichert, das nicht von Macie signiert wurde. Macie kann die Integrität und Authentizität des Ermittlungsergebnisses sensibler Daten nicht überprüfen. Daher kann Macie den Speicherort der abzurufenden sensiblen Daten nicht überprüfen.
- Mitgliedsrolle zu freizügig — Die Vertrauens- oder Berechtigungsrichtlinie für die IAM-Rolle im betroffenen Mitgliedskonto entspricht nicht den Anforderungen von Macie zur Beschränkung des Zugriffs auf die Rolle. Oder die Vertrauensrichtlinie der Rolle gibt nicht die richtige externe ID für Ihre Organisation an. Macie kann die Rolle zum Abrufen der sensiblen Daten nicht übernehmen.
- Fehlende GetMember Erlaubnis — Sie dürfen keine Informationen über die Verknüpfung zwischen Ihrem Konto und dem betroffenen Konto abrufen. Macie kann nicht feststellen, ob Sie als delegierter Macie-Administrator für das betroffene Konto auf das betroffene S3-Objekt zugreifen dürfen.
- Objekt überschreitet Größenkontingent — Die Speichergröße des betroffenen S3-Objekts überschreitet das Größenkontingent für das Abrufen und Offenlegen von Stichproben vertraulicher Daten aus diesem Dateityp.
- Objekt nicht verfügbar — Das betroffene S3-Objekt ist nicht verfügbar. Das Objekt wurde umbenannt, verschoben oder gelöscht, oder sein Inhalt wurde geändert, nachdem Macie das Ergebnis erstellt hatte. Oder das Objekt ist mit einem verschlüsselt AWS KMS key , das derzeit deaktiviert ist.
- Ergebnis nicht signiert — Das entsprechende Ergebnis der Erkennung sensibler Daten wird in einem S3-Objekt gespeichert, das nicht signiert wurde. Macie kann die Integrität und Authentizität des Ermittlungsergebnisses sensibler Daten nicht überprüfen. Daher kann Macie den Speicherort der abzurufenden sensiblen Daten nicht überprüfen.
- Rolle zu freizügig — Ihr Konto ist so konfiguriert, dass vertrauliche Daten mithilfe einer IAM-Rolle abgerufen werden, deren Vertrauens- oder Berechtigungsrichtlinie nicht den Anforderungen von Macie zur Beschränkung des Zugriffs auf die Rolle entspricht. Macie kann die Rolle zum Abrufen der sensiblen Daten nicht übernehmen.
- Nicht unterstützter Objekttyp — Das betroffene S3-Objekt verwendet ein Datei- oder Speicherformat, das Macie nicht unterstützt, um Beispiele vertraulicher Daten abzurufen

und offenzulegen. Der MIME-Typ des betroffenen S3-Objekts gehört nicht zu den Werten in der vorherigen Liste.

Wenn es ein Problem mit dem Ergebnis der Erkennung sensibler Daten für den Befund gibt, können Ihnen die Informationen im Feld Detaillierter Ergebnisort des Befundes helfen, das Problem zu untersuchen. Dieses Feld gibt den ursprünglichen Pfad zum Ergebnis in Amazon S3 an. Um ein Problem mit einer IAM-Rolle zu untersuchen, stellen Sie sicher, dass die Richtlinien der Rolle alle Anforderungen erfüllen, damit Macie die Rolle übernehmen kann. Diese Einzelheiten finden Sie unter. Konfiguration einer IAM-Rolle für den Zugriff auf betroffene S3-Objekte

API

Verwenden Sie den GetSensitiveDataOccurrencesAvailabilityBetrieb der Amazon Macie Macie-API, um programmgesteuert zu ermitteln, ob Stichproben sensibler Daten für einen Befund verfügbar sind. Wenn Sie Ihre Anfrage einreichen, verwenden Sie den `findingId` Parameter, um die eindeutige Kennung für das Ergebnis anzugeben. Um diese Kennung zu erhalten, können Sie die ListFindingsOperation verwenden.

Wenn Sie AWS Command Line Interface (AWS CLI) verwenden, führen Sie den Befehl get-sensitive-data-occurrences-availability aus und verwenden Sie den `finding-id` Parameter, um den eindeutigen Bezeichner für den Befund anzugeben. Um diesen Bezeichner zu erhalten, können Sie den Befehl list-findings ausführen.

Wenn Ihre Anfrage erfolgreich ist und Beispiele für den Befund verfügbar sind, erhalten Sie eine Ausgabe, die der folgenden ähnelt:

```
{
    "code": "AVAILABLE",
    "reasons": []
}
```

Wenn Ihre Anfrage erfolgreich ist und keine Stichproben für die Suche verfügbar sind, lautet der Wert für das `code` Feld `UNAVAILABLE` und das `reasons` Array gibt an, warum. Beispielsweise:

```
{
    "code": "UNAVAILABLE",
    "reasons": [
```

```
        "UNSUPPORTED_OBJECT_TYPE"
    ]
}
```

Wenn es ein Problem mit dem Ergebnis der Entdeckung sensibler Daten für den Befund gibt, können Ihnen die Informationen im `classificationDetails.detailedResultsLocation` Feld des Ergebnisses bei der Untersuchung des Problems helfen. Dieses Feld gibt den ursprünglichen Pfad zum Ergebnis in Amazon S3 an. Um ein Problem mit einer IAM-Rolle zu untersuchen, stellen Sie sicher, dass die Richtlinien der Rolle alle Anforderungen erfüllen, damit Macie die Rolle übernehmen kann. Diese Einzelheiten finden Sie unter. Konfiguration einer IAM-Rolle für den Zugriff auf betroffene S3-Objekte

Stichproben sensibler Daten für einen Befund abrufen und offenlegen

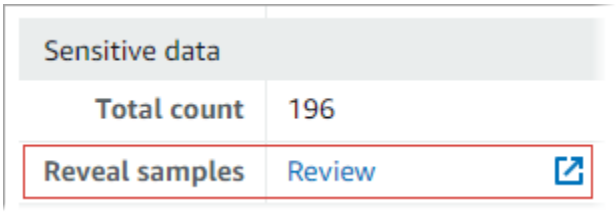
Um sensible Datenproben für einen Befund abzurufen und aufzudecken, können Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden.

Console

Gehen Sie wie folgt vor, um mithilfe der Amazon Macie Macie-Konsole sensible Datenproben für einen Befund abzurufen und anzuzeigen.

So rufen Sie Stichproben sensibler Daten für einen Befund ab und legen diese offen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich Findings aus.
3. Wählen Sie auf der Seite Ergebnisse das Ergebnis aus. Im Detailbereich werden Informationen zum Ergebnis angezeigt.
4. Scrollen Sie im Detailbereich zum Abschnitt Vertrauliche Daten. Wählen Sie dann im Feld Reveal-Beispiele die Option Überprüfen aus:

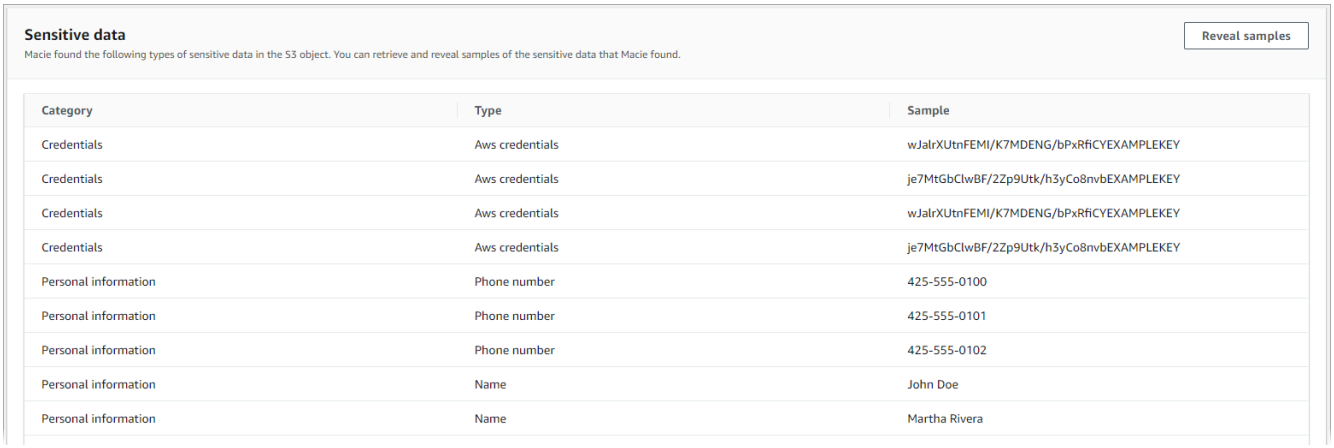


> **Note**
>
> Wenn der Link Überprüfen nicht im Feld Stichproben anzeigen angezeigt wird, sind sensible Datenproben für den Befund nicht verfügbar. Informationen dazu, warum dies der Fall ist, finden Sie im vorherigen Thema.

Nachdem Sie „Überprüfen“ ausgewählt haben, zeigt Macie eine Seite an, auf der die wichtigsten Details des Ergebnisses zusammengefasst sind. Zu den Details gehören die Kategorien, Typen und die Anzahl der Vorkommen vertraulicher Daten, die Macie im betroffenen S3-Objekt gefunden hat.

5. Wählen Sie auf der Seite im Bereich Vertrauliche Daten die Option Beispiele anzeigen aus. Macie ruft dann Stichproben der ersten 1—10 Fälle sensibler Daten ab, die im Rahmen des Befundes gemeldet wurden, und zeigt sie an. Jede Stichprobe enthält die ersten 1—128 Zeichen eines Vorkommens sensibler Daten. Das Abrufen und Aufdecken der Proben kann mehrere Minuten dauern.

   Wenn das Ergebnis mehrere Arten sensibler Daten meldet, ruft Macie Stichproben für bis zu 100 Typen ab und zeigt sie an. Die folgende Abbildung zeigt beispielsweise Stichproben, die sich über mehrere Kategorien und Typen vertraulicher Daten erstrecken:AWS Anmeldeinformationen, US-Telefonnummern und Namen von Personen.



   Die Stichproben sind zuerst nach Kategorien sensibler Daten und dann nach sensiblen Datentypen geordnet.

API

Verwenden Sie den GetSensitiveDataOccurrencesBetrieb der Amazon Macie Macie-API, um sensible Datenproben für einen Befund programmatisch abzurufen und aufzudecken. Wenn Sie Ihre Anfrage einreichen, verwenden Sie den `findingId` Parameter, um die eindeutige Kennung für das Ergebnis anzugeben. Um diese Kennung zu erhalten, können Sie die ListFindingsOperation verwenden.

Um Stichproben vertraulicher Daten mithilfe von AWS Command Line Interface (AWS CLI) abzurufen und aufzudecken, führen Sie den get-sensitive-data-occurrencesBefehl aus und verwenden Sie den `finding-id` Parameter, um den eindeutigen Bezeichner für den Befund anzugeben. Beispielsweise:

```
C:\> aws macie2 get-sensitive-data-occurrences --finding-id
 "1f1c2d74db5d8caa76859ec52example"
```

Wobei *1f1c2d74db5d8caa76859ec52example* der eindeutige Bezeichner für den Befund ist. Um diesen Bezeichner mithilfe von zu erhalten, können Sie den Befehl list-findings AWS CLI ausführen.

Wenn Ihre Anfrage erfolgreich ist, beginnt Macie mit der Bearbeitung Ihrer Anfrage und Sie erhalten eine Ausgabe, die der folgenden ähnelt:

```
{
    "status": "PROCESSING"
}
```

Die Bearbeitung Ihrer Anfrage kann mehrere Minuten dauern. Reichen Sie Ihre Anfrage innerhalb weniger Minuten erneut ein.

Wenn Macie die sensiblen Datenproben lokalisieren, abrufen und verschlüsseln kann, gibt Macie die Beispiele in einer Map zurück. `sensitiveDataOccurrences` In der Karte sind 1—100 Arten sensibler Daten angegeben, die aufgrund des Ergebnisses gemeldet wurden, und für jeden Typ 1—10 Stichproben. Jede Stichprobe enthält die ersten 1—128 Zeichen eines Vorkommens sensibler Daten, das aufgrund des Ergebnisses gemeldet wurde.

In der Zuordnung ist jeder Schlüssel die ID der verwalteten Daten-ID, die die sensiblen Daten erkannt hat, oder der Name und die eindeutige Kennung für die benutzerdefinierte Daten-ID, mit der die vertraulichen Daten erkannt wurden. Bei den Werten handelt es sich um Beispiele für den angegebenen verwalteten Datenbezeichner oder den benutzerdefinierten Datenbezeichner.

Die folgende Antwort enthält beispielsweise drei Stichproben für Personennamen und zwei Beispiele für AWS geheime Zugriffsschlüssel, die anhand verwalteter Datenkennungen (`NAME`bzw.`AWS_CREDENTIALS`) erkannt wurden.

```
{
    "sensitiveDataOccurrences": {
        "NAME": [
            {
                "value": "Akua Mansa"
            },
            {
                "value": "John Doe"
            },
            {
                "value": "Martha Rivera"
            }
        ],
        "AWS_CREDENTIALS": [
            {
                "value": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
            },
            {
                "value": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY"
            }
        ]
    },
    "status": "SUCCESS"
}
```

Wenn Ihre Anfrage erfolgreich ist, aber keine Stichproben sensibler Daten für die Suche verfügbar sind, erhalten Sie eine `UnprocessableEntityException` Meldung, in der angegeben wird, warum keine Stichproben verfügbar sind. Beispielsweise:

```
{
    "message": "An error occurred (UnprocessableEntityException) when calling the
 GetSensitiveDataOccurrences operation: OBJECT_UNAVAILABLE"
}
```

Im vorherigen Beispiel hat Macie versucht, Stichproben aus dem betroffenen S3-Objekt abzurufen, aber das Objekt ist nicht mehr verfügbar. Der Inhalt des Objekts wurde geändert, nachdem Macie den Befund erstellt hatte.

Wenn Ihre Anfrage erfolgreich ist, Macie jedoch aufgrund eines anderen Fehlers nicht in der Lage war, Stichproben vertraulicher Daten für den Befund abzurufen und offenzulegen, erhalten Sie eine Ausgabe, die der folgenden ähnelt:

```
{
    "error": "Macie can't retrieve the samples. You're not allowed to access the
 affected S3 object or the object is encrypted with a key that you're not allowed to
 use.",
    "status": "ERROR"
}
```

Der Wert für das `status` Feld ist `ERROR` und das `error` Feld beschreibt den aufgetretenen Fehler. Die Informationen im vorherigen Thema können Ihnen bei der Untersuchung des Fehlers helfen.

JSON-Schema für sensible Datenspeicherorte

Amazon Macie verwendet standardisierte JSON-Strukturen, um Informationen darüber zu speichern, wo sensible Daten in Amazon Simple Storage Service (Amazon S3) -Objekten gefunden werden. Die Strukturen werden für sensible Datenfunde und vertrauliche Datenerfassungsergebnisse verwendet. Bei Ergebnissen sensibler Daten sind die Strukturen Teil des JSON-Schemas für Ergebnisse. Um das vollständige JSON-Schema auf Ergebnisse zu überprüfen, siehe Ergebnisse in der Amazon Macie API-Referenz. Weitere Informationen zu den Ergebnissen der Erkennung vertraulicher Daten finden Sie unterSpeicherung und Beibehaltung der Erkennungsergebnisse von vertraulichen Daten.

Themen

- Überblick über das JSON-Schema für Speicherorte sensibler Daten
- JSON-Schemadetails und Beispiele für Speicherorte sensibler Daten

Überblick über das JSON-Schema für Speicherorte sensibler Daten

Um den Speicherort vertraulicher Daten zu melden, die Amazon Macie in einem betroffenen S3-Objekt gefunden hat, umfasst das JSON-Schema für vertrauliche Datenfunde und Ergebnisse der Erkennung vertraulicher Daten ein `customDataIdentifiers` Objekt und ein `sensitiveData` Objekt. Das `customDataIdentifiers` Objekt enthält Details zu Daten, die Macie mithilfe benutzerdefinierter Datenkennungen erkannt hat. Das `sensitiveData` Objekt enthält Details zu Daten, die Macie mithilfe verwalteter Datenkennungen erkannt hat.

Jedes `customDataIdentifiers` `sensitiveData` Objekt enthält ein oder mehrere `detections` Arrays:

- In einem `customDataIdentifiers` Objekt gibt das `detections` Array an, welche benutzerdefinierten Datenkennungen die Daten erkannt und das Ergebnis generiert haben. Für jeden benutzerdefinierten Datenbezeichner gibt das Array auch die Anzahl der Vorkommen der Daten an, die der Identifier erkannt hat. Es kann auch den Speicherort der Daten angeben, die der Identifier erkannt hat.
- In einem `sensitiveData` Objekt gibt ein `detections` Array die Arten vertraulicher Daten an, die Macie mithilfe verwalteter Datenkennungen erkannt hat. Für jeden Typ sensibler Daten gibt das Array auch die Anzahl der Vorkommen der Daten an und kann den Speicherort der Daten angeben.

Bei der Suche nach vertraulichen Daten kann ein `detections` Array 1—15 `occurrences` Objekte enthalten. Jedes `occurrences` Objekt gibt an, wo Macie einzelne Vorkommen eines bestimmten Typs sensibler Daten entdeckt hat.

Das folgende `detections` Array gibt beispielsweise den Speicherort von drei Vorkommen vertraulicher Daten (US-Sozialversicherungsnummern) an, die Macie in einer CSV-Datei gefunden hat.

```
"sensitiveData": [
     {
       "category": "PERSONAL_INFORMATION",
       "detections": [
          {
             "count": 30,
             "occurrences": {
                "cells": [
                   {
                      "cellReference": null,
                      "column": 1,
                      "columnName": "SSN",
                      "row": 2
                   },
                   {
                      "cellReference": null,
                      "column": 1,
                      "columnName": "SSN",
                      "row": 3
```

```
                },
                {
                   "cellReference": null,
                   "column": 1,
                   "columnName": "SSN",
                   "row": 4
                }
             ]
          },
          "type": "USA_SOCIAL_SECURITY_NUMBER"
       }
```

Die Position und Anzahl der `occurrences` Objekte in einem `detections` Array hängt von den Kategorien, Typen und der Anzahl der Vorkommen vertraulicher Daten ab, die Macie während eines automatisierten Analysezyklus zur Erkennung vertraulicher Daten oder einer Ausführung eines Auftrags zur Erkennung vertraulicher Daten erkennt. Für jeden Analysezyklus oder Auftragsdurchlauf verwendet Macie einen Algorithmus zur Tiefensuche, um die resultierenden Ergebnisse mit Positionsdaten für 1—15 Vorkommen vertraulicher Daten zu füllen, die Macie in S3-Objekten erkennt. Diese Vorkommnisse geben Aufschluss über die Kategorien und Typen vertraulicher Daten, die ein betroffener S3-Bucket und ein betroffenes S3-Objekt enthalten könnten.

Ein `occurrences` Objekt kann je nach Dateityp oder Speicherformat eines betroffenen S3-Objekts die folgenden Strukturen enthalten:

- `cells`array — Dieses Array gilt für Microsoft Excel-Arbeitsmappen, CSV-Dateien und TSV-Dateien. Ein Objekt in diesem Array gibt eine Zelle oder ein Feld an, in dem Macie ein Vorkommen vertraulicher Daten erkannt hat.
- `lineRanges`array — Dieses Array gilt für E-Mail-Nachrichtendateien (EML) und andere nichtbinäre Textdateien als CSV-, JSON-, JSON-Zeilen- und TSV-Dateien, z. B. HTML-, TXT- und XML-Dateien. Ein Objekt in diesem Array gibt eine Zeile oder einen einschließenden Zeilenbereich an, in dem Macie ein Vorkommen vertraulicher Daten erkannt hat, sowie die Position der Daten auf der oder den angegebenen Zeilen.

  In bestimmten Fällen gibt ein Objekt in einem `lineRanges` Array den Ort der Erkennung vertraulicher Daten in einem Dateityp oder Speicherformat an, das von einem anderen Array-Typ unterstützt wird. Bei diesen Fällen handelt es sich um: eine Entdeckung in einem unstrukturierten Abschnitt einer ansonsten strukturierten Datei, z. B. ein Kommentar in einer Datei, eine Entdeckung in einer falsch formatierten Datei, die Macie als Klartext analysiert, und eine CSV- oder TSV-Datei mit einem oder mehreren Spaltennamen, in denen Macie vertrauliche Daten entdeckt hat.

- `offsetRanges`array — Dieses Array ist für die zukünftige Verwendung reserviert. Wenn dieses Array vorhanden ist, ist der Wert dafür Null.
- `pages`array — Dieses Array gilt für Dateien im Adobe Portable Document Format (PDF). Ein Objekt in diesem Array gibt eine Seite an, auf der Macie ein Vorkommen vertraulicher Daten festgestellt hat.
- `records`array — Dieses Array gilt für Apache Avro-Objektcontainer, Apache Parquet-Dateien, JSON-Dateien und JSON Lines-Dateien. Für Avro-Objektcontainer und Parquet-Dateien gibt ein Objekt in diesem Array einen Datensatzindex und den Pfad zu einem Feld in einem Datensatz an, in dem Macie ein Vorkommen vertraulicher Daten erkannt hat. Für JSON- und JSON Lines-Dateien gibt ein Objekt in diesem Array den Pfad zu einem Feld oder Array an, in dem Macie ein Vorkommen vertraulicher Daten erkannt hat. Für JSON Lines-Dateien gibt es auch den Index der Zeile an, die die Daten enthält.

Der Inhalt dieser Arrays variiert je nach Dateityp oder Speicherformat des betroffenen S3-Objekts und seinem Inhalt.

JSON-Schemadetails und Beispiele für Speicherorte sensibler Daten

Amazon Macie passt den Inhalt der verwendeten JSON-Strukturen an, um anzugeben, wo sensible Daten in bestimmten Dateien und Inhalten erkannt wurden. In den folgenden Themen werden diese Strukturen erläutert und Beispiele dafür bereitgestellt.

Themen

- Zellenanordnung
- LineRangesReihe
- Seiten-Array
- Reihe von Datensätzen

Eine vollständige Liste der JSON-Strukturen, die in eine Suche nach vertraulichen Daten aufgenommen werden können, finden Sie unter Ergebnisse in der Amazon Macie API-Referenz.

Zellenanordnung

Gilt für: Microsoft Excel-Arbeitsmappen, CSV-Dateien und TSV-Dateien

In einem `cells` Array gibt ein `Cell` Objekt eine Zelle oder ein Feld an, in dem Macie ein Vorkommen vertraulicher Daten erkannt hat. In der folgenden Tabelle wird der Zweck jedes Felds in einem `Cell` Objekt beschrieben.

Feld	Typ	Beschreibung
`cellReference`	Zeichenfolge	Die Position der Zelle als absolute Zellreferenz, die das Vorkommen enthält. Dieses Feld gilt nur für Excel-Arb eitsmappen. Dieser Wert ist Null für CSV- und TSV-Datei en.
`column`	Ganzzahl	Die Spaltennummer der Spalte, die das Vorkommen enthält. Bei einer Excel-Arb eitsmappe entspricht dieser Wert den alphabetischen Zeichen für einen Spaltenbe zeichner, z. B. für Spalte A, 1 2 für Spalte B usw.
`columnName`	Zeichenfolge	Der Name der Spalte, die das Vorkommen enthält, falls verfügbar.
`row`	Ganzzahl	Die Zeilennummer der Zeile, die das Vorkommen enthält.

Das folgende Beispiel zeigt die Struktur eines `Cell` Objekts, das den Ort eines Vorkommens vertraulicher Daten angibt, die Macie in einer CSV-Datei erkannt hat.

```
"cells": [
   {
      "cellReference": null,
      "column": 3,
      "columnName": "SSN",
```

```
      "row": 5
   }
]
```

Im vorherigen Beispiel deutet das Ergebnis darauf hin, dass Macie vertrauliche Daten in dem Feld in der fünften Zeile der dritten Spalte (mit dem Namen SSN) der Datei erkannt hat.

Das folgende Beispiel zeigt die Struktur eines `Cell` Objekts, das den Ort eines Vorkommens vertraulicher Daten angibt, das Macie in einer Excel-Arbeitsmappe erkannt hat.

```
"cells": [
   {
      "cellReference": "Sheet2!C5",
      "column": 3,
      "columnName": "SSN",
      "row": 5
   }
]
```

Im vorherigen Beispiel deutet das Ergebnis darauf hin, dass Macie vertrauliche Daten in dem Arbeitsblatt mit dem Namen Sheet2 in der Arbeitsmappe entdeckt hat. In diesem Arbeitsblatt entdeckte Macie sensible Daten in der Zelle in der fünften Zeile der dritten Spalte (Spalte C, SSN genannt).

LineRangesReihe

Gilt für: E-Mail-Nachrichtendateien (EML) und andere nichtbinäre Textdateien als CSV-, JSON-, JSON-Zeilen- und TSV-Dateien, z. B. HTML-, TXT- und XML-Dateien

In einem `lineRanges` Array gibt ein `Range` Objekt eine Zeile oder einen einschließenden Zeilenbereich an, in dem Macie ein Vorkommen vertraulicher Daten erkannt hat, sowie die Position der Daten auf der oder den angegebenen Zeilen.

Dieses Objekt ist oft leer für Dateitypen, die von anderen Arten von Arrays in `occurrences` Objekten unterstützt werden. Ausnahmen sind:

- Daten in unstrukturierten Abschnitten einer ansonsten strukturierten Datei, z. B. ein Kommentar in einer Datei.
- Daten in einer falsch formatierten Datei, die Macie als Klartext analysiert.
- Eine CSV- oder TSV-Datei mit einem oder mehreren Spaltennamen, in denen Macie vertrauliche Daten entdeckt hat.

In der folgenden Tabelle wird der Zweck jedes Felds in einem `Range` Objekt eines `lineRanges` Arrays beschrieben.

Feld	Typ	Beschreibung
`end`	Ganzzahl	Die Anzahl der Zeilen vom Anfang der Datei bis zum Ende des Vorfalls.
`start`	Ganzzahl	Die Anzahl der Zeilen vom Anfang der Datei bis zum Beginn des Vorfalls.
`startColumn`	Ganzzahl	Die Anzahl der Zeichen, mit Leerzeichen und beginnend mit 1, vom Anfang der ersten Zeile, die das Vorkommen (`start`) enthält, bis zum Beginn des Vorkommens.

Das folgende Beispiel zeigt die Struktur eines `Range` Objekts, das die Position eines Vorkommens vertraulicher Daten angibt, die Macie in einer einzigen Zeile in einer TXT-Datei erkannt hat.

```
"lineRanges": [
   {
      "end": 1,
      "start": 1,
      "startColumn": 119
   }
]
```

Im vorherigen Beispiel deutet das Ergebnis darauf hin, dass Macie in der ersten Zeile der Datei ein vollständiges Vorkommen vertraulicher Daten (eine Postanschrift) entdeckt hat. Das erste Zeichen des Vorkommens liegt 119 Zeichen (mit Leerzeichen) vom Zeilenanfang entfernt.

Das folgende Beispiel zeigt die Struktur eines `Range` Objekts, das die Position eines Vorkommens vertraulicher Daten angibt, das sich über mehrere Zeilen in einer TXT-Datei erstreckt.

```
"lineRanges": [
```

```
   {
      "end": 54,
      "start": 51,
      "startColumn": 1
   }
]
```

Im vorherigen Beispiel deutet das Ergebnis darauf hin, dass Macie ein Vorkommen sensibler Daten (eine Postanschrift) in den Zeilen 51 bis 54 der Datei entdeckt hat. Das erste Zeichen des Vorkommnisses ist das erste Zeichen in Zeile 51 der Datei.

Seiten-Array

Gilt für: Adobe Portable Document Format (PDF) -Dateien

In einem `pages` Array gibt ein `Page` Objekt eine Seite an, auf der Macie ein Vorkommen vertraulicher Daten festgestellt hat. Das Objekt enthält ein `pageNumber` Feld. Das `pageNumber` Feld speichert eine Ganzzahl, die die Seitennummer der Seite angibt, die das Vorkommen enthält.

Das folgende Beispiel zeigt die Struktur eines `Page` Objekts, das den Ort eines Vorkommens vertraulicher Daten angibt, die Macie in einer PDF-Datei erkannt hat.

```
"pages": [
   {
      "pageNumber": 10
   }
]
```

Im vorherigen Beispiel deutet das Ergebnis darauf hin, dass Seite 10 der Datei das Ereignis enthält.

Reihe von Datensätzen

Gilt für: Apache Avro-Objektcontainer, Apache Parquet-Dateien, JSON-Dateien und JSON Lines-Dateien

Für einen Avro-Objektcontainer oder eine Parquet-Datei gibt ein `Record` Objekt in einem `records` Array einen Datensatzindex und den Pfad zu einem Feld in einem Datensatz an, in dem Macie ein Vorkommen vertraulicher Daten erkannt hat. Für JSON- und JSON Lines-Dateien gibt ein `Record` Objekt den Pfad zu einem Feld oder Array an, in dem Macie ein Vorkommen vertraulicher Daten erkannt hat. Für JSON-Lines-Dateien gibt es auch den Index der Zeile an, die das Vorkommen enthält.

In der folgenden Tabelle wird der Zweck jedes Felds in einem `Record` Objekt beschrieben.

Feld	Typ	Beschreibung
`jsonPath`	Zeichenfolge	Der Pfad zum Vorkommen als JsonPath-Ausdruck. Bei einem Avro-Objektcontainer oder einer Parquet-Datei ist dies der Pfad zu dem Feld im Datensatz (`recordIndex`), das das Vorkommen enthält. Für eine JSON- oder JSON Lines-Datei ist dies der Pfad zu dem Feld oder Array, das das Vorkommen enthält. Wenn es sich bei den Daten um einen Wert in einem Array handelt, gibt der Pfad auch an, welcher Wert das Vorkommen enthält. Wenn Macie vertrauliche Daten im Namen eines Elements im Pfad erkennt, lässt Macie das `jsonPath` Feld in einem Objekt aus. `Record` Wenn der Name eines Pfadelements 240 Zeichen überschreitet, kürzt Macie den Namen, indem er Zeichen vom Anfang des Namens entfernt. Wenn der resultierende vollständige Pfad mehr als 250 Zeichen enthält, kürzt Macie auch den Pfad ab, beginnend mit dem ersten

Feld	Typ	Beschreibung
		Element im Pfad, bis der Pfad 250 oder weniger Zeichen enthält.
`recordIndex`	Ganzzahl	Für einen Avro-Objektcontainer oder eine Parquet-Datei der Datensatzindex, beginnend bei 0, für den Datensatz, der das Vorkommen enthält. Für eine JSON-Lines-Datei der Zeilenindex, beginnend bei 0, für die Zeile, die das Vorkommen enthält. Dieser Wert gilt immer `0` für JSON-Dateien.

Das folgende Beispiel zeigt die Struktur eines `Record` Objekts, das den Speicherort eines Vorkommens vertraulicher Daten angibt, die Macie in einer Parquet-Datei erkannt hat.

```
"records": [
   {
      "jsonPath": "$['abcdefghijklmnopqrstuvwxyz']",
      "recordIndex": 7663
   }
]
```

Im vorherigen Beispiel deutet das Ergebnis darauf hin, dass Macie sensible Daten im Datensatz des Index 7663 (Datensatznummer 7664) entdeckt hat. In diesem Datensatz entdeckte Macie sensible Daten in dem genannten `abcdefghijklmnopqrstuvwxyz` Feld. Der vollständige JSON-Pfad zum Feld im Datensatz lautet`$.abcdefghijklmnopqrstuvwxyz`. Das Feld ist ein direkter Abkömmling des Stammobjekts (äußere Ebene).

Das folgende Beispiel zeigt auch die Struktur eines `Record` Objekts für ein Vorkommen vertraulicher Daten, die Macie in einer Parquet-Datei erkannt hat. In diesem Beispiel hat Macie den Namen des Felds, das das Vorkommen enthält, jedoch gekürzt, da der Name die Zeichenbeschränkung überschreitet.

```
"records": [
   {
      "jsonPath":
 "$['...uvwxyzabcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyzabc
      "recordIndex": 7663
   }
]
```

Im vorherigen Beispiel ist das Feld ein direkter Abkömmling des Stammobjekts (äußere Ebene).

Im folgenden Beispiel hat Macie bei einem Vorkommen vertraulicher Daten, das Macie in einer Parquet-Datei entdeckt hat, den vollständigen Pfad zu dem Feld gekürzt, das das Vorkommen enthält. Der vollständige Pfad überschreitet das Zeichenlimit.

```
"records": [
   {
      "jsonPath":
 "$..usssn2.usssn3.usssn4.usssn5.usssn6.usssn7.usssn8.usssn9.usssn10.usssn11.usssn12.usssn13.us
      "recordIndex": 2335
   }
]
```

Im vorherigen Beispiel deutet das Ergebnis darauf hin, dass Macie sensible Daten im Datensatz des Index 2335 (Datensatznummer 2336) entdeckt hat. In diesem Datensatz entdeckte Macie sensible Daten in dem genannten `abcdefghijklmnopqrstuvwxyz` Feld. Der vollständige JSON-Pfad zum Feld im Datensatz lautet:

```
$['1234567890']usssn1.usssn2.usssn3.usssn4.usssn5.usssn6.usssn7.usssn8.usssn9.us
```

Das folgende Beispiel zeigt die Struktur eines `Record` Objekts, das den Speicherort eines Vorkommens vertraulicher Daten angibt, die Macie in einer JSON-Datei erkannt hat. In diesem Beispiel ist das Vorkommen ein bestimmter Wert in einem Array.

```
"records": [
   {
      "jsonPath": "$.access.key[2]",
      "recordIndex": 0
   }
]
```

Im vorherigen Beispiel deutet das Ergebnis darauf hin, dass Macie sensible Daten im zweiten Wert eines Arrays mit dem Namen `key` erkannt hat. Das Array ist ein untergeordnetes Objekt mit dem Name`access`.

Das folgende Beispiel zeigt die Struktur eines `Record` Objekts, das den Ort eines Vorkommens vertraulicher Daten angibt, das Macie in einer JSON Lines-Datei erkannt hat.

```
"records": [
   {
      "jsonPath": "$.access.key",
      "recordIndex": 3
   }
]
```

Im vorherigen Beispiel deutet das Ergebnis darauf hin, dass Macie sensible Daten im dritten Wert (Zeile) der Datei erkannt hat. In dieser Zeile befindet sich das Vorkommen in einem Feld mit dem Name`key`, das einem Objekt mit dem Namen untergeordnet ist`access`.

Unterdrückung von Amazon Macie Macie-Ergebnissen

Um Ihre Analyse der Ergebnisse zu optimieren, können Sie Unterdrückungsregeln erstellen und verwenden. Eine Unterdrückungsregel besteht aus einer Reihe von attributbasierten Filterkriterien, die Fälle definieren, in denen Amazon Macie Ergebnisse automatisch archivieren soll. Unterdrückungsregeln sind in Situationen hilfreich, in denen Sie eine Gruppe von Ergebnissen überprüft haben und nicht erneut darüber informiert werden möchten.

Sie könnten beispielsweise festlegen, dass S3-Buckets Postanschriften enthalten dürfen, wenn die Buckets keinen öffentlichen Zugriff zulassen und sie neue Objekte automatisch mit einer bestimmten Adresse verschlüsseln. AWS KMS key In diesem Fall können Sie eine Unterdrückungsregel erstellen, die Filterkriterien für die folgenden Felder festlegt: Erkennungstyp vertraulicher Daten, öffentliche Zugriffsberechtigung für S3-Buckets und KMS-Schlüssel-ID für die S3-Bucket-Verschlüsselung. Die Regel unterdrückt future Ergebnisse, die den Filterkriterien entsprechen.

Wenn Sie Ergebnisse mit einer Unterdrückungsregel unterdrücken, generiert Macie weiterhin Ergebnisse für nachfolgende Fälle vertraulicher Daten und potenzieller Richtlinienverstöße, die den Kriterien der Regel entsprechen. Macie ändert den Status der Ergebnisse jedoch automatisch in archiviert. Das bedeutet, dass die Ergebnisse nicht standardmäßig auf der Amazon Macie Macie-Konsole angezeigt werden, sondern in Macie gespeichert werden, bis sie ablaufen. Macie speichert Ergebnisse 90 Tage lang.

Darüber hinaus veröffentlicht Macie unterdrückte Ergebnisse nicht EventBridge als Ereignisse oder für Amazon. AWS Security Hub Macie erstellt und speichert jedoch weiterhin Ergebnisse der Entdeckung sensibler Daten, die mit Ergebnissen vertraulicher Daten korrelieren, die Sie unterdrücken. Auf diese Weise können Sie sicherstellen, dass Sie über eine unveränderliche Historie an Ergebnissen sensibler Daten verfügen, die bei von Ihnen durchgeführten Datenschutzprüfungen oder Untersuchungen ermittelt wurden.

> **Note**
>
> Wenn Ihr Konto Teil einer Organisation ist, die mehrere Macie-Konten zentral verwaltet, gelten die Sperrregeln für Ihr Konto möglicherweise anders. Dies hängt von der Kategorie der Ergebnisse ab, die Sie unterdrücken möchten, und davon, ob Sie ein Macie-Administrator- oder Mitgliedskonto haben:
>
> - Richtlinienergebnisse — Nur ein Macie-Administrator kann Richtlinienergebnisse für die Konten der Organisation unterdrücken.
>
>   Wenn Sie ein Macie-Administratorkonto haben und eine Unterdrückungsregel erstellen, wendet Macie die Regel auf die Richtlinienfeststellungen für alle Konten in Ihrer Organisation an, sofern Sie die Regel nicht so konfigurieren, dass bestimmte Konten ausgeschlossen werden. Wenn Sie ein Macie-Mitgliedskonto haben und die Richtlinienfeststellungen für Ihr Konto unterdrücken möchten, wenden Sie sich an Ihren Macie-Administrator.
> - Ergebnisse sensibler Daten — Ein Macie-Administrator und einzelne Mitglieder können die Ergebnisse sensibler Daten unterdrücken, die bei ihren Aufträgen zur Entdeckung sensibler Daten entstehen. Ein Macie-Administrator kann auch Ergebnisse unterdrücken, die Macie bei der automatisierten Erkennung sensibler Daten für das Unternehmen generiert.
>
>   Nur das Konto, das einen Auftrag zur Erkennung sensibler Daten erstellt, kann die Ergebnisse, die der Job generiert, unterdrücken oder auf andere Weise darauf zugreifen. Nur das Macie-Administratorkonto einer Organisation kann Ergebnisse unterdrücken oder auf andere Weise darauf zugreifen, die bei der automatischen Erkennung sensibler Daten für Konten in der Organisation entstehen.
>
> Weitere Informationen zu den Aufgaben, die Administratoren und Mitglieder ausführen können, finden Sie unterDie Beziehung zwischen Amazon Macie-Administrator- und Mitgliedskonten verstehen.

Um Unterdrückungsregeln zu erstellen und zu verwalten, können Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden. In den folgenden Themen wird erklärt, wie das geht. Für die API enthalten die Themen Beispiele dafür, wie diese Aufgaben mithilfe von AWS Command Line Interface(AWS CLI) ausgeführt werden können. Sie können diese Aufgaben auch ausführen, indem Sie eine aktuelle Version eines anderen AWS Befehlszeilentools oder eines AWS SDK verwenden oder indem Sie HTTPS-Anfragen direkt an Macie senden. Informationen zu AWS Tools und SDKs finden Sie unter Tools, auf denen Sie aufbauen können. AWS

Themen

- Unterdrückungsregeln erstellen
- Überprüfung unterdrückter Ergebnisse
- Unterdrückungsregeln ändern
- Löschen von Unterdrückungsregeln

Unterdrückungsregeln erstellen

Bevor Sie eine Unterdrückungsregel erstellen, sollten Sie beachten, dass Sie Ergebnisse, die Sie mithilfe einer Unterdrückungsregel unterdrückt haben, nicht wiederherstellen (die Archivierung aufheben) können. Sie können jedoch unterdrückte Ergebnisse auf der Amazon Macie Macie-Konsole überprüfen und mit der Amazon Macie Macie-API auf unterdrückte Ergebnisse zugreifen.

Wenn Sie eine Unterdrückungsregel erstellen, geben Sie Filterkriterien, einen Namen und optional eine Beschreibung der Regel an. Sie können mithilfe der Amazon Macie-Konsole oder der Amazon Macie Macie-API eine Unterdrückungsregel erstellen.

Console

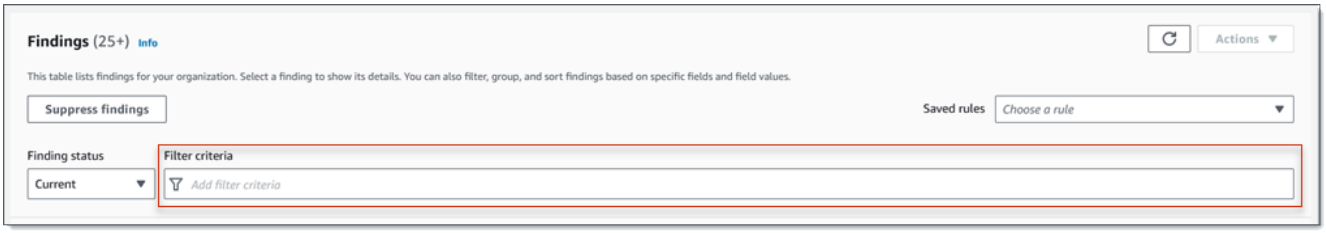
Gehen Sie wie folgt vor, um mithilfe der Amazon Macie Macie-Konsole eine Unterdrückungsregel zu erstellen.

So erstellen Sie eine Unterdrückungsregel

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich Findings aus.

> **Tip**
>
> Um eine bestehende Unterdrückungs- oder Filterregel als Ausgangspunkt zu verwenden, wählen Sie die Regel aus der Liste Gespeicherte Regeln aus.
> Sie können die Erstellung einer Regel auch vereinfachen, indem Sie die Ergebnisse zunächst anhand einer vordefinierten logischen Gruppe durchblättern und anschließend aufschlüsseln. In diesem Fall erstellt Macie automatisch die entsprechenden Filterbedingungen und wendet sie an. Dies kann ein hilfreicher Ausgangspunkt für die Erstellung einer Regel sein. Wählen Sie dazu im Navigationsbereich (unter Ergebnisse) die Option Nach Bereich, Nach Typ oder Nach Auftrag und wählen Sie dann ein Element in der Tabelle aus. Wählen Sie im Detailbereich den Link für das Feld aus, auf das Sie sich konzentrieren möchten.

3. Fügen Sie im Feld Filterkriterien Filterbedingungen hinzu, die die Attribute der Ergebnisse angeben, die durch die Regel unterdrückt werden sollen.



   Informationen zum Hinzufügen von Filterbedingungen finden Sie unterFilter erstellen und auf Ergebnisse anwenden.

4. Wenn Sie mit dem Hinzufügen von Filterbedingungen für die Regel fertig sind, wählen Sie Ergebnisse unterdrücken aus.
5. Geben Sie unter Unterdrückungsregel einen Namen und optional eine Beschreibung der Regel ein.
6. Wählen Sie Speichern aus.

API

Um eine Unterdrückungsregel programmgesteuert zu erstellen, verwenden Sie den CreateFindingsFilterBetrieb der Amazon Macie Macie-API und geben Sie die entsprechenden Werte für die erforderlichen Parameter an:

- Geben Sie für den `action` Parameter an, `ARCHIVE` um sicherzustellen, dass Macie Ergebnisse unterdrückt, die den Kriterien der Regel entsprechen.
- Geben Sie für den `criterion` Parameter eine Zuordnung von Bedingungen an, die die Filterkriterien für die Regel definieren.

  In der Map sollte jede Bedingung ein Feld, einen Operator und einen oder mehrere Werte für das Feld angeben. Der Typ und die Anzahl der Werte hängen vom ausgewählten Feld und Operator ab. Informationen zu den Feldern, Operatoren und Wertetypen, die Sie in einer Bedingung verwenden können, finden Sie unter Felder zum Filtern von ErgebnissenVerwenden von Operatoren unter bestimmten Bedingungen, undWerte für Felder angeben.

Um mit dem eine Unterdrückungsregel zu erstellenAWS CLI, führen Sie den create-findings-filterBefehl aus und geben Sie die entsprechenden Werte für die erforderlichen Parameter an. In den folgenden Beispielen wird eine Unterdrückungsregel erstellt, die alle Ergebnisse aus der aktuellen Version zurückgibt AWS-Region und das Vorkommen von Postanschriften (und keine anderen Arten vertraulicher Daten) in S3-Objekten meldet.

Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\), um die Lesbarkeit zu verbessern.

```
$ aws macie2 create-findings-filter \
--action ARCHIVE \
--name my_suppression_rule \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.detections.type":{"eqExactMatch":
["ADDRESS"]}}}'
```

Dieses Beispiel ist für Microsoft Windows formatiert und verwendet das Zeilenfortsetzungszeichen Caret (^), um die Lesbarkeit zu verbessern.

```
C:\> aws macie2 create-findings-filter ^
--action ARCHIVE ^
--name my_suppression_rule ^
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.detections.type\":{\"eqExactMatch\":
[\"ADDRESS\"]}}}
```

Wobei gilt:

- *my_suppression_rule* ist der benutzerdefinierte Name für die Regel.
- `criterion`ist eine Übersicht der Filterbedingungen für die Regel:
  - *ClassificationDetails.Result.SensitiveData.Detections.Type ist der JSON-Name des Felds für den Erkennungstyp* sensible Daten.
  - *eqExactMatch*gibt den Gleichheitsoperator für exakte Übereinstimmung an.
  - *ADDRESS* ist ein Aufzählungswert für das Feld Typ der Erkennung sensibler Daten.

Wird der Befehl erfolgreich ausgeführt, erhalten Sie eine Ausgabe ähnlich der folgenden:

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a3c5608-
aa2f-4940-b347-d1451example",
    "id": "8a3c5608-aa2f-4940-b347-d1451example"
}
```

Wo `arn` ist der Amazon-Ressourcenname (ARN) der Unterdrückungsregel, die erstellt wurde, und `id` ist der eindeutige Bezeichner für die Regel.

Weitere Beispiele für Filterkriterien finden Sie unterProgrammgesteuertes Filtern von Ergebnissen mit der Amazon Macie API.

Überprüfung unterdrückter Ergebnisse

Standardmäßig zeigt Macie keine unterdrückten Ergebnisse auf der Amazon Macie Macie-Konsole an. Sie können diese Ergebnisse jedoch auf der Konsole überprüfen, indem Sie Ihre Filtereinstellungen ändern.

Um unterdrückte Ergebnisse auf der Konsole zu überprüfen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich Findings aus. Auf der Seite mit den Ergebnissen werden Ergebnisse angezeigt, die Macie in den letzten 90 Tagen für Ihr Konto erstellt oder aktualisiert hat. AWS-Region Standardmäßig sind hier keine Ergebnisse enthalten, die durch eine Unterdrückungsregel unterdrückt wurden.
3. Führen Sie unter Status suchen einen der folgenden Schritte aus:

   - Um nur unterdrückte Ergebnisse anzuzeigen, wählen Sie Archiviert.

- Um sowohl unterdrückte als auch nicht unterdrückte Ergebnisse anzuzeigen, wählen Sie Alle.
- Um die unterdrückten Ergebnisse wieder auszublenden, wählen Sie „Aktuell“.

Sie können auch mithilfe der Amazon Macie Macie-API auf unterdrückte Ergebnisse zugreifen. Um eine Liste mit unterdrückten Ergebnissen abzurufen, verwenden Sie den ListFindingsVorgang und fügen Sie eine Filterbedingung hinzu, die `true` für das Feld spezifiziert ist. `archived` Ein Beispiel dafür, wie Sie dies mit dem tun könnenAWS CLI, finden Sie unterProgrammgesteuertes Filtern von Ergebnissen. Um anschließend die Details eines oder mehrerer unterdrückter Ergebnisse abzurufen, verwenden Sie den GetFindingsVorgang und geben Sie die eindeutige Kennung für jedes abzurufende Ergebnis an.

Unterdrückungsregeln ändern

Sie können die Einstellungen für eine Unterdrückungsregel jederzeit mithilfe der Amazon Macie Macie-Konsole oder der Amazon Macie Macie-API ändern. Sie können der Regel auch Tags zuweisen und verwalten.

Ein Tag ist eine Bezeichnung, die Sie definieren und bestimmten Ressourcentypen AWS zuweisen. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Mithilfe von Tags können Sie Ressourcen auf unterschiedliche Weise identifizieren, kategorisieren und verwalten, z. B. nach Zweck, Eigentümer, Umgebung oder anderen Kriterien. Weitere Informationen hierzu finden Sie unter Kennzeichnen von Amazon Macie-Ressourcen.

Console

Gehen Sie wie folgt vor, um die Einstellungen für eine bestehende Unterdrückungsregel mithilfe der Amazon Macie Macie-Konsole zu ändern.

Um eine Unterdrückungsregel zu ändern

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich Findings aus.
3. Wählen Sie in der Liste Gespeicherte Regeln das Bearbeitungssymbol (✎) neben der Unterdrückungsregel aus, die Sie ändern möchten.
4. Führen Sie eine der folgenden Aktionen aus:

- Um die Kriterien der Regel zu ändern, geben Sie im Feld Filterkriterien Bedingungen ein, die Attribute der Ergebnisse angeben, die von der Regel unterdrückt werden sollen. Um zu erfahren wie dies geht, vgl. Filter erstellen und auf Ergebnisse anwenden.
- Um den Namen der Regel zu ändern, geben Sie im Feld Name unter Unterdrückungsregel einen neuen Namen ein.
- Um die Beschreibung der Regel zu ändern, geben Sie im Feld Beschreibung unter Unterdrückungsregel eine neue Beschreibung ein.
- Um der Regel Tags zuzuweisen, zu überprüfen oder zu bearbeiten, wählen Sie unter Unterdrückungsregel die Option Tags verwalten aus. Überprüfen Sie dann die Tags und ändern Sie sie nach Bedarf. Eine Regel kann bis zu 50 Tags enthalten.

5. Wenn Sie die gewünschten Änderungen vorgenommen haben, wählen Sie Save (Speichern) aus.

API

Um eine Unterdrückungsregel programmgesteuert zu ändern, verwenden Sie den UpdateFindingsFilterBetrieb der Amazon Macie Macie-API. Wenn Sie Ihre Anfrage einreichen, verwenden Sie die unterstützten Parameter, um für jede Einstellung, die Sie ändern möchten, einen neuen Wert anzugeben.

Geben Sie für den `id` Parameter den eindeutigen Bezeichner für die zu ändernde Regel an. Sie können diese Kennung abrufen, indem Sie den ListFindingsFilterVorgang verwenden, um eine Liste von Unterdrückungs- und Filterregeln für Ihr Konto abzurufen. Wenn Sie den verwendenAWS CLI, führen Sie den list-findings-filtersBefehl aus, um diese Liste abzurufen.

Um eine Unterdrückungsregel mithilfe von zu ändernAWS CLI, führen Sie den update-findings-filterBefehl aus und geben Sie mithilfe der unterstützten Parameter für jede Einstellung, die Sie ändern möchten, einen neuen Wert an. Mit dem folgenden Befehl wird beispielsweise der Name einer vorhandenen Unterdrückungsregel geändert.

```
C:\> aws macie2 update-findings-filter --id 8a3c5608-aa2f-4940-b347-d1451example --
name mailing_addresses_only
```

Wobei gilt:

- *`8a3c5608-aa2f-4940-b347-d1451example`* ist der eindeutige Bezeichner für die Regel.
- *`mailing_addresses_only ist der neue Name für die`* Regel.

Wird der Befehl erfolgreich ausgeführt, erhalten Sie eine Ausgabe ähnlich der folgenden:

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a3c5608-
aa2f-4940-b347-d1451example",
    "id": "8a3c5608-aa2f-4940-b347-d1451example"
}
```

Wo `arn` ist der Amazon-Ressourcenname (ARN) der Regel, die geändert wurde, und `id` ist der eindeutige Bezeichner für die Regel.

In ähnlicher Weise konvertiert das folgende Beispiel eine Filterregel in eine Unterdrückungsregel, indem der Wert für den `action` Parameter von `NOOP` bis geändert wird`ARCHIVE`.

```
C:\> aws macie2 update-findings-filter --id 8a1c3508-aa2f-4940-b347-d1451example --
action ARCHIVE
```

Wobei gilt:

- *`8a1c3508-aa2f-4940-b347-d1451example`* ist der eindeutige Bezeichner für die Regel.
- *`ARCHIVE`* ist die neue Aktion, die Macie bei Ergebnissen durchführen kann, die den Kriterien der Regel entsprechen — Ergebnisse unterdrücken.

Wenn der Befehl erfolgreich ausgeführt wird, erhalten Sie eine Ausgabe, die der folgenden ähnelt:

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a1c3508-
aa2f-4940-b347-d1451example",
    "id": "8a1c3508-aa2f-4940-b347-d1451example"
}
```

Wo `arn` ist der Amazon-Ressourcenname (ARN) der Regel, die geändert wurde, und `id` ist der eindeutige Bezeichner für die Regel.

Löschen von Unterdrückungsregeln

Sie können eine Unterdrückungsregel jederzeit mithilfe der Amazon Macie Macie-Konsole oder der Amazon Macie Macie-API löschen. Wenn Sie eine Unterdrückungsregel löschen, beendet Macie die

Unterdrückung neuer und nachfolgender Ergebnisse, die den Kriterien der Regel entsprechen und nicht durch andere Regeln unterdrückt werden. Beachten Sie jedoch, dass Macie möglicherweise weiterhin Ergebnisse unterdrückt, die gerade verarbeitet werden und die Kriterien der Regel erfüllen.

Nachdem Sie eine Unterdrückungsregel gelöscht haben, erhalten neue und nachfolgende Ergebnisse, die den Kriterien der Regel entsprechen, den Status Aktuell (nicht archiviert). Dies bedeutet, dass sie standardmäßig auf der Amazon Macie Macie-Konsole angezeigt werden. Darüber hinaus veröffentlicht Macie diese Ergebnisse EventBridge als Ereignisse bei Amazon. Abhängig von den Veröffentlichungseinstellungen für Ihr Konto veröffentlicht Macie die Ergebnisse auch auf. AWS Security Hub

Console

Gehen Sie wie folgt vor, um eine Unterdrückungsregel mithilfe der Amazon Macie Macie-Konsole zu löschen.

Um eine Unterdrückungsregel zu löschen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich Findings aus.
3. Wählen Sie in der Liste Gespeicherte Regeln das Bearbeitungssymbol (✎) neben der Unterdrückungsregel aus, die Sie löschen möchten.
4. Wählen Sie unter Unterdrückungsregel die Option Löschen aus.

API

Um eine Unterdrückungsregel programmgesteuert zu löschen, verwenden Sie den DeleteFindingsFilterBetrieb der Amazon Macie Macie-API. Geben Sie für den `id` Parameter die eindeutige Kennung für die zu löschende Unterdrückungsregel an. Sie können diese Kennung abrufen, indem Sie den ListFindingsFilterVorgang verwenden, um eine Liste von Unterdrückungs- und Filterregeln für Ihr Konto abzurufen. Wenn Sie den verwendenAWS CLI, führen Sie den list-findings-filtersBefehl aus, um diese Liste abzurufen.

Um eine Unterdrückungsregel mithilfe von zu löschenAWS CLI, führen Sie den delete-findings-filterBefehl aus. Beispiele:

```
C:\> aws macie2 delete-findings-filter --id 8a3c5608-aa2f-4940-b347-d1451example
```

Wobei *8a3c5608-aa2f-4940-b347-d1451example* der eindeutige Bezeichner für die zu löschende Unterdrückungsregel ist.

Wenn der Befehl erfolgreich ausgeführt wird, gibt Macie eine leere HTTP 200-Antwort zurück. Andernfalls gibt Macie eine HTTP 4 xx - oder 500-Antwort zurück, die angibt, warum der Vorgang fehlgeschlagen ist.

Bewertung des Schweregrads der Amazon Macie Macie-Ergebnisse

Wenn Amazon Macie eine Richtlinie oder ein Ergebnis sensibler Daten generiert, weist es dem Ergebnis automatisch einen Schweregrad zu. Der Schweregrad eines Ergebnisses spiegelt die Hauptmerkmale des Ergebnisses wider und kann Ihnen dabei helfen, Ihre Ergebnisse zu bewerten und zu priorisieren. Der Schweregrad eines Ergebnisses impliziert nicht die Wichtigkeit oder Bedeutung, die eine betroffene Ressource für Ihr Unternehmen haben könnte, und gibt auch keinen Hinweis darauf.

Der Schweregrad der Richtlinien hängt von der Art eines potenziellen Problems mit der Sicherheit oder dem Datenschutz Ihrer Amazon Simple Storage Service (Amazon S3) -Daten ab. Bei Feststellungen zu sensiblen Daten hängt der Schweregrad von der Art und Anzahl der Vorkommen sensibler Daten ab, die Macie in einem S3-Objekt gefunden hat.

In Macie wird der Schweregrad eines Befundes auf zwei Arten dargestellt.

Schweregrad

Dies ist eine qualitative Darstellung des Schweregrads. Die Schweregrade reichen von Low„am leichtesten“ bis High„am schwersten“.

Schweregrade werden direkt auf der Amazon Macie Macie-Konsole angezeigt. Sie sind auch in JSON-Darstellungen von Ergebnissen auf der Macie-Konsole, in der Amazon Macie Macie-API und in Ergebnissen der Erkennung sensibler Daten verfügbar, die mit Ergebnissen sensibler Daten korrelieren. Schweregrade werden auch bei der Suche nach Ereignissen berücksichtigt, die Macie auf Amazon veröffentlicht, EventBridge und bei Ergebnissen, für die Macie veröffentlicht. AWS Security Hub

Schweregrad

Dies ist eine numerische Darstellung des Schweregrads. Die Schweregrade reichen von 1 bis 3 und werden direkt den Schweregraden zugeordnet:

Schweregrad	Schweregrad
1	Niedrig
2	Mittelschwer
3	Hoch

Schweregrade werden nicht direkt auf der Amazon Macie Macie-Konsole angezeigt. Sie sind jedoch in JSON-Darstellungen von Ergebnissen auf der Macie-Konsole, in der Amazon Macie Macie-API und in Ergebnissen der Erkennung sensibler Daten verfügbar, die mit Ergebnissen sensibler Daten korrelieren. Schweregrade werden auch bei der Suche nach Ereignissen berücksichtigt, die Macie auf Amazon EventBridge veröffentlicht. Sie sind nicht in den Ergebnissen enthalten, für die Macie veröffentlicht. AWS Security Hub

Die Themen in diesem Abschnitt zeigen, wie Macie den Schweregrad von politischen Feststellungen und Ergebnissen sensibler Daten bestimmt.

Themen

- Bewertung des Schweregrads von politischen Ergebnissen
- Bewertung des Schweregrads von Ergebnissen sensibler Daten

Bewertung des Schweregrads von politischen Ergebnissen

Der Schweregrad einer Richtlinienfeststellung hängt von der Art eines potenziellen Problems mit der Sicherheit oder dem Datenschutz eines S3-Buckets ab. In der folgenden Tabelle sind die Schweregrade aufgeführt, die Macie jeder Art von Richtlinienfeststellung zuweist. Eine Beschreibung der einzelnen Typen finden Sie unter. Arten von Ergebnissen

Ergebnistyp	Schweregrad
Policy:IAMUser/S3BlockPublicAccessDisabled	Hoch
Policy:IAMUser/S3BucketEncryptionDisabled	Niedrig
Policy:IAMUser/S3BucketPublic	Hoch

Ergebnistyp	Schweregrad
Policy:IAMUser/S3BucketReplicatedExternally	Hoch
Policy:IAMUser/S3BucketSharedExternally	Hoch
Policy:IAMUser/S3BucketSharedWithCloudFront	Mittelschwer

Der Schweregrad einer Richtlinienfeststellung hängt nicht von der Anzahl der Fälle ab.

Bewertung des Schweregrads von Ergebnissen sensibler Daten

Der Schweregrad einer Entdeckung sensibler Daten hängt von der Art und Anzahl der Vorkommen sensibler Daten ab, die Macie in einem S3-Objekt gefunden hat. In den folgenden Themen wird beschrieben, wie Macie den Schweregrad der einzelnen Arten von Ergebnissen sensibler Daten bestimmt:

- SensitiveData:S3Object/Credentials
- SensitiveData:S3Object/CustomIdentifier
- SensitiveData:S3Object/Financial
- SensitiveData:S3Object/Personal
- SensitiveData:S3Object/Multiple

Ausführliche Informationen zu den Arten vertraulicher Daten, die Macie erkennen und als Ergebnisse sensibler Daten melden kann, finden Sie unter Verwenden von verwalteten Datenbezeichnern und. Erstellen von benutzerdefinierten Datenbezeichnern

SensitiveData:S3Object/Credentials

A:Der SensitiveDataBefund S3Object/Credentials weist darauf hin, dass ein S3-Objekt vertrauliche Anmeldeinformationen enthält. Bei dieser Art von Entdeckung bestimmt Macie den Schweregrad anhand der Art und Anzahl der Vorkommen der Anmeldedaten, die Macie im Objekt gefunden hat.

In der folgenden Tabelle sind die Schweregrade aufgeführt, die Macie Ergebnissen zuweist, bei denen das Vorkommen von Anmeldedaten in einem S3-Objekt gemeldet wird.

Vertraulicher Datentyp	1 Vorkommen	2—99 Vorkommen	100 oder mehr Vorkommen
Geheimer AWS-Zugriffsschlüssel	Hoch	Hoch	Hoch
Google Cloud-API-Schlüssel	Hoch	Hoch	Hoch
Header für die grundlegende HTTP-Autorisierung	Hoch	Hoch	Hoch
JSON-Webtoken (JWT)	Hoch	Hoch	Hoch
Privater OpenSSH-Schlüssel	Hoch	Hoch	Hoch
Privater PGP-Schlüssel	Hoch	Hoch	Hoch
Privater Schlüssel nach dem Public Key Cryptography Standard (PKCS)	Hoch	Hoch	Hoch
Privater PuTTY-Schlüssel	Hoch	Hoch	Hoch
Stripe-API-Schlüssel	Hoch	Hoch	Hoch

SensitiveData:S3Object/CustomIdentifier

A:S3Object/ CustomIdentifier gibt an SensitiveData, dass ein S3-Objekt Text enthält, der den Erkennungskriterien eines oder mehrerer benutzerdefinierter Datenbezeichner entspricht. Das Objekt kann mehr als einen Typ sensibler Daten enthalten.

Standardmäßig weist Macie dieser Art von Ergebnissen den Schweregrad Mittel zu. Wenn das S3-Objekt mindestens einmal Text enthält, der den Erkennungskriterien mindestens einer benutzerdefinierten Daten-ID entspricht, weist Macie dem Ergebnis automatisch den Schweregrad Mittel zu. Der Schweregrad des Ergebnisses ändert sich nicht, je nachdem, wie oft Text vorkommt, der den Kriterien einer benutzerdefinierten Daten-ID entspricht.

Der Schweregrad dieser Art von Befund kann jedoch variieren, wenn Sie benutzerdefinierte Schweregradeinstellungen für eine benutzerdefinierte Daten-ID definiert haben, die zu dem Ergebnis geführt hat. Wenn dies der Fall ist, bestimmt Macie den Schweregrad wie folgt:

- Wenn das S3-Objekt Text enthält, der den Erkennungskriterien nur eines benutzerdefinierten Datenbezeichners entspricht, bestimmt Macie den Schweregrad des Ergebnisses anhand der Schweregradeinstellungen für diesen Bezeichner.
- Wenn das S3-Objekt Text enthält, der den Erkennungskriterien mehrerer benutzerdefinierter Datenbezeichner entspricht, bestimmt Macie den Schweregrad des Ergebnisses, indem es die Schweregradeinstellungen für jede benutzerdefinierte Daten-ID auswertet, bestimmt, welche dieser Einstellungen den höchsten Schweregrad ergibt, und dann dem Ergebnis den höchsten Schweregrad zuweist.

Um die Schweregradeinstellungen für eine benutzerdefinierte Daten-ID zu überprüfen, wählen Sie im Navigationsbereich der Amazon Macie Macie-Konsole Benutzerdefinierte Datenkennungen aus. Wählen Sie dann den Namen der benutzerdefinierten Daten-ID. Im Abschnitt Schweregrad werden die Einstellungen angezeigt. Weitere Informationen finden Sie unter Definieren von Einstellungen für den Schweregrad der Suche für benutzerdefinierte Datenkennungen.

SensitiveData:S3Object/Financial

A:Das SensitiveDataErgebnis S3Object/Financial weist darauf hin, dass ein S3-Objekt vertrauliche Finanzinformationen enthält. Für diese Art von Feststellung bestimmt Macie den Schweregrad anhand der Art und Anzahl der Vorkommen der Finanzinformationen, die Macie in dem Objekt gefunden hat.

In der folgenden Tabelle sind die Schweregrade aufgeführt, die Macie Ergebnissen zuweist, die das Vorkommen von Finanzinformationen in einem S3-Objekt melden.

Vertraulicher Datentyp	1 Vorkommen	2—99 Vorkommen	100 oder mehr Vorkommen
Bankkonto Nummer [1]	Hoch	Hoch	Hoch
Ablaufdatum der Kreditkarte	Niedrig	Medium	Hoch
Magnetstreifendaten der Kreditkarte	Hoch	Hoch	Hoch
Kreditkarte Nummer [2]	Hoch	Hoch	Hoch
Bestätigungscode für die Kreditkarte	Medium	Hoch	Hoch

1. Der Schweregrad ist für jede Art von Bankkontonummer identisch — eine Basisbankkontonummer (BBAN), eine internationale Bankkontonummer (IBAN) oder eine kanadische oder US-amerikanische Bankkontonummer.
2. Der Schweregrad ist derselbe für Kreditkartennummern, die sich in der Nähe eines Schlüsselworts befinden oder nicht.

Wenn bei einem Ergebnis mehrere Arten von Finanzinformationen in einem Objekt gemeldet werden, bestimmt Macie den Schweregrad des Ergebnisses, indem er den Schweregrad für jede Art von Finanzinformationen berechnet, die Macie gefunden hat, bestimmt, welcher Typ den höchsten Schweregrad ergibt, und dem Ergebnis den höchsten Schweregrad zuweist. Wenn Macie beispielsweise 10 Kreditkartenablaufdaten (mittlerer Schweregrad) und 10 Kreditkartennummern (Schweregrad hoch) in einem Objekt erkennt, weist Macie dem Ergebnis den Schweregrad Hoch zu.

SensitiveData:S3Object/Personal

A:Der SensitiveDataBefund S3Object/Personal weist darauf hin, dass ein S3-Objekt sensible personenbezogene Daten enthält — persönliche Gesundheitsinformationen (PHI), persönlich identifizierbare Informationen (PII) oder eine Kombination aus beidem. Bei dieser Art von

Befund bestimmt Macie den Schweregrad anhand der Art und Anzahl der Vorkommen der personenbezogenen Daten, die Macie in dem Objekt gefunden hat.

In der folgenden Tabelle sind die Schweregrade aufgeführt, die Macie den Ergebnissen vertraulicher Daten zuweist, bei denen das Auftreten von PHI in einem S3-Objekt gemeldet wird.

Vertraulicher Datentyp	1 Vorkommen	2—99 Vorkommen	100 oder mehr Vorkommen
Registrierungsnummer der Drug Enforcement Agency (DEA)	Hoch	Hoch	Hoch
Krankenversicherungsantragsnummer (HICN)	Hoch	Hoch	Hoch
Krankenversicherungs- oder medizinische Identifizierungsnummer	Hoch	Hoch	Hoch
Code des HCPCS (Common Procedure Coding System) für das Gesundheitswesen	Hoch	Hoch	Hoch
Nationaler Arzneimittelkodex (NDC)	Hoch	Hoch	Hoch
Nationale Anbieterkennzeichnung (NPI)	Hoch	Hoch	Hoch
Eindeutige Gerätekennung (UDI)	Niedrig	Medium	Hoch

In der folgenden Tabelle sind die Schweregrade aufgeführt, die Macie Ergebnissen vertraulicher Daten zuweist, die das Vorkommen personenbezogener Daten in einem S3-Objekt melden.

Vertraulicher Datentyp	1 Vorkommen	2—99 Vorkommen	100 oder mehr Vorkommen
Geburtsdatum	Niedrig	Medium	Hoch
Identifikationsnummer des Führerscheins	Niedrig	Medium	Hoch
Nummer der Wählerliste	Hoch	Hoch	Hoch
Vollständiger Name	Niedrig	Medium	Hoch
Koordinaten des Global Positioning Systems (GPS)	Niedrig	Mittelschwer	Mittelschwer
HTTP-Cookie	Niedrig	Medium	Hoch
Postanschrift	Niedrig	Medium	Hoch
Nationale Identifikationsnummern	Hoch	Hoch	Hoch
Nationale Versicherungsnummer (NINO)	Hoch	Hoch	Hoch
Passnummer	Medium	Hoch	Hoch
Ständige Wohnsitznummer	Hoch	Hoch	Hoch
Phone number (Telefonnummer)	Niedrig	Medium	Hoch

Vertraulicher Datentyp	1 Vorkommen	2—99 Vorkommen	100 oder mehr Vorkommen
Sozialversicherungsnummer (SIN)	Hoch	Hoch	Hoch
Sozialversicherungsnummer (SSN)	Hoch	Hoch	Hoch
Steuerpflichtigen-Identifikationsnummer oder Referenznummer	Hoch	Hoch	Hoch
Fahrzeugidentifikationsnummer (VIN)	Niedrig	Niedrig	Mittelschwer

Wenn bei einem Befund mehrere Typen von PHI, PII oder sowohl PHI als auch PII in einem Objekt gemeldet werden, bestimmt Macie den Schweregrad des Ergebnisses, indem er den Schweregrad für jeden Typ berechnet, bestimmt, welcher Typ den höchsten Schweregrad erzeugt, und dem Befund diesen höchsten Schweregrad zuweist.

Wenn Macie beispielsweise 10 vollständige Namen (mittlerer Schweregrad) und 5 Passnummern (Schweregrad hoch) in einem Objekt erkennt, weist Macie dem Ergebnis den Schweregrad Hoch zu. Ähnlich verhält es sich, wenn Macie 10 vollständige Namen (mittlerer Schweregrad) und 10 Krankenversicherungsnummern (Schweregrad hoch) in einem Objekt erkennt, weist Macie dem Ergebnis den Schweregrad Hoch zu.

SensitiveData:S3Object/Multiple

A:Das SensitiveDataErgebnis S3Object/Multiple weist darauf hin, dass ein S3-Objekt Daten enthält, die sich über mehrere Kategorien sensibler Daten erstrecken. Dabei handelt es sich um eine beliebige Kombination von Anmeldedaten, Finanzinformationen, persönlichen Informationen oder Text, die den Erkennungskriterien einer oder mehrerer benutzerdefinierter Datenkennungen entspricht.

Für diese Art von Befund bestimmt Macie den Schweregrad, indem er den Schweregrad für jeden Typ von vertraulichen Daten berechnet, die Macie gefunden hat (wie in den vorherigen Themen beschrieben), bestimmt, welcher Typ den höchsten Schweregrad erzeugt, und dem Ergebnis diesen höchsten Schweregrad zuweist.

Wenn Macie beispielsweise 10 vollständige Namen (mittlerer Schweregrad) und 10 AWS geheime Zugriffsschlüssel (Schweregrad hoch) in einem Objekt erkennt, weist Macie dem Ergebnis den Schweregrad Hoch zu.

Überwachung und Verarbeitung von Amazon Macie Macie-Ergebnissen

Um die Integration mit anderen Anwendungen, Diensten und Systemen wie Überwachungs- oder Eventmanagementsystemen zu unterstützen, veröffentlicht Amazon Macie automatisch Richtlinien und sensible Daten EventBridge als Ereignisse an Amazon. Für zusätzliche Unterstützung und eine umfassendere Analyse der Sicherheitslage Ihres Unternehmens können Sie Macie so konfigurieren, dass auch Ergebnisse aus Richtlinien und vertraulichen Daten veröffentlicht werdenAWS Security Hub.

Amazon EventBridge

AmazonEventBridge, früher Amazon CloudWatch Events, ist ein Serverless-Ereignisbus-Service, mit dem Sie einen Stream von Echtzeitdaten aus Anwendungen und -Services bereit und leitet diese Daten dann an Ziele wie AWS Lambda Funktionen, Amazon Simple Notification Service Themen und Amazon Kinesis Kinesis-Streams weiter. Mit EventBridge können Sie die Überwachung und Verarbeitung bestimmter Arten von Ereignissen automatisieren, einschließlich Ereignissen, die Macie als Ergebnis veröffentlicht. Weitere Informationen EventBridge finden Sie im EventBridgeAmazon-Benutzerhandbuch.

Wenn Sie AWS-Benutzerbenachrichtigungen in Macie integrieren, können Sie EventBridge Ereignisse auch verwenden, um automatisch Benachrichtigungen über Ereignisse zu generieren, die Macie für Ergebnisse veröffentlicht. Mit Benutzerbenachrichtigungen erstellen Sie benutzerdefinierte Regeln und konfigurieren Übermittlungskanäle für den Empfang von Benachrichtigungen über interessante EventBridge Ereignisse. Zu den Versandkanälen gehören E-Mail, AWS Chatbot Chat-Benachrichtigungen und AWS Console Mobile Application Push-Benachrichtigungen. Sie können Benachrichtigungen auch an einer zentralen Stelle auf der überprüfenAWS Management Console. Weitere Informationen zu Benutzerbenachrichtigungen finden Sie im AWS User Notifications User Guide.

AWS Security Hub

AWS Security Hubist ein Sicherheits-Service, mit dem Sie einen umfassenden Überblick über Ihren Sicherheitsstatus in Ihrer AWS Umgebung erhalten. Sie sammelt Sicherheitsdaten aus AWS Partner Network Sicherheitslösungen AWS-Services und hilft Ihnen Ihre Umgebung anhand der Standards und bewährten Methoden der Branche zu überprüfen. Sie hilft Ihnen Ihnen auch Sicherheitstrends zu analysieren und Sicherheitstrstrends mit höchster Priorität zu identifizieren. Mit Security Hub können Sie die Ergebnisse von Macie im Rahmen einer umfassenderen Analyse

der Sicherheitslage Ihrer Organisation überprüfen. Sie können auch Ergebnisse aus mehreren AWS-Regionen zusammenfassen und aggregierte Ergebnisdaten aus einer einzelnen Region überwachen und verarbeiten. Weitere Informationen zu Security Hub finden Sie im AWS Security Hub-Benutzerhandbuch.

Wenn Macie ein Ergebnis erstellt, veröffentlicht es das Ergebnis automatisch EventBridge als neues Ereignis. Abhängig von den Veröffentlichungseinstellungen, die Sie für Ihr Konto wählen, kann Macie das Ergebnis auch im Security Hub veröffentlichen. Macie veröffentlicht jedes neue Ergebnis unmittelbar nach Abschluss der Bearbeitung des Ergebnisses. Wenn Macie feststellt, dass ein vorhandener Richtlinienbefund nachträglich auftritt, veröffentlicht es eine Aktualisierung des bestehenden EventBridge Ereignisses für diesen Befund. Abhängig von Ihren Veröffentlichungseinstellungen kann Macie das Update auch im Security Hub veröffentlichen. Macie veröffentlicht diese Updates regelmäßig und verwendet dabei eine Veröffentlichungshäufigkeit, die Sie in den Veröffentlichungseinstellungen für Ihr Konto angeben.

Themen

- Konfigurieren der Veröffentlichungseinstellungen für Amazon Macie-Ergebnisse
- Integration von Amazon Macie mit Amazon EventBridge
- Amazon MacieIntegration mit AWS Security Hub
- Amazon Macie Macie-Integration mit AWS-Benutzerbenachrichtigungen
- EventBridge Amazon-Ereignisschema für Amazon Macie-Ergebnisse

Konfigurieren der Veröffentlichungseinstellungen für Amazon Macie-Ergebnisse

Um die Integration mit anderen Anwendungen, Services und Systemen zu unterstützen, veröffentlicht Amazon Macie automatisch sowohl Richtlinienergebnisse als auch Ergebnisse zu sensiblen Daten EventBridge als Ereignisse in Amazon. Informationen darüber, wie Sie verwenden können EventBridge , um Ergebnisse zu überwachen und zu verarbeiten, finden Sie unter Integration von Amazon Macie mit Amazon EventBridge.

Sie können Macie so konfigurieren, dass Ergebnisse AWS Security Hub auch automatisch in veröffentlicht werden, indem Sie Zieloptionen verwenden, die Sie in den Veröffentlichungseinstellungen für Ihr Konto angeben. Mit diesen Optionen können Sie Macie so konfigurieren, dass nur Richtlinienergebnisse, nur Ergebnisse für sensible Daten oder sowohl

Richtlinien- als auch vertrauliche Datenergebnisse in Security Hub veröffentlicht werden. Sie können Macie auch so konfigurieren, dass keine Ergebnisse mehr in Security Hub veröffentlicht werden. Informationen dazu, wie Sie Security Hub verwenden können, um Ergebnisse zu überwachen und zu verarbeiten, finden Sie unter Amazon MacieIntegration mit AWS Security Hub.

Bei Richtlinienergebnissen hängt das Timing, mit dem Macie ein Ergebnis in einem anderen veröffentlicht, AWS-Service davon ab, ob das Ergebnis neu ist, und von der Veröffentlichungshäufigkeit, die Sie für Ihr Konto angeben. Bei Ergebnissen mit sensiblen Daten ist das Timing immer sofort –Macie veröffentlicht sofort nach Abschluss der Verarbeitung des Ergebnisses ein Ergebnis mit sensiblen Daten. Im Gegensatz zu den Erkenntnissen aus Richtlinien behandelt Macie alle Erkenntnisse zu sensiblen Daten als neu (eindeutig).

Beachten Sie, dass Macie keine Ergebnisse zu Richtlinien oder sensiblen Daten veröffentlicht, die automatisch durch eine Unterdrückungsregel archiviert werden. Mit anderen Worten, Macie veröffentlicht keine unterdrückten Ergebnisse in anderen AWS-Services.

Themen

- Auswählen von Veröffentlichungszielen für Ergebnisse
- Bestimmung der Veröffentlichungshäufigkeit für Ergebnisse
- Ändern der Veröffentlichungshäufigkeit für Ergebnisse

Auswählen von Veröffentlichungszielen für Ergebnisse

Sie können Amazon Macie so konfigurieren, dass AWS Security Hub zusätzlich zu Amazon automatisch Erkenntnisse zu Richtlinien und sensiblen Daten in veröffentlicht werden EventBridge. Macie veröffentlicht standardmäßig nur neue und aktualisierte Richtlinienergebnisse in Security Hub. Um die Standardkonfiguration zu ändern oder zu erweitern, passen Sie die Einstellungen für das Veröffentlichungsziel für Ihr Konto an.

Wenn Sie Ihre Zieleinstellungen anpassen, wählen Sie die Ergebniskategorien aus, die Macie in Security Hub veröffentlichen soll – nur Richtlinienergebnisse, nur vertrauliche Datenergebnisse oder sowohl Richtlinien- als auch vertrauliche Datenergebnisse. Sie können auch festlegen, dass keine Erkenntniskategorien mehr in Security Hub veröffentlicht werden.

Wenn Sie Ihre Zieleinstellungen ändern, gilt Ihre Änderung nur für das aktuelle AWS-Region. Wenn Sie der Macie-Administrator für eine Organisation sind, gilt Ihre Änderung nur für Ihr Konto. Sie gilt nicht für zugeordnete Mitgliedskonten. Weitere Informationen finden Sie unter Verwalten mehrerer Konten.

So wählen Sie Veröffentlichungsziele für Ergebnisse aus

1. Öffnen Sie die Amazon Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie im Abschnitt Veröffentlichung von Erkenntnissen unter Ziele eine der folgenden Optionen aus:

   - Richtlinienergebnisse in Security Hub veröffentlichen – Aktivieren Sie dieses Kontrollkästchen, um automatisch mit der Veröffentlichung neuer und aktualisierter Richtlinienergebnisse in Security Hub zu beginnen. Um die Veröffentlichung neuer und aktualisierter Richtlinienergebnisse in Security Hub zu beenden, deaktivieren Sie dieses Kontrollkästchen.

     Wenn Sie dieses Kontrollkästchen aktivieren und bereits Richtlinienergebnisse vorliegen, veröffentlicht Macie diese nicht automatisch in Security Hub. Stattdessen veröffentlicht Macie nur die Richtlinienergebnisse, die es erstellt oder aktualisiert, nachdem Sie Ihre Änderung gespeichert haben.
   - Ergebnisse zu sensiblen Daten in Security Hub veröffentlichen – Aktivieren Sie dieses Kontrollkästchen, um automatisch mit der Veröffentlichung neuer Ergebnisse zu sensiblen Daten in Security Hub zu beginnen. Um die Veröffentlichung neuer Erkenntnisse zu sensiblen Daten in Security Hub zu beenden, deaktivieren Sie dieses Kontrollkästchen.

     Wenn Sie dieses Kontrollkästchen aktivieren und bereits Erkenntnisse zu sensiblen Daten vorliegen, veröffentlicht Macie diese nicht automatisch in Security Hub. Stattdessen veröffentlicht Macie nur die Ergebnisse der sensiblen Daten, die es nach dem Speichern Ihrer Änderung erstellt.
4. Wählen Sie Speichern.

Wenn Sie eine beliebige Erkenntniskategorie in Security Hub veröffentlichen möchten, stellen Sie sicher, dass Sie Security Hub auch in der aktuellen Region aktivieren, und konfigurieren Sie es so, dass es Ergebnisse von Macie akzeptiert. Andernfalls können Sie nicht auf die Ergebnisse in Security Hub zugreifen. Informationen zum Annehmen von Erkenntnissen in Security Hub finden Sie unter Verwalten von Produktintegrationen im AWS Security Hub -Benutzerhandbuch.

Bestimmung der Veröffentlichungshäufigkeit für Ergebnisse

In Amazon Macie hat jede Erkenntnis eine eindeutige Kennung. Macie verwendet diese Kennung, um zu bestimmen, wann ein Ergebnis in einem anderen veröffentlicht werden soll AWS-Service:

- Neue Erkenntnisse – Wenn Macie eine neue Richtlinie oder ein Ergebnis mit sensiblen Daten erstellt, weist es dem Ergebnis im Rahmen der Verarbeitung des Ergebnisses eine eindeutige Kennung zu. Unmittelbar nachdem Macie die Verarbeitung der Erkenntnis abgeschlossen hat, veröffentlicht es die Erkenntnis als neues Amazon- EventBridge Ereignis. Abhängig von den Veröffentlichungseinstellungen für Ihr Konto veröffentlicht Macie die Erkenntnis auch als neue Erkenntnis in AWS Security Hub.
- Aktualisierte Ergebnisse – Wenn Macie ein nachfolgendes Auftreten einer vorhandenen Richtlinienerkenntnis erkennt, aktualisiert es die vorhandene Erkenntnis, indem es Details zum nachfolgenden Auftreten hinzufügt und die Anzahl der Vorkommen erhöht. Macie veröffentlicht diese Updates auch für das vorhandene EventBridge Ereignis und, abhängig von den Veröffentlichungseinstellungen für Ihr Konto, für das vorhandene Security Hub-Ergebnis. Macie tut dies nur für Richtlinienergebnisse. Erkenntnisse zu sensiblen Daten werden im Gegensatz zu Richtlinienergebnissen alle als neu (eindeutig) behandelt.

  Standardmäßig veröffentlicht Macie im Rahmen eines wiederkehrenden Veröffentlichungszyklus alle 15 Minuten aktualisierte Ergebnisse. Das bedeutet, dass alle Richtlinienergebnisse, die nach dem letzten Veröffentlichungszyklus aktualisiert werden, beibehalten, bei Bedarf erneut aktualisiert und in den nächsten Veröffentlichungszyklus aufgenommen werden (etwa 15 Minuten später). Sie können diesen Zeitplan ändern, indem Sie eine andere Veröffentlichungshäufigkeit auswählen. Wenn Sie Macie beispielsweise so konfigurieren, dass aktualisierte Ergebnisse stündlich veröffentlicht werden, und eine Veröffentlichung um 12:00 Uhr erfolgt, werden alle Aktualisierungen, die nach 12:00 Uhr stattfinden, um 13:00 Uhr veröffentlicht.

Beachten Sie, dass keiner dieser Fälle für Erkenntnisse gilt, die automatisch durch eine Unterdrückungsregel archiviert werden. Macie veröffentlicht keine unterdrückten Ergebnisse in anderen AWS-Services.

Ändern der Veröffentlichungshäufigkeit für Ergebnisse

Sie können den Zeitplan ändern, den Amazon Macie verwendet, um Aktualisierungen vorhandener Richtlinienergebnisse in anderen zu veröffentlichen AWS-Services. Macie veröffentlicht standardmäßig alle 15 Minuten aktualisierte Ergebnisse. Wenn Sie diesen Zeitplan ändern, gilt Ihre Änderung nur für das aktuelle AWS-Region. Wenn Sie der Macie-Administrator für eine Organisation sind, gilt Ihre Änderung auch für alle zugehörigen Mitgliedskonten in der Region. Weitere Informationen finden Sie unter Verwalten mehrerer Konten.

So ändern Sie die Veröffentlichungshäufigkeit für aktualisierte Ergebnisse

1. Öffnen Sie die Amazon Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie im Abschnitt Veröffentlichung von Erkenntnissen unter Aktualisierungshäufigkeit für Richtlinienergebnisse aus, wie oft Macie aktualisierte Richtlinienergebnisse in anderen veröffentlichen soll AWS-Services.
4. Klicken Sie auf Speichern.

Integration von Amazon Macie mit Amazon EventBridge

AmazonEventBridge, ehemals Amazon CloudWatch Events, ist ein serverloser Event-Bus-Service. EventBridgestellt einen Stream von Echtzeitdaten aus Anwendungen und Services und leitet diese Daten dann an Ziele wie AWS Lambda Funktionen, Amazon Simple Notification Service (Amazon SNS) -Themen und Amazon Kinesis Streams. Weitere Informationen EventBridge finden Sie im EventBridgeAmazon-Benutzerhandbuch.

Mit EventBridge können Sie die Überwachung und Verarbeitung bestimmter Arten von Ereignissen automatisieren. Dazu gehören Ereignisse, die Amazon Macie automatisch veröffentlicht, um neue politische Erkenntnisse und Erkenntnisse aus sensiblen Daten zu erhalten. Dazu gehören auch Ereignisse, die Macie automatisch veröffentlicht, wenn bestehende politische Erkenntnisse später wieder auftauchen. Einzelheiten darüber, wie und wann Macie diese Ereignisse veröffentlicht, finden Sie unterKonfigurieren von Veröffentlichungseinstellungen für Ergebnisse.

Indem Sie EventBridge die von Macie veröffentlichten Ereignisse für Ergebnisse verwenden, können Sie die Ergebnisse nahezu in Echtzeit überwachen und verarbeiten. Sie können dann auf der Grundlage der Ergebnisse handeln, indem Sie andere Anwendungen und Dienste verwenden. Sie können dies beispielsweise verwenden, EventBridge um bestimmte Arten neuer Ergebnisse an eine AWS Lambda Funktion zu senden. Die Lambda-Funktion verarbeitet und sendet die Daten dann möglicherweise und sendet sie an Ihr Sicherheitsvorfall- und Ereignismanagementsystem (SIEM). Wenn Sie AWS-Benutzerbenachrichtigungen in Macie integrieren, können Sie die Ereignisse auch verwenden, um automatisch über die von Ihnen angegebenen Lieferkanäle über Ergebnisse informiert zu werden.

Zusätzlich zur automatisierten Überwachung und Verarbeitung EventBridge ermöglicht die Verwendung von eine längerfristige Aufbewahrung Ihrer Ergebnisdaten. Macie speichert die

Ergebnisse 90 Tage lang. Mit EventBridge können Sie Ergebnisdaten an Ihre bevorzugte Speicherplattform senden und die Daten so lange speichern, wie Sie möchten.

> **Note**
>
> Für eine langfristige Aufbewahrung können Sie Macie auch so konfigurieren, dass die Ergebnisse der Erkennung vertraulicher Daten in einem S3-Bucket gespeichert werden. Ein Erkennungsergebnis ist ein Datensatz, der Details zu der Analyse protokolliert. Weitere Informationen hierzu finden Sie unter Speicherung und Beibehaltung der Erkennungsergebnisse von vertraulichen Daten.

Themen

- Zusammenarbeit mit Amazon EventBridge
- EventBridgeAmazon-Regeln für Ergebnisse erstellen

Zusammenarbeit mit Amazon EventBridge

Mit Amazon erstellen Sie RegelnEventBridge, um festzulegen, welche Ereignisse Sie überwachen möchten und welche Ziele Sie für diese Ereignisse automatisierte Aktionen ausführen möchten. Ein Ziel ist ein Ziel, EventBridge an das Ereignisse gesendet werden.

Um die Überwachungs- und Verarbeitungsaufgaben für Ergebnisse zu automatisieren, können Sie eine EventBridge Regel erstellen, die Amazon Macie-Findereignisse automatisch erkennt und diese Ereignisse zur Verarbeitung oder anderen Aktion an eine andere Anwendung oder einen anderen Dienst sendet. Sie können die Regel so anpassen, dass nur die Ereignisse gesendet werden, die bestimmte Kriterien erfüllen. Geben Sie dazu Kriterien an, die sich aus dem EventBridge Ereignisschema für Ergebnisse ableiten.

Sie können beispielsweise eine Regel erstellen, die bestimmte Arten von neuen Ergebnissen an eine AWS Lambda -Funktion sendet. Die Lambda-Funktion kann dann folgende Aufgaben ausführen: die Daten verarbeiten und an Ihr SIEM-System senden, automatisch eine bestimmte Art der serverseitigen Verschlüsselung auf ein S3-Objekt anwenden oder den Zugriff auf ein S3-Objekt einschränken, indem Sie die Zugriffskontrollliste (ACL) des Objekts ändern. Oder Sie können eine Regel erstellen, die automatisch neue Ergebnisse mit hohem Schweregrad an ein Amazon SNS SNS-Thema sendet, das dann Ihr Incident-Response-Team über das Ergebnis informiert.

Zusätzlich zum Aufrufen von Lambda-Funktionen und zur Benachrichtigung von Amazon SNS SNS-Themen EventBridge unterstützt es auch andere Arten von Zielen und Aktionen, z. B. das Weiterleiten von Ereignissen an Amazon Kinesis Streams, das Aktivieren von AWS Step Functions -Zustandsmaschinen und das Aufrufen des Run Command. AWS Systems Manager Informationen zu unterstützten Zielen finden Sie unter EventBridgeAmazon-Ziele im EventBridgeAmazon-Benutzerhandbuch.

EventBridgeAmazon-Regeln für Ergebnisse erstellen

In den folgenden Verfahren wird erläutert, wie Sie die EventBridge Amazon-Konsole und die AWS Command Line Interface(AWS CLI) verwenden, um eine EventBridge Regel für Amazon Macie Macie-Ergebnisse zu erstellen. Die Regel erkennt EventBridge Ereignisse, die das Ereignisschema und das Muster für Macie-Ereignisse verwenden, und sendet diese Ereignisse zur Verarbeitung an eine AWS Lambda -Funktion.

AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Sie packen Ihren Code und laden ihn auf AWS Lambda als Lambda-Funktion hoch. AWS Lambda führt die Funktion aus, wenn die Funktion aufgerufen wird. Eine Funktion kann manuell von Ihnen, automatisch als Reaktion auf Ereignisse oder als Reaktion auf Anforderungen von Anwendungen oder Diensten aufgerufen werden. Informationen zum Erstellen und Aufrufen von Lambda-Funktionen finden Sie im AWS LambdaDeveloper Guide.

Console

In diesem Verfahren wird erklärt, wie Sie mithilfe der EventBridge Amazon-Konsole eine Regel erstellen, die automatisch alle Macie-Findereignisse zur Verarbeitung an eine Lambda-Funktion sendet. Die Regel verwendet Standardeinstellungen für Regeln, die ausgeführt werden, wenn bestimmte Ereignisse empfangen werden. Einzelheiten zu Regeleinstellungen oder um zu erfahren, wie Sie eine Regel erstellen, die benutzerdefinierte Einstellungen verwendet, finden Sie im EventBridgeAmazon-Benutzerhandbuch unter Regeln erstellen, die auf Ereignisse reagieren.

> **Tip**
>
> Sie können auch eine Regel erstellen, die ein benutzerdefiniertes Muster verwendet. Diese Teilmenge kann auf bestimmten Feldern basieren, die Macie in ein Suchereignis einschließt. Weitere Informationen zu den verfügbaren Feldern finden Sie unterEventBridge Ereignisschema für Ergebnisse. Informationen zum Erstellen dieser Art

von Regel finden Sie unter Inhaltsfilterung in Ereignismustern im EventBridgeAmazon-Benutzerhandbuch.

Bevor Sie diese Regel erstellen, erstellen Sie die Lambda-Funktion, die von der Regel als Ziel verwendet werden soll. Wenn Sie die Regel erstellen, müssen Sie diese Funktion als Ziel für die Regel angeben.

So erstellen Sie eine Ereignisregel mit der Konsole

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im Navigationsbereich unter Events (Ereignisse) die Option Rules (Regeln) aus.
3. Wählen Sie im Abschnitt Rules (Regeln) die Option Create rule (Regel erstellen) aus.
4. Führen Sie die folgenden Schritte aus:
   - Geben Sie für Rule name (Regelname) einen Namen für die Regel ein.
   - Geben Sie unter Description (Beschreibung) eine kurze Beschreibung der Regel ein.
   - Stellen Sie sicher, dass für den Event-Bus die Standardeinstellung ausgewählt und die Option Regel auf dem ausgewählten Event-Bus aktivieren aktiviert ist.
   - Bei Rule type (Regeltyp) wählen Sie Rule with an event pattern (Regel mit einem Ereignismuster) aus.
5. Wenn Sie fertig sind, wählen Sie Next (Weiter) aus.
6. Führen Sie die folgenden Schritte aus:
   - Wählen Sie als Eventquelle AWS Ereignisse oder EventBridge Partner aus.
   - (Optional) Sehen Sie sich unter Beispielereignis ein Musterereignis für Macie an, um zu erfahren, was ein Ereignis beinhalten könnte. Wählen Sie dazu AWSEreignisse aus. Wählen Sie dann für Beispielereignisse die Option Macie Finding aus.
   - Wählen Sie für Event-Muster die Option Event-Musterformular aus. Geben Sie dann die folgenden Einstellungen ein:
     - Wählen Sie für Ereignisquelle die Option AWS-Services aus.
     - Für AWS-Service, geben Sie Macie ein.
     - Geben Sie als Ereignistyp Macie Finding ein.
7. Wenn Sie fertig sind, wählen Sie Next (Weiter) aus.
8. Führen Sie die folgenden Schritte aus:

- Für Target types (Zieltypen), wählen Sie AWS-Service aus.
- Geben Sie für Select a target die Lambda-Funktion ein. Wählen Sie dann unter Function die Lambda-Funktion aus, an die Sie Suchereignis senden möchten.
- Geben Sie Version/Alias Lambda.
- (Optional) Geben Sie für Zusätzliche Einstellungen benutzerdefinierte Einstellungen ein, um anzugeben, welche Ereignisdaten Sie an die Lambda-Funktion senden möchten. Sie können auch angeben, wie mit Ereignissen umgegangen werden soll, die nicht erfolgreich an die Funktion übermittelt wurden.

9. Wenn Sie fertig sind, wählen Sie Next (Weiter) aus.
10. Geben Sie auf der Seite Tags konfigurieren optional ein oder mehrere Tags ein, die der Regel zugewiesen werden. Wählen Sie anschließend Next (Weiter).
11. Überprüfen und erstellen überprüfen Sie die Regeleinstellungen und bestätigen Sie, dass diese korrekt sind.

    Um eine Einstellung zu ändern, wählen Sie in dem Abschnitt, der die Einstellung enthält, Bearbeiten aus, und geben Sie dann die richtige Einstellung ein. Sie können auch die Navigations-Tabs verwenden, um zu der Seite zu gelangen, die eine Einstellung enthält.
12. Wenn Sie mit der Überprüfung der Einstellungen fertig sind, wählen Sie Regel erstellen.

AWS CLI

In diesem Verfahren wird erklärt, wie Sie AWS CLI mit eine EventBridge Regel erstellen, die alle Macie-Suchereignisse zur Verarbeitung an eine Lambda-Funktion sendet. Die Regel verwendet Standardeinstellungen für Regeln, die ausgeführt werden, wenn bestimmte Ereignisse empfangen werden. In der Prozedur werden die Befehle für Microsoft Windows formatiert. Ersetzen Sie für Linux, macOS oder Unix das Zeilenfortsetzungszeichen Caret (^) durch einen umgekehrten Schrägstrich (\).

Bevor Sie diese Regel erstellen, erstellen Sie die Lambda-Funktion, die von der Regel als Ziel verwendet werden soll. Notieren Sie beim Erstellen der Funktion den Amazon-Ressourcennamen (ARN) der Funktion. Sie müssen diesen ARN eingeben, wenn Sie das Ziel für die Regel angeben.

Um eine Ereignisregel zu erstellen, verwenden Sie die AWS CLI

1. Erstellen Sie eine Regel, die Ereignisse für alle Ergebnisse erkennt, in denen Macie veröffentlicht. EventBridge Verwenden Sie dazu den Befehl EventBridge put-rule. Beispiel:

```
C:\> aws events put-rule ^
--name MacieFindings ^
--event-pattern "{\"source\":[\"aws.macie\"]}"
```

Wo *MacieFindings*ist der Name, den Sie für die Regel benötigen.

Wird der Befehl erfolgreich ausgeführt, EventBridge antwortet er mit dem ARN der Regel. Notieren Sie diesen ARN. Sie müssen ihn in Schritt 3 eingeben.

> **Tip**
>
> Sie können auch eine Regel erstellen, die ein benutzerdefiniertes Muster verwendet. Diese Teilmenge kann auf bestimmten Feldern basieren, die Macie in ein Suchereignis einschließt. Weitere Informationen zu den verfügbaren Feldern finden Sie unterEventBridge Ereignisschema für Ergebnisse. Informationen zum Erstellen dieser Art von Regel finden Sie unter Inhaltsfilterung in Ereignismustern im EventBridgeAmazon-Benutzerhandbuch.

2. Geben Sie die Lambda-Funktion an, die als Ziel für die Regel verwendet werden soll. Verwenden Sie dazu den Befehl EventBridge put-targets. Beispiel:

```
C:\> aws events put-targets ^
--rule MacieFindings ^
--targets Id=1,Arn=arn:aws:lambda:regionalEndpoint:accountID:function:my-
findings-function
```

Dabei *MacieFindings*ist der Name, den Sie für die Regel angegeben haben, und der Wert für den `Arn` Parameter ARN Funktion, die von der Regel als Ziel verwendet werden soll.

3. Fügen Sie Berechtigungen hinzu, die es der Regel ermöglichen, die Zielfunktion aufzurufen. Verwenden Sie dazu den Lambda-Befehl add-permission. Beispiel:

```
C:\> aws lambda add-permission ^
--function-name my-findings-function ^
--statement-id Sid ^
--action lambda:InvokeFunction ^
--principal events.amazonaws.com ^
--source-arn arn:aws:events:regionalEndpoint:accountId:rule:MacieFindings
```

Wobei gilt:

- *my-findings-function*ist der Name der Lambda-Funktion, die von der Regel als Ziel verwendet werden soll.
- *Sid* ist ein Anweisungsbezeichner, den Sie definieren, um die Anweisung in der Lambda-Funktionsrichtlinie zu beschreiben.
- `source-arn`ist der ARN der EventBridge Regel.

Wird der Befehl erfolgreich ausgeführt, erhalten Sie eine Ausgabe ähnlich der folgenden:

```
{
  "Statement": "{\"Sid\":\"sid\",
    \"Effect\":\"Allow\",
    \"Principal\":{\"Service\":\"events.amazonaws.com\"},
    \"Action\":\"lambda:InvokeFunction\",
    \"Resource\":\"arn:aws:lambda:us-east-1:111122223333:function:my-findings-
function\",
    \"Condition\":
      {\"ArnLike\":
        {\"AWS:SourceArn\":
         \"arn:aws:events:us-east-1:111122223333:rule/MacieFindings\"}}}"
}
```

Der `Statement`-Wert ist eine JSON-Zeichenfolgenversion der Anweisung, die der Lambda-Funktionsrichtlinie hinzugefügt wurde.

Amazon MacieIntegration mit AWS Security Hub

AWS Security Hub ist ein Service, der Ihnen einen umfassenden Überblick über Ihre Sicherheitslage in Ihrer gesamten -AWSUmgebung bietet und Ihnen hilft, Ihre -Umgebung anhand von Sicherheitsstandards und bewährten Methoden der Branche zu überprüfen. Dies geschieht zum Teil durch den Verbrauch, die Aggregierung, die Organisation und die Priorisierung von Erkenntnissen aus mehreren AWS-Services und unterstützten AWS Partner Network Sicherheitslösungen. Security Hub hilft Ihnen dabei, Ihre Sicherheitstrends zu analysieren und Sicherheitsprobleme mit höchster Priorität zu identifizieren. Mit Security Hub können Sie auch Ergebnisse aus mehreren aggregieren AWS-Regionenund dann alle aggregierten Ergebnisdaten aus einer einzigen Region

überwachen und verarbeiten. Weitere Informationen zu Security Hub finden Sie im AWS Security Hub -Benutzerhandbuch.

Amazon Macie lässt sich in Security Hub integrieren, was bedeutet, dass Sie Ergebnisse automatisch von Macie in Security Hub veröffentlichen können. Der Security Hub kann diese Erkenntnisse dann in die Analyse Ihres Sicherheitsniveaus einbeziehen. Darüber hinaus können Sie Security Hub verwenden, um die Ergebnisse von Richtlinien und sensiblen Daten als Teil eines größeren, aggregierten Satzes von Ergebnisdaten für Ihre AWS Umgebung zu überwachen und zu verarbeiten. Mit anderen Worten, Sie können Macie-Erkenntnisse analysieren und gleichzeitig umfassendere Analysen der Sicherheitslage Ihrer Organisation durchführen und die Erkenntnisse nach Bedarf korrigieren. Security Hub reduziert die Komplexität der Handhabung großer Mengen von Erkenntnissen mehrerer Anbieter. Darüber hinaus verwendet es ein Standardformat für alle Erkenntnisse, einschließlich der Erkenntnisse von Macie. Durch die Verwendung dieses Formats, des AWS Security Finding Format (ASFF), müssen Sie keine zeitaufwändigen Datenkonvertierungsbemühungen durchführen.

Themen

- Wie Amazon Macie Ergebnisse in veröffentlicht AWS Security Hub
- Beispiele für Amazon Macie-Erkenntnisse in AWS Security Hub
- Aktivieren und Konfigurieren der AWS Security Hub Integration
- Beenden der Veröffentlichung von Erkenntnissen in AWS Security Hub

Wie Amazon Macie Ergebnisse in veröffentlicht AWS Security Hub

In AWS Security Hub werden Sicherheitsprobleme als Ergebnisse nachverfolgt. Einige Erkenntnisse stammen von Problemen, die von erkannt werdenAWS-Services, wie Amazon Macie oder von unterstützten AWS Partner Network Sicherheitslösungen. Security Hub verwendet ebenfalls verschiedene Regeln, um Sicherheitsprobleme zu erkennen und Ergebnisse zu generieren.

Security Hub bietet Tools zur Verwaltung von Erkenntnissen aus all diesen Quellen. Sie können Ergebnislisten und Filterlisten sowie die Details einzelner Ergebnisse überprüfen. Weitere Informationen finden Sie unter Anzeigen von Erkenntnislisten und Details im AWS Security Hub -Benutzerhandbuch. Sie können auch den Status einer Untersuchung zu einer Erkenntnis nachverfolgen. Weitere Informationen finden Sie unter Ergreifen von Maßnahmen zu Erkenntnissen im AWS Security Hub -Benutzerhandbuch.

Alle Erkenntnisse in Security Hub verwenden ein Standard-JSON-Format, das so genannte AWS-Security Finding Format (ASFF). Die ASFF enthält Details zur Ursache eines Problems, zu den betroffenen Ressourcen und zum aktuellen Status einer Erkenntnis. Weitere Informationen finden Sie unter AWS-Security Finding-Format (ASFF) im AWS Security Hub-Benutzerhandbuch.

Arten von Erkenntnissen, die Macie veröffentlicht

Abhängig von den Veröffentlichungseinstellungen, die Sie für Ihr Macie-Konto wählen, kann Macie alle Ergebnisse, die es erstellt, in Security Hub veröffentlichen, sowohl vertrauliche Datenergebnisse als auch Richtlinienergebnisse. Informationen zu diesen Einstellungen und deren Änderung finden Sie unter Konfigurieren von Veröffentlichungseinstellungen für Ergebnisse. Macie veröffentlicht standardmäßig nur neue und aktualisierte Richtlinienergebnisse in Security Hub. Macie veröffentlicht keine Erkenntnisse zu sensiblen Daten in Security Hub.

Ergebnisse zu sensiblen Daten

Wenn Sie Macie so konfigurieren, dass vertrauliche Datenergebnisse in Security Hub veröffentlicht werden, veröffentlicht Macie automatisch jede Erkenntnis zu vertraulichen Daten, die es für Ihr Konto erstellt, und zwar sofort, nachdem es die Verarbeitung der Erkenntnis abgeschlossen hat. Macie tut dies für alle Erkenntnisse zu sensiblen Daten, die nicht automatisch durch eine Unterdrückungsregel archiviert werden.

Wenn Sie der Macie-Administrator für eine Organisation sind, ist die Veröffentlichung auf Erkenntnisse aus von Ihnen ausgeführten Aufträgen zur Erkennung vertraulicher Daten und automatisierte Aktivitäten zur Erkennung vertraulicher Daten beschränkt, die Macie für Ihre Organisation ausgeführt hat. Nur das Konto, das einen Auftrag erstellt, kann Ergebnisse zu sensiblen Daten veröffentlichen, die der Auftrag erzeugt. Nur das Macie-Administratorkonto kann Erkenntnisse zu sensiblen Daten veröffentlichen, die die automatische Erkennung sensibler Daten für seine Organisation generiert.

Wenn Macie vertrauliche Datenergebnisse in Security Hub veröffentlicht, verwendet es das AWS Security Finding Format (ASFF), das das Standardformat für alle Ergebnisse in Security Hub ist. In der ASFF gibt das `Types` Feld den Typ einer Erkenntnis an. In diesem Feld wird eine Taxonomalie verwendet, die sich geringfügig von der Erkenntnistyp-Tastatur in Macie unterscheidet.

In der folgenden Tabelle ist der ASFF-Erkenntnistyp für jeden Typ von Erkenntnissen für sensible Daten aufgeführt, die Macie erstellen kann.

Macie-Erkenntnistyp	ASFF-Ergebnistyp
SensitiveData:S3Object/Credentials	Sensitive Data Identifications/Passwords/SensitiveData:S3Object-Credentials
SensitiveData:S3Object/CustomIdentifier	Sensitive Data Identifications/PII/SensitiveData:S3Object-CustomIdentifier
SensitiveData:S3Object/Financial	Sensitive Data Identifications/Financial/SensitiveData:S3Object-Financial
SensitiveData:S3Object/Multiple	Sensitive Data Identifications/PII/SensitiveData:S3Object-Multiple
SensitiveData:S3Object/Personal	Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal

Richtlinienergebnisse

Wenn Sie Macie so konfigurieren, dass Richtlinienergebnisse in Security Hub veröffentlicht werden, veröffentlicht Macie automatisch jedes neue Richtlinienergebnis, das es erstellt, und zwar sofort, nachdem es die Verarbeitung des Ergebnisses abgeschlossen hat. Wenn Macie ein nachfolgendes Auftreten einer vorhandenen Richtlinienerkenntnis erkennt, veröffentlicht es automatisch eine Aktualisierung der vorhandenen Erkenntnis in Security Hub unter Verwendung einer Veröffentlichungshäufigkeit, die Sie für Ihr Konto angeben. Macie führt diese Aufgaben für alle Richtlinienergebnisse aus, die nicht automatisch von einer Unterdrückungsregel archiviert werden.

Wenn Sie der Macie-Administrator für eine Organisation sind, ist die Veröffentlichung auf Richtlinienergebnisse für S3-Buckets beschränkt, die direkt Ihrem Konto gehören. Macie veröffentlicht keine Richtlinienergebnisse, die es für Mitgliedskonten in Ihrer Organisation erstellt oder aktualisiert. Dadurch wird sichergestellt, dass Sie keine doppelten Ergebnisdaten in Security Hub haben.

Wie bei Ergebnissen mit sensiblen Daten verwendet Macie das AWS Security Finding Format (ASFF), wenn neue und aktualisierte Richtlinienergebnisse in Security Hub veröffentlicht werden. In

der ASFF verwendet das `Types` Feld eine Taxonomalie, die sich geringfügig von der Erkenntnistyp-Tastatur in Macie unterscheidet.

Die folgende Tabelle listet den ASFF-Erkenntnistyp für jeden Typ von Richtlinienerkenntnis auf, den Macie erstellen kann. Wenn Macie am oder nach dem 28. Januar 2021 ein Richtlinienergebnis in Security Hub erstellt oder aktualisiert hat, hat das Ergebnis einen der folgenden Werte für das ASFF-`Types`Feld in Security Hub.

Macie-Erkenntnistyp	ASFF-Ergebnistyp
Policy:IAMUser/S3BlockPublicAccessDisabled	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BlockPublicAccessDisabled
Policy:IAMUser/S3BucketEncryptionDisabled	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketEncryptionDisabled
Policy:IAMUser/S3BucketPublic	Effects/Data Exposure/Policy:IAMUser-S3BucketPublic
Policy:IAMUser/S3BucketReplicatedExternally	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketReplicatedExternally
Policy:IAMUser/S3BucketSharedExternally	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketSharedExternally
Policy:IAMUser/S3BucketSharedWithCloudFront	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketSharedWithCloudFront

Wenn Macie ein Richtlinienergebnis vor dem 28. Januar 2021 erstellt oder zuletzt aktualisiert hat, hat das Ergebnis einen der folgenden Werte für das ASFF-`Types`Feld in Security Hub:

- Policy:IAMUser/S3BlockPublicAccessDisabled
- Policy:IAMUser/S3BucketEncryptionDisabled
- Policy:IAMUser/S3BucketPublic
- Policy:IAMUser/S3BucketReplicatedExternally
- Policy:IAMUser/S3BucketSharedExternally

Die Werte in der vorherigen Liste werden direkt den Werten für das Feld Erkenntnistyp (`type`) in Macie zugeordnet.

> **Note**
>
> Beachten Sie bei der Überprüfung und Verarbeitung der Richtlinienergebnisse in Security Hub die folgenden Ausnahmen:
>
> - In bestimmten begann Macie bereits am 25. Januar 2021 AWS-Regionenmit der Verwendung von ASFF-Erkenntnistypen für neue und aktualisierte Erkenntnisse.
> - Wenn Sie auf eine Richtlinienerkenntnis in Security Hub reagiert haben, bevor Macie mit der Verwendung von ASFF-Erkenntnistypen in Ihrem begonnen hatAWS-Region, ist der Wert für das ASFF-`Types`Feld der Erkenntnis einer der Macie-Erkenntnistypen in der vorherigen Liste. Es wird keiner der ASFF-Erkenntnistypen in der vorherigen Tabelle sein. Dies gilt für Richtlinienergebnisse, auf die Sie mithilfe der AWS Security Hub Konsole oder der AWS Security Hub-BatchUpdateFindingsOperation der API reagiert haben.

Latenz beim Veröffentlichen von Ergebnissen

Wenn Macie eine neue Richtlinie oder Erkenntnis zu sensiblen Daten erstellt, veröffentlicht es die Erkenntnis sofort nach Abschluss der Verarbeitung der Erkenntnis in Security Hub.

Wenn Macie ein nachfolgendes Auftreten einer vorhandenen Richtlinienerkenntnis erkennt, veröffentlicht es eine Aktualisierung der vorhandenen Security Hub-Erkenntnis. Der Zeitpunkt der Aktualisierung hängt von der Veröffentlichungshäufigkeit ab, die Sie für Ihr Macie-Konto auswählen. Macie veröffentlicht standardmäßig alle 15 Minuten Updates. Weitere Informationen,

einschließlich der Änderung der Einstellung für Ihr Konto, finden Sie unter Konfigurieren von Veröffentlichungseinstellungen für Ergebnisse.

Wiederholen der Veröffentlichung, wenn Security Hub nicht verfügbar ist

Wenn Security Hub nicht verfügbar ist, erstellt Macie eine Warteschlange mit Ergebnissen, die nicht vom Security Hub empfangen wurden. Wenn das System wiederhergestellt wird, wiederholt Macie die Veröffentlichung, bis die Ergebnisse vom Security Hub empfangen werden.

Aktualisieren von vorhandenen Erkenntnissen in Security Hub

Nachdem Macie eine Richtlinienerkenntnis in Security Hub veröffentlicht hat, aktualisiert Macie die Erkenntnis, um alle zusätzlichen Vorkommen der Erkenntnis oder Erkenntnisaktivität widerzuspiegeln. Macie tut dies nur für Richtlinienergebnisse. Erkenntnisse zu sensiblen Daten werden im Gegensatz zu Richtlinienergebnissen alle als neu (eindeutig) behandelt.

Wenn Macie ein Update für ein Richtlinienergebnis veröffentlicht, aktualisiert Macie den Wert für das Feld Aktualisiert am (`UpdatedAt`) des Ergebnisses. Sie können diesen Wert verwenden, um festzustellen, wann Macie zuletzt ein nachfolgendes Auftreten des potenziellen Richtlinienverstoßes oder -problems entdeckt hat, das das Ergebnis verursacht hat.

Macie kann auch den Wert für das Feld Typen (`Types`) einer Erkenntnis aktualisieren, wenn der vorhandene Wert für das Feld kein ASFF-Erkenntnistyp ist. Dies hängt davon ab, ob Sie auf die Erkenntnis in Security Hub reagiert haben. Wenn Sie nicht auf die Erkenntnis reagiert haben, ändert Macie den Wert des Felds in den entsprechenden ASFF-Erkenntnistyp. Wenn Sie über die AWS Security Hub Konsole oder die -BatchUpdateFindingsOperation der AWS Security Hub API auf die Erkenntnis reagiert haben, ändert Macie den Wert des Felds nicht.

Beispiele für Amazon Macie-Erkenntnisse in AWS Security Hub

Wenn Amazon Macie Ergebnisse in veröffentlichtAWS Security Hub, verwendet es das AWS Security Finding Format (ASFF). Dies ist das Standardformat für alle Erkenntnisse in Security Hub. In den folgenden Beispielen werden Beispieldaten verwendet, um die Struktur und Art der Erkenntnisdaten zu demonstrieren, die Macie in diesem Format in Security Hub veröffentlicht:

- Beispiel für eine Erkenntnis zu sensiblen Daten
- Beispiel für eine Richtlinienerkenntnis

Beispiel für eine Erkenntnis zu sensiblen Daten in Security Hub

Hier ist ein Beispiel für eine Erkenntnis zu sensiblen Daten, die Macie mithilfe der ASFF in Security Hub veröffentlicht hat.


```
{
    "SchemaVersion": "2018-10-08",
    "Id": "5be50fce24526e670df77bc00example",
    "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/macie",
    "ProductName": "Macie",
    "CompanyName": "Amazon",
    "Region": "us-east-1",
    "GeneratorId": "aws/macie",
    "AwsAccountId": "111122223333",
    "Types":[
        "Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal"
    ],
    "CreatedAt": "2022-05-11T10:23:49.667Z",
    "UpdatedAt": "2022-05-11T10:23:49.667Z",
    "Severity": {
        "Label": "HIGH",
        "Normalized": 70
    },
    "Title": "The S3 object contains personal information.",
    "Description": "The object contains personal information such as first or last
 names, addresses, or identification numbers.",
    "ProductFields": {
        "JobArn": "arn:aws:macie2:us-east-1:111122223333:classification-
job/698e99c283a255bb2c992feceexample",
        "S3Object.Path": "DOC-EXAMPLE-BUCKET1/2022 Sourcing.tsv",
        "S3Object.Extension": "tsv",
        "S3Bucket.effectivePermission": "NOT_PUBLIC",
        "OriginType": "SENSITIVE_DATA_DISCOVERY_JOB",
        "S3Object.PublicAccess": "false",
        "S3Object.Size": "14",
        "S3Object.StorageClass": "STANDARD",
        "S3Bucket.allowsUnencryptedObjectUploads": "TRUE",
        "JobId": "698e99c283a255bb2c992feceexample",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
macie/5be50fce24526e670df77bc00example",
        "aws/securityhub/ProductName": "Macie",
        "aws/securityhub/CompanyName": "Amazon"
    },
```

```
    "Resources": [
        {
            "Type": "AwsS3Bucket",
            "Id": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
            "Partition": "aws",
            "Region": "us-east-1",
            "Details": {
                "AwsS3Bucket": {
                    "OwnerId":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example",
                    "OwnerName": "johndoe",
                    "OwnerAccountId": "444455556666",
                    "CreatedAt": "2020-12-30T18:16:25.000Z",
                    "ServerSideEncryptionConfiguration": {
                        "Rules": [
                            {
                                "ApplyServerSideEncryptionByDefault": {
                                    "SSEAlgorithm": "aws:kms",
                                    "KMSMasterKeyID": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                                }
                            }
                        ]
                    },
                    "PublicAccessBlockConfiguration": {
                        "BlockPublicAcls": true,
                        "BlockPublicPolicy": true,
                        "IgnorePublicAcls": true,
                        "RestrictPublicBuckets": true
                    }
                }
            }
        },
        {
            "Type": "AwsS3Object",
            "Id": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1/2022 Sourcing.tsv",
            "Partition": "aws",
            "Region": "us-east-1",
            "DataClassification": {
                "DetailedResultsLocation": "s3://macie-data-discovery-results/
AWSLogs/111122223333/Macie/us-east-1/
                698e99c283a255bb2c992feceexample/111122223333/32b8485d-4f3a-3aa1-be33-
aa3f0example.jsonl.gz",
                "Result":{
```

```
                    "MimeType": "text/tsv",
                    "SizeClassified": 14,
                    "AdditionalOccurrences": false,
                    "Status": {
                        "Code": "COMPLETE"
                    },
                    "SensitiveData": [
                        {
                            "Category": "PERSONAL_INFORMATION",
                            "Detections": [
                                {
                                    "Count": 1,
                                    "Type": "USA_SOCIAL_SECURITY_NUMBER",
                                    "Occurrences": {
                                        "Cells": [
                                            {
                                                "Column": 10,
                                                "Row": 1,
                                                "ColumnName": "Other"
                                            }
                                        ]
                                    }
                                }
                            ],
                            "TotalCount": 1
                        }
                    ],
                    "CustomDataIdentifiers": {
                        "Detections": [
                        ],
                        "TotalCount": 0
                    }
                }
            },
            "Details": {
                "AwsS3Object": {
                    "LastModified": "2022-04-22T18:16:46.000Z",
                    "ETag": "ebe1ca03ee8d006d457444445example",
                    "VersionId": "SlBC72z5hArgexOJifxw_IN57example",
                    "ServerSideEncryption": "aws:kms",
                    "SSEKMSKeyId": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                }
            }
```

```
        }
    ],
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "NEW"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "HIGH"
        },
        "Types": [
            "Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal"
        ]
    },
    "Sample": false,
    "ProcessedAt": "2022-05-11T10:23:49.667Z"
}
```

Beispiel für eine Richtlinienerkenntnis in Security Hub

Hier ist ein Beispiel für eine neue Richtlinienerkenntnis, die Macie in Security Hub in der ASFF veröffentlicht hat.

```
{
    "SchemaVersion": "2018-10-08",
    "Id": "36ca8ba0-caf1-4fee-875c-37760example",
    "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/macie",
    "ProductName": "Macie",
    "CompanyName": "Amazon",
    "Region": "us-east-1",
    "GeneratorId": "aws/macie",
    "AwsAccountId": "111122223333",
    "Types": [
        "Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-
S3BlockPublicAccessDisabled"
    ],
    "CreatedAt": "2022-04-24T09:27:43.313Z",
    "UpdatedAt": "2022-04-24T09:27:43.313Z",
    "Severity": {
        "Label": "HIGH",
        "Normalized": 70
    },
```

```
    "Title": "Block Public Access settings are disabled for the S3 bucket",
    "Description": "All Amazon S3 block public access settings are disabled for the
 Amazon S3 bucket. Access to the bucket is
      controlled only by access control lists (ACLs) or bucket policies.",
    "ProductFields": {
        "S3Bucket.effectivePermission": "NOT_PUBLIC",
        "S3Bucket.allowsUnencryptedObjectUploads": "FALSE",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
macie/36ca8ba0-caf1-4fee-875c-37760example",
        "aws/securityhub/ProductName": "Macie",
        "aws/securityhub/CompanyName": "Amazon"
    },
    "Resources": [
        {
        "Type": "AwsS3Bucket",
        "Id": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
        "Partition": "aws",
        "Region": "us-east-1",
        "Tags": {
            "Team": "Recruiting",
            "Division": "HR"
        },
        "Details": {
            "AwsS3Bucket": {
              "OwnerId":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example",
              "OwnerName": "johndoe",
              "OwnerAccountId": "444455556666",
              "CreatedAt": "2020-11-25T18:24:38.000Z",
              "ServerSideEncryptionConfiguration": {
                "Rules": [
                    {
                    "ApplyServerSideEncryptionByDefault": {
                        "SSEAlgorithm": "aws:kms",
                        "KMSMasterKeyID": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                    }
                  }
                ]
              },
              "PublicAccessBlockConfiguration": {
                "BlockPublicAcls": false,
                "BlockPublicPolicy": false,
                "IgnorePublicAcls": false,
```

```
                "RestrictPublicBuckets": false
               }
            }
         }
      }
    ],
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "NEW"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "HIGH"
        },
        "Types": [
            "Software and Configuration Checks/AWS Security Best Practices/
Policy:IAMUser-S3BlockPublicAccessDisabled"
        ]
    },
    "Sample": false
}
```

Aktivieren und Konfigurieren der AWS Security Hub Integration

Um Amazon Macie in zu integrierenAWS Security Hub, aktivieren Sie Security Hub für Ihr AWS-Konto. Weitere Informationen finden Sie unter Aktivieren von Security Hub im AWS Security Hub - Benutzerhandbuch.

Wenn Sie sowohl Macie als auch Security Hub aktivieren, wird die Integration automatisch aktiviert. Macie beginnt standardmäßig, neue und aktualisierte Richtlinienergebnisse automatisch in Security Hub zu veröffentlichen. Sie müssen keine zusätzlichen Schritte unternehmen, um die Integration zu konfigurieren. Wenn Sie bereits Richtlinienergebnisse haben, wenn die Integration aktiviert ist, veröffentlicht Macie diese nicht in Security Hub. Stattdessen veröffentlicht Macie nur die Richtlinienergebnisse, die es erstellt oder aktualisiert, nachdem die Integration aktiviert wurde.

Sie können Ihre Konfiguration optional anpassen, indem Sie die Häufigkeit auswählen, mit der Macie Aktualisierungen der Richtlinienergebnisse in Security Hub veröffentlicht. Sie können auch vertrauliche Datenergebnisse in Security Hub veröffentlichen. Um zu erfahren wie dies geht, vgl. Konfigurieren von Veröffentlichungseinstellungen für Ergebnisse.

Beenden der Veröffentlichung von Erkenntnissen in AWS Security Hub

Um die Veröffentlichung von Ergebnissen in zu beendenAWS Security Hub, können Sie die Veröffentlichungseinstellungen für Ihr Amazon Macie-Konto ändern. Um zu erfahren wie dies geht, vgl. Auswählen von Veröffentlichungszielen für Ergebnisse. Sie können dies auch über die Security Hub-Konsole oder die Security Hub-API tun. Weitere Informationen finden Sie unter Deaktivieren und Aktivieren des Flows von Erkenntnissen aus einer Integration (Konsole) oder Deaktivieren des Flows von Erkenntnissen aus einer Integration (Security Hub API, AWS CLI) im AWS Security Hub - Benutzerhandbuch.

Amazon Macie Macie-Integration mit AWS-Benutzerbenachrichtigungen

AWS User Notifications ist ein Service, der als zentraler Ort für IhreAWS Benachrichtigungen auf der fungiertAWS Management Console. Dazu gehören Benachrichtigungen wie CloudWatch Amazon-Alarme,AWS Support Fälle und Mitteilungen von anderenAWS-Services. Mit Benutzerbenachrichtigungen können Sie benutzerdefinierte Regeln und Versandkanäle für den Empfang von Benachrichtigungen über bestimmte Arten von EventBridge Amazon-Ereignissen konfigurieren. Zu den Versandkanälen gehören E-Mail,AWS Chatbot Chat-Benachrichtigungen undAWS Console Mobile Application Push-Benachrichtigungen. Sie können Benachrichtigungen auch in der AWS-Benutzerbenachrichtigungskonsole überprüfen. Weitere Informationen zu Benutzerbenachrichtigungen finden Sie im AWS User Notifications User Guide.

Macie ist in AWS-Benutzerbenachrichtigungen integriert. Das bedeutet, dass Sie Benutzerbenachrichtigungen so konfigurieren können, dass Sie über Ereignisse informiert werden, zu denen Macie Informationen EventBridge zu Richtlinien und vertraulichen Daten veröffentlicht. Wenn ein Findungsereignis den von Ihnen angegebenen Kriterien entspricht, generiert User Notifications eine Benachrichtigung. Die Benachrichtigung enthält wichtige Informationen zum zugehörigen Befund, z. B. Art und Schweregrad des Befundes sowie den Namen der betroffenen Ressource. Benutzerbenachrichtigungen können die Benachrichtigung auch an einen oder mehrere von Ihnen angegebene Versandkanäle senden. Sie können die von Ihnen gewählten Lieferkanäle an Ihre Sicherheits- und Compliance-Workflows anpassen.

Sie können Benutzerbenachrichtigungen beispielsweise so konfigurieren, dass Benachrichtigungen für bestimmte Arten neuer, schwerwiegender Befunde generiert werden. Sie könnenAWS Chatbot auch einen Versandkanal für diese Benachrichtigungen angeben. Benutzerbenachrichtigungen erkennen dann EventBridge Ereignisse für die Ergebnisse, generieren Benachrichtigungen, die

Daten aus den Ergebnissen enthalten, und sendet die Benachrichtigungen anAWS Chatbot. AWS Chatbotkönnte die Benachrichtigungen dann an einen Slack-Channel oder einen Amazon Chime Chime-Chatroom weiterleiten, um Ihr Incident-Response-Team zu benachrichtigen.

Themen

- Arbeiten mit AWS-Benutzerbenachrichtigungen arbeiten arbeiten
- Aktivierung und Konfiguration von AWS-Benutzerbenachrichtigungen für Amazon Macie Macie-Ergebnisse
- Zuordnung von AWS-Benutzerbenachrichtigungsfeldern zu Amazon Macie-Suchfeldern
- Änderung der Einstellungen für AWS-Benutzerbenachrichtigungen für die Ergebnisse von Amazon Macie
- Deaktivieren von AWS-Benutzerbenachrichtigungen für Amazon Macie Macie-Ergebnisse

Arbeiten mit AWS-Benutzerbenachrichtigungen arbeiten arbeiten

Mit AWS-Benutzerbenachrichtigungen erstellen Sie Regeln, um die Arten von EventBridge Amazon-Ereignissen festzulegen, die Sie überwachen und für die Sie Benachrichtigungen erhalten möchten. Eine Regel definiert Kriterien, die ein EventBridge Ereignis erfüllen muss, um eine Benachrichtigung zu generieren. Sie können auch einen oder mehrere Lieferkanäle für eine Regel auswählen. Die Versandkanäle geben an, wo Sie Benachrichtigungen für Ereignisse erhalten möchten, die den Kriterien einer Regel entsprechen.

Wenn Benutzerbenachrichtigungen ein EventBridge Ereignis erkennen, das den Kriterien einer Regel entspricht, werden die folgenden allgemeinen Aufgaben ausgeführt:

1. Extrahiert eine Teilmenge der Daten aus dem Ereignis.
2. Generiert eine Benachrichtigung, die extrahierten Daten.
3. Sendet die Benachrichtigung an die Übermittlungskanäle, die Sie für diese Art von Ereignis angeben.

Das Design und die Struktur der Benachrichtigung sind für jeden Versandkanal optimiert, an den sie gesendet wird.

Um die Häufigkeit oder Anzahl der Benachrichtigungen zu steuern, die Sie erhalten, können Sie die Aggregationseinstellungen für eine Regel konfigurieren. Wenn Sie diese Einstellungen aktivieren, kombiniert Benutzerbenachrichtigungen Daten für mehrere Ereignisse in einer einzigen

Benachrichtigung. Sie können festlegen, dass aggregierte Ereignisbenachrichtigungen schnell und häufig gesendet werden sollen, was Sie möglicherweise tun sollten, wenn Ereignisse mit hohem Schweregrad gefunden werden. Oder senden Sie sie weniger häufig, um weniger Benachrichtigungen zu erhalten, was Sie möglicherweise für Ereignisse mit geringem Schweregrad tun sollten. Wenn Sie Ereignisdaten kombinieren, können Sie mithilfe der AWS-Konsole für Benutzerbenachrichtigungen einen Drilldown durchführen, um die Details jedes aggregierten Ereignisses zu überprüfen. Von dort aus können Sie auch zu den einzelnen zugehörigen Ergebnissen auf der Amazon Macie Macie-Konsole navigieren.

Aktivierung und Konfiguration von AWS-Benutzerbenachrichtigungen für Amazon Macie Macie-Ergebnisse

Damit AWS-Benutzerbenachrichtigungen Benachrichtigungen für Amazon Macie Macie-Ergebnisse generieren können, erstellen Sie in Benutzerbenachrichtigungen eine Benachrichtigungskonfiguration für Macie. Eine Benachrichtigungskonfiguration spezifiziert die Kriterien für eine Regel. Es spezifiziert auch Versandkanäle und andere Einstellungen für die Überwachung und den Versand von Benachrichtigungen über EventBridge Amazon-Ereignisse, die den Kriterien der Regel entsprechen. Ausführliche Informationen zum Erstellen einer Benachrichtigungskonfiguration finden Sie unter Erste Schritte mit AWS-Benutzerbenachrichtigungen im AWS-Benutzerhandbuch für Benutzerbenachrichtigungen.

Um eine Benachrichtigungskonfiguration für Macie-Ergebnisse zu erstellen, wählen Sie die folgenden Optionen für die Ereignisregel:

- Wählen Sie als AWS-ServiceNamen Macie.
- Wählen Sie als Ereignistyp Macie Finding aus.
- Wählen Sie unter Regionen jede Region aus,AWS-Region in der Sie Macie verwenden und über die Ergebnisse informiert werden möchten.

Mit dieser Konfiguration überwacht Benutzerbenachrichtigungen EventBridge Ereignisse für SieAWS-Konto und generiert Benachrichtigungen für alle Ereignisse, die Macie in den von Ihnen ausgewählten Regionen findet. Die Ereignisse erfüllen die folgenden Kriterien:

- `source`entsprich`aws.macie`
- `detail-type`entsprich`Macie Finding`

Das zugrunde liegende JSON-Muster für die Ereignisregel lautet:

```
{
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"]
}
```

Um die Regel zu verfeinern und Benachrichtigungen nur für einen Teil der Ergebnisse zu generieren, können Sie das JSON-Muster für die Regel anpassen. Geben Sie dazu zusätzliche Kriterien an, die sich aus dem EventBridge Ereignisschema für Macie-Ergebnisse ableiten.

Wenn Sie eine Regel erstellen, die ein benutzerdefiniertes JSON-Muster verwendet, können Sie mehrere Benachrichtigungskonfigurationen für Macie-Ergebnisse erstellen. Anschließend können Sie die Bereitstellungskanäle und andere Einstellungen für jede Konfiguration an Ihre Sicherheits- und Compliance-Workflows für bestimmte Arten von Ergebnissen anpassen.

Sie können beispielsweise eine Regel erstellen, die Sie benachrichtigt, wenn Macie ein Policy:IAMUser/S3BucketPublicErgebnis generiert oder aktualisiert. In diesem Fall könnte das Muster für die Regel wie folgt aussehen:

```
{
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"],
    "detail": {
        "type": ["Policy:IAMUser/S3BucketPublic"]
    }
}
```

Und Sie könnten eine weitere Regel erstellen, die Sie benachrichtigt, wenn Macie ein Ergebnis mit vertraulichen Daten für einen öffentlich zugänglichen S3-Bucket generiert. In diesem Fall könnte das Muster für die Regel wie folgt aussehen:

```
{
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"],
    "detail": {
        "type": [ { "prefix": "SensitiveData" } ],
        "resourcesAffected": {
            "effectivePermission": ["PUBLIC"]
        }
    }
}
```

Wenn Sie mehrere Benachrichtigungskonfigurationen für Macie-Ergebnisse erstellen, sollten Sie sicherstellen, dass die Regel für jede Konfiguration einzigartig ist. Andernfalls erhalten Sie möglicherweise doppelte Benachrichtigungen für einzelne Ergebnisse.

Weitere Informationen zum Anpassen von Ereignismustern für Regeln finden Sie unter Verwenden benutzerdefinierter JSON-Ereignismuster im AWS-Benutzerhandbuch für Benutzerbenachrichtigungen.

Zuordnung von AWS-Benutzerbenachrichtigungsfeldern zu Amazon Macie-Suchfeldern

Wenn AWS User Notifications eine Benachrichtigung für einen Amazon Macie Macie-Befund generiert, füllt es die Benachrichtigung mit Daten aus einer Teilmenge von Feldern des entsprechenden EventBridge Amazon-Ereignisses. Diese Felder enthalten wichtige Details des zugehörigen Befundes, z. B. Art und Schweregrad des Befundes sowie den Namen der betroffenen Ressource.

Wenn Sie eine Benachrichtigung in der AWS-Benutzerbenachrichtigungskonsole überprüfen, enthält die Benachrichtigung alle Daten für diese Teilmenge von Feldern. Es enthält auch einen Link zu den zugehörigen Ergebnissen auf der Amazon Macie Macie-Konsole. Wenn Sie eine Benachrichtigung in anderen Versandkanälen überprüfen, enthält sie möglicherweise nur Daten für einige der Felder. Dies liegt daran, dass User Notifications das Design und die Struktur seiner Benachrichtigungen so anpasst, dass sie mit jedem unterstützten Versandkanaltyp funktionieren.

In der folgenden Tabelle sind die Felder aufgeführt, die in einer Benachrichtigung für ein Ergebnis enthalten sein könnten. In der Tabelle beschreibt die Spalte „Benachrichtigungsfeld“ den Namen eines Felds in einer Benachrichtigung (kursiv) oder gibt ihn an. In der Spalte „Ereignis suchen“ wird in Punktnotation der Name des entsprechenden JSON-Felds in einem EventBridge Ereignis für ein Ergebnis angegeben. Die Spalte Beschreibung beschreibt die Daten, die in dem Feld gespeichert sind.

Feld „Benachrichtigung“	Suche nach einem Ereignisf eld finden	Beschreibung
Überschrift der Nachricht	`detail.type`	Der Typ des Befundes. Beispiel: `Policy:IAMUser/S3BucketPublic` oder

Feld „Benachrichtigung“	Suche nach einem Ereignisfeld finden	Beschreibung
		`SensitiveData:S3Object/Financial` .
Übersicht	`detail.title`	Eine kurze Beschreibung des Befundes. Beispiel: `The S3 object contains financial information.`
Beschreibung	`detail.description`	Die vollständige Beschreibung des Befundes. Beispiel: `The S3 object contains financial information such as bank account numbers or credit card numbers.`
Schweregrad	`detail.severity.description`	Die qualitative Darstellung des Schweregrads des Befundes: `Low`,`Medium`, oder`High`.
Die ID des Ergebnisses	`detail.id`	Die eindeutige Kennung für das Ergebnis.
Erstellt	`detail.createdAt`	Das Datum und die Uhrzeit, zu der Macie das Ergebnis erstellt wurde.

Feld „Benachrichtigung“	Suche nach einem Ereignisfeld finden	Beschreibung
Aktualisiert	`detail.updatedAt`	Das Datum und die Uhrzeit, zu der Macie das Ergebnis zuletzt aktualisiert wurde. Bei Ergebnissen mit vertraulichen Daten entspricht dieser Wert dem Wert für das Feld Created (`detail.createdAt`). Alle Erkenntnisse sensibler Daten werden als neu (einzigartig) betrachtet.
Betroffener S3-Buckets	`detail.resourcesAffected.s3Bucket.arn`	Der AmazResource Name (ARN) des betroffen ist.
Betroffenes S3-Objekt	`detail.resourcesAffected.s3Object.path`	Der Name (Schlüssel) des betroffenen S3-Objekts, einschließlich des Namens des Buckets, in dem das Objekt gespeichert ist, und gegebenenfalls des Objektpräfixes. Dieses Feld ist nicht in Benachrichtigungen für politische Ergebnisse enthalten.

Feld „Benachrichtigung“	Suche nach einem Ereignisfeld finden	Beschreibung

Erkennung sensibler Daten	`detail.classificationDetails.result.sensitiveData.detections...`
	
	Und/oder
	
	`detail.classificationDetails.result.customDataIdentifiers.detections...`
		Dies ist eine Verkettung mehrerer Felder in einem Ereignis für die Suche nach sensiblen Daten. Dieses Feld ist nicht in Benachrichtigungen für politische Ergebnisse enthalten.
		
		Wenn ein verwalteter Datenbezeichner die sensiblen Daten erkannt hat, gibt dieses Feld die Kategorie, den Typ und die Anzahl (`count`) der erkannten vertraulichen Daten an. Zum Beispiel: `PERSONAL_INFORMATION: USA_SOCIAL_SECURITY_NUMBER 100 occurrences .`
		
		Wenn ein benutzerdefinierter Datenbezeichner die sensiblen Daten erkannt hat, gibt dieses Feld den Namen des benutzerdefinierten Datenbezeichners und die Anzahl (`count`) der erkannten vertraulichen Daten an. Zum Beispiel: `Employee ID 20 occurrences .`
		
		Wenn ein Ergebnis mehrere Arten sensibler Daten meldet, enthält die Benachrichtigung

Feld „Benachrichtigung“	Suche nach einem Ereignisf eld finden	Beschreibung
		Daten für bis zu vier Typen. Die Daten werden zuerst mit allen anwendbaren benutzerd efinierten Datenkennungen und dann mit allen zutreffen den verwalteten Datenkenn ungen gefüllt.

Änderung der Einstellungen für AWS-Benutzerbenachrichtigungen für die Ergebnisse von Amazon Macie

Sie können Ihre Einstellungen für AWS-Benutzerbenachrichtigungen für die Ergebnisse von Amazon Macie jederzeit ändern. Bearbeiten Sie dazu die Benachrichtigungskonfiguration in Benutzerbenachrichtigungen. Wie das geht, erfahren Sie unter Verwaltung von Benachrichtigungskonfigurationen im AWS User Notifications User Guide.

Wenn Sie mehrere Benachrichtigungskonfigurationen für Macie-Ergebnisse haben, wirkt sich das Ändern der Einstellungen für eine Konfiguration nicht auf die Einstellungen für Ihre anderen Konfigurationen aus. Sie können alle oder nur einige Ihrer Konfigurationen bearbeiten.

Deaktivieren von AWS-Benutzerbenachrichtigungen für Amazon Macie Macie-Ergebnisse

Um die Generierung und den Empfang von Benachrichtigungen aus den Ergebnissen von AWS User Notifications for Amazon Macie zu beenden, löschen Sie die Benachrichtigungskonfiguration unter Benutzerbenachrichtigungen. Wie das geht, erfahren Sie unter Verwaltung von Benachrichtigungskonfigurationen im AWS User Notifications User Guide.

Wenn Sie mehrere Benachrichtigungskonfigurationen für Macie-Ergebnisse haben, wirkt sich das Löschen einer Konfiguration nicht auf Ihre anderen Konfigurationen aus. Sie können alle oder nur einige Ihrer Konfigurationen löschen.

EventBridge Amazon-Ereignisschema für Amazon Macie-Ergebnisse

Um die Integration mit anderen Anwendungen, Diensten und Systemen wie Überwachungs- oder Eventmanagementsystemen zu unterstützen, veröffentlicht Amazon Macie die Ergebnisse automatisch EventBridge als Ereignisse an Amazon. EventBridge, ehemals Amazon CloudWatch Events, ist ein serverloser Event-Bus-Service, der einen Stream von Echtzeitdaten aus Anwendungen und anderen AWS-Services an Ziele wie AWS Lambda Funktionen, Amazon Simple Notification Service-Themen und Amazon Kinesis Kinesis-Streams übermittelt. Weitere Informationen EventBridge finden Sie im EventBridge Amazon-Benutzerhandbuch.

> **Note**
>
> Wenn Sie derzeit CloudWatch Events verwenden, beachten Sie, dass es sich bei EventBridge und CloudWatch Events um denselben zugrunde liegenden Service und dieselbe API handelt. EventBridge Enthält jedoch zusätzliche Funktionen, mit denen Sie Ereignisse von SaaS-Anwendungen (Software as a Service) und Ihren eigenen Anwendungen empfangen können. Da der zugrunde liegende Dienst und die API identisch sind, ist auch das Ereignisschema für Macie-Ergebnisse identisch.

Macie veröffentlicht automatisch Ereignisse für alle neuen Ergebnisse und das nachfolgende Auftreten vorhandener Richtlinienfeststellungen, mit Ausnahme von Ergebnissen, die automatisch durch eine Unterdrückungsregel archiviert werden. Bei den Ereignissen handelt es sich um JSON-Objekte, die dem EventBridge Schema für Ereignisse entsprechen. AWS Jedes Ereignis enthält eine JSON-Repräsentation eines bestimmten Ergebnisses. Da die Daten als EventBridge Ereignis strukturiert sind, können Sie ein Ergebnis einfacher überwachen, verarbeiten und darauf reagieren, indem Sie andere Anwendungen, Dienste und Tools verwenden. Weitere Informationen darüber, wie und wann Macie Ereignisse zu Ergebnissen veröffentlicht, finden Sie unterKonfigurieren von Veröffentlichungseinstellungen für Ergebnisse.

Themen

- Schema des Ereignisses
- Beispiel für ein Ereignis für ein Richtlinienergebnis
- Beispiel für ein Ereignis, bei dem sensible Daten gefunden wurden

Schema des Ereignisses

Das folgende Beispiel zeigt das Schema eines EventBridge Amazon-Ereignisses für einen Amazon Macie-Befund. Eine ausführliche Beschreibung der Felder, die in ein Finding-Event aufgenommen werden können, finden Sie unter Ergebnisse in der Amazon Macie API-Referenz. Die Struktur und die Felder eines Findereignisses sind eng mit dem Finding-Objekt der Amazon Macie Macie-API verknüpft.

```
{
    "version": "0",
    "id": "event ID",
    "detail-type": "Macie Finding",
    "source": "aws.macie",
    "account": "AWS-Konto ID (string)",
    "time": "event timestamp (string)",
    "region": "AWS-Region (string)",
    "resources": [
        <-- ARNs of the resources involved in the event -->
    ],
    "detail": {
        <-- Details of a policy or sensitive data finding -->
    },
    "policyDetails": null, <-- Additional details of a policy finding or null for a
 sensitive data finding -->
    "sample": Boolean,
    "archived": Boolean
}
```

Beispiel für ein Ereignis für ein Richtlinienergebnis

Im folgenden Beispiel werden anhand von Beispieldaten die Struktur und Art von Objekten und Feldern in einem EventBridge Amazon-Ereignis für eine Richtlinienfeststellung veranschaulicht.

In diesem Beispiel meldet das Ereignis ein späteres Auftreten einer bestehenden Richtlinienfeststellung: Einstellungen zum Blockieren des öffentlichen Zugriffs wurden für einen S3-Bucket deaktiviert. Anhand der folgenden Felder und Werte können Sie feststellen, ob dies der Fall ist:

- Das `type` Feld ist auf eingestelltPolicy:IAMUser/S3BlockPublicAccessDisabled.

- Die `updatedAt` Felder `createdAt` und haben unterschiedliche Werte. Dies ist ein Indikator dafür, dass das Ereignis auf ein späteres Eintreten einer bestehenden politischen Feststellung hinweist. Die Werte für diese Felder wären dieselben, wenn das Ereignis ein neues Ergebnis melden würde.
- Das `count` Feld ist auf gesetzt2, was darauf hinweist, dass der Befund zum zweiten Mal auftritt.
- Das `category` Feld ist auf eingestelltPOLICY.
- Der Wert für das `classificationDetails` Feld ist`null`, was dazu beiträgt, dieses Ereignis für ein Richtlinienergebnis von einem Ereignis für ein Ergebnis vertraulicher Daten zu unterscheiden. Bei einem Ergebnis vertraulicher Daten entspricht dieser Wert einer Gruppe von Objekten und Feldern, die Informationen darüber liefern, wie und welche vertraulichen Daten gefunden wurden.

Beachten Sie auch, dass der Wert für das `sample` Feld lautet`true`. Dieser Wert unterstreicht, dass es sich um ein Beispielereignis zur Verwendung in der Dokumentation handelt.

```
{
    "version": "0",
    "id": "0948ba87-d3b8-c6d4-f2da-732a1example",
    "detail-type": "Macie Finding",
    "source": "aws.macie",
    "account": "123456789012",
    "time": "2021-04-30T23:12:15Z",
    "region":"us-east-1",
    "resources": [],
    "detail": {
        "schemaVersion": "1.0",
        "id": "64b917aa-3843-014c-91d8-937ffexample",
        "accountId": "123456789012",
        "partition": "aws",
        "region": "us-east-1",
        "type": "Policy:IAMUser/S3BlockPublicAccessDisabled",
        "title": "Block public access settings are disabled for the S3 bucket",
        "description": "All bucket-level block public access settings were disabled for
 the S3 bucket. Access to the bucket is controlled by account-level block public access
 settings, access control lists (ACLs), and the bucket's bucket policy.",
        "severity": {
            "score": 3,
            "description": "High"
        },
        "createdAt": "2021-04-29T15:46:02Z",
        "updatedAt": "2021-04-30T23:12:15Z",
        "count": 2,
```

```
        "resourcesAffected": {
            "s3Bucket": {
                "arn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
                "name": "DOC-EXAMPLE-BUCKET1",
                "createdAt": "2020-04-03T20:46:56.000Z",
                "owner":{
                    "displayName": "johndoe",
                    "id":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example"
                },
                "tags": [
                    {
                        "key": "Division",
                        "value": "HR"
                    },
                    {
                        "key": "Team",
                        "value": "Recruiting"
                    }
                ],
                "defaultServerSideEncryption": {
                    "encryptionType": "aws:kms",
                    "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                },
                "publicAccess": {
                    "permissionConfiguration": {
                        "bucketLevelPermissions": {
                            "accessControlList": {
                                "allowsPublicReadAccess": false,
                                "allowsPublicWriteAccess": false
                            },
                            "bucketPolicy": {
                                "allowsPublicReadAccess": false,
                                "allowsPublicWriteAccess": false
                            },
                            "blockPublicAccess": {
                                "ignorePublicAcls": false,
                                "restrictPublicBuckets": false,
                                "blockPublicAcls": false,
                                "blockPublicPolicy": false
                            }
                        },
                        "accountLevelPermissions": {
```

```
                            "blockPublicAccess": {
                                "ignorePublicAcls": true,
                                "restrictPublicBuckets": true,
                                "blockPublicAcls": true,
                                "blockPublicPolicy": true
                            }
                        }
                    },
                    "effectivePermission": "NOT_PUBLIC"
                },
                "allowsUnencryptedObjectUploads": "FALSE"
            },
            "s3Object": null
        },
        "category": "POLICY",
        "classificationDetails": null,
        "policyDetails": {
            "action": {
                "actionType": "AWS_API_CALL",
                "apiCallDetails": {
                    "api": "PutBucketPublicAccessBlock",
                    "apiServiceName": "s3.amazonaws.com",
                    "firstSeen": "2021-04-29T15:46:02.401Z",
                    "lastSeen": "2021-04-30T23:12:15.401Z"
                }
            },
            "actor": {
                "userIdentity": {
                    "type": "AssumedRole",
                    "assumedRole": {
                        "principalId": "AROA1234567890EXAMPLE:AssumedRoleSessionName",
                        "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/
MySessionName",
                        "accountId": "111122223333",
                        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                        "sessionContext": {
                            "attributes": {
                                "mfaAuthenticated": false,
                                "creationDate": "2021-04-29T10:25:43.511Z"
                            },
                            "sessionIssuer": {
                                "type": "Role",
                                "principalId": "AROA1234567890EXAMPLE",
```

```
                                "arn": "arn:aws:iam::123456789012:role/
RoleToBeAssumed",
                                "accountId": "123456789012",
                                "userName": "RoleToBeAssumed"
                            }
                        }
                    },
                    "root": null,
                    "iamUser": null,
                    "federatedUser": null,
                    "awsAccount": null,
                    "awsService": null
                },
                "ipAddressDetails":{
                    "ipAddressV4": "192.0.2.0",
                    "ipOwner": {
                        "asn": "-1",
                        "asnOrg": "ExampleFindingASNOrg",
                        "isp": "ExampleFindingISP",
                        "org": "ExampleFindingORG"
                    },
                    "ipCountry": {
                        "code": "US",
                        "name": "United States"
                    },
                    "ipCity": {
                        "name": "Ashburn"
                    },
                    "ipGeoLocation": {
                        "lat": 39.0481,
                        "lon": -77.4728
                    }
                },
                "domainDetails": null
            }
        },
        "sample": true,
        "archived": false
    }
}
```

Beispiel für ein Ereignis, bei dem sensible Daten gefunden wurden

Im folgenden Beispiel werden anhand von Beispieldaten die Struktur und Art von Objekten und Feldern in einem EventBridge Amazon-Ereignis veranschaulicht, bei dem sensible Daten gefunden wurden.

In diesem Beispiel meldet das Ereignis ein neues Ergebnis vertraulicher Daten: Amazon Macie hat in einem S3-Objekt mehr als eine Kategorie sensibler Daten gefunden. Mithilfe der folgenden Felder und Werte können Sie feststellen, ob dies der Fall ist:

- Das `type` Feld ist auf eingestellt`SensitiveData:S3Object/Multiple`.
- Die `updatedAt` Felder `createdAt` und haben dieselben Werte. Im Gegensatz zu politischen Ergebnissen ist dies bei Ergebnissen sensibler Daten immer der Fall. Alle Ergebnisse sensibler Daten gelten als neu.
- Das `count` Feld ist auf eingestellt`1`, was darauf hinweist, dass es sich um ein neues Ergebnis handelt. Im Gegensatz zu politischen Erkenntnissen ist dies bei Ergebnissen sensibler Daten immer der Fall. Alle Ergebnisse sensibler Daten gelten als einzigartig (neu).
- Das `category` Feld ist auf eingestellt`CLASSIFICATION`.
- Der Wert für das `policyDetails` Feld ist`null`, was dazu beiträgt, dieses Ereignis für eine Entdeckung vertraulicher Daten von einem Ereignis für eine Richtlinienfeststellung zu unterscheiden. Bei einem Richtlinienergebnis entspricht dieser Wert einer Gruppe von Objekten und Feldern, die Informationen über einen potenziellen Richtlinienverstoß oder ein Problem mit der Sicherheit oder dem Datenschutz eines S3-Buckets bereitstellen.

Beachten Sie auch, dass der Wert für das `sample` Feld lautet`true`. Dieser Wert unterstreicht, dass es sich um ein Beispielereignis zur Verwendung in der Dokumentation handelt.

```
{
    "version": "0",
    "id": "14ddd0b1-7c90-b9e3-8a68-6a408example",
    "detail-type": "Macie Finding",
    "source": "aws.macie",
    "account": "123456789012",
    "time": "2022-04-20T08:19:10Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "schemaVersion": "1.0",
```

```
        "id": "4ed45d06-c9b9-4506-ab7f-18a57example",
        "accountId": "123456789012",
        "partition": "aws",
        "region": "us-east-1",
        "type": "SensitiveData:S3Object/Multiple",
        "title": "The S3 object contains multiple categories of sensitive data",
        "description": "The S3 object contains more than one category of sensitive
 data.",
        "severity": {
            "score": 3,
            "description": "High"
        },
        "createdAt": "2022-04-20T18:19:10Z",
        "updatedAt": "2022-04-20T18:19:10Z",
        "count": 1,
        "resourcesAffected": {
            "s3Bucket": {
                "arn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
                "name": "DOC-EXAMPLE-BUCKET2",
                "createdAt": "2020-05-15T20:46:56.000Z",
                "owner": {
                    "displayName": "johndoe",
                    "id":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example"
                },
                "tags":[
                    {
                        "key":"Division",
                        "value":"HR"
                    },
                    {
                        "key":"Team",
                        "value":"Recruiting"
                    }
                ],
                "defaultServerSideEncryption": {
                    "encryptionType": "aws:kms",
                    "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                },
                "publicAccess": {
                    "permissionConfiguration": {
                        "bucketLevelPermissions": {
                            "accessControlList": {
```

```
                                "allowsPublicReadAccess": false,
                                "allowsPublicWriteAccess": false
                            },
                            "bucketPolicy":{
                                "allowsPublicReadAccess": false,
                                "allowsPublicWriteAccess": false
                            },
                            "blockPublicAccess": {
                                "ignorePublicAcls": true,
                                "restrictPublicBuckets": true,
                                "blockPublicAcls": true,
                                "blockPublicPolicy": true
                            }
                        },
                        "accountLevelPermissions": {
                            "blockPublicAccess": {
                                "ignorePublicAcls": false,
                                "restrictPublicBuckets": false,
                                "blockPublicAcls": false,
                                "blockPublicPolicy": false
                            }
                        }
                    },
                    "effectivePermission": "NOT_PUBLIC"
                },
                "allowsUnencryptedObjectUploads": "TRUE"
            },
            "s3Object":{
                "bucketArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
                "key": "2022 Sourcing.csv",
                "path": "DOC-EXAMPLE-BUCKET2/2022 Sourcing.csv",
                "extension": "csv",
                "lastModified": "2022-04-19T22:08:25.000Z",
                "versionId": "",
                "serverSideEncryption": {
                    "encryptionType": "aws:kms",
                    "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                },
                "size": 4750,
                "storageClass": "STANDARD",
                "tags":[
                    {
                        "key":"Division",
```

```
                        "value":"HR"
                    },
                    {
                        "key":"Team",
                        "value":"Recruiting"
                    }
                ],
                "publicAccess": false,
                "etag": "6bb7fd4fa9d36d6b8fb8882caexample"
            }
        },
        "category": "CLASSIFICATION",
        "classificationDetails": {
            "jobArn": "arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample",
            "jobId": "3ce05dbb7ec5505def334104bexample",
            "result": {
                "status": {
                    "code": "COMPLETE",
                    "reason": null
                },
                "sizeClassified": 4750,
                "mimeType": "text/csv",
                "additionalOccurrences": true,
                "sensitiveData": [
                    {
                        "category": "PERSONAL_INFORMATION",
                        "totalCount": 65,
                        "detections": [
                            {
                                "type": "USA_SOCIAL_SECURITY_NUMBER",
                                "count": 30,
                                "occurrences": {
                                    "lineRanges": null,
                                    "offsetRanges": null,
                                    "pages": null,
                                    "records": null,
                                    "cells": [
                                        {
                                            "row": 2,
                                            "column": 1,
                                            "columnName": "SSN",
                                            "cellReference": null
                                        },
```

```
                                {
                                    "row": 3,
                                    "column": 1,
                                    "columnName": "SSN",
                                    "cellReference": null
                                },
                                {
                                    "row": 4,
                                    "column": 1,
                                    "columnName": "SSN",
                                    "cellReference": null
                                }
                            ]
                        }
                    },
                    {
                        "type": "NAME",
                        "count": 35,
                        "occurrences": {
                            "lineRanges": null,
                            "offsetRanges": null,
                            "pages": null,
                            "records": null,
                            "cells": [
                                {
                                    "row": 2,
                                    "column": 3,
                                    "columnName": "Name",
                                    "cellReference": null
                                },
                                {
                                    "row": 3,
                                    "column": 3,
                                    "columnName": "Name",
                                    "cellReference": null
                                }
                            ]
                        }
                    }
                ]
            },
            {
                "category": "FINANCIAL_INFORMATION",
                "totalCount": 30,
```

```
                        "detections": [
                            {
                                "type": "CREDIT_CARD_NUMBER",
                                "count": 30,
                                "occurrences": {
                                    "lineRanges": null,
                                    "offsetRanges": null,
                                    "pages": null,
                                    "records": null,
                                    "cells": [
                                        {
                                            "row": 2,
                                            "column": 14,
                                            "columnName": "CCN",
                                            "cellReference": null
                                        },
                                        {
                                            "row": 3,
                                            "column": 14,
                                            "columnName": "CCN",
                                            "cellReference": null
                                        }
                                    ]
                                }
                            }
                        ]
                    }
                ],
                "customDataIdentifiers": {
                    "totalCount": 0,
                    "detections": []
                }
            },
            "detailedResultsLocation": "s3://macie-data-discovery-results/
AWSLogs/123456789012/Macie/us-east-1/3ce05dbb7ec5505def334104bexample/
d48bf16d-0deb-3e49-9d8c-d407cexample.jsonl.gz",
            "originType": "SENSITIVE_DATA_DISCOVERY_JOB"
        },
        "policyDetails": null,
        "sample": true,
        "archived": false
    }
}
```

Prognose und Überwachung der Amazon Macie Macie-Kosten

Um Ihnen bei der Prognose und Überwachung Ihrer Kosten für die Nutzung von Amazon Macie zu helfen, berechnet Macie die geschätzten Nutzungskosten für Ihr Konto und stellt diese bereit. Mit diesen Daten können Sie bestimmen, ob Sie die Nutzung des Service oder Ihre Kontingente anpassen möchten. Wenn Sie derzeit an einer kostenlosen 30-Tage-Testversion von Macie teilnehmen, können Sie anhand dieser Daten Ihre Kosten für die Nutzung von Macie nach Ablauf der kostenlosen Testversion abschätzen. Sie können auch den Status Ihrer Testversion überprüfen.

Sie können Ihre geschätzten Nutzungskosten auf der Amazon Macie Macie-Konsole überprüfen und mit der Amazon Macie Macie-API programmgesteuert darauf zugreifen. Wenn Sie der Macie-Administrator für ein Unternehmen sind, können Sie sowohl aggregierte Daten für Ihr Unternehmen als auch Aufschlüsselungen der Daten für Konten in Ihrer Organisation überprüfen und darauf zugreifen.

Zusätzlich zu den geschätzten Nutzungskosten, die Macie angibt, können Sie Ihre tatsächlichen Kosten überprüfen und überwachen, indem AWS Billing and Cost Management Sie AWS Billing and Cost Managementbietet Funktionen, mit denen Sie Ihre Kosten für AWS-Services Ihr Konto oder Ihre Organisation verfolgen und analysieren sowie Budgets verwalten können. Es bietet auch Funktionen, mit denen Sie die Nutzungskosten auf der Grundlage historischer Daten prognostizieren können. Weitere Informationen finden Sie im AWS Billing-Benutzerhandbuch.

Themen

- Grundlegendes zur Berechnung der geschätzten Nutzungskosten für Amazon Macie
- Überprüfung der geschätzten Nutzungskosten für Amazon Macie
- Teilnahme an der kostenlosen Amazon Macie-Testversion

Grundlegendes zur Berechnung der geschätzten Nutzungskosten für Amazon Macie

Die Preise von Amazon Macie basieren auf den folgenden Dimensionen.

Präventive Kontrollüberwachung

Diese Kosten entstehen durch die Pflege Ihres Amazon Simple Storage Service (Amazon S3) -Bucket-Inventars sowie die Bewertung und Überwachung der Buckets auf Sicherheits- und Zugriffskontrolle. Weitere Informationen finden Sie unter So überwacht Macie die Amazon S3 S3-Datensicherheit.

Die Abrechnung erfolgt auf der Grundlage der Gesamtzahl der S3-Buckets, die Macie für Ihr Konto überwacht. Die Gebühren werden anteilig pro Tag berechnet.

Objektüberwachung für die automatische Erkennung sensibler Daten

Diese Kosten entstehen durch die Überwachung und Bewertung Ihres S3-Bucket-Inventars, um S3-Objekte zu identifizieren, die für eine Analyse in Frage kommen, durch die automatische Erkennung vertraulicher Daten. Weitere Informationen finden Sie unter So funktioniert die automatische Erkennung vertraulicher Daten.

Die Gebühren richten sich nach der Gesamtzahl der S3-Objekte, die Macie für Ihr Konto überwacht. Die Gebühren werden anteilig pro Tag berechnet.

Objektanalyse anhand von Aufträgen zur Erkennung vertraulicher Daten und automatisierter Erkennung vertraulicher Daten

Diese Kosten ergeben sich aus der Analyse von S3-Objekten und der Berichterstattung vertraulicher Daten, die Macie in den Objekten findet. Dazu gehören Analysen und Berichte nach Aufträgen zur Erkennung sensibler Daten und zur automatisierten Erkennung vertraulicher Daten.

Ihnen wird die Menge der unkomprimierten Daten berechnet, die Macie in S3-Objekten analysiert. Für Objekte, die Macie aus Gründen wie der Verwendung einer nicht unterstützten Amazon S3 S3-Speicherklasse, der Verwendung einer nicht unterstützten Datei oder eines nicht unterstützten Speicherformats oder der Berechtigungseinstellungen nicht analysieren kann, fallen keine Gebühren an. Weitere Informationen finden Sie unter Erkennen vertraulicher Daten. Darüber hinaus hängen diese Kosten nicht von der Anzahl der Ergebnisse vertraulicher Daten ab, die bei Ihren Aufträgen oder bei der automatisierten Erkennung vertraulicher Daten anfallen.

Um die Kosten für die automatische Erkennung vertraulicher Daten zu verwalten, können Sie einzelne S3-Buckets von den Analysen ausschließen. Sie können beispielsweise Buckets ausschließen, von denen bekannt ist, dass sie die Sicherheits- und Compliance-Anforderungen Ihres Unternehmens erfüllen. Um Buckets auszuschließen, können Sie die Konfigurationseinstellungen für Ihr Konto aktualisieren. Sie können Buckets auch case-by-case

einzeln ausschließen, während Sie die Details der einzelnen Buckets in Ihrem Bucket-Inventar überprüfen.

Die Kosten für Aufträge zur Erkennung vertraulicher Daten sind durch das monatliche Kontingent für die Erkennung vertraulicher Daten für Ihr Konto begrenzt. (Das Standardkontingent beträgt 5 TB Daten.) Wenn ein Job läuft und die Analyse der in Frage kommenden Objekte dieses Kontingent erreicht, pausiert Macie den Job automatisch, bis der nächste Kalendermonat beginnt (und das monatliche Kontingent für Ihr Konto zurückgesetzt wird) oder Sie das Kontingent für Ihr Konto erhöhen.

Wenn Sie der Macie-Administrator für ein Unternehmen sind, sind die Kosten für die Erkennung vertraulicher Daten durch das monatliche Kontingent für die Erkennung vertraulicher Daten für jedes Konto begrenzt, für das Sie Daten analysieren. Das Kontingent für ein Mitgliedskonto definiert die maximale Datenmenge, die Ihre Jobs und die Jobs des Mitgliedskontos für das Konto während eines Kalendermonats analysieren können. Wenn ein Job ausgeführt wird und die Analyse der in Frage kommenden Objekte dieses Kontingent für ein Mitgliedskonto erreicht, beendet Macie die Analyse der Objekte, die dem Konto gehören. Wenn Macie die Analyse der Objekte für alle anderen Konten abgeschlossen hat, die das Kontingent nicht erreicht haben, unterbricht Macie den Job automatisch. Wenn es sich um einen einmaligen Job handelt, nimmt Macie den Job automatisch wieder auf, wenn der nächste Kalendermonat beginnt, oder das Kontingent wird für alle betroffenen Konten erhöht, je nachdem, was zuerst eintritt. Wenn es sich um einen periodischen Job handelt, nimmt Macie den Job automatisch wieder auf, wenn der nächste Lauf geplant ist oder der nächste Kalendermonat beginnt, je nachdem, was zuerst eintritt. Wenn ein geplanter Lauf vor Beginn des nächsten Kalendermonats beginnt oder das Kontingent für ein betroffenes Konto erhöht wird, analysiert Macie keine Objekte, die dem Konto gehören.

> **Tip**
>
> Hilfreiche Tipps zur Verwaltung oder Reduzierung der Kosten für die Erkennung vertraulicher Daten finden Sie im Blogbeitrag How to use Amazon Macie to reduce the cost of discovery sensitive data im AWSSecurity Blog.

Detaillierte Informationen und Beispiele für Nutzungskosten finden Sie unter Amazon Macie Macie-Preise.

Wenn Sie Macie verwenden, um Ihre geschätzten Nutzungskosten zu überprüfen, ist es wichtig zu wissen, wie die Kostenschätzungen berechnet werden. Berücksichtigen Sie dabei Folgendes:

- Die Schätzungen sind in US-Dollar angegeben und gelten AWS-Region nur für den aktuellen Stand. Wenn Sie Macie in mehreren Regionen verwenden, werden die Daten nicht für alle Regionen aggregiert, in denen Sie Macie verwenden.
- Auf der Konsole beinhalten die Schätzungen den aktuellen Kalendermonat bis heute. Wenn Sie die Daten programmgesteuert mit der Amazon Macie Macie-API abfragen, können Sie einen inklusiven Zeitraum für die Schätzungen wählen. Dies kann ein fortlaufender Zeitraum der letzten 30 Tage oder des aktuellen Kalendermonats bis heute sein.
- Die Schätzungen spiegeln nicht alle Rabatte wider, die möglicherweise für Ihr Konto gelten. Die Ausnahme bilden Rabatte, die sich aus regionalen Volumenpreisstufen ergeben, wie in der Amazon Macie Macie-Preisgestaltung beschrieben. Wenn Ihr Konto für diese Art von discount in Frage kommt, spiegeln die Schätzungen diesen discount wider.
- Wenn Sie der Macie-Administrator einer Organisation sind, spiegeln die Schätzungen nicht die kombinierten Rabatte für das Nutzungsvolumen für Ihre Organisation wider. Informationen zu diesen Rabatten finden Sie unter Mengenrabatte im AWS BillingBenutzerhandbuch.
- Bei der präventiven Kontrolle basiert die Schätzung auf den durchschnittlichen Tageskosten für den jeweiligen Zeitraum. Die Kosten werden anteilig pro Tag berechnet.
- Für die automatische Erkennung sensibler Daten basiert die Gesamtschätzung auf den durchschnittlichen täglichen Kosten für die Objektüberwachung (anteilig pro Tag) und der Menge unkomprimierter Daten, die Macie im geltenden Zeitraum bisher analysiert hat. Wenn Sie der Macie-Administrator für eine Organisation sind und Daten für ein Mitgliedskonto analysieren, sind die geschätzten Kosten dieser Aktivitäten in den Schätzungen für jedes entsprechende Konto enthalten.
- Bei Aufträgen zur Erkennung vertraulicher Daten basiert die Schätzung auf der Menge der unkomprimierten Daten, die Ihre Jobs im jeweiligen Zeitraum bisher analysiert haben. Wenn Sie der Macie-Administrator für eine Organisation sind und Jobs ausführen, die Daten für ein Mitgliedskonto analysieren, sind die geschätzten Kosten dieser Jobs in der Schätzung für das entsprechende Mitgliedskonto enthalten.
- Wenn es sich bei Ihrem Konto um ein Mitgliedskonto in einer Organisation handelt und Ihr Macie-Administrator die automatische Erkennung vertraulicher Daten durchführt oder Aufgaben zur Erkennung vertraulicher Daten ausführt, die Ihre Daten analysieren, sind die geschätzten Kosten dieser Aktivitäten in den Schätzungen für Ihr Konto enthalten.
- Die Schätzungen beinhalten keine Kosten, die Ihnen für die Nutzung anderer Funktionen AWS-Services mit bestimmten Macie-Funktionen entstehen. Verwenden Sie beispielsweise Customer Managed, AWS KMS keys um S3-Objekte zu entschlüsseln, die Sie auf vertrauliche Daten überprüfen möchten.

Beachten Sie auch, dass Macie ein monatliches kostenloses Kontingent für die Analyse von S3-Objekten anhand von Aufträgen zur Erkennung vertraulicher Daten und zur automatisierten Erkennung vertraulicher Daten anbietet. Jeden Monat ist die Analyse von bis zu 1 GB an Daten kostenlos, um sensible Daten in S3-Objekten zu erkennen und zu melden. Wenn in einem bestimmten Monat mehr als 1 GB an Daten analysiert werden, fallen für Ihr Konto nach den ersten 1 GB an Daten Gebühren für die Erkennung vertraulicher Daten an. Wenn in einem Monat weniger als 1 GB Daten analysiert werden, wird die verbleibende Kontingente nicht auf den nächsten Monat übertragen. Wenn Ihr Konto Teil einer Organisation mit konsolidierter Abrechnung ist, gilt das kostenlose Kontingent für die kombinierte Datenmenge, die für Ihr Unternehmen analysiert wurde. Mit anderen Worten, die Analyse von bis zu 1 GB Daten pro Monat für alle Konten in Ihrem Unternehmen ist kostenlos.

Überprüfung der geschätzten Nutzungskosten für Amazon Macie

Um Ihre aktuellen geschätzten Nutzungskosten für Amazon Macie zu überprüfen, können Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden. Sowohl die Konsole als auch die API bieten geschätzte Kosten für Macie-Preisdimensionen. Wenn Sie derzeit an einer kostenlosen 30-Tage-Testversion teilnehmen, können Sie anhand dieser Daten Ihre Kosten für die Nutzung von Macie nach Ablauf Ihrer kostenlosen Testversion abschätzen. Informationen zu den Preisdimensionen und Überlegungen bei Macie finden Sie unterVerstehen, wie die geschätzten Nutzungskosten berechnet werden. Detaillierte Informationen und Beispiele für Nutzungskosten finden Sie unter Amazon Macie Macie-Preise.

In Macie werden die geschätzten Nutzungskosten in US-Dollar angegeben und gelten nur für den StromAWS-Region. Wenn Sie die Daten mithilfe der Konsole überprüfen, beziehen sich die Kostenschätzungen auf den aktuellen Kalendermonat bis heute (einschließlich). Wenn Sie die Daten programmgesteuert mit der Amazon Macie Macie-API abfragen, können Sie einen inklusiven Zeitraum für die Schätzungen angeben, entweder einen fortlaufenden Zeitraum der letzten 30 Tage oder den aktuellen Kalendermonat bis heute.

Themen

- Überprüfung der geschätzten Nutzungskosten auf der Amazon Macie Macie-Konsole
- Abfragen der geschätzten Nutzungskosten mit der Amazon Macie API

Überprüfung der geschätzten Nutzungskosten auf der Amazon Macie Macie-Konsole

Auf der Amazon Macie Macie-Konsole sind die Kostenschätzungen wie folgt organisiert:

- Präventive Kontrollüberwachung — Dies sind die geschätzten Kosten für die Wartung Ihres Amazon Simple Storage Service (Amazon S3) -Bucket-Inventars und die Bewertung und Überwachung der Buckets im Hinblick auf Sicherheit und Zugriffskontrolle.
- Erkennungsaufträge für sensible Daten — Dies sind die geschätzten Kosten der von Ihnen ausgeführten Aufträge zur Erkennung vertraulicher Daten.
- Automatisierte Erkennung vertraulicher Daten — Dies sind die geschätzten Kosten für die Durchführung der automatisierten Erkennung vertraulicher Daten. Dazu gehört die Überwachung und Bewertung Ihres S3-Bucket-Inventars, um S3-Objekte zu identifizieren, die für eine Analyse in Frage kommen. Dazu gehören auch die Analyse geeigneter Objekte und die Berichterstattung über sensible Daten, Statistiken, Ergebnisse und andere Arten von Ergebnissen.

Gehen Sie wie folgt vor, um Ihre geschätzten Nutzungskosten mithilfe der Amazon Macie Macie-Konsole zu überprüfen.

Um deine geschätzten Nutzungskosten auf der Konsole zu überprüfen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. AWS-RegionWählen Sie die -Region aus, in der Sie Ihre geschätzten Kosten überprüfen möchten.
3. Wählen Sie im Navigationsbereich Verwendung aus.

Wenn Sie ein eigenständiges Macie-Konto haben oder Ihr Konto ein Mitgliedskonto in einer Organisation ist, wird auf der Seite Nutzung eine Aufschlüsselung der geschätzten Nutzungskosten für Ihr Konto angezeigt.

Wenn Sie der Macie-Administrator einer Organisation sind, werden auf der Seite Verwendung Konten in Ihrer Organisation aufgeführt:

- In der Tabelle gibt das Feld Summe die geschätzten Gesamtkosten für jedes Konto an.
- Der Abschnitt Geschätzte Kosten enthält die geschätzten Gesamtkosten für Ihr Unternehmen und eine Aufschlüsselung dieser Kosten.

Um die Aufschlüsselung der geschätzten Kosten für ein bestimmtes Konto in Ihrer Organisation zu überprüfen, wählen Sie das Konto in der Tabelle aus. Der Abschnitt Geschätzte Kosten zeigt dann diese Aufschlüsselung. Um diese Daten für ein anderes Konto anzuzeigen, wählen Sie das Konto in der Tabelle aus. Um Ihre Kontoauswahl zu löschen, wählen Sie das X neben der Konto-ID aus.

Abfragen der geschätzten Nutzungskosten mit der Amazon Macie API

Um Ihre geschätzten Nutzungskosten programmgesteuert abzufragen, können Sie die folgenden Operationen der Amazon Macie Macie-API verwenden:

- GetUsageTotals— Dieser Vorgang gibt die geschätzten Gesamtnutzungskosten für Ihr Konto zurück, gruppiert nach Nutzungskennzahlen. Wenn Sie der Macie-Administrator einer Organisation sind, gibt dieser Vorgang aggregierte Kostenschätzungen für alle Konten in Ihrer Organisation zurück. Weitere Informationen zu diesem Vorgang finden Sie unter Nutzungsgesamtwerte in der Amazon Macie API-Referenz.
- GetUsageStatistics— Dieser Vorgang gibt Nutzungsstatistiken und zugehörige Daten für Ihr Konto zurück, gruppiert nach Konto und dann nach Nutzungsmetrik. Die Daten beinhalten die geschätzten Gesamtnutzungskosten und die Leistungsbilanzkontingente. Gegebenenfalls wird auch angegeben, wann Ihre kostenlose 30-Tage-Testversion für Macie und für die automatische Erkennung vertraulicher Daten gestartet wurde. Wenn Sie der Macie-Administrator einer Organisation sind, gibt dieser Vorgang eine Aufschlüsselung der Daten für alle Konten in Ihrer Organisation zurück. Sie können Ihre Abfrage anpassen, indem Sie die Abfrageergebnisse sortieren und filtern. Weitere Informationen zu diesem Vorgang finden Sie unter Nutzungsstatistiken in der Amazon Macie API-Referenz.

Wenn Sie eine der beiden Operationen verwenden, können Sie optional einen inklusiven Zeitbereich für die Daten angeben. Bei diesem Zeitraum kann es sich um einen fortlaufenden Zeitraum der letzten 30 Tage (`PAST_30_DAYS`) oder um den aktuellen Kalendermonat bis heute (`MONTH_TO_DATE`) handeln. Wenn Sie keinen Zeitraum angeben, gibt Macie die Daten der letzten 30 Tage zurück.

Die folgenden Beispiele zeigen, wie geschätzte Nutzungskosten und Statistiken mithilfe von AWS Command Line Interface(AWS CLI) abgefragt werden. Sie können die Daten auch abfragen, indem Sie eine aktuelle Version eines anderen AWS Befehlszeilentools oder eines AWS SDK verwenden oder HTTPS-Anfragen direkt an Macie senden. Informationen zu AWS Tools und SDKs finden Sie unter Tools, auf AWS denen Sie aufbauen können.

Beispiele

- Beispiel 1: Abfrage der geschätzten Gesamtnutzungskosten
- Beispiel 2: Nutzungsstatistiken abfragen

Beispiel 1: Abfrage der geschätzten Gesamtnutzungskosten

Um die geschätzten Gesamtnutzungskosten mithilfe von abzufragenAWS CLI, führen Sie den get-usage-totalsBefehl aus und geben Sie optional einen Zeitraum für die Daten an. Beispiel:

```
C:\> aws macie2 get-usage-totals --time-range MONTH_TO_DATE
```

Wo *MONTH_TO_DATE*gibt den aktuellen Kalendermonat bis heute als Zeitbereich für die Daten an.

Wird der Befehl erfolgreich ausgeführt, erhalten Sie eine Ausgabe ähnlich der folgenden:

```
{
    "timeRange": "MONTH_TO_DATE",
    "usageTotals": [
        {
            "currency": "USD",
            "estimatedCost": "153.45",
            "type": "SENSITIVE_DATA_DISCOVERY"
        },
        {
            "currency": "USD",
            "estimatedCost": "65.18",
            "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
        },
        {
            "currency": "USD",
            "estimatedCost": "1.51",
            "type": "DATA_INVENTORY_EVALUATION"
        },
        {
            "currency": "USD",
            "estimatedCost": "0.98",
            "type": "AUTOMATED_OBJECT_MONITORING"
        }
    ]
}
```

Wo `estimatedCost` sind die geschätzten Gesamtnutzungskosten für die zugehörige Nutzungskennzahl (`type`):

- `SENSITIVE_DATA_DISCOVERY`, für die Analyse von S3-Objekten mit Aufträgen zur Erkennung vertraulicher Daten.
- `AUTOMATED_SENSITIVE_DATA_DISCOVERY`, für die Analyse von S3-Objekten mit automatisierter Erkennung vertraulicher Daten.
- `DATA_INVENTORY_EVALUATION`, zur Überwachung und Bewertung von S3-Buckets für Sicherheit und Zugriffskontrolle.
- `AUTOMATED_OBJECT_MONITORING`, um Ihr S3-Bucket-Inventar auszuwerten und zu überwachen, um S3-Objekte zu identifizieren, die für eine Analyse in Frage kommen, durch die automatische Erkennung vertraulicher Daten.

Beispiel 2: Nutzungsstatistiken abfragen

Führen Sie den get-usage-statisticsBefehl ausAWS CLI, um Nutzungsstatistiken mithilfe von abzufragen. Sie können optional einen Zeitraum für die Abfrageergebnisse sortieren, filtern und angeben. Im folgenden Beispiel werden Nutzungsstatistiken für ein Macie-Administratorkonto für die letzten 30 Tage abgerufen. Die Ergebnisse sind in aufsteigender Reihenfolge nach AWS-Konto ID sortiert.

Verwenden Sie für Linux, macOS oder Unix den umgekehrten Schrägstrich (\) zur Zeilenfortsetzung, um die Lesbarkeit zu verbessern:

```
$ aws macie2 get-usage-statistics \
--sort-by '{"key":"accountId","orderBy":"ASC"}' \
--time-range PAST_30_DAYS
```

Verwenden Sie für Microsoft Windows das Caret-Zeichen (^) zur Zeilenfortsetzung, um die Lesbarkeit zu verbessern:

```
C:\> aws macie2 get-usage-statistics ^
--sort-by={\"key\":\"accountId\",\"orderBy\":\"ASC\"} ^
--time-range PAST_30_DAYS
```

Wobei gilt:

- *`accountId`* gibt das Feld an, das zum Sortieren der Ergebnisse verwendet werden soll.

- *ASC* ist die Sortierreihenfolge, die auf die Ergebnisse angewendet wird, basierend auf dem Wert für das angegebene Feld (*accountId*).
- *PAST_30_DAYS*gibt die vorangegangenen 30 Tage als Zeitbereich für die Daten an.

Wird der Befehl erfolgreich ausgeführt, gibt Macie ein `records` Array zurück. Das Array enthält ein Objekt für jedes Konto, das in den Abfrageergebnissen enthalten ist. Beispiel:

```
{
    "records": [
        {
            "accountId": "111122223333",
            "automatedDiscoveryFreeTrialStartDate": "2022-11-28T16:00:00+00:00",
            "freeTrialStartDate": "2020-05-20T12:26:36.917000+00:00",
            "usage": [
                {
                    "currency": "USD",
                    "estimatedCost": "1.51",
                    "type": "DATA_INVENTORY_EVALUATION"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "65.18",
                    "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "153.45",
                    "serviceLimit": {
                        "isServiceLimited": false,
                        "unit": "TERABYTES",
                        "value": 50
                    },
                    "type": "SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "0.98",
                    "type": "AUTOMATED_OBJECT_MONITORING"
                }
            ]
        },
        {
```

```
            "accountId": "444455556666",
            "automatedDiscoveryFreeTrialStartDate": "2022-11-28T16:00:00+00:00",
            "freeTrialStartDate": "2020-05-18T16:26:36.917000+00:00",
            "usage": [
                {
                    "currency": "USD",
                    "estimatedCost": "1.58",
                    "type": "DATA_INVENTORY_EVALUATION"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "63.13",
                    "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "145.12",
                    "serviceLimit": {
                        "isServiceLimited": false,
                        "unit": "TERABYTES",
                        "value": 50
                    },
                    "type": "SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "1.02",
                    "type": "AUTOMATED_OBJECT_MONITORING"
                }
            ]
        }
    ],
    "timeRange": "PAST_30_DAYS"
}
```


Wo `estimatedCost` sind die geschätzten Gesamtnutzungskosten für die zugehörige Nutzungsmetrik (`type`) für ein Konto:

- `DATA_INVENTORY_EVALUATION`, zur Überwachung und Bewertung von S3-Buckets für Sicherheit und Zugriffskontrolle.
- `AUTOMATED_SENSITIVE_DATA_DISCOVERY`, für die Analyse von S3-Objekten mit automatisierter Erkennung vertraulicher Daten.

- `SENSITIVE_DATA_DISCOVERY`, für die Analyse von S3-Objekten mit Aufträgen zur Erkennung vertraulicher Daten.
- `AUTOMATED_OBJECT_MONITORING`, um das S3-Bucket-Inventar des Kontos auszuwerten und zu überwachen, um S3-Objekte zu identifizieren, die für eine Analyse in Frage kommen, durch die automatische Erkennung vertraulicher Daten.

Teilnahme an der kostenlosen Amazon Macie-Testversion

Wenn Sie Amazon Macie zum ersten Mal aktivieren, AWS-Konto wird Ihr Gerät automatisch für die kostenlose 30-Tage-Testversion von Macie registriert. Dies schließt einzelne Mitgliedskonten in einer AWS Organizations Organisation ein.

Während der kostenlosen Testphase fallen keine Gebühren für die Nutzung von Macie für folgende Zwecke AWS-Region an:

- Führen Sie eine präventive Kontrollüberwachung durch — Dazu gehört die Erstellung und Pflege eines Inventars Ihrer Amazon Simple Storage Service (Amazon S3) -Buckets in der Region. Dazu gehören auch die Bewertung und Überwachung der Buckets auf Sicherheits- und Zugriffskontrolle. Weitere Informationen finden Sie unter So überwacht Macie die Amazon S3 S3-Datensicherheit.
- Führen Sie eine automatische Erkennung vertraulicher Daten durch — Dazu gehört die Überwachung und Bewertung Ihres S3-Bucket-Inventars in der Region, um S3-Objekte zu identifizieren, die für eine Analyse in Frage kommen. Dazu gehören auch die Analyse geeigneter Objekte und die Berichterstattung über sensible Daten, Statistiken, Ergebnisse und andere Arten von Ergebnissen. Weitere Informationen finden Sie unter So funktioniert die automatische Erkennung vertraulicher Daten.

  Die automatische Erkennung vertraulicher Daten ist nur für Macie-Administratorkonten und eigenständige Macie-Konten verfügbar. Wenn Sie über ein Macie-Administratorkonto verfügen, können Sie diese Funktion verwenden, um Objekte in S3-Buckets zu analysieren, die Ihren Mitgliedskonten gehören.

Eine Liste der Regionen, in denen Macie derzeit verfügbar ist, finden Sie unter Amazon Macie Macie-Endpoints und Kontingente in der. Allgemeine AWS-Referenz

Die kostenlose Testversion läuft an 30 aufeinanderfolgenden Tagen. Sie können es nicht unterbrechen, nachdem es gestartet ist. Nach Ablauf der kostenlosen Testversion fallen Gebühren für die Durchführung der präventiven Kontrollüberwachung an. Außerdem fallen allmählich Gebühren

für die automatische Erkennung vertraulicher Daten an. Wenn Sie der Macie-Administrator einer Organisation sind, fallen für jedes Konto in Ihrer Organisation Gebühren an. Sie können Macie verwenden, um die Aufschlüsselung der geschätzten Nutzungskosten für einzelne Konten in Ihrer Organisation zu überprüfen.

> **Note**
>
> Die kostenlose Testversion beinhaltet nicht die Analyse von S3-Objekten anhand von Aufträgen zur Erkennung vertraulicher Daten. Wenn Sie während der kostenlosen Testversion Aufträge zur Erkennung vertraulicher Daten erstellen und ausführen, bei denen mehr als 1 GB unkomprimierter Daten analysiert werden, fallen Gebühren an. (Macie bietet ein monatliches kostenloses Kontingent für die Erkennung vertraulicher Daten an. Jeden Monat ist die Analyse von bis zu 1 GB unkomprimierter Daten in S3-Objekten kostenlos. Nach den ersten 1 GB Daten fallen Kosten an.) Möglicherweise fallen auch Gebühren für andere Funktionen anAWS-Services, die Sie mit bestimmten Macie-Funktionen verwenden, z. B. die Verwendung von Customer Managed AWS KMS keys zur Entschlüsselung von S3-Objekten, die Sie auf vertrauliche Daten überprüfen möchten.

Um Ihren Status und die geschätzten Kosten während der kostenlosen Testversion zu überprüfen

Während der kostenlosen Testphase können Sie den Status Ihrer Testversion überprüfen und die geschätzten Nutzungskosten für Ihr Konto überprüfen. Die Kostenschätzungen basieren auf Ihrer bisherigen Verwendung von Macie während der kostenlosen Testversion. Sie können Ihnen helfen, zu verstehen, wie hoch Ihre Nutzungskosten nach Ablauf der Testphase sein könnten. Einzelheiten zur Berechnung dieser Werte durch Macie finden Sie unter. Verstehen, wie die geschätzten Nutzungskosten berechnet werden

Gehen Sie wie folgt vor, um den Status Ihrer Testversion und Ihre geschätzten Nutzungskosten auf der Amazon Macie Macie-Konsole zu überprüfen. Sie können auch programmgesteuert auf diese Daten zugreifen, indem Sie die GetUsageStatisticsAmazon Macie Macie-API verwenden.

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie mit der AWS-Region Auswahl in der oberen rechten Ecke der Seite die -Region aus, in der Sie den Status Ihrer kostenlosen Testversion und Ihre geschätzten Kosten für Nutzung überprüfen möchten.
3. Wählen Sie im Navigationsbereich Verwendung aus.

Auf der Nutzungsseite wird die Anzahl der verbleibenden Tage Ihrer kostenlosen Testversion angezeigt. Es zeigt auch eine Aufschlüsselung Ihrer geschätzten Nutzungskosten in US-Dollar:

- Präventive Kontrollüberwachung — Dies sind die voraussichtlichen Gesamtkosten für die Wartung Ihres S3-Bucket-Inventars und die Bewertung und Überwachung der Buckets im Hinblick auf Sicherheit und Zugriffskontrolle nach Ablauf der kostenlosen Testversion.
- Erkennungsaufträge für sensible Daten — Dies sind die geschätzten Gesamtkosten aller von Ihnen ausgeführten Aufträge zur Erkennung vertraulicher Daten. Aufträge zur Erkennung vertraulicher Daten sind in der kostenlosen Testversion nicht enthalten.
- Automatisierte Erkennung vertraulicher Daten — Dies sind die prognostizierten Gesamtkosten für die automatische Erkennung vertraulicher Daten nach Ablauf der kostenlosen Testversion, aufgeschlüsselt nach Preisdimensionen — Objektüberwachung und Objektanalyse.

Wenn Sie der Macie-Administrator einer Organisation sind, finden Sie auf der Seite Verwendung Details zu den Macie-Konten in Ihrer Organisation:

- In der Tabelle geben die Felder Kostenlose Testversion an, ob ein Konto derzeit an der kostenlosen Testversion für präventive Kontrollüberwachung oder automatische Erkennung vertraulicher Daten teilnimmt. Das Feld Kostenlose Testversion ist leer, wenn die entsprechende kostenlose Testversion für ein Konto abgelaufen ist. Das Feld Summe gibt die geschätzten Gesamtkosten für jedes Konto an.
- Der Abschnitt Geschätzte Kosten für Ihre Organisation insgesamt.

Um die Aufschlüsselung der geschätzten Kosten für ein bestimmtes Konto in Ihrer Organisation zu überprüfen, wählen Sie das Konto in der Tabelle aus. Der Abschnitt Geschätzte Kosten zeigt dann diese Aufschlüsselung. Um diese Daten für ein anderes Konto anzuzeigen, wählen Sie das Konto in der Tabelle aus. Um Ihre Kontoauswahl zu löschen, wählen Sie das X neben der Konto-ID aus.

> **Note**
>
> Wenn ein Konto mehr als 150 TB an Daten in Amazon S3 speichert, können die geschätzten und tatsächlichen Kosten des Kontos für die automatische Erkennung vertraulicher Daten höher sein als die Kostenprognosen, die Macie während der kostenlosen 30-Tage-Testversion angibt. Dies liegt daran, dass die Objektanalyse durch die automatische Erkennung vertraulicher Daten unterbrochen wird, wenn 150 GB unkomprimierter Daten für ein Konto analysiert wurden, das für die kostenlose Testversion registriert ist. Die

Objektanalyse für das Konto wird nach Ablauf der kostenlosen Testversion wieder aufgenommen.

Wenn Sie Unterstützung bei der Kostenprognose für ein Konto benötigen, das mehr als 150 TB an Daten in Amazon S3 speichert, wenden Sie sich anAWS Support. Um die Kosten für die automatische Erkennung vertraulicher Daten nach Ablauf der kostenlosen Testversion zu verwalten, können Sie einzelne S3-Buckets von nachfolgenden Analysen ausschließen. Um Buckets auszuschließen, können Sie die Konfigurationseinstellungen für Ihr Konto aktualisieren. Sie können Buckets auch case-by-case einzeln ausschließen, während Sie die Details der einzelnen Buckets in Ihrem Bucket-Inventar überprüfen.

Verwaltung mehrerer Amazon Macie Macie-Konten

Wenn Ihre AWS Umgebung über mehrere Konten verfügt, können Sie die Amazon Macie Macie-Konten in Ihrer Umgebung verknüpfen und sie als Organisation in Macie zentral verwalten. Mit dieser Konfiguration kann ein designierter Macie-Administrator die allgemeine Sicherheitslage des Amazon Simple Storage Service (Amazon S3) -Datenbestands Ihres Unternehmens beurteilen und überwachen und sensible Daten in den S3-Buckets Ihres Unternehmens erkennen. Der Administrator kann auch verschiedene Kontoverwaltungs- und Verwaltungsaufgaben in großem Maßstab ausführen, z. B. die Überwachung der geschätzten Nutzungskosten und die Bewertung von Kontokontingenten.

In Macie besteht eine Organisation aus einem bestimmten Macie-Administratorkonto und einem oder mehreren zugehörigen Mitgliedskonten. Sie können die Konten auf zwei Arten verknüpfen, indem Sie Macie in Macie integrieren AWS Organizations oder indem Sie Einladungen zur Mitgliedschaft in Macie senden und annehmen. Wir empfehlen Ihnen empfehlen Ihnen empfehlen Ihnen empfehlen Ihnen empfehlen Ihnen empfehlen Ihnen empfehlen Ihnen empfehlen Ihnen empfehlen Ihnen AWS Organizations

AWS Organizationsist ein globaler Account-Management-Service, der es AWS Administratoren ermöglicht, mehrere AWS-Konten Konten zu konsolidieren und zentral zu verwalten. Sie umfasst Kontoverwaltungs- und konsolidierte Fakturierung, die Budget-, Sicherheits- und Compliance-Anforderungen erfüllen. Es wird ohne zusätzliche Kosten angeboten und lässt sich in mehrere integrierenAWS-Services, darunter MacieAWS Security Hub, und AmazonGuardDuty. Weitere Informationen finden Sie im AWS Organizations-Benutzerhandbuch.

Wenn Sie es vorziehen, mehrere Macie-Konten zentral zu verwalten, ohne sie zu verwendenAWS Organizations, können Sie stattdessen Mitgliedschaftseinladungen verwenden. Wenn Sie eine Einladung senden und sie von einem anderen Konto akzeptiert wird, wird Ihr Konto zum Macie-Administratorkonto für das andere Konto. Wenn Sie eine Einladung erhalten und annehmen, wird Ihr Konto zu einem Macie-Mitgliedskonto und das Macie-Administratorkonto kann auf bestimmte Einstellungen, Daten und Ressourcen für Ihr Macie-Konto zugreifen und diese verwalten.

Themen

- Die Beziehung zwischen Amazon Macie-Administrator- und Mitgliedskonten verstehen
- Verwaltung von Amazon Macie-Konten mit AWS Organizations
- Amazon Macie Macie-Konten nach Einladung verwalten

Die Beziehung zwischen Amazon Macie-Administrator- und Mitgliedskonten verstehen

Wenn Sie als Organisation mehrere Amazon Macie Macie-Konten zentral verwalten, hat der Macie-Administrator Zugriff auf Inventardaten, Richtlinienfeststellungen und bestimmte Macie-Einstellungen und Ressourcen für zugehörige Mitgliedskonten von Amazon Simple Storage Service (Amazon S3). Der Administrator kann auch eine automatische Erkennung sensibler Daten durchführen und Aufgaben zur Erkennung sensibler Daten ausführen, um sensible Daten in S3-Buckets zu erkennen, die Mitgliedskonten gehören. Die Support bestimmter Aufgaben hängt davon ab, ob ein Macie-Administratorkonto über AWS Organizations oder auf Einladung mit einem Mitgliedskonto verknüpft ist.

Die folgende Tabelle enthält Einzelheiten zur Beziehung zwischen Macie-Administrator- und Mitgliedskonten. Sie gibt die Standardberechtigungen für jeden Kontotyp an. Um den Zugriff auf Macie-Funktionen und -Operationen weiter einzuschränken, können Sie benutzerdefinierte Richtlinien AWS Identity and Access Management(IAM) verwenden.

In der Tabelle:

- Self gibt an, dass das Konto die Aufgabe für keine verknüpften Konten ausführen kann.
- Any bedeutet, dass das Konto die Aufgabe für ein einzelnes zugeordnetes Konto ausführen kann.
- All bedeutet, dass das Konto die Aufgabe ausführen kann und dass die Aufgabe für alle zugehörigen Konten gilt.

Ein Bindestrich (—) bedeutet, dass das Konto die Aufgabe nicht ausführen kann.

Aufgabe	Durch AWS Organizations		Auf Einladung	
	Administrator	Mitglied	Administrator	Mitglied
Enable Macie	Any	–	Self	Self
Review the organization's account inventory [1]	All	–	All	–

Add a member account	Any	–	Any	–
Review statistics and metadata for S3 buckets	All	Self	All	Self
Review policy findings	All	Self	All	Self
Suppress (archive) policy findings [2]	All	–	All	–
Publish policy findings [3]	Self	Self	Self	Self
Configure a repository for sensitive data discovery results	Self	Self	Self	Self
Create and use allow lists	Self	Self	Self	Self
Create and use custom data identifiers	Self	Self	Self	Self
Configure and perform automated sensitive data discovery	All	–	All	–

Review automated sensitive data discovery statistics, data, and results	All	–	All	–
Create and run sensitive data discovery jobs [4]	Any	Self	Any	Self
Review the details of sensitive data discovery jobs [5]	Self	Self	Self	Self
Review sensitive data findings [6]	Self	Self	Self	Self
Suppress (archive) sensitive data findings [6]	Self	Self	Self	Self
Publish sensitive data findings [6]	Self	Self	Self	Self
Configure Macie to retrieve sensitive data samples for findings	Self	Self	Self	Self
Retrieve sensitive data samples for findings [7]	Self	Self	Self	Self

Configure publication destinations for findings	Self	Self	Self	Self
Set the publication frequency for findings	All	Self	All	Self
Create sample findings	Self	Self	Self	Self
Review account quotas and estimated usage costs	All	Self	All	Self
Suspend Macie [8]	Any	–	Any	Self
Disable Macie [9]	Self	Self	Self	Self
Remove (disassociate) a member account	Any	–	Any	–
Disassociate from an administrator account	–	–	–	Self
Delete an association with another account [10]	Any	–	Any	Self

1. Der Administrator einer Organisation in AWS Organizations kann alle Konten in der Organisation überprüfen, auch Konten, für die Macie nicht aktiviert wurde. Der Administrator einer Organisation, die auf Einladung basiert, kann nur die Konten überprüfen, die er seinem Inventar hinzugefügt hat.

2. Nur ein Administrator kann Richtlinienfeststellungen unterdrücken. Wenn ein Administrator eine Unterdrückungsregel erstellt, wendet Macie die Regel auf die Richtlinienergebnisse für alle Konten in der Organisation an, sofern die Regel nicht so konfiguriert ist, dass bestimmte Konten ausgeschlossen werden. Wenn ein Mitglied eine Unterdrückungsregel erstellt, wendet Macie die Regel nicht auf die Richtlinienfeststellungen für das Konto des Mitglieds an.
3. Nur das Konto, dem eine betroffene Ressource gehört, kann Richtlinienergebnisse für die Ressource veröffentlichen. AWS Security Hub Sowohl Administrator- als auch Mitgliedskonten veröffentlichen automatisch Richtlinienergebnisse für eine betroffene Ressource auf Amazon EventBridge.
4. Ein Mitglied kann einen Job so konfigurieren, dass nur Objekte in S3-Buckets analysiert werden, die seinem Konto gehören. Ein Administrator kann einen Job zur Analyse von Objekten in Buckets konfigurieren, die seinem Konto oder einem Mitgliedskonto gehören. Informationen zur Anwendung von Kontingenten und zur Berechnung der Kosten für Jobs mit mehreren Konten finden Sie unter. Verstehen, wie die geschätzten Nutzungskosten berechnet werden
5. Nur das Konto, das einen Job erstellt, kann auf die Details des Jobs zugreifen. Dazu gehören auftragsbezogene Details im S3-Bucket-Inventar.
6. Nur das Konto, das einen Job erstellt, kann auf die Ergebnisse sensibler Daten, die der Job generiert, zugreifen, diese unterdrücken oder veröffentlichen. Nur ein Administrator kann auf die Ergebnisse sensibler Daten zugreifen, diese unterdrücken oder veröffentlichen, die durch die automatische Erkennung sensibler Daten gewonnen werden.
7. Wenn ein Ergebnis vertraulicher Daten auf ein S3-Objekt zutrifft, das einem Mitgliedskonto gehört, kann der Administrator möglicherweise Stichproben sensibler Daten abrufen, die im Rahmen des Ergebnisses gemeldet wurden. Dies hängt von der Quelle des Ergebnisses sowie von den Konfigurationseinstellungen und Ressourcen im Administratorkonto und im Mitgliedskonto ab. Weitere Informationen finden Sie unter Konfigurationsoptionen und Anforderungen für das Abrufen vertraulicher Datenproben.
8. Damit ein Administrator Macie für sein eigenes Konto sperren kann, muss er zunächst sein Konto von allen Mitgliedskonten trennen.
9. Damit ein Administrator Macie für sein eigenes Konto deaktivieren kann, muss er zunächst sein Konto von allen Mitgliedskonten trennen und die Verknüpfungen zwischen seinem Konto und all

diesen Konten löschen. Der Administrator einer Organisation in AWS Organizations kann dies tun, indem er mit dem Verwaltungskonto der Organisation ein anderes Konto als Administratorkonto festlegt.

Damit ein Mitglied einer AWS Organizations Organisation Macie deaktivieren kann, muss der Administrator zuerst das Konto des Mitglieds von seinem Administratorkonto trennen. In einer Organisation, die auf Einladung basiert, kann das Mitglied sein Konto von seinem Administratorkonto trennen und dann Macie deaktivieren.

10. Der Administrator einer Organisation in AWS Organizations kann eine Verknüpfung mit einem Mitgliedskonto löschen, nachdem er das Konto von seinem Administratorkonto getrennt hat. Das Konto wird weiterhin im Kontoinventar des Administrators angezeigt, sein Status gibt jedoch an, dass es sich nicht um ein Mitgliedskonto handelt. In einer Organisation, die auf Einladung basiert, können ein Administrator und ein Mitglied eine Verknüpfung mit einem anderen Konto löschen, nachdem sie ihr Konto von dem anderen Konto getrennt haben. Das andere Konto wird dann nicht mehr in seinem Kontoinventar angezeigt.

Verwaltung von Amazon Macie-Konten mit AWS Organizations

Wenn Sie AWS Organizations früher mehrere Konten zentral verwaltenAWS-Konten, können Sie Amazon Macie in Macie integrieren AWS Organizations und Macie dann zentral für Konten in Ihrem Unternehmen verwalten. Mit dieser Konfiguration kann ein designierter Macie-Administrator Macie für bis zu 10.000 Konten aktivieren und verwalten. Der Administrator kann auch auf die Inventardaten von Amazon Simple Storage Service (Amazon S3) zugreifen und sensible Daten in S3-Buckets entdecken, die den Konten gehören. Einzelheiten zu Aufgaben, die der Administrator ausführen kann, finden Sie unterDie Beziehung zwischen Amazon Macie-Administrator- und Mitgliedskonten verstehen.

Um Macie in zu integrierenAWS Organizations, legen Sie zunächst ein Konto als delegiertes Macie-Administratorkonto für die Organisation fest. Der Macie-Administrator aktiviert Macie dann für andere Konten in der Organisation, fügt diese Konten als Macie-Mitgliedskonten hinzu und konfiguriert Macie-Einstellungen und Ressourcen für die Konten.

> **Tip**
>
> Wenn Sie mithilfe von Einladungen bereits ein Macie-Administratorkonto mit Mitgliedskonten verknüpft haben, können Sie dieses Konto als delegiertes Macie-Administratorkonto für Ihre Organisation in festlegen. AWS Organizations Wenn Sie dies tun, bleiben alle aktuell

verknüpften Mitgliedskonten Mitglieder und Sie können die Vorteile der Kontoverwaltung in vollem Umfang nutzen, indem Sie AWS Organizations Weitere Informationen finden Sie unter Umstellung von einer Organisation, die auf Einladungen basiert.

In den Themen in diesem Abschnitt wird erläutert, wie Macie in Konten in einer Organisation integriert wird AWS Organizations und wie Macie für Konten in einer Organisation verwaltet und verwaltet wird.

Themen

- Überlegungen und Empfehlungen zur Verwendung von Amazon Macie mit AWS Organizations
- Integration und Konfiguration einer Organisation in Amazon Macie
- Amazon Macie Macie-Konten für eine Organisation überprüfen
- Amazon Macie Macie-Mitgliedskonten für eine Organisation verwalten
- Ein anderes Amazon Macie-Administratorkonto für eine Organisation festlegen
- Deaktivierung der Amazon Macie Macie-Integration mit AWS Organizations

Überlegungen und Empfehlungen zur Verwendung von Amazon Macie mit AWS Organizations

Bevor Sie Amazon Macie in Macie integrieren AWS Organizations und Ihre Organisation in Macie konfigurieren, sollten Sie die folgenden Anforderungen und Empfehlungen berücksichtigen. Stellen Sie außerdem sicher, dass Sie die Beziehung zwischen Macie-Administrator- und Mitgliedskonten verstehen.

Themen

- Benennen eines Macie-Administratorkontos
- Änderung oder Entfernung der Bezeichnung eines Macie-Administratorkontos
- Macie-Mitgliedskonten hinzufügen und entfernen
- Umstellung von einer Organisation, die auf Einladungen basiert

Benennen eines Macie-Administratorkontos

Beachten Sie bei der Entscheidung, welches Konto das delegierte Macie-Administratorkonto für Ihre Organisation sein soll, Folgendes:

- Eine Organisation kann nur über ein delegiertes Macie-Administratorkonto verfügen.
- Ein Konto kann nicht gleichzeitig Macie-Administrator und Mitgliedskonto sein.
- Nur das AWS Organizations Verwaltungskonto für eine Organisation kann das delegierte Macie-Administratorkonto für die Organisation festlegen, und nur das Verwaltungskonto kann diese Bezeichnung anschließend ändern oder entfernen.
- Das AWS Organizations Verwaltungskonto für eine Organisation kann auch das delegierte Macie-Administratorkonto für die Organisation sein. Wir empfehlen jedoch nicht, diese Konfiguration auf der Grundlage bewährter AWS Sicherheitsverfahren und des Prinzips der geringsten Rechte zu verwenden. Benutzer, die zu Abrechnungszwecken Zugriff auf das Verwaltungskonto haben, unterscheiden sich wahrscheinlich von Benutzern, die aus Gründen der Informationssicherheit Zugriff auf Macie benötigen.

  Wenn Sie diese Konfiguration bevorzugen, müssen Sie Macie für das Verwaltungskonto der Organisation in mindestens einem aktivieren, AWS-Region bevor Sie das Konto als delegiertes Macie-Administratorkonto festlegen. Andernfalls kann das Konto nicht auf Macie-Einstellungen und Ressourcen für Mitgliedskonten zugreifen und diese verwalten.
- Im AWS Organizations Gegensatz dazu ist Macie ein regionaler Dienst. Dies bedeutet, dass die Bezeichnung eines Macie-Administratorkontos eine regionale Bezeichnung ist. Dies bedeutet auch, dass die Verknüpfungen zwischen Macie-Administrator- und Mitgliedskonten regional sind. Wenn das Verwaltungskonto beispielsweise ein Macie-Administratorkonto in der Region USA Ost (Nord-Virginia) festlegt, kann der Macie-Administrator Macie nur für Mitgliedskonten in dieser Region verwalten.

  Um Macie-Konten in mehreren Regionen zentral zu verwalten AWS-Regionen, muss sich das Verwaltungskonto in jeder Region anmelden, in der die Organisation Macie derzeit verwendet oder verwenden wird, und dann das Macie-Administratorkonto für jede dieser Regionen festlegen. Der Macie-Administrator kann dann die Organisation in jeder dieser Regionen konfigurieren. Eine Liste der Regionen, in denen Macie derzeit verfügbar ist, finden Sie unter Amazon Macie Macie-Endpunkte und Kontingente in der. Allgemeine AWS-Referenz
- Ein Konto kann jeweils nur einem Macie-Administratorkonto zugeordnet werden. Wenn Ihre Organisation Macie in mehreren Regionen verwendet, muss das angegebene Macie-Administratorkonto in all diesen Regionen identisch sein. Das Verwaltungskonto Ihrer Organisation muss das Administratorkonto jedoch in jeder Region separat angeben.
- Ein Konto kann das delegierte Macie-Administratorkonto für jeweils nur eine Organisation sein. Wenn Sie mehrere Organisationen in verwalten AWS Organizations, müssen Sie für jede Organisation ein anderes Macie-Administratorkonto einrichten. Dies ist auf eine AWS

Organizations Anforderung zurückzuführen: Ein Konto kann jeweils nur Mitglied einer Organisation sein.

- Wenn das Konto des Macie-Administrators gesperrt, isoliert oder geschlossen AWS-Konto wird, werden alle zugehörigen Macie-Mitgliedskonten automatisch als Macie-Mitgliedskonten entfernt, aber Macie wird für diese Konten nicht deaktiviert.

Änderung oder Entfernung der Bezeichnung eines Macie-Administratorkontos

Nur das AWS Organizations Verwaltungskonto für eine Organisation kann die Bezeichnung eines delegierten Macie-Administratorkontos für die Organisation ändern oder entfernen.

Wenn das Verwaltungskonto die Bezeichnung aufhebt, werden alle zugehörigen Mitgliedskonten als Macie-Mitgliedskonten entfernt, Macie wird jedoch nicht für die Konten deaktiviert. Damit ein Konto auch die Nutzung von Macie pausieren oder beenden kann, muss ein Nutzer des Accounts Macie für das Konto sperren (pausieren) oder deaktivieren (beenden).

Macie-Mitgliedskonten hinzufügen und entfernen

Beachten Sie beim Hinzufügen, Entfernen und anderweitigen Verwalten von Mitgliedskonten für Ihre Organisation Folgendes:

- Ein Macie-Administratorkonto kann jeweils nicht mehr als 10.000 aktiven (aktivierten) Macie-Mitgliedskonten zugeordnet werden. AWS-Region Wenn Ihre Organisation dieses Kontingent überschreitet, kann der Macie-Administrator erst dann Mitgliedskonten hinzufügen, wenn er die erforderliche Anzahl vorhandener Mitgliedskonten in der Region entfernt hat.

  Wenn eine Organisation dieses Kontingent erreicht, benachrichtigen wir den Macie-Administrator, indem wir CloudWatch Amazon-Events für ihr Konto erstellen AWS Health . Wir senden auch E-Mails an die Adresse, die mit ihrem Konto verknüpft ist.

  Wenn Sie der Macie-Administrator einer Organisation sind, können Sie mithilfe der Kontoseite in der Amazon Macie-Konsole oder mithilfe der Amazon Macie Macie-API feststellen, wie viele aktive Mitgliedskonten derzeit mit Ihrem Konto verknüpft sind. DescribeOrganizationConfiguration Weitere Informationen finden Sie unter Amazon Macie Macie-Konten für eine Organisation überprüfen.
- Ein Konto kann jeweils nur einem Macie-Administratorkonto zugeordnet werden. Das bedeutet, dass ein Konto keine Macie-Einladung von einem anderen Konto annehmen kann, wenn es bereits mit dem Macie-Administratorkonto für eine Organisation in verknüpft ist. AWS Organizations

Ebenso AWS Organizations kann der Macie-Administrator einer Organisation das Konto nicht als Macie-Mitgliedskonto hinzufügen, wenn ein Konto bereits eine Einladung angenommen hat. Das Konto muss zuerst von seinem aktuellen Administratorkonto getrennt werden, das auf Einladung basiert.

- Um das AWS Organizations Verwaltungskonto als Macie-Mitgliedskonto hinzuzufügen, muss ein Benutzer des Verwaltungskontos zuerst Macie für das Konto aktivieren. Der Macie-Administrator darf Macie nicht für das Verwaltungskonto aktivieren.
- Ein Mitgliedskonto kann nicht von seinem Macie-Administratorkonto getrennt werden. Nur der Macie-Administrator kann ein Konto als Macie-Mitgliedskonto entfernen.
- Wenn der Macie-Administrator ein Macie-Mitgliedskonto entfernt, ist Macie weiterhin für das Konto aktiviert. Um Macie auch pausieren oder beenden zu können, muss ein Benutzer des Accounts Macie für das Konto sperren (pausieren) oder deaktivieren (beenden).

Umstellung von einer Organisation, die auf Einladungen basiert

Wenn Sie mithilfe von Macie-Mitgliedschaftseinladungen bereits ein Macie-Administratorkonto mit Mitgliedskonten verknüpft haben, empfehlen wir Ihnen, dieses Konto als delegiertes Macie-Administratorkonto für Ihre Organisation in festzulegen. AWS Organizations Dies vereinfacht den Übergang von einer Organisation, die auf Einladungen basiert.

Wenn Sie dies tun, bleiben alle derzeit verknüpften Mitgliedskonten weiterhin Mitglieder. Wenn ein Mitgliedskonto Teil Ihrer Organisation ist AWS Organizations, ändert sich die Zuordnung des Kontos automatisch von Auf Einladung zu Via AWS Organizations in Macie. Wenn ein Mitgliedskonto nicht Teil Ihrer Organisation ist AWS Organizations, gilt die Zuordnung des Kontos weiterhin als Auf Einladung. In beiden Fällen werden die Konten weiterhin dem delegierten Macie-Administratorkonto als Mitgliedskonten zugeordnet.

Wir empfehlen diesen Ansatz, da ein Konto nicht mit mehr als einem Macie-Administratorkonto gleichzeitig verknüpft werden kann. Wenn Sie in ein anderes Konto als Macie-Administratorkonto für Ihre Organisation festlegen AWS Organizations, kann der angegebene Administrator Konten, die bereits mit einem anderen Macie-Administratorkonto verknüpft sind, nicht per Einladung verwalten. Jedes Mitgliedskonto muss zunächst von seinem aktuellen Administratorkonto getrennt werden, das auf Einladung basiert. Der Macie-Administrator für Ihre Organisation in AWS Organizations kann das Konto dann als Macie-Mitgliedskonto hinzufügen und mit der Verwaltung des Kontos beginnen.

Nachdem Sie Macie in Macie integriert AWS Organizations und Ihre Organisation dort konfiguriert haben, können Sie optional ein anderes Macie-Administratorkonto für die Organisation festlegen. Sie

können auch weiterhin Einladungen verwenden, um Mitgliedskonten zuzuordnen und zu verwalten, die nicht Teil Ihrer Organisation sind. AWS Organizations

Integration und Konfiguration einer Organisation in Amazon Macie

Um mit der Nutzung von Amazon Macie zu beginnenAWS Organizations, legt das AWS Organizations Verwaltungskonto für die Organisation ein Konto als delegiertes Macie-Administratorkonto für die Organisation fest. Dadurch wird Macie als vertrauenswürdiger Service in aktiviert. AWS Organizations Es aktiviert Macie auch im aktuellen Konto AWS-Region für das angegebene Administratorkonto, und es ermöglicht dem designierten Administratorkonto, Macie für andere Konten in der Organisation in dieser Region zu aktivieren und zu verwalten. Informationen dazu, wie diese Berechtigungen gewährt werden, finden Sie AWS-Services im AWS OrganizationsBenutzerhandbuch unter Zusammen AWS Organizations mit anderen verwenden.

Der delegierte Macie-Administrator konfiguriert dann die Organisation in Macie, hauptsächlich indem er die Konten der Organisation als Macie-Mitgliedskonten in der Region hinzufügt. Der Administrator kann dann auf bestimmte Macie-Einstellungen, Daten und Ressourcen für diese Konten in dieser Region zugreifen.

In diesem Thema wird erklärt, wie Sie einen delegierten Macie-Administrator für eine Organisation bestimmen und die Konten der Organisation als Macie-Mitgliedskonten hinzufügen. Bevor Sie diese Aufgaben ausführen, sollten Sie sicherstellen, dass Sie die Beziehung zwischen Administrator - und Mitgliedskonten verstehen. Es ist auch eine gute Idee, die Überlegungen und Empfehlungen zur Verwendung von Macie mit AWS Organizations zu lesen.

Aufgaben

- Schritt 1: Überprüfen Sie Ihre Berechtigungen
- Schritt 2: Bestimmen Sie das delegierte Macie-Administratorkonto für die Organisation
- Schritt 3: Automatisches Aktivieren und Hinzufügen neuer Organisationskonten als Macie-Mitgliedskonten
- Schritt 4: Aktivieren und fügen Sie bestehende Organisationskonten als Macie-Mitgliedskonten hinzu

Um die Organisation in mehreren Regionen zu integrieren und zu konfigurieren, wiederholen das AWS Organizations Verwaltungskonto und der delegierte Macie-Administrator diese Schritte in jeder weiteren Region.

Schritt 1: Überprüfen Sie Ihre Berechtigungen

Bevor Sie das delegierte Macie-Administratorkonto für Ihre Organisation festlegen, stellen Sie sicher, dass Sie (als Benutzer des AWS Organizations Verwaltungskontos) die folgende Macie-Aktion ausführen dürfen:. `macie2:EnableOrganizationAdminAccount` Mit dieser Aktion können Sie mithilfe von Macie das delegierte Macie-Administratorkonto für Ihre Organisation festlegen.

Stellen Sie außerdem sicher, dass Sie die folgenden Aktionen ausführen dürfen: AWS Organizations

- `organizations:DescribeOrganization`
- `organizations:EnableAWSServiceAccess`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:RegisterDelegatedAdministrator`

Mit diesen Aktionen können Sie: Informationen über Ihre Organisation abrufen, Macie in Ihr Unternehmen integrierenAWS Organizations, Informationen darüber abrufen, in welche AWS-Services Sie sich integriert habenAWS Organizations, und ein delegiertes Macie-Administratorkonto für Ihre Organisation festlegen.

Um diese Berechtigungen zu gewähren, fügen Sie die folgende Erklärung in eine AWS Identity and Access Management (IAM-) Richtlinie für Ihr Konto ein:

```
{
   "Sid": "Grant permissions to designate a delegated Macie administrator",
   "Effect": "Allow",
   "Action": [
      "macie2:EnableOrganizationAdminAccount",
      "organizations:DescribeOrganization",
      "organizations:EnableAWSServiceAccess",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:RegisterDelegatedAdministrator"
   ],
   "Resource": "*"
}
```

Wenn Sie Ihr AWS Organizations Verwaltungskonto als delegiertes Macie-Administratorkonto für die Organisation festlegen möchten, benötigt Ihr Konto außerdem die Erlaubnis, die folgende IAM-Aktion auszuführen:. `CreateServiceLinkedRole` Mit dieser Aktion können Sie Macie für das

Verwaltungskonto aktivieren. Aufgrund bewährter AWS Sicherheitsmethoden und des Prinzips der geringsten Rechte empfehlen wir Ihnen jedoch, dies nicht zu tun.

Wenn Sie sich entscheiden, diese Berechtigung zu erteilen, fügen Sie der IAM-Richtlinie für Ihr AWS Organizations Verwaltungskonto die folgende Erklärung hinzu:

```
{
   "Sid": "Grant permissions to enable Macie",
   "Effect": "Allow",
   "Action": [
      "iam:CreateServiceLinkedRole"
   ],
   "Resource": "arn:aws:iam::111122223333:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie",
   "Condition": {
      "StringLike": {
         "iam:AWSServiceName": "macie.amazonaws.com"
      }
   }
}
```

Ersetzen Sie in der Erklärung *111122223333* durch die Konto-ID für das Verwaltungskonto.

Wenn Sie Macie in einem Opt-In verwalten möchten AWS-Region (Region, die standardmäßig deaktiviert ist), aktualisieren Sie auch den Wert für den Macie-Dienstprinzipal im Element und in der Bedingung. `Resource` `iam:AWSServiceName` Der Wert muss den Regionalcode für die Region angeben. Gehen Sie beispielsweise wie folgt vor, um Macie in der Region Naher Osten (Bahrain) mit dem Regionalcode me-south-1 zu verwalten:

- Ersetzen Sie im Element `Resource`

  `arn:aws:iam::111122223333:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`

  mit

  `arn:aws:iam::111122223333:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie`

  Wobei *111122223333* die Konto-ID für das Verwaltungskonto und *me-south-1* den Regionalcode für die Region angibt.

- Ersetzen Sie die `iam:AWSServiceName` Bedingung durch`macie.me-south-1.amazonaws.com`, `macie.amazonaws.com` wobei *`me-south-1`* den Regionalcode für die Region angibt.

Eine Liste der Regionen, in denen Macie derzeit verfügbar ist, sowie den Regionalcode für jede Region finden Sie unter Amazon Macie Macie-Endpunkte und Kontingente in der. Allgemeine AWS-Referenz Informationen zu Regionen, für die Sie sich anmelden können, finden Sie im Referenzhandbuch unter Spezifizieren, welche Regionen AWS-Regionen Ihr Konto verwenden kann. AWS Account Management

Schritt 2: Bestimmen Sie das delegierte Macie-Administratorkonto für die Organisation

Nachdem Sie Ihre Berechtigungen überprüft haben, können Sie (als Benutzer des AWS Organizations Verwaltungskontos) das delegierte Macie-Administratorkonto für Ihre Organisation festlegen.

Um das delegierte Macie-Administratorkonto für eine Organisation festzulegen

Um das delegierte Macie-Administratorkonto für Ihre Organisation festzulegen, können Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden. Nur ein Benutzer des AWS Organizations Verwaltungskontos kann diese Aufgabe ausführen.

Console

Gehen Sie wie folgt vor, um das delegierte Macie-Administratorkonto mithilfe der Amazon Macie Macie-Konsole festzulegen.

Um das delegierte Macie-Administratorkonto zu bestimmen

1. Melden Sie sich AWS Management Console mit Ihrem AWS Organizations Verwaltungskonto bei an.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie das delegierte Macie-Administratorkonto für Ihre Organisation festlegen möchten.
3. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
4. Führen Sie je nachdem, ob Macie für Ihr Verwaltungskonto in der aktuellen Region aktiviert ist, einen der folgenden Schritte aus:

- Wenn Macie nicht aktiviert ist, wählen Sie auf der Willkommensseite die Option Erste Schritte aus.
- Wenn Macie aktiviert ist, wählen Sie im Navigationsbereich Einstellungen aus.

5. Geben Sie unter Delegierter Administrator die 12-stellige Konto-ID für das Konto einAWS-Konto, das Sie als Macie-Administratorkonto festlegen möchten.
6. Wählen Sie Delegate (Delegieren).

Wiederholen Sie die vorherigen Schritte in jeder weiteren Region, in der Sie Ihre Organisation in Macie integrieren möchten. Sie müssen in jeder dieser Regionen dasselbe Macie-Administratorkonto angeben.

API

Verwenden Sie den EnableOrganizationAdminAccountBetrieb der Amazon Macie-API, um das delegierte Macie-Administratorkonto programmgesteuert zuzuweisen. Um das Konto in mehreren Regionen zuzuweisen, reichen Sie die Bezeichnung für jede Region ein, in der Sie Ihre Organisation mit Macie integrieren möchten. Sie müssen in jeder dieser Regionen dasselbe Macie-Administratorkonto angeben.

Wenn Sie die Bezeichnung einreichen, verwenden Sie den erforderlichen `adminAccountId` Parameter, um die 12-stellige Konto-ID anzugeben, die als Macie-Administratorkonto für die Organisation bestimmt werden AWS-Konto soll. Stellen Sie außerdem sicher, dass Sie die Region angeben, für die die Benennung gilt.

Führen Sie den Befehl aus, um das Macie-Administratorkonto mithilfe von AWS Command Line Interface(AWS CLI) festzulegen. enable-organization-admin-account Geben Sie für den `admin-account-id` Parameter die 12-stellige Konto-ID an, die AWS-Konto Sie angeben möchten. Verwenden Sie den `region` Parameter, um die Region anzugeben, für die die Bezeichnung gilt. Beispiel:

```
C:\> aws macie2 enable-organization-admin-account --region us-east-1 --admin-account-id 111122223333
```

Dabei ist *`us-east-1`* die Region, für die die Bezeichnung gilt (die Region USA Ost (Nord-Virginia)), und *`111122223333`* die Konto-ID für das auszuweisende Konto ist.

Nachdem Sie das Macie-Administratorkonto für Ihre Organisation festgelegt haben, kann der Macie-Administrator mit der Konfiguration der Organisation in Macie beginnen.

Schritt 3: Automatisches Aktivieren und Hinzufügen neuer Organisationskonten als Macie-Mitgliedskonten

Standardmäßig ist Macie nicht automatisch für neue Konten aktiviert, wenn die Konten zu Ihrer Organisation in AWS Organizations hinzugefügt werden. Darüber hinaus werden die Konten nicht automatisch als Macie-Mitgliedskonten hinzugefügt. Die Konten werden im Kontoinventar des Macie-Administrators angezeigt. Macie ist jedoch nicht unbedingt für die Konten aktiviert, und der Macie-Administrator kann nicht unbedingt auf die Macie-Einstellungen, Daten und Ressourcen für die Konten zugreifen.

Wenn Sie der delegierte Macie-Administrator für die Organisation sind, können Sie diese Konfigurationseinstellung für Ihre Organisation ändern. Wenn Sie die Einstellung Automatisch aktivieren aktivieren aktivieren, wird Macie automatisch für neue Konten aktiviert, wenn die Konten zu Ihrer Organisation in hinzugefügt werdenAWS Organizations, und die Konten werden Ihrem Macie-Administratorkonto automatisch als Mitgliedskonten zugeordnet. Die Aktivierung dieser Einstellung hat keine Auswirkungen auf bestehende Konten in Ihrer Organisation. Um Macie für bestehende Konten zu aktivieren und zu verwalten, müssen Sie die Konten manuell als Macie-Mitgliedskonten hinzufügen. Im nächsten Schritt wird erklärt, wie das geht.

> **Note**
>
> Beachten Sie die folgenden Ausnahmen, wenn Sie die Einstellung Automatisch aktivieren aktivieren:
>
> - Wenn ein neues Konto bereits mit einem anderen Macie-Administratorkonto verknüpft ist, fügt Macie das Konto nicht automatisch als Mitgliedskonto in Ihrer Organisation hinzu.
>
> Das Konto muss von seinem aktuellen Macie-Administratorkonto getrennt werden, bevor es Teil Ihrer Organisation in Macie werden kann. Sie können das Konto dann manuell hinzufügen. Um Konten zu identifizieren, bei denen dies der Fall ist, können Sie den Kontobestand für Ihre Organisation überprüfen.
> - Wenn Ihre Organisation das Kontingent von 10.000 Macie-Mitgliedskonten in einem erreichtAWS-Region, deaktiviert Macie diese Einstellung automatisch in der Region.
>
> In diesem Fall benachrichtigen wir Sie, indem AWS Health wir CloudWatch Amazon-Ereignisse für Ihr Macie-Administratorkonto erstellen. Wir senden auch E-Mails an

die Adresse, die mit diesem Konto verknüpft ist. Wenn die Gesamtzahl der Konten anschließend auf weniger als 10.000 Konten sinkt, aktiviert Macie die Einstellung automatisch wieder.

Um automatisch neue Organisationskonten als Macie-Mitgliedskonten zu aktivieren und hinzuzufügen

Um automatisch neue Konten als Macie-Mitgliedskonten zu aktivieren und hinzuzufügen, können Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden. Nur der delegierte Macie-Administrator für die Organisation kann diese Aufgabe ausführen.

Console

Um diese Aufgabe mithilfe der Konsole ausführen zu können, müssen Sie berechtigt sein, die folgende AWS Organizations Aktion auszuführen:. `organizations:ListAccounts` Mit dieser Aktion können Sie Informationen zu den Konten in Ihrer Organisation abrufen und anzeigen. Wenn Sie über diese Berechtigungen verfügen, gehen Sie wie folgt vor, um automatisch neue Organisationskonten als Macie-Mitgliedskonten zu aktivieren und hinzuzufügen.

Um automatisch neue Organisationskonten zu aktivieren und hinzuzufügen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie automatisch neue Konten als Macie-Mitgliedskonten aktivieren und hinzufügen möchten.
3. Klicken Sie im Navigationsbereich unter Settings auf Accounts.
4. Aktivieren Sie auf der Seite Konten neben Konten hinzufügen die Einstellung Automatisch aktivieren.

Wiederholen Sie die vorherigen Schritte in jeder weiteren Region, in der Sie Ihre Organisation in Macie konfigurieren möchten.

Um diese Einstellung später zu ändern und das automatische Aktivieren und Hinzufügen neuer Konten zu beenden, wiederholen Sie die vorherigen Schritte und deaktivieren Sie die Einstellung Automatisch aktivieren.

API

Verwenden Sie die Amazon Macie-API, um automatisch programmgesteuert neue Macie-Mitgliedskonten zu aktivieren und hinzuzufügen. UpdateOrganizationConfiguration Wenn Sie Ihre Anfrage einreichen, setzen Sie den Wert für den Parameter auf. `autoEnable` `true` (Der Standardwert ist `false`.) Stellen Sie außerdem sicher, dass Sie die Region angeben, für die sich Ihre Anfrage bezieht. Um automatisch neue Konten in weiteren Regionen zu aktivieren und hinzuzufügen, reichen Sie die Anfrage für jede weitere Region ein.

Wenn Sie AWS CLI zum Senden der Anfrage verwenden, führen Sie den update-organization-configurationBefehl aus und geben Sie den `auto-enable` Parameter an, um neue Konten automatisch zu aktivieren und hinzuzufügen. Beispiel:

```
$ aws macie2 update-organization-configuration --region us-east-1 --auto-enable
```

Dabei ist *`us-east-1`* die Region, in der neue Konten automatisch aktiviert und hinzugefügt werden, die Region USA Ost (Nord-Virginia).

Um diese Einstellung später zu ändern und das automatische Aktivieren und Hinzufügen neuer Konten zu beenden, führen Sie denselben Befehl erneut aus und verwenden Sie den `no-auto-enable` Parameter anstelle des `auto-enable` Parameters in jeder zutreffenden Region.

Schritt 4: Aktivieren und fügen Sie bestehende Organisationskonten als Macie-Mitgliedskonten hinzu

Wenn Sie Macie mit integrierenAWS Organizations, wird Macie nicht automatisch für alle vorhandenen Konten in Ihrer Organisation aktiviert. Darüber hinaus werden die Konten nicht automatisch als Macie-Mitgliedskonten mit dem delegierten Macie-Administratorkonto verknüpft.

Daher besteht der letzte Schritt bei der Integration und Konfiguration Ihrer Organisation in Macie darin, bestehende Organisationskonten als Macie-Mitgliedskonten hinzuzufügen. Wenn Sie ein vorhandenes Konto als Macie-Mitgliedskonto hinzufügen, wird Macie automatisch für das Konto aktiviert und Sie (als delegierter Macie-Administrator) erhalten Zugriff auf bestimmte Macie-Einstellungen, Daten und Ressourcen für das Konto.

Beachten Sie, dass Sie kein Konto hinzufügen können, das derzeit mit einem anderen Macie-Administratorkonto verknüpft ist. Um das Konto hinzuzufügen, arbeiten Sie mit dem Kontoinhaber zusammen, um das Konto zunächst von seinem aktuellen Administratorkonto zu trennen. Außerdem können Sie kein vorhandenes Konto hinzufügen, wenn Macie derzeit für das Konto gesperrt ist.

Der Kontoinhaber muss Macie zunächst für das Konto erneut aktivieren. Wenn Sie das AWS Organizations Verwaltungskonto als Mitgliedskonto hinzufügen möchten, muss ein Benutzer dieses Kontos schließlich zuerst Macie für das Konto aktivieren.

Um bestehende Organisationskonten als Macie-Mitgliedskonten zu aktivieren und hinzuzufügen

Um bestehende Organisationskonten als Macie-Mitgliedskonten zu aktivieren und hinzuzufügen, können Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden. Nur der delegierte Macie-Administrator für die Organisation kann diese Aufgabe ausführen.

Console

Um diese Aufgabe mithilfe der Konsole ausführen zu können, müssen Sie berechtigt sein, die folgende AWS Organizations Aktion auszuführen:. `organizations:ListAccounts` Mit dieser Aktion können Sie Informationen zu den Konten in Ihrer Organisation abrufen und anzeigen. Wenn Sie über diese Berechtigungen verfügen, gehen Sie wie folgt vor, um bestehende Konten als Macie-Mitgliedskonten zu aktivieren und hinzuzufügen.

Um bestehende Organisationskonten zu aktivieren und hinzuzufügen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie bestehende Konten als Macie-Mitgliedskonten aktivieren und hinzufügen möchten.
3. Klicken Sie im Navigationsbereich unter Settings auf Accounts.

   Die Seite Konten wird geöffnet und zeigt eine Tabelle der Konten an, die mit Ihrem Macie-Konto verknüpft sind. Wenn ein Konto Teil Ihrer Organisation in istAWS Organizations, lautet sein Typ Via AWS Organizations. Wenn es sich bei einem Konto nicht um ein Macie-Mitgliedskonto handelt, lautet sein Status Kein Mitglied.
4. Aktivieren Sie in der Tabelle Konten das Kontrollkästchen für jedes Konto, das Sie als Macie-Mitgliedskonto hinzufügen möchten.

> **Tip**
>
> Um die hinzuzufügenden Konten leichter identifizieren zu können, können Sie die Tabelle filtern. Platzieren Sie dazu den Cursor in dem Filterfeld über der Tabelle und wählen Sie dann Status aus. Wählen Sie dann Status = Kein Mitglied.

5. Wählen Sie im Menü Aktionen die Option Mitglied hinzufügen aus.
6. Bestätigen Sie, dass Sie die ausgewählten Konten als Mitgliedskonten hinzufügen möchten.

Nachdem Sie das Hinzufügen der ausgewählten Konten bestätigt haben, ändert sich der Status der Konten in Erstellen/Aktivieren und dann in Aktiviert.

Wiederholen Sie die vorherigen Schritte in jeder weiteren Region, in der Sie Ihre Organisation in Macie konfigurieren möchten.

API

Verwenden Sie die Amazon Macie Macie-API, um ein oder mehrere bestehende Konten programmgesteuert als Macie-Mitgliedskonten CreateMemberzu aktivieren und hinzuzufügen. Wenn Sie Ihre Anfrage einreichen, verwenden Sie die unterstützten Parameter, um die 12-stellige Konto-ID und E-Mail-Adresse für jedes AWS-Konto zu aktivierende und hinzuzufügende Konto anzugeben. Geben Sie auch die Region an, für die sich die Anfrage bezieht. Um bestehende Konten in weiteren Regionen zu aktivieren und hinzuzufügen, reichen Sie die Anfrage für jede weitere Region ein.

Um die Konto-ID und E-Mail-Adresse eines abzurufen, das aktiviert und hinzugefügt werden AWS-Konto soll, können Sie optional den ListMembersBetrieb der Amazon Macie Macie-API verwenden. Dieser Vorgang liefert Details zu den Konten, die mit Ihrem Macie-Konto verknüpft sind, einschließlich Konten, die keine Macie-Mitgliedskonten sind. Wenn der Wert für das `relationshipStatus` Eigentum eines Kontos nicht lautet`Enabled`, handelt es sich bei dem Konto nicht um ein Macie-Mitgliedskonto.

Um ein oder mehrere bestehende Konten mit dem zu aktivieren und hinzuzufügenAWS CLI, führen Sie den Befehl create-member aus. Verwenden Sie den `region` Parameter, um die Region anzugeben, in der die Konten aktiviert und hinzugefügt werden sollen. Verwenden Sie die `account` Parameter, um die Konto-ID und die E-Mail-Adresse für jedes AWS-Konto hinzuzufügende Konto anzugeben. Beispiel:

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"123456789012\",\"email\":\"janedoe@example.com\"}
```

Dabei ist us-east-1 die Region, in der das Konto als Macie-Mitgliedskonto aktiviert und hinzugefügt werden soll (Region USA Ost (Nord-Virginia)), und die account Parameter geben die Konto-ID

(123456789012) und die E-Mail-Adresse (janedoe@example.com) für das Konto an.

Wenn Ihre Anfrage erfolgreich ist, ändert sich der Status (`relationshipStatus`) des angegebenen Kontos in Ihrem Kontobestand. `Enabled`

Amazon Macie Macie-Konten für eine Organisation überprüfen

Nachdem eine AWS Organizations Organisation in Amazon Macie integriert und konfiguriert wurde, kann der delegierte Macie-Administrator der Organisation auf ein Inventar der Konten der Organisation in Macie zugreifen. Als Macie-Administrator für eine Organisation können Sie dieses Inventar verwenden, um Statistiken und Details für die Macie-Konten Ihrer Organisation in einem zu überprüfen. AWS-Region Sie können dieses Inventar auch verwenden, um Macie-Mitgliedskonten in einer Region zu verwalten.

Um die Macie-Konten einer Organisation zu überprüfen

Um die Konten für Ihre Organisation zu überprüfen, können Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden.

Console

Gehen Sie wie folgt vor, um die Macie-Konten Ihrer Organisation mithilfe der Amazon Macie Macie-Konsole zu überprüfen.

Um die Konten Ihrer Organisation zu überprüfen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie die Konten Ihrer Organisation überprüfen möchten.
3. Klicken Sie im Navigationsbereich unter Settings auf Accounts.

Die Seite Konten wird geöffnet. Dort werden aggregierte Statistiken und eine Tabelle der Konten angezeigt, die derzeit mit Ihrem Macie-Konto verknüpft sind. AWS-Region

Oben auf der Kontoseite finden Sie die folgenden aggregierten Statistiken.

Über AWS Organizations

Active meldet die Gesamtzahl der Konten, die mit Ihrem Konto verknüpft sind AWS Organizations und derzeit Macie-Mitgliedskonten in Ihrer Organisation sind. Macie ist für diese Konten aktiviert und Sie sind der Macie-Administrator der Konten.

Alle meldet die Gesamtzahl der Konten, die mit Ihrem Konto verknüpft sindAWS Organizations, einschließlich Konten, bei denen es sich derzeit nicht um Macie-Mitgliedskonten handelt.

Auf Einladung

Aktiv meldet die Gesamtzahl der Konten, die auf Einladung von Macie mit Ihrem Konto verknüpft sind und derzeit Macie-Mitgliedskonten sind. (Diese Konten sind nicht mit Ihrem Konto verknüpft.) AWS Organizations Macie ist für die Konten aktiviert und Sie sind der Macie-Administrator der Konten, weil sie eine Einladung zur Macie-Mitgliedschaft von Ihnen akzeptiert haben.

Alle meldet die Gesamtzahl der Konten, die auf Einladung von Macie mit Ihrem Konto verknüpft sind, einschließlich Konten, die nicht auf eine Einladung von Ihnen geantwortet haben.

Aktiv/Alle

Aktiv meldet die Gesamtzahl der Konten, die derzeit Macie-Mitgliedskonten für Ihr Konto sind, entweder durch AWS Organizations oder auf Einladung von Macie. Macie ist für diese Konten aktiviert und Sie sind der Macie-Administrator der Konten.

Alle meldet die Gesamtzahl der Konten, die entweder über AWS Organizations oder auf Einladung von Macie mit Ihrem Konto verknüpft sind. Dazu gehören Konten, die Teil Ihrer Organisation sind AWS Organizations und derzeit keine Macie-Mitgliedskonten sind, sowie alle Konten, die nicht auf eine Einladung zur Macie-Mitgliedschaft von Ihnen geantwortet haben.

In der Tabelle finden Sie Details zu den einzelnen Konten in der aktuellen Region. Die Tabelle enthält alle Konten, die entweder über AWS Organizations oder auf Einladung von Macie mit Ihrem Macie-Konto verknüpft sind.

Konto-ID

Die Konto-ID und E-Mail-Adresse für dieAWS-Konto.

Name

Der Kontoname für dieAWS-Konto. Dieser Wert ist in der Regel N/A für Konten, die auf Einladung von Macie mit Ihrem Konto verknüpft wurden.

Typ

Wie das Konto über AWS Organizations oder auf Einladung von Macie mit Ihrem Konto verknüpft ist.

Status

Der Status der Beziehung zwischen Ihrem Konto und dem Konto. Für ein Konto in einer AWS Organizations Organisation (Typ ist Via AWS Organizations) sind folgende Werte möglich:

- Konto gesperrt — Das AWS-Konto ist gesperrt.
- Erstellt/Aktiviert — Macie bearbeitet eine Anfrage zur Aktivierung und zum Hinzufügen des Kontos als Macie-Mitgliedskonto.
- Aktiviert — Das Konto ist ein Macie-Mitgliedskonto. Macie ist für das Konto aktiviert und Sie sind der Macie-Administrator für das Konto.
- Kein Mitglied — Das Konto ist Teil Ihrer Organisation, AWS Organizations aber es ist kein Macie-Mitgliedskonto.
- Pausiert (gesperrt) — Das Konto ist ein Macie-Mitgliedskonto, aber Macie ist derzeit für dieses Konto gesperrt.
- Region deaktiviert — Das Konto ist Teil Ihrer Organisation in, AWS Organizations aber die aktuelle Region ist für deaktiviert. AWS-Konto
- Entfernt (getrennt) — Das Konto war zuvor ein Macie-Mitgliedskonto, wurde aber später als Mitgliedskonto entfernt. Sie haben das Konto von Ihrem Macie-Administratorkonto getrennt. Macie ist weiterhin für das Konto aktiviert.

Letzte Aktion

Wann Sie oder das zugehörige Konto zuletzt eine Aktion ausgeführt haben, die sich auf die Beziehung zwischen Ihren Konten ausgewirkt hat.

Um die Tabelle nach einem bestimmten Feld zu sortieren, klicken Sie auf die Spaltenüberschrift für das Feld. Um die Sortierreihenfolge zu ändern, klicken Sie erneut auf die Spaltenüberschrift. Um die Tabelle zu filtern, platzieren Sie den Cursor in das Filterfeld und fügen Sie dann eine Filterbedingung für ein Feld hinzu. Um die Ergebnisse weiter zu verfeinern, fügen Sie Filterbedingungen für weitere Felder hinzu.

API

Um die Konten Ihrer Organisation programmgesteuert zu überprüfen, verwenden Sie den ListMembersBetrieb der Amazon Macie Macie-API und geben Sie unbedingt die Region an, für die Ihre Anfrage gilt. Um die Konten in weiteren Regionen zu überprüfen, reichen Sie Ihre Anfrage in jeder weiteren Region ein.

Wenn Sie Ihre Anfrage einreichen, verwenden Sie den `onlyAssociated` Parameter, um anzugeben, welche Konten in die Antwort aufgenommen werden sollen. Standardmäßig gibt Macie nur Details zu den Konten zurück, bei denen es sich um Macie-Mitgliedskonten in der angegebenen Region handelt, entweder über AWS Organizations oder auf Einladung von Macie. Um diese Informationen für alle Konten abzurufen, die mit Ihrem Macie-Konto verknüpft sind, einschließlich Konten, die keine Mitgliedskonten sind, nehmen Sie den `onlyAssociated` Parameter in Ihre Anfrage auf und setzen Sie den Wert des Parameters auf. `false`

Um die Konten Ihrer Organisation mithilfe von AWS Command Line Interface(AWS CLI) zu überprüfen, führen Sie den Befehl list-members aus. Geben Sie für den `only-associated` Parameter an, ob alle zugehörigen Konten oder nur Macie-Mitgliedskonten eingeschlossen werden sollen. Um nur Mitgliedskonten einzubeziehen, lassen Sie diesen Parameter weg oder setzen Sie den Wert des Parameters auf. `true` Um alle Konten einzubeziehen, legen Sie diesen Wert auf `false` fest. Beispiele:

```
C:\> aws macie2 list-members --region us-east-1 --only-associated false
```

Dabei ist *`us-east-1`* die Region, für die sich die Anfrage bezieht, die Region USA Ost (Nord-Virginia).

Wenn Ihre Anfrage erfolgreich ist, gibt Macie ein Array zurück. `members` Das Array enthält ein `member` Objekt für jedes Konto, das die in der Anfrage angegebenen Kriterien erfüllt. In diesem Objekt gibt das `relationshipStatus` Feld den aktuellen Status der Beziehung zwischen Ihrem Konto und dem anderen Konto in der angegebenen Region an. Für ein Konto in einer AWS Organizations Organisation sind folgende Werte möglich:

- `AccountSuspended`— Das AWS-Konto ist gesperrt.
- `Created`— Macie bearbeitet eine Anfrage zur Aktivierung und zum Hinzufügen des Kontos als Macie-Mitgliedskonto.
- `Enabled`— Das Konto ist ein Macie-Mitgliedskonto. Macie ist für das Konto aktiviert und Sie sind der Macie-Administrator für das Konto.

- `Paused`— Das Konto ist ein Macie-Mitgliedskonto, aber Macie ist derzeit für das Konto gesperrt (pausiert).
- `RegionDisabled`— Das Konto ist Teil Ihrer Organisation in, AWS Organizations aber die aktuelle Region ist für die deaktiviert. AWS-Konto
- `Removed`— Das Konto war zuvor ein Macie-Mitgliedskonto, wurde aber später als Mitgliedskonto entfernt. Sie haben das Konto von Ihrem Macie-Administratorkonto getrennt. Macie ist weiterhin für das Konto aktiviert.

Informationen zu anderen Feldern im `member` Objekt finden Sie unter Mitglieder in der Amazon Macie API-Referenz.

Amazon Macie Macie-Mitgliedskonten für eine Organisation verwalten

Nachdem eine AWS Organizations Organisation in Amazon Macie integriert und konfiguriert wurde, kann der delegierte Macie-Administrator der Organisation auf bestimmte Macie-Einstellungen, Daten und Ressourcen für Mitgliedskonten zugreifen.

Als Macie-Administrator für eine Organisation können Sie bestimmte Kontoverwaltungs- und Verwaltungsaufgaben in Macie zentral ausführen. Beispiele:

- Macie-Mitgliedskonten hinzufügen und entfernen
- Den Status von Macie für einzelne Konten verwalten, z. B. Macie für ein Konto aktivieren oder sperren
- Überwachen Sie die Macie-Kontingente und die geschätzten Nutzungskosten für einzelne Konten und die gesamte Organisation

Sie können sich auch die Inventardaten und Richtlinienergebnisse von Amazon Simple Storage Service (Amazon S3) für Macie-Mitgliedskonten ansehen. Und Sie können sensible Daten in S3-Buckets entdecken, die den Konten gehören. Eine ausführliche Liste der Aufgaben, die Sie ausführen können, finden Sie unterDie Beziehung zwischen Amazon Macie-Administrator- und Mitgliedskonten verstehen.

Standardmäßig bietet Ihnen Macie Einblick in relevante Daten und Ressourcen für alle Macie-Mitgliedskonten in Ihrer Organisation. Sie können sich auch die Daten und Ressourcen einzelner Konten genauer ansehen. Wenn Sie beispielsweise das Übersichts-Dashboard verwenden, um den Amazon S3-Sicherheitsstatus Ihres Unternehmens zu bewerten, können Sie die Daten nach Konto

filtern. Wenn Sie die geschätzten Nutzungskosten überwachen, können Sie auf ähnliche Weise auf Aufschlüsselungen der geschätzten Kosten für einzelne Mitgliedskonten zugreifen.

Zusätzlich zu den Aufgaben, die für Administrator- und Mitgliedskonten üblich sind, können Sie verschiedene Verwaltungsaufgaben für Ihre Organisation ausführen.

Aufgaben

- Amazon Macie Macie-Mitgliedskonten zu einer Organisation hinzufügen
- Amazon Macie für Mitgliedskonten in einer Organisation sperren
- Amazon Macie Macie-Mitgliedskonten aus einer Organisation entfernen

Als Macie-Administrator einer Organisation können Sie diese Aufgaben mithilfe der Amazon Macie Macie-Konsole oder der Amazon Macie Macie-API ausführen. Wenn Sie lieber die Konsole verwenden möchten, beachten Sie, dass Sie die folgende AWS Organizations Aktion ausführen dürfen müssen:. `organizations:ListAccounts` Mit dieser Aktion können Sie Informationen zu Konten, die Teil Ihrer Organisation sind, in abrufen und anzeigenAWS Organizations.

Amazon Macie Macie-Mitgliedskonten zu einer Organisation hinzufügen

In einigen Fällen müssen Sie möglicherweise manuell ein Konto als Macie-Mitgliedskonto hinzufügen. Dies ist bei Konten der Fall, die Sie zuvor als Mitgliedskonten entfernt (getrennt) haben. Dies ist auch der Fall, wenn Sie Macie nicht so konfiguriert haben, dass neue Konten automatisch als Mitgliedskonten aktiviert und hinzugefügt werden, wenn Konten zu Ihrer Organisation in hinzugefügt werden. AWS Organizations

Wenn Sie ein Konto als Macie-Mitgliedskonto hinzufügen, wird Macie für das aktuelle Konto aktiviertAWS-Region, sofern es in dieser Region noch nicht aktiviert ist, und das Konto ist Ihrem Macie-Administratorkonto als Mitgliedskonto in der Region zugeordnet. Das Mitgliedskonto erhält keine Einladung oder andere Benachrichtigung darüber, dass Sie diese Beziehung zwischen Ihren Konten hergestellt haben.

Beachten Sie, dass Sie kein Konto hinzufügen können, das bereits mit einem anderen Macie-Administratorkonto verknüpft ist. Das Konto muss zuerst von seinem aktuellen Administratorkonto getrennt werden. Darüber hinaus können Sie das AWS Organizations Verwaltungskonto nicht als Mitgliedskonto hinzufügen, es sei denn, das Verwaltungskonto hat Macie bereits für das Konto aktiviert. Weitere Informationen zu zusätzlichen Anforderungen finden Sie unterÜberlegungen und Empfehlungen zur Verwendung von Amazon Macie mit AWS Organizations.

So fügen Sie einer Organisation ein Macie-Mitgliedskonto hinzu

Um Ihrer Organisation ein oder mehrere Macie-Mitgliedskonten hinzuzufügen, können Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden.

Console

Gehen Sie wie folgt vor, um mithilfe der Amazon Macie-Konsole ein oder mehrere Macie-Mitgliedskonten hinzuzufügen.

Um ein Macie-Mitgliedskonto hinzuzufügen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie ein Mitgliedskonto hinzufügen möchten.
3. Klicken Sie im Navigationsbereich unter Settings auf Accounts. Die Seite Konten wird geöffnet und zeigt eine Tabelle der Konten an, die mit Ihrem Konto verknüpft sind.
4. (Optional) Verwenden Sie das Filterfeld über der Tabelle, um Konten, die Teil Ihrer Organisation sind AWS Organizations und keine Macie-Mitgliedskonten sind, einfacher zu identifizieren, um die folgenden Filterbedingungen hinzuzufügen:

   - Typ = Organisation
   - Status = Kein Mitglied

   Um auch Konten anzuzeigen, die Sie zuvor entfernt haben und die Sie möglicherweise als Mitgliedskonten hinzufügen möchten, fügen Sie außerdem die Filterbedingung Status = Entfernt hinzu.
5. Aktivieren Sie in der Tabelle Konten das Kontrollkästchen für jedes Konto, das Sie als Mitgliedskonto hinzufügen möchten.
6. Wählen Sie im Menü Aktionen die Option Mitglied hinzufügen aus.
7. Bestätigen Sie, dass Sie die ausgewählte Anzahl von Konten als Mitgliedskonten hinzufügen möchten.

Nachdem Sie Ihre Auswahl bestätigt haben, ändert sich der Status der ausgewählten Konten in Ihrem Kontoinventar auf Erstellt/Aktiviert und anschließend auf Aktiviert.

Wiederholen Sie die vorherigen Schritte in jeder weiteren Region, in der Sie ein Mitgliedskonto hinzufügen möchten.

API

Um ein oder mehrere Macie-Mitgliedskonten programmgesteuert hinzuzufügen, verwenden Sie den CreateMemberBetrieb der Amazon Macie Macie-API.

Wenn Sie Ihre Anfrage einreichen, verwenden Sie die unterstützten Parameter, um die 12-stellige Konto-ID und E-Mail-Adresse für jeden, den Sie hinzufügen möchtenAWS-Konto, anzugeben. Geben Sie auch die Region an, für die sich die Anfrage bezieht. Um ein Konto in weiteren Regionen hinzuzufügen, reichen Sie Ihre Anfrage in jeder weiteren Region ein.

Um die Konto-ID und E-Mail-Adresse eines hinzuzufügenden Kontos abzurufen, können Sie die Ausgabe des API-Betriebs und des ListAccountsBetriebs der Amazon Macie AWS Organizations Macie-API korrelieren. ListMembers Nehmen Sie für den ListMembers Betrieb der Macie-API den `onlyAssociated` Parameter in Ihre Anfrage auf und setzen Sie den Wert des Parameters auf. `false` Wenn der Vorgang erfolgreich ist, gibt Macie ein `members` Array zurück, das Details zu allen Konten enthält, die Ihrem Macie-Administratorkonto in der angegebenen Region zugeordnet sind, einschließlich Konten, die derzeit keine Mitgliedskonten sind. Beachten Sie Folgendes im Array:

- Wenn der Wert für die `relationshipStatus` Eigenschaft eines Kontos nicht lautet`Enabled`, ist das Konto mit Ihrem Konto verknüpft, es handelt sich jedoch nicht um ein Macie-Mitgliedskonto.
- Wenn ein Konto nicht im Array enthalten ist, aber in der Ausgabe des ListAccounts AWS Organizations API-Betriebs enthalten ist, ist das Konto Teil Ihrer Organisation, AWS Organizations aber es ist nicht mit Ihrem Konto verknüpft und ist daher kein Macie-Mitgliedskonto.

Um mit dem ein Mitgliedskonto hinzuzufügenAWS CLI, führen Sie den Befehl create-member aus. Verwenden Sie den `region` Parameter, um die Region anzugeben, in der das Konto hinzugefügt werden soll. Verwenden Sie die `account` Parameter, um die Konto-ID und die E-Mail-Adresse für jedes hinzuzufügende Konto anzugeben. Beispiele:

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"123456789012\",\"email\":\"janedoe@example.com\"}
```

Dabei ist us-east-1 die Region, in der das Konto als Mitgliedskonto hinzugefügt werden soll (Region USA Ost (Nord-Virginia)), und die account Parameter geben die Konto-ID (123456789012) und die E-Mail-Adresse (janedoe@example.com) für das Konto an.

Wenn Ihre Anfrage erfolgreich ist, ändert sich der Status (`relationshipStatus`) des angegebenen Kontos in Ihrem Kontoinventar. `Enabled`

Amazon Macie für Mitgliedskonten in einer Organisation sperren

Als Macie-Administrator für eine Organisation in AWS Organizations können Sie Macie für ein Mitgliedskonto in Ihrer Organisation sperren. In diesem Fall können Sie Macie auch zu einem späteren Zeitpunkt wieder für das Konto aktivieren.

Wenn du Macie für ein Mitgliedskonto sperrst:

- Macie verliert den Zugriff auf die aktuellen AWS-Region Amazon S3 S3-Daten des Kontos und stellt diese nicht mehr bereit.
- Macie beendet die Ausführung aller Aktivitäten für das Konto in der Region. Dazu gehören die Überwachung von S3-Buckets im Hinblick auf Sicherheit und Zugriffskontrolle, die automatische Erkennung sensibler Daten und die Ausführung von Aufgaben zur Erkennung sensibler Daten, die derzeit ausgeführt werden.
- Macie storniert alle Aufträge zur Erkennung sensibler Daten, die von dem Konto in der Region erstellt wurden. Ein Auftrag kann nicht wieder aufgenommen oder neu gestartet werden, nachdem er storniert wurde.

  Wenn Sie Jobs zur Analyse von Daten erstellt haben, die dem Mitgliedskonto gehören, storniert Macie Ihre Jobs nicht. Stattdessen werden bei den Jobs Ressourcen übersprungen, die dem Konto gehören.

Solange ein Konto gesperrt ist, behält Macie die Macie-Sitzungs-ID, die Einstellungen und Ressourcen für das Konto in der entsprechenden Region. Beispielsweise bleiben die Ergebnisse des Kontos erhalten und sind bis zu 90 Tage lang nicht betroffen. Ihrem Unternehmen fallen für das Konto in der entsprechenden Region keine Macie-Gebühren an, während Macie für das Konto in dieser Region gesperrt ist.

Um Macie für ein Mitgliedskonto in einer Organisation zu sperren

Um Macie für ein Mitgliedskonto in einer Organisation zu sperren, können Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden.

Console

Gehen Sie wie folgt vor, um Macie mithilfe der Amazon Macie Macie-Konsole für ein Mitgliedskonto zu sperren.

Um Macie für ein Mitgliedskonto zu sperren

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie Macie für das Mitgliedskonto sperren möchten.
3. Klicken Sie im Navigationsbereich unter Settings auf Accounts.
4. Wählen Sie in der Tabelle Konten das Kontrollkästchen für das Konto aus, das gesperrt werden soll.
5. Wählen Sie im Menü Aktionen die Option Macie sperren aus.
6. Bestätigen Sie, dass Sie Macie für das Konto sperren möchten.

Nachdem du die Sperrung bestätigt hast, ändert sich der Status des Accounts in deinem Kontobestand auf Pausiert (gesperrt).

Wiederhole die vorherigen Schritte in jeder weiteren Region, in der du Macie für das Konto sperren möchtest.

API

Um Macie für ein Mitgliedskonto programmgesteuert zu sperren, verwenden Sie den UpdateMemberSessionBetrieb der Amazon Macie Macie-API.

Wenn Sie Ihre Anfrage einreichen, verwenden Sie den `id` Parameter, um die 12-stellige Konto-ID für das Konto anzugeben, für AWS-Konto das Sie Macie sperren möchten. Geben Sie `PAUSED` für den `status` Parameter den neuen Status für das Macie-Konto an. Geben Sie auch die Region an, für die sich die Anfrage bezieht. Um das Konto in weiteren Regionen zu sperren, reichen Sie Ihre Anfrage in jeder weiteren Region ein.

Um die Konto-ID für das zu sperrende Konto abzurufen, können Sie den ListMembersBetrieb der Amazon Macie Macie-API verwenden. Wenn Sie dies tun, sollten Sie erwägen, die Ergebnisse zu filtern, indem Sie den `onlyAssociated` Parameter in Ihre Anfrage aufnehmen. Wenn Sie den

Wert dieses Parameters auf setzen`true`, gibt Macie ein `members` Array zurück, das nur Details zu den Konten enthält, bei denen es sich derzeit um Mitgliedskonten handelt.

Um Macie mithilfe von für ein Mitgliedskonto zu sperrenAWS CLI, führen Sie den update-member-sessionBefehl aus. Geben Sie mit dem `region` Parameter die Region an, in der Macie gesperrt werden soll, und geben Sie mit dem `id` Parameter die Konto-ID an, für die Macie gesperrt werden AWS-Konto soll. Geben Sie für den `status` Parameter an. `PAUSED` Beispiele:

```
C:\> aws macie2 update-member-session --region us-east-1 --id 123456789012 --status
 PAUSED
```

Dabei ist *`us-east-1`* die Region, in der Macie gesperrt werden soll (Region USA Ost (Nord-Virginia)), *`123456789012`* ist die Konto-ID für das Konto, für das Macie gesperrt werden soll, und `PAUSED` ist der neue Macie-Status für das Konto.

Wenn Ihre Anfrage erfolgreich ist, gibt Macie eine leere Antwort zurück und der Status des angegebenen Kontos ändert sich in Ihrem Kontobestand. `Paused`

Amazon Macie Macie-Mitgliedskonten aus einer Organisation entfernen

Wenn Sie nicht mehr auf die Macie-Einstellungen, -Daten und -Ressourcen für ein Mitgliedskonto zugreifen möchten, können Sie das Konto als Macie-Mitgliedskonto entfernen. Dazu trennen Sie das Konto von Ihrem Macie-Administratorkonto. Beachten Sie, dass nur Sie dies für ein Mitgliedskonto tun können. Ein AWS Organizations Mitgliedskonto kann nicht von seinem Macie-Administratorkonto getrennt werden.

Wenn Sie ein Macie-Mitgliedskonto entfernen, bleibt Macie für das aktuelle Konto aktiviert. AWS-Region Das Konto wird jedoch von Ihrem Macie-Administratorkonto getrennt und es wird zu einem eigenständigen Macie-Konto. Dies bedeutet, dass Sie den Zugriff auf alle Macie-Einstellungen, Daten und Ressourcen für das Konto verlieren, einschließlich Metadaten und Richtlinienergebnissen für die Amazon S3 S3-Daten des Kontos. Dies bedeutet auch, dass Sie Macie nicht mehr verwenden können, um sensible Daten in S3-Buckets zu ermitteln, die dem Konto gehören. Wenn Sie zu diesem Zweck bereits vertrauliche Discovery-Jobs erstellt haben, überspringen die Jobs Buckets, die dem Konto gehören.

Nachdem Sie ein Macie-Mitgliedskonto entfernt haben, erscheint das Konto weiterhin in Ihrem Kontoinventar. Macie benachrichtigt den Kontoinhaber nicht darüber, dass Sie das Konto entfernt haben.

Um ein Macie-Mitgliedskonto aus einer Organisation zu entfernen

Um ein Macie-Mitgliedskonto aus Ihrer Organisation zu entfernen, können Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden.

Console

Gehen Sie wie folgt vor, um ein Macie-Mitgliedskonto mithilfe der Amazon Macie Macie-Konsole zu entfernen.

Um ein Macie-Mitgliedskonto zu entfernen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie das Mitgliedskonto entfernen möchten.
3. Klicken Sie im Navigationsbereich unter Settings auf Accounts.
4. Aktivieren Sie in der Tabelle Konten das Kontrollkästchen für das Konto, das Sie als Mitgliedskonto entfernen möchten.
5. Wählen Sie im Menü Aktionen die Option Konto trennen aus.
6. Bestätigen Sie, dass Sie das ausgewählte Konto als Mitgliedskonto entfernen möchten.

Nachdem Sie Ihre Auswahl bestätigt haben, ändert sich der Status des Kontos in Ihrem Kontobestand auf Entfernt (getrennt).

Wiederholen Sie die vorherigen Schritte in jeder weiteren Region, in der Sie das Mitgliedskonto entfernen möchten.

API

Verwenden Sie die Amazon Macie-API, um ein Macie-Mitgliedskonto programmgesteuert zu entfernen. DisassociateMember

Wenn Sie Ihre Anfrage einreichen, geben Sie mithilfe des `id` Parameters die 12-stellige AWS-Konto ID für das Mitgliedskonto an, das entfernt werden soll. Geben Sie auch die Region an, für die sich die Anfrage bezieht. Um das Konto in weiteren Regionen zu entfernen, reichen Sie Ihre Anfrage in jeder weiteren Region ein.

Um die Konto-ID für das zu entfernende Mitgliedskonto abzurufen, können Sie den ListMembersBetrieb der Amazon Macie Macie-API verwenden. Wenn Sie dies tun, sollten Sie

erwägen, die Ergebnisse zu filtern, indem Sie den `onlyAssociated` Parameter in Ihre Anfrage aufnehmen. Wenn Sie den Wert dieses Parameters auf setzen`true`, gibt Macie ein `members` Array zurück, das nur Details zu den Konten enthält, bei denen es sich derzeit um Macie-Mitgliedskonten handelt.

Um ein Macie-Mitgliedskonto mithilfe von zu entfernenAWS CLI, führen Sie den Befehl disassociate-member aus. Verwenden Sie den `region` Parameter, um die Region anzugeben, in der das Konto entfernt werden soll. Verwenden Sie den `id` Parameter, um die Konto-ID für das Mitgliedskonto anzugeben, das entfernt werden soll. Beispiele:

```
C:\> aws macie2 disassociate-member --region us-east-1 --id 123456789012
```

Dabei ist *`us-east-1`* die Region, in der das Konto entfernt werden soll (Region USA Ost (Nord-Virginia)), und *`123456789012`* ist die Konto-ID für das zu entfernende Konto.

Wenn Ihre Anfrage erfolgreich ist, gibt Macie eine leere Antwort zurück und der Status des angegebenen Kontos ändert sich in Ihrem Kontobestand. `Removed`

Ein anderes Amazon Macie-Administratorkonto für eine Organisation festlegen

Nachdem eine AWS Organizations Organisation in Amazon Macie integriert und konfiguriert wurde, kann das AWS Organizations Verwaltungskonto ein anderes Konto als delegiertes Macie-Administratorkonto für die Organisation festlegen.

Stellen Sie als Benutzer des AWS Organizations Verwaltungskontos für eine Organisation sicher, dass Sie die folgenden Berechtigungsanforderungen erfüllen, bevor Sie ein anderes Macie-Administratorkonto für Ihre Organisation festlegen:

- Sie müssen über dieselben Berechtigungen verfügen, die ursprünglich für die Festlegung eines Macie-Administratorkontos für Ihre Organisation erforderlich waren. Sie müssen außerdem berechtigt sein, die folgende AWS Organizations Aktion auszuführen:. `organizations:DeregisterDelegatedAdministrator` Mit dieser zusätzlichen Aktion können Sie die aktuelle Bezeichnung entfernen.
- Wenn es sich bei Ihrem Konto derzeit um ein Macie-Mitgliedskonto handelt, muss der aktuelle Macie-Administrator Ihr Konto als Macie-Mitgliedskonto entfernen. Andernfalls dürfen Sie nicht auf Macie-Operationen zugreifen, um ein anderes Administratorkonto festzulegen. Nachdem Sie ein

neues Administratorkonto festgelegt haben, kann der neue Macie-Administrator Ihr Konto erneut als Macie-Mitgliedskonto hinzufügen.

Wenn Ihre Organisation Macie in mehreren Fällen verwendet, stellen Sie außerdem sicher AWS-Regionen, dass Sie das delegierte Macie-Administratorkonto in jeder Region ändern, in der Ihre Organisation Macie verwendet. Das delegierte Macie-Administratorkonto muss in all diesen Regionen identisch sein. Wenn Sie mehrere Organisationen verwalten, beachten Sie außerdem AWS Organizations, dass ein Konto das delegierte Macie-Administratorkonto für jeweils nur eine Organisation sein kann. Weitere Informationen zu zusätzlichen Anforderungen finden Sie unter. Überlegungen und Empfehlungen zur Verwendung von Amazon Macie mit AWS Organizations

So legen Sie ein anderes Macie-Administratorkonto für Ihre Organisation fest

Um ein anderes Macie-Administratorkonto für Ihre Organisation festzulegen, können Sie die Amazon Macie-Konsole oder eine Kombination aus Amazon Macie und APIs verwenden. AWS Organizations Nur ein Benutzer des AWS Organizations Verwaltungskontos kann die Bezeichnung für seine Organisation ändern.

Console

Gehen Sie wie folgt vor, um die Bezeichnung mithilfe der Amazon Macie Macie-Konsole zu ändern.

Um ein anderes Macie-Administratorkonto zuzuweisen

1. Melden Sie sich AWS Management Console mit Ihrem AWS Organizations Verwaltungskonto bei an.
2. Wählen Sie mithilfe der AWS-Region Auswahltaste in der oberen rechten Ecke der Seite die Region aus, in der Sie die Bezeichnung ändern möchten.
3. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
4. Führen Sie je nachdem, ob Macie für Ihr Verwaltungskonto in der aktuellen Region aktiviert ist, einen der folgenden Schritte aus:

   - Wenn Macie nicht aktiviert ist, wählen Sie auf der Willkommensseite die Option Erste Schritte aus.
   - Wenn Macie aktiviert ist, wählen Sie im Navigationsbereich Einstellungen aus.
5. Wählen Sie unter Delegierter Administrator die Option Entfernen aus. Um die Bezeichnung zu ändern, müssen Sie zuerst die aktuelle Bezeichnung entfernen.

6. Bestätigen Sie, dass Sie die aktuelle Bezeichnung entfernen möchten.
7. Geben Sie unter Delegierter Administrator die 12-stellige Konto-ID ein, die als neues Macie-Administratorkonto für die Organisation bezeichnet werden AWS-Konto soll.
8. Wählen Sie Delegate (Delegieren).

Wiederholen Sie die vorherigen Schritte in jeder weiteren Region, in die Sie Macie integriert haben. AWS Organizations

API

Um die Bezeichnung programmgesteuert zu ändern, verwenden Sie zwei Operationen der Amazon Macie Macie-API und eine Operation der API. AWS Organizations Dies liegt daran, dass Sie die aktuelle Bezeichnung sowohl in Macie als auch AWS Organizations vor dem Einreichen der neuen Bezeichnung entfernen müssen.

Um die aktuelle Bezeichnung zu entfernen:

1. Verwenden Sie den DisableOrganizationAdminAccountBetrieb der Macie-API. Geben Sie für den erforderlichen `adminAccountId` Parameter die 12-stellige Konto-ID für das Konto an AWS-Konto , das derzeit als Macie-Administratorkonto für die Organisation festgelegt ist.
2. Verwenden Sie den DeregisterDelegatedAdministratorBetrieb der AWS Organizations API. Geben Sie für den `AccountId` Parameter die 12-stellige Konto-ID für das Konto an, das derzeit als Macie-Administratorkonto für die Organisation festgelegt ist. Dieser Wert sollte mit der Konto-ID übereinstimmen, die Sie in der vorherigen Macie-Anfrage angegeben haben. Geben Sie für den `ServicePrincipal` Parameter den Macie-Dienstprinzipal () `macie.amazonaws.com` an.

Nachdem Sie die aktuelle Bezeichnung entfernt haben, reichen Sie die neue Bezeichnung mithilfe der EnableOrganizationAdminAccountMacie-API ein. Geben Sie für den erforderlichen `adminAccountId` Parameter die 12-stellige Konto-ID an, die als neues Macie-Administratorkonto für die Organisation bezeichnet werden AWS-Konto soll.

Um die Bezeichnung mithilfe von zu ändern AWS CLI, führen Sie den disable-organization-admin-accountBefehl der Macie-API und den deregister-delegated-administratorBefehl der API aus. AWS Organizations Mit diesen Befehlen wird die aktuelle Bezeichnung in Macie bzw. AWS Organizations entfernt. Geben Sie für die `account-id` Parameter `admin-account-id` und die 12-stellige Konto-ID an, die als aktuelles Macie-Administratorkonto entfernt werden AWS-Konto

soll. Verwenden Sie den `region` Parameter, um die Region anzugeben, für die das Entfernen gilt. Beispielsweise:

```
C:\> aws macie2 disable-organization-admin-account --region us-east-1 --admin-
account-id 111122223333 && aws organizations deregister-delegated-administrator --
region us-east-1 --account-id 111122223333 --service-principal macie.amazonaws.com
```

Wobei gilt:

- *`us-east-1`* ist die Region, für die die Entfernung gilt, die Region USA Ost (Nord-Virginia).
- *`111122223333`* ist die Konto-ID für das Konto, das als Macie-Administratorkonto entfernt werden soll.
- `macie.amazonaws.com`ist der Macie-Service Principal.

Nachdem Sie die aktuelle Bezeichnung entfernt haben, reichen Sie die neue Bezeichnung ein, indem Sie den enable-organization-admin-accountBefehl der Macie-API ausführen. Geben Sie für den `admin-account-id` Parameter die 12-stellige Konto-ID an, die als neues Macie-Administratorkonto für die Organisation bezeichnet werden AWS-Konto soll. Verwenden Sie den `region` Parameter, um die Region anzugeben, für die die Bezeichnung gilt. Beispielsweise:

```
C:\> aws macie2 enable-organization-admin-account --region us-east-1 --admin-
account-id 444455556666
```

Dabei ist *`us-east-1`* die Region, für die die Bezeichnung gilt (Region USA Ost (Nord-Virginia)), und *`444455556666`* ist die Konto-ID für das Konto, das als neues Macie-Administratorkonto bestimmt werden soll.

Deaktivierung der Amazon Macie Macie-Integration mit AWS Organizations

Nachdem eine AWS Organizations Organisation in Amazon Macie integriert wurde, kann das AWS Organizations Verwaltungskonto die Integration anschließend deaktivieren. Als Benutzer des AWS Organizations Verwaltungskontos können Sie dies tun, indem Sie den vertrauenswürdigen Servicezugriff für Macie in deaktivieren. AWS Organizations

Wenn Sie den vertrauenswürdigen Dienstzugriff für Macie deaktivieren, passiert Folgendes:

- Macie verliert seinen Status als vertrauenswürdiger Dienst in. AWS Organizations

- Das Macie-Administratorkonto der Organisation verliert den Zugriff auf alle Macie-Einstellungen, -Daten und -Ressourcen für alle Macie-Mitgliedskonten insgesamt. AWS-Regionen
- Alle Macie-Mitgliedskonten werden zu eigenständigen Macie-Konten. Wenn Macie für ein Mitgliedskonto in einer oder mehreren Regionen aktiviert wurde, ist Macie weiterhin für das Konto in diesen Regionen aktiviert. Das Konto ist jedoch in keiner Region mehr mit einem Macie-Administratorkonto verknüpft.

Weitere Informationen zu den Ergebnissen der Deaktivierung des Zugriffs auf vertrauenswürdige Dienste finden Sie AWS-Services im AWS OrganizationsBenutzerhandbuch unter Zusammen AWS Organizations mit anderen verwenden.

So deaktivieren Sie den vertrauenswürdigen Dienstzugriff für Macie

Um den Zugriff auf vertrauenswürdige Dienste zu deaktivieren, können Sie die AWS Organizations Konsole oder die AWS Organizations API verwenden. Nur ein Benutzer des AWS Organizations Verwaltungskontos kann den vertrauenswürdigen Dienstzugriff für Macie deaktivieren. Einzelheiten zu den Berechtigungen, die Sie benötigen, finden Sie im AWS OrganizationsBenutzerhandbuch unter Erforderliche Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs.

Bevor Sie den Zugriff auf vertrauenswürdige Dienste deaktivieren, sollten Sie optional mit dem delegierten Macie-Administrator für Ihr Unternehmen zusammenarbeiten, um Macie für Mitgliedskonten zu sperren oder zu deaktivieren und die Macie-Ressourcen für diese Konten zu bereinigen.

Console

Gehen Sie wie folgt vor, um den Zugriff auf vertrauenswürdige Dienste mithilfe der AWS Organizations Konsole zu deaktivieren.

So deaktivieren Sie einen vertrauenswürdigen Servicezugriff

1. Melden Sie sich AWS Management Console mit Ihrem AWS Organizations Verwaltungskonto bei der an.
2. Öffnen Sie die AWS Organizations Konsole unter https://console.aws.amazon.com/organizations/.
3. Wählen Sie im Navigationsbereich Dienste aus.
4. Wählen Sie unter Integrierte Dienste Amazon Macie aus.
5. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.

6. Bestätigen Sie, dass Sie den vertrauenswürdigen Zugriff deaktivieren möchten.

API

Um den Zugriff auf vertrauenswürdige Dienste programmgesteuert zu deaktivieren, verwenden Sie den AWSServiceAccess Disable-Vorgang der AWS Organizations API. Geben Sie für den `ServicePrincipal` Parameter den Macie-Dienstprinzipal () an. `macie.amazonaws.com`

Um den vertrauenswürdigen Dienstzugriff mithilfe von AWS Command Line Interface(AWS CLI) zu deaktivieren, führen Sie den disable-aws-service-accessBefehl der AWS Organizations API aus. Geben Sie für den `service-principal` Parameter den Macie-Dienstprinzipal (`macie.amazonaws.com`) an. Beispiele:

```
C:\> aws organizations disable-aws-service-access --service-principal
 macie.amazonaws.com
```

Amazon Macie Macie-Konten nach Einladung verwalten

Sie können mehrere Amazon Macie Macie-Konten auf zwei Arten zentral verwalten, indem Sie Macie in Mitgliedschaftseinladungen integrieren AWS Organizations oder indem Sie Mitgliedschaftseinladungen verwenden. Wenn Sie Einladungen zur Mitgliedschaft verwenden, kann ein bestimmter Macie-Administrator Macie für bis zu 1.000 Konten verwalten. Der Administrator kann auch auf Amazon Simple Storage Service (Amazon S3) -Inventardaten zugreifen und vertrauliche Daten in S3 Buckets finden, die den Konten gehören. Einzelheiten zu den Aufgaben, die Administratoren ausführen können, finden Sie unterDie Beziehung zwischen Amazon Macie-Administrator- und Mitgliedskonten verstehen.

In einer Organisation, die auf Einladungen basiert, verknüpfen Sie Macie-Konten miteinander, indem Sie Einladungen zur Mitgliedschaft in Macie senden und annehmen. Wenn Sie eine Einladung senden und sie von einem anderen Konto akzeptiert wird, werden Sie Macie-Administrator für das andere Konto und das andere Konto wird ein Mitgliedskonto in Ihrer Organisation. Wenn Sie eine Einladung erhalten und annehmen, wird Ihr Konto zu einem Mitgliedskonto und der Macie-Administrator kann auf bestimmte Macie-Einstellungen, Daten und Ressourcen für Ihr Konto zugreifen.

> **Tip**
>
> Wenn Sie in Macie eine Organisation erstellen, die auf Einladungen basiert, können Sie anschließend auf die Verwendung dieser Organisation umsteigen. AWS Organizations Sie können auch beide Methoden gleichzeitig verwenden, um mehrere Macie-Konten zu verwalten. Wenn Ihre AWS Umgebung beispielsweise Testkonten enthält, können Sie die Konten Ihrer Organisation in ausschließen AWS Organizations und sie auf Einladung separat verwalten.

In den Themen in diesem Abschnitt wird erläutert, wie Sie eine auf Einladung basierende Organisation erstellen und an ihr teilnehmen und wie Sie verschiedene Verwaltungsaufgaben für die Organisation ausführen.

Themen

- Überlegungen und Empfehlungen für Organisationen auf Einladung in Amazon Macie
- Eine auf Einladung basierende Organisation in Amazon Macie erstellen und verwalten
- Überprüfung von Amazon Macie Macie-Konten für eine Organisation, die auf Einladung basiert
- Benennen eines anderen Amazon Macie-Administratorkontos für eine Organisation, die auf Einladung basiert
- Verwaltung Ihrer Mitgliedschaft in einer Organisation, die auf Einladungen basiert, in Amazon Macie

Überlegungen und Empfehlungen für Organisationen auf Einladung in Amazon Macie

Bevor Sie eine Organisation auf Einladung in Amazon Macie erstellen oder mit der Verwaltung beginnen, sollten Sie die folgenden Anforderungen und Empfehlungen berücksichtigen. Stellen Sie außerdem sicher, dass Sie die Beziehung zwischen Macie-Administrator - und Mitgliedskonten verstehen.

Themen

- Auswahl eines Macie-Administratorkontos
- Einladungen versenden und Macie-Mitgliedskonten verwalten
- Beantwortung und Verwaltung von Mitgliedschaftseinladungen

- Übergang zu AWS Organizations

Auswahl eines Macie-Administratorkontos

Beachten Sie bei der Entscheidung, welches Konto das Macie-Administratorkonto für die Organisation sein soll, Folgendes:

- Eine Organisation kann nur ein Macie-Administratorkonto haben.
- Ein Konto kann nicht gleichzeitig ein Macie-Administrator- und ein Mitgliedskonto sein.
- Macie ist ein regionaler Dienst. Das bedeutet, dass die Zuordnung zwischen einem Macie-Administratorkonto und einem Mitgliedskonto regional ist. Die Zuordnung besteht nur in demAWS-Region, von dem eine Einladung gesendet und angenommen wird. Wenn der Macie-Administrator beispielsweise Einladungen in der Region USA Ost (Nord-Virginia) versendet und diese Einladungen akzeptiert werden, kann der Macie-Administrator die Mitgliedskonten nur in dieser Region verwalten.

  Um Macie-Konten in mehreren Regionen zentral zu verwaltenAWS-Regionen, kann sich der Macie-Administrator in jeder Region anmelden, in der die Organisation Macie derzeit verwendet oder verwenden wird, und Einladungen an die entsprechenden Konten in jeder dieser Regionen senden. Eine Liste der Regionen, in denen Macie derzeit verfügbar ist, finden Sie unter Amazon Macie Macie-Endpunkte und Kontingente in der. Allgemeine AWS-Referenz
- Ein Mitgliedskonto kann jeweils nur einem Macie-Administratorkonto zugeordnet werden. Wenn Ihre Organisation Macie in mehreren Regionen verwendet, bedeutet dies, dass das Macie-Administratorkonto in all diesen Regionen identisch sein muss. Administrator- und Mitgliedskonten müssen Einladungen jedoch in jeder Region getrennt versenden und annehmen.
- Wenn das Konto des Macie-Administrators gesperrt, isoliert oder geschlossen AWS-Konto wird, werden alle zugehörigen Mitgliedskonten automatisch als Mitgliedskonten entfernt, aber Macie ist weiterhin für diese Konten aktiviert.

Einladungen versenden und Macie-Mitgliedskonten verwalten

Als Macie-Administrator einer Organisation, die auf Einladungen basiert, sollten Sie Folgendes beachten, wenn Sie Einladungen versenden und Konten in der Organisation verwalten:

- Wenn Sie eine Einladung versenden, werden möglicherweise zugehörige Daten übertragen. AWS-Regionen Dies ist der Fall, weil Macie die E-Mail-Adresse des Empfängerkontos mithilfe eines E-Mail-Bestätigungsdienstes verifiziert, der nur in der Region USA Ost (Nord-Virginia) verfügbar ist.

- Sie können eine Einladung an alle aktiven Konten sendenAWS-Konto, auch an Konten, für die Macie nicht aktiviert wurde. Um eine Einladung anzunehmen oder abzulehnen, muss das Empfängerkonto jedoch Macie in der Region aktivieren, aus der die Einladung gesendet wurde.
- Ein Macie-Administratorkonto kann jeweils nicht mehr als 1.000 Konten zugeordnet werden. AWS-Region Dies schließt Konten ein, die noch nicht auf Einladungen geantwortet haben. Wenn Ihr Konto dieses Kontingent erfüllt, können Sie keine weiteren Konten hinzufügen oder einladen, bis Sie die erforderliche Anzahl verknüpfter Konten entfernt haben, die erforderliche Anzahl an abgelehnten Einladungen erhalten haben oder eine Kombination aus beidem erhalten haben.

  Um festzustellen, wie viele Konten derzeit mit Ihrem Konto verknüpft sind, können Sie die Seite Konten in der Amazon Macie Macie-Konsole oder den ListMembersBetrieb der Amazon Macie Macie-API verwenden. Weitere Informationen finden Sie unter Überprüfung von Amazon Macie Macie-Konten für eine Organisation, die auf Einladung basiert.
- Ein Konto kann jeweils nur einem Macie-Administratorkonto zugeordnet werden. Das bedeutet, dass ein Konto Ihre Einladung nicht annehmen kann, wenn es bereits mit einem anderen Macie-Administratorkonto verknüpft ist. Das Konto muss zuerst von seinem aktuellen Macie-Administratorkonto getrennt werden.
- In einer Organisation, die auf Einladung basiert, kann ein Mitgliedskonto jederzeit die Verbindung zu seinem Macie-Administratorkonto trennen. In diesem Fall bleibt Macie weiterhin für das Konto aktiviert und das Konto wird zu einem eigenständigen Macie-Konto. Macie benachrichtigt Sie nicht, wenn ein Mitgliedskonto von Ihrem Administratorkonto getrennt wird. Das Konto erscheint jedoch weiterhin in Ihrem Kontoinventar und hat den Status Mitglied gekündigt.
- Wenn Sie ein Mitgliedskonto aus Ihrer Organisation entfernen, ist Macie weiterhin für das Konto aktiviert und das Konto wird zu einem eigenständigen Macie-Konto.

Beantwortung und Verwaltung von Mitgliedschaftseinladungen

Als Empfänger einer Einladung oder als Mitglied einer Organisation, die auf Einladungen basiert, sollten Sie Folgendes beachten, wenn Sie auf Einladungen antworten und diese verwalten:

- Bevor Sie eine Einladung annehmen, stellen Sie sicher, dass Sie die Beziehung zwischen Macie-Administrator- und Mitgliedskonten verstehen.
- Ihr Konto kann jeweils nur einem Macie-Administratorkonto zugeordnet werden. Wenn Sie eine Einladung annehmen und anschließend einer anderen Organisation beitreten möchten (auf Einladung oder überAWS Organizations), müssen Sie zunächst die Verknüpfung Ihres Kontos

mit dem aktuellen Macie-Administratorkonto trennen. Sie können dann der anderen Organisation beitreten.

- Um eine Einladung anzunehmen oder abzulehnen, müssen Sie Macie in dem Ordner aktivieren, von dem AWS-Region die Einladung gesendet wurde. Das Konto, das die Einladung gesendet hat, kann Macie in dieser Region nicht für Sie aktivieren. Das Ablehnen einer Einladung ist optional. Wenn Sie eine Einladung ablehnen, können Sie Macie optional in der entsprechenden Region deaktivieren, nachdem Sie die Einladung abgelehnt haben.
- Wenn Sie ein Macie-Administrator sind, können Sie eine Einladung, ein Mitgliedskonto zu werden, nicht annehmen. Ein Konto kann nicht gleichzeitig Macie-Administrator und Mitgliedskonto sein. Um ein Mitgliedskonto zu werden, müssen Sie zunächst Ihr Konto von allen Mitgliedskonten trennen, indem Sie alle Mitgliedskonten aus Ihrer aktuellen Organisation entfernen.
- Macie ist ein regionaler Dienst. Wenn Sie eine Einladung annehmen, ist die Zuordnung zwischen Ihrem Konto und dem Macie-Administratorkonto regional — die Zuordnung besteht nur in demAWS-Region, von dem die Einladung gesendet und angenommen wurde.
- Wenn Sie Macie in mehreren Regionen verwenden, muss das Macie-Administratorkonto für Ihr Konto in all diesen Regionen identisch sein. Der Macie-Administrator muss Ihnen jedoch Einladungen in jeder Region separat senden, und Sie müssen die Einladungen in jeder Region separat annehmen.
- Sie können Ihr Konto jederzeit von einem Macie-Administratorkonto trennen. Wenn Sie dies tun, bleibt Macie weiterhin für Ihr Konto aktiviert und Ihr Konto wird zu einem eigenständigen Macie-Konto.
- Wenn Ihr Macie-Administrator Ihr Konto aus seiner Organisation entfernt, bleibt Macie weiterhin für Ihr Konto aktiviert und Ihr Konto wird zu einem eigenständigen Macie-Konto.

Übergang zu AWS Organizations

Nachdem Sie in Macie eine Organisation erstellt haben, die auf Einladung basiert, können Sie stattdessen verwenden. AWS Organizations Um den Übergang zu vereinfachen, empfehlen wir, dass Sie das bestehende, auf Einladung basierende Administratorkonto als Macie-Administratorkonto für die Organisation in festlegen. AWS Organizations

Wenn Sie dies tun, bleiben alle derzeit verknüpften Mitgliedskonten weiterhin Mitglieder. Wenn ein Mitgliedskonto Teil der Organisation istAWS Organizations, ändert sich die Zuordnung des Kontos automatisch von „Auf Einladung“ zu „Via AWS Organizations in Macie“. Wenn ein Mitgliedskonto nicht Teil der Organisation istAWS Organizations, in der es sich um ein Mitgliedskonto handelt, bleibt die

Zuordnung des Kontos weiterhin „Auf Einladung“. In beiden Fällen werden die Konten weiterhin als Mitgliedskonten mit dem Macie-Administratorkonto verknüpft.

Wir empfehlen diesen Ansatz, da ein Mitgliedskonto jeweils nur einem Macie-Administratorkonto zugeordnet werden kann. Wenn Sie ein anderes Konto als Macie-Administratorkonto für eine Organisation in festlegenAWS Organizations, kann der angegebene Administrator Konten, die bereits mit einem anderen Macie-Administratorkonto verknüpft sind, nicht per Einladung verwalten. Jedes Mitgliedskonto muss zunächst von seinem aktuellen Administratorkonto getrennt werden, das auf Einladung basiert. Erst dann kann der Macie-Administrator der AWS Organizations Organisation das Mitgliedskonto zu seiner Organisation hinzufügen und mit der Verwaltung von Macie für das Konto beginnen.

Nachdem Sie Macie in Macie integriert AWS Organizations und Ihre Organisation dort konfiguriert haben, können Sie optional ein anderes Macie-Administratorkonto für die Organisation festlegen. Sie können auch weiterhin Einladungen verwenden, um Mitgliedskonten zuzuordnen und zu verwalten, die nicht Teil Ihrer Organisation sind. AWS Organizations

Eine auf Einladung basierende Organisation in Amazon Macie erstellen und verwalten

Um eine Organisation auf Einladung in Amazon Macie zu erstellen, legen Sie zunächst fest, welches Konto Sie als Macie-Administratorkonto für die Organisation verwenden möchten. Anschließend verwenden Sie dieses Konto, um Mitgliedskonten hinzuzufügen. Sie senden Mitgliedschaftseinladungen an andere und laden die Konten einAWS-Konten, der Organisation als aktuelle Macie-Mitgliedskonten beizutreten. AWS-Region Um die Organisation in mehreren Regionen zu erstellen, senden Sie Mitgliedschaftseinladungen aus jeder Region, in der die anderen Konten Macie derzeit verwenden oder werden.

Wenn ein Konto eine Einladung annimmt, wird es zu einem Macie-Mitgliedskonto, das mit dem Macie-Administratorkonto in der entsprechenden Region verknüpft ist. Das Macie-Administratorkonto kann dann auf bestimmte Macie-Einstellungen, Daten und Ressourcen für das Mitgliedskonto in dieser Region zugreifen.

Als Macie-Administrator für eine Organisation, die auf Einladung basiert, können Sie die Inventardaten und Richtlinienergebnisse von Amazon Simple Storage Service (Amazon S3) für Mitgliedskonten überprüfen. Sie können auch eine automatische Erkennung sensibler Daten durchführen und Aufgaben zur Erkennung sensibler Daten ausführen, um sensible Daten in S3-Buckets zu erkennen, die Mitgliedskonten gehören. Eine ausführliche Liste der Aufgaben, die Sie

ausführen können, finden Sie unterDie Beziehung zwischen Amazon Macie-Administrator- und Mitgliedskonten verstehen.

Standardmäßig bietet Ihnen Macie Einblick in relevante Daten und Ressourcen für Ihr Unternehmen insgesamt. Sie können auch detaillierte Informationen zu Daten und Ressourcen für einzelne Konten in Ihrer Organisation abrufen. Wenn Sie beispielsweise das Übersichts-Dashboard verwenden, um den Amazon S3-Sicherheitsstatus Ihres Unternehmens zu bewerten, können Sie die Daten nach Konto filtern. Wenn Sie die geschätzten Nutzungskosten überwachen, können Sie auf ähnliche Weise auf Aufschlüsselungen der geschätzten Kosten für einzelne Mitgliedskonten zugreifen.

Zusätzlich zu den Aufgaben, die für Administrator- und Mitgliedskonten üblich sind, können Sie verschiedene Verwaltungsaufgaben für Ihr Unternehmen zentral ausführen. Bevor Sie diese Aufgaben ausführen, sollten Sie sich mit den Überlegungen und Empfehlungen zur Verwaltung von Organisationen, die auf Einladung basieren, in Macie vertraut machen.

Aufgaben

- Hinzufügen von Amazon Macie Macie-Mitgliedskonten zu einer Organisation, die auf Einladung basiert
- Sperren von Amazon Macie für Mitgliedskonten in einer Organisation, die auf Einladung basiert
- Amazon Macie Macie-Mitgliedskonten aus einer Organisation entfernen, die auf Einladung basiert
- Verknüpfungen mit anderen Konten werden gelöscht

Hinzufügen von Amazon Macie Macie-Mitgliedskonten zu einer Organisation, die auf Einladung basiert

Als Macie-Administrator für eine Organisation, die auf Einladung basiert, fügen Sie Ihrer Organisation Mitgliedskonten hinzu, indem Sie zwei Hauptschritte ausführen:

1. Fügen Sie die Konten Ihrem Kontoinventar in Macie hinzu. Dadurch werden die Konten Ihrem Konto zugeordnet.
2. Senden Sie Mitgliedschaftseinladungen an die Konten.

Wenn ein Konto Ihre Einladung annimmt, wird es zu einem Mitgliedskonto in Ihrer Organisation.

Schritt 1: Fügen Sie die Konten hinzu

Um Ihrem Kontobestand ein oder mehrere Konten hinzuzufügen, können Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden.

Console

Mit der Amazon Macie Macie-Konsole können Sie jeweils ein Konto hinzufügen oder mehrere Konten gleichzeitig hinzufügen, indem Sie eine Datei mit kommagetrennten Werten (CSV) hochladen. Gehen Sie wie folgt vor, um mithilfe der Konsole ein oder mehrere Konten hinzuzufügen.

Um ein Konto hinzuzufügen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie ein Konto hinzufügen möchten.
3. Klicken Sie im Navigationsbereich unter Settings auf Accounts.
4. Klicken Sie auf Add accounts.
5. Wählen Sie im Abschnitt Kontodetails eingeben die Registerkarte Konto hinzufügen. Führen Sie dann die folgenden Schritte aus:
   - Geben Sie unter Konto-ID die 12-stellige Konto-ID ein, die hinzugefügt AWS-Konto werden soll.
   - Geben Sie unter E-Mail-Adresse die E-Mail-Adresse ein, die hinzugefügt AWS-Konto werden soll.
6. Wählen Sie Hinzufügen und dann Weiter.

Macie fügt das Konto Ihrem Kontoinventar hinzu. Der Kontotyp ist Auf Einladung und der Status lautet Erstellt. Wiederholen Sie die vorherigen Schritte in jeder weiteren Region, in der Sie das Konto hinzufügen möchten.

Um mehrere Konten hinzuzufügen

1. Erstellen Sie mithilfe eines Texteditors eine CSV-Datei wie folgt:
   a. Fügen Sie den folgenden Header als erste Zeile der Datei hinzu: `Account ID,Email`

b. Erstellen Sie für jedes Konto eine neue Zeile mit der 12-stelligen Konto-ID für das AWS-Konto hinzuzufügende Konto und der E-Mail-Adresse für das Konto. Trennen Sie die Einträge durch ein Komma, zum Beispiel: `111111111111,janedoe@example.com`

   Die E-Mail-Adresse muss mit der E-Mail-Adresse übereinstimmen, die dem AWS-Konto zugeordnet ist.

c. Stellen Sie sicher, dass der Inhalt der Datei wie im folgenden Beispiel formatiert ist, das den erforderlichen Header und die erforderlichen Informationen für drei Konten enthält:

```
Account ID,Email
111111111111,janedoe@example.com
222222222222,jorgesouza@example.com
333333333333,lijuan@example.com
```

d. Speichern Sie die Datei auf Ihrem Computer.

2. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
3. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie die Konten hinzufügen möchten.
4. Klicken Sie im Navigationsbereich unter Settings auf Accounts.
5. Klicken Sie auf Add accounts.
6. Wählen Sie im Abschnitt Kontodetails eingeben den Tab Liste hochladen (CSV) aus.
7. Wählen Sie Durchsuchen und wählen Sie dann die CSV-Datei aus, die Sie in Schritt 1 erstellt haben.
8. Wählen Sie Konten hinzufügen und dann Weiter aus.

Macie fügt die Konten zu Ihrem Kontoinventar hinzu. Ihr Typ ist Auf Einladung und ihr Status ist Erstellt. Wiederholen Sie die Schritte 3 bis 8 in jeder weiteren Region, in der Sie die Konten hinzufügen möchten.

API

Um ein oder mehrere Konten programmgesteuert hinzuzufügen, verwenden Sie den CreateMemberBetrieb der Amazon Macie Macie-API. Wenn Sie Ihre Anfrage einreichen, verwenden Sie die unterstützten Parameter, um die 12-stellige Konto-ID und E-Mail-Adresse für jedes hinzuzufügende Konto anzugeben. AWS-Konto Geben Sie auch die Region an, für die sich die Anfrage bezieht. Um Konten in weiteren Regionen hinzuzufügen, reichen Sie die Anfrage in jeder weiteren Region ein.

Um Konten mithilfe von AWS Command Line Interface(AWS CLI) hinzuzufügen, führen Sie den Befehl create-member aus. Verwenden Sie den `region` Parameter, um die Region anzugeben, in der die Konten hinzugefügt werden sollen. Verwenden Sie die `account` Parameter, um die Konto-ID und die E-Mail-Adresse für jedes AWS-Konto hinzuzufügende Konto anzugeben. Beispiele:

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"111111111111\",\"email\":\"janedoe@example.com\"}
```

Dabei ist *us-east-1* die Region, in der das Konto hinzugefügt werden soll (Region USA Ost (Nord-Virginia)), und die `account` Parameter geben die Konto-ID (*111111111111*) und die E-Mail-Adresse (*janedoe@example.com*) für das hinzuzufügende Konto an.

Wenn Ihre Anfrage erfolgreich ist, fügt Macie Ihrem Kontobestand jedes Konto mit dem Status hinzu und Sie erhalten eine Ausgabe, die der `Created` folgenden ähnelt:

```
{
    "arn": "arn:aws:macie2:us-east-1:123456789012:member/111111111111"
}
```

Wo `arn` ist der Amazon-Ressourcenname (ARN) der Ressource, die für die Verknüpfung zwischen Ihrem Konto und dem Konto, das Sie hinzugefügt haben, erstellt wurde. In diesem Beispiel `123456789012` ist dies die Konto-ID für das Konto, mit dem die Verknüpfung erstellt wurde, und `111111111111` die Konto-ID für das Konto, das hinzugefügt wurde.

Schritt 2: Senden Sie Mitgliedschaftseinladungen an die Konten

Nachdem Sie Ihrem Kontobestand ein Konto hinzugefügt haben, können Sie das Konto einladen, Ihrer Organisation als Macie-Mitgliedskonto beizutreten. Senden Sie dazu eine Einladung zur Mitgliedschaft an das Konto. Wenn Sie eine Einladung versenden, werden ein Konto-Badge und eine Benachrichtigung auf der Amazon Macie Macie-Konsole für das Konto des Empfängers angezeigt, sofern Macie für das Konto aktiviert ist. Macie erstellt auch ein AWS Health Ereignis für das Konto.

Je nachdem, ob Sie die Amazon Macie Macie-Konsole oder die API zum Senden der Einladung verwenden, sendet Macie die Einladung auch an die E-Mail-Adresse, die Sie beim Hinzufügen des Kontos für das Konto des Empfängers angegeben haben. Die E-Mail-Nachricht gibt an, dass Sie der Macie-Administrator für ihr Konto werden möchten, und sie enthält die Konto-ID für Sie AWS-Konto und die des Empfängers. AWS-Konto In der Nachricht wird auch erklärt, wie Sie auf die Einladung zugreifen können. Sie können der Nachricht optional benutzerdefinierten Text hinzufügen.

Um eine Mitgliedschaftseinladung an ein oder mehrere Konten zu senden, können Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden.

Console

Gehen Sie wie folgt vor, um mithilfe der Amazon Macie Macie-Konsole eine Einladung zur Mitgliedschaft zu senden.

Um eine Einladung zur Mitgliedschaft zu versenden

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in die Sie die Einladung versenden möchten.
3. Klicken Sie im Navigationsbereich unter Settings auf Accounts.
4. Aktivieren Sie in der Tabelle Konten das Kontrollkästchen für jedes Konto, an das Sie die Einladung senden möchten.

   > **Tip**
   >
   > Um Konten, die Sie hinzugefügt haben und an die Sie noch keine Einladungen gesendet haben, leichter identifizieren zu können, können Sie die Tabelle filtern. Platzieren Sie dazu den Cursor in dem Filterfeld über der Tabelle und wählen Sie dann Status aus. Wählen Sie dann Status = Erstellt.

5. Wählen Sie im Menü Aktionen die Option Einladen aus.
6. (Optional) Geben Sie im Feld Nachricht einen beliebigen benutzerdefinierten Text ein, den Sie in die E-Mail-Nachricht mit der Einladung aufnehmen möchten. Der Text kann bis zu 80 alphanumerische Zeichen enthalten.
7. Klicken Sie auf Invite.

Um die Einladung zusätzlich zu versendenAWS-Regionen, wiederholen Sie die vorherigen Schritte in jeder weiteren Region.

Nachdem Sie die Einladung gesendet haben, ändert sich der Status eines Empfängerkontos in Ihrem Kontobestand auf E-Mail-Bestätigung läuft. Wenn Macie die E-Mail-Adresse eines Accounts verifizieren kann, ändert sich der Status des Accounts anschließend auf Eingeladen. Wenn Macie die Adresse nicht verifizieren kann, ändert sich der Status des Kontos in „E-Mail-Bestätigung“. In diesem Fall wenden Sie sich an den Kontoinhaber, um die richtige E-Mail-Adresse zu erhalten.

Löschen Sie dann die Verknüpfung zwischen Ihren Konten, fügen Sie das Konto erneut hinzu und senden Sie die Einladung erneut.

Wenn ein Empfänger eine Einladung annimmt, ändert sich der Status des Empfängerkontos in Ihrem Kontoinventar auf Aktiviert. Wenn ein Empfänger eine Einladung ablehnt, wird das Konto des Empfängers von Ihrem Konto getrennt und aus Ihrem Kontobestand entfernt.

API

Verwenden Sie den CreateInvitationsBetrieb der Amazon Macie Macie-API, um eine Einladung programmgesteuert zu versenden. Wenn Sie Ihre Anfrage einreichen, geben Sie mithilfe der unterstützten Parameter jeweils die 12-stellige Konto-ID an, an die die Einladung gesendet AWS-Konto werden soll. Eine Konto-ID muss mit der Konto-ID für ein Konto in Ihrem Kontobestand übereinstimmen. Andernfalls tritt ein Fehler auf. Geben Sie auch die Region an, aus der die Einladung gesendet werden soll. Um die Einladung aus weiteren Regionen zu versenden, reichen Sie die Anfrage in jeder weiteren Region ein.

In Ihrer Anfrage können Sie auch angeben, ob die Einladung als E-Mail-Nachricht gesendet werden soll und ob diese Nachricht benutzerdefinierten Text enthalten soll. Wenn Sie sich dafür entscheiden, eine E-Mail-Nachricht zu senden, sendet Macie die Einladung an die E-Mail-Adresse, die Sie für ein Konto angegeben haben, als Sie das Konto zu Ihrem Kontobestand hinzugefügt haben. Um die Einladung als E-Mail-Nachricht zu versenden, lassen Sie den `disableEmailNotification` Parameter weg oder setzen Sie den Wert für den Parameter auf. `false` (Der Standardwert ist `false`.) Um der Nachricht benutzerdefinierten Text hinzuzufügen, verwenden Sie den `message` Parameter, um den hinzuzufügenden Text anzugeben. Der Text kann bis zu 80 alphanumerische Zeichen enthalten.

Um Einladungen mit dem zu versendenAWS CLI, führen Sie den Befehl create-invitations aus. Verwenden Sie den `region` Parameter, um die Region anzugeben, aus der die Einladung gesendet werden soll. Verwenden Sie den `account-ids` Parameter, um die Konto-ID für jedes Konto anzugebenAWS-Konto, an das die Einladung gesendet werden soll. Beispiele:

```
C:\> aws macie2 create-invitations --region us-east-1 --account-
ids=[\"111111111111\",\"222222222222\",\"333333333333\"]
```

Dabei ist *`us-east-1`* die Region, aus der die Einladung gesendet werden soll (Region USA Ost (Nord-Virginia)), und der `account-ids` Parameter gibt die Konto-IDs für drei Konten an, an die die Einladung gesendet werden soll. Um eine Einladung auch als E-Mail-Nachricht zu senden, geben Sie auch den `no-disable-email-notification` Parameter an und fügen

Sie optional den `message` Parameter hinzu, um benutzerdefinierten Text anzugeben, der der Nachricht hinzugefügt werden soll.

Nachdem Sie die Einladung gesendet haben, ändert sich der Status jedes Empfängerkontos auf`EmailVerificationInProgress`. Wenn Macie die E-Mail-Adresse eines Kontos verifizieren kann, ändert sich der Status des Kontos anschließend auf`Invited`. Wenn Macie die Adresse nicht verifizieren kann, ändert sich der Status des Kontos auf. `EmailVerificationFailed` In diesem Fall wenden Sie sich an den Kontoinhaber, um die richtige Adresse zu ermitteln. Löschen Sie dann die Verknüpfung zwischen Ihren Konten, fügen Sie das Konto erneut hinzu und senden Sie die Einladung erneut.

Wenn ein Empfänger eine Einladung annimmt, ändert sich der Status des Kontos des Empfängers `Enabled` in Ihrem Kontoinventar. Wenn ein Empfänger eine Einladung ablehnt, wird das Konto des Empfängers von Ihrem Konto getrennt und aus Ihrem Kontobestand entfernt.

Sperren von Amazon Macie für Mitgliedskonten in einer Organisation, die auf Einladung basiert

Als Macie-Administrator einer Organisation können Sie Macie nur AWS-Region für einzelne Mitgliedskonten in Ihrer Organisation sperren. Beachten Sie jedoch, dass Sie Macie für ein Mitgliedskonto nicht wieder aktivieren können, nachdem Sie es gesperrt haben. Nur ein Benutzer des Kontos kann Macie anschließend für das Konto wieder aktivieren.

Wenn Sie Macie für ein Mitgliedskonto sperren:

- Macie verliert den Zugriff auf die Amazon S3 S3-Daten des Kontos in der Region und stellt keine Metadaten mehr bereit.
- Macie beendet die Ausführung aller Aktivitäten für das Konto in der Region. Dazu gehören die Überwachung von S3-Buckets im Hinblick auf Sicherheit und Zugriffskontrolle, die automatische Erkennung sensibler Daten und die Ausführung von Aufgaben zur Erkennung sensibler Daten, die derzeit ausgeführt werden.
- Macie storniert alle Aufträge zur Erkennung sensibler Daten, die von dem Konto in der Region erstellt wurden. Ein Auftrag kann nicht wieder aufgenommen oder neu gestartet werden, nachdem er storniert wurde.

  Wenn Sie Jobs zur Analyse von Daten erstellt haben, die dem Mitgliedskonto gehören, storniert Macie diese Jobs nicht. Stattdessen werden bei den Jobs Ressourcen übersprungen, die dem Konto gehören.

Solange ein Konto gesperrt ist, behält Macie die Macie-Sitzungs-ID, die Einstellungen und Ressourcen für das Konto in der entsprechenden Region. Beispielsweise bleiben die Ergebnisse des Kontos erhalten und sind bis zu 90 Tage lang nicht betroffen. Dem Konto werden keine Gebühren für die Nutzung von Macie in der entsprechenden Region berechnet, während Macie für das Konto in dieser Region gesperrt ist.

Um Macie für ein Mitgliedskonto in einer Organisation zu sperren, die auf Einladung basiert

Um Macie für ein Mitgliedskonto in einer Organisation, die auf Einladung basiert, zu sperren, können Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden.

Console

Gehen Sie wie folgt vor, um Macie mithilfe der Amazon Macie Macie-Konsole für ein Mitgliedskonto zu sperren.

Um Macie für ein Mitgliedskonto zu sperren

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie Macie für ein Mitgliedskonto sperren möchten.
3. Klicken Sie im Navigationsbereich unter Settings auf Accounts.
4. Wählen Sie in der Tabelle Konten das Kontrollkästchen für das Konto aus, das gesperrt werden soll.
5. Wählen Sie im Menü Aktionen die Option Macie sperren aus.
6. Bestätigen Sie, dass Sie Macie für das ausgewählte Konto sperren möchten.

Nachdem du die Sperrung bestätigt hast, ändert sich der Status des Accounts in deinem Kontobestand auf Pausiert (gesperrt).

Wiederhole die vorherigen Schritte in jeder weiteren Region, in der du Macie für das Konto sperren möchtest.

API

Um Macie für ein Mitgliedskonto programmgesteuert zu sperren, verwenden Sie den UpdateMemberSessionBetrieb der Amazon Macie Macie-API. Wenn Sie Ihre Anfrage einreichen, verwenden Sie den `id` Parameter, um die 12-stellige Konto-ID des Kontos anzugeben, für AWS-Konto das Sie Macie sperren möchten. Geben Sie `PAUSED` als `status` Parameter den neuen

Status für das Macie-Konto an. Geben Sie auch die Region an, für die sich die Anfrage bezieht. Um Macie in weiteren Regionen zu sperren, reichen Sie Ihre Anfrage in jeder weiteren Region ein.

Um die Konto-ID für das Mitgliedskonto abzurufen, können Sie den ListMembersBetrieb der Amazon Macie Macie-API verwenden. Wenn Sie dies tun, sollten Sie erwägen, die Ergebnisse zu filtern, indem Sie den `onlyAssociated` Parameter in Ihre Anfrage aufnehmen. Wenn Sie den Wert dieses Parameters auf setzen`true`, gibt Macie ein `members` Array zurück, das nur Details zu den Konten enthält, die derzeit Mitgliedskonten für Ihr Administratorkonto sind.

Um Macie für ein Mitgliedskonto mithilfe von zu sperrenAWS CLI, führen Sie den update-member-sessionBefehl aus. Verwenden Sie den `region` Parameter, um die Region anzugeben, in der Macie gesperrt werden soll, und verwenden Sie den `id` Parameter, um die Konto-ID für das Konto anzugeben, für das Macie gesperrt werden soll. Geben Sie für den `status` Parameter an. `PAUSED` Beispiele:

```
C:\> aws macie2 update-member-session --region us-east-1 --id 123456789012 --status
 PAUSED
```

Dabei ist *`us-east-1`* die Region, in der Macie gesperrt werden soll (Region USA Ost (Nord-Virginia)), *`123456789012`* ist die Konto-ID für das Konto, für das Macie gesperrt werden soll, und `PAUSED` ist der neue Macie-Status für das Konto.

Wenn Ihre Anfrage erfolgreich ist, gibt Macie eine leere Antwort zurück und der Status des angegebenen Kontos ändert sich in Ihrem Kontobestand. `Paused`

Amazon Macie Macie-Mitgliedskonten aus einer Organisation entfernen, die auf Einladung basiert

Als Macie-Administrator können Sie ein Mitgliedskonto aus Ihrer Organisation entfernen. Dazu trennen Sie das Konto von Ihrem Macie-Administratorkonto.

Wenn Sie ein Mitgliedskonto entfernen, ist Macie weiterhin für das Konto aktiviert und das Konto erscheint weiterhin in Ihrem Kontoinventar. Das Konto wird jedoch zu einem eigenständigen Macie-Konto. Macie benachrichtigt den Kontoinhaber nicht, wenn Sie das Konto entfernen. Erwägen Sie daher, den Kontoinhaber zu kontaktieren, um sicherzustellen, dass er mit der Verwaltung der Einstellungen und Ressourcen für sein Konto beginnt.

Wenn Sie ein Mitgliedskonto entfernen, verlieren Sie den Zugriff auf alle Macie-Einstellungen, Ressourcen und Daten für das Konto. Dazu gehören politische Ergebnisse und Metadaten für S3-

Buckets, die dem Konto gehören. Darüber hinaus können Sie Macie nicht mehr verwenden, um sensible Daten in S3-Buckets zu ermitteln, die dem Konto gehören. Wenn Sie zu diesem Zweck bereits Aufträge zur Erkennung sensibler Daten erstellt haben, überspringen die Jobs Buckets, die dem Konto gehören.

Nachdem Sie ein Mitgliedskonto entfernt haben, können Sie es anschließend wieder zu Ihrer Organisation hinzufügen, indem Sie eine neue Einladung an das Konto senden. Sie können es auch vollständig aus Ihrem Kontoinventar entfernen, indem Sie die Verknüpfung zwischen Ihren Konten löschen.

So entfernen Sie ein Mitgliedskonto aus einer Organisation, die auf Einladung basiert

Um ein Mitgliedskonto aus Ihrer Organisation zu entfernen, können Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden.

Console

Gehen Sie wie folgt vor, um ein Mitgliedskonto mithilfe der Amazon Macie Macie-Konsole zu entfernen.

Um ein Mitgliedskonto zu entfernen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie das Mitgliedskonto entfernen möchten.
3. Klicken Sie im Navigationsbereich unter Settings auf Accounts.
4. Aktivieren Sie in der Tabelle Konten das Kontrollkästchen für das Konto, das Sie entfernen möchten.
5. Wählen Sie im Menü Aktionen die Option Konto trennen aus.
6. Bestätigen Sie, dass Sie das ausgewählte Konto als Mitgliedskonto entfernen möchten.

Nachdem Sie Ihre Auswahl bestätigt haben, ändert sich der Status des Kontos in Ihrem Kontobestand auf Entfernt (getrennt).

Wiederholen Sie die vorherigen Schritte in jeder weiteren Region, in der Sie das Mitgliedskonto entfernen möchten.

API

Verwenden Sie die Amazon Macie Macie-API, um ein Mitgliedskonto programmgesteuert zu entfernen. DisassociateMember Wenn Sie Ihre Anfrage einreichen, geben Sie mithilfe des `id` Parameters die 12-stellige AWS-Konto ID für das Mitgliedskonto an, das entfernt werden soll. Geben Sie auch die Region an, für die sich die Anfrage bezieht. Um das Konto in weiteren Regionen zu entfernen, reichen Sie Ihre Anfrage in jeder weiteren Region ein.

Um die Konto-ID für das zu entfernende Konto abzurufen, können Sie den ListMembersBetrieb der Amazon Macie Macie-API verwenden. Wenn Sie dies tun, sollten Sie erwägen, die Ergebnisse zu filtern, indem Sie den `onlyAssociated` Parameter in Ihre Anfrage aufnehmen. Wenn Sie den Wert dieses Parameters auf setzen`true`, gibt Macie ein `members` Array zurück, das nur Details zu den Konten enthält, die derzeit Mitgliedskonten für Ihr Konto sind.

Um ein Mitgliedskonto mithilfe von zu entfernenAWS CLI, führen Sie den Befehl disassociate-member aus. Verwenden Sie den `region` Parameter, um die Region anzugeben, in der das Konto entfernt werden soll. Verwenden Sie den `id` Parameter, um die Konto-ID für das zu entfernende Konto anzugeben. Beispiele:

```
C:\> aws macie2 disassociate-member --region us-east-1 --id 123456789012
```

Dabei ist *`us-east-1`* die Region, in der das Konto entfernt werden soll (Region USA Ost (Nord-Virginia)), und *`123456789012`* ist die Konto-ID für das zu entfernende Konto.

Wenn Ihre Anfrage erfolgreich ist, gibt Macie eine leere Antwort zurück und der Status des angegebenen Kontos ändert sich in Ihrem Kontobestand. `Removed`

Verknüpfungen mit anderen Konten werden gelöscht

Nachdem Sie Ihrem Kontobestand ein Konto hinzugefügt haben, können Sie die Verknüpfung zwischen Ihrem Konto und dem anderen Konto löschen. Du kannst dies für jedes Konto in deinem Inventar tun, mit Ausnahme von:

- Ein Konto, das Teil Ihrer Organisation in istAWS Organizations. Diese Art der Zuordnung wird AWS Organizations nicht von Macie gesteuert.
- Ein Mitgliedskonto, das eine Einladung einer Macie-Mitgliedschaft zum Beitritt zu Ihrer Organisation akzeptiert hat. In diesem Fall müssen Sie das Mitgliedskonto entfernen, bevor Sie die Assoziation löschen können.

Wenn Sie eine Assoziation löschen, entfernt Macie das Konto aus Ihrem Kontoinventar. Wenn Sie die Zuordnung anschließend wiederherstellen möchten, müssen Sie das Konto erneut hinzufügen, als wäre es ein völlig neues Konto.

Um eine Verknüpfung mit einem anderen Konto zu löschen

Um eine Verknüpfung zwischen Ihrem Konto und einem anderen Konto zu löschen, können Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden.

Console

Gehen Sie wie folgt vor, um die Amazon Macie Macie-Konsole zum Löschen einer Verknüpfung mit einem anderen Konto zu verwenden.

Löschen einer Zuordnung

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie die Zuordnung löschen möchten.
3. Klicken Sie im Navigationsbereich unter Settings auf Accounts.
4. Aktivieren Sie in der Tabelle Konten das Kontrollkästchen für das Konto, dessen Zuordnung Sie löschen möchten.
5. Wählen Sie im Menü Aktionen die Option Konto löschen aus.
6. Bestätigen Sie, dass Sie die ausgewählte Zuordnung löschen möchten.

Wiederholen Sie die vorherigen Schritte in jeder weiteren Region, in der Sie die Zuordnung löschen möchten.

API

Verwenden Sie die Amazon Macie Macie-API, um eine Verknüpfung mit einem anderen Konto programmgesteuert zu löschen. DeleteMember Wenn Sie Ihre Anfrage einreichen, verwenden Sie den `id` Parameter, um die 12-stellige Konto-ID anzugeben, mit der die Verknüpfung gelöscht AWS-Konto werden soll. Geben Sie auch die Region an, für die sich die Anfrage bezieht. Um die Zuordnung in weiteren Regionen zu löschen, reichen Sie Ihre Anfrage in jeder weiteren Region ein.

Um die Konto-ID für das Konto abzurufen, können Sie den ListMembersBetrieb der Amazon Macie Macie-API verwenden. Wenn Sie dies tun, nehmen Sie den `onlyAssociated` Parameter

in Ihre Anfrage auf und setzen Sie den Wert des Parameters auf`false`. Wenn der Vorgang erfolgreich ist, gibt Macie ein `members` Array zurück, das Details zu allen Konten enthält, die mit Ihrem Konto verknüpft sind, einschließlich Konten, die derzeit keine Mitgliedskonten sind.

Um eine Verknüpfung mit einem anderen Konto mithilfe von zu löschenAWS CLI, führen Sie den Befehl delete-member aus. Verwenden Sie den `region` Parameter, um die Region anzugeben, in der die Zuordnung gelöscht werden soll, und den `id` Parameter, um die Konto-ID für das Konto anzugeben. Beispiele:

```
C:\> aws macie2 delete-member --region us-east-1 --id 123456789012
```

Dabei ist *`us-east-1`* die Region, in der die Verknüpfung mit dem anderen Konto gelöscht werden soll (Region USA Ost (Nord-Virginia)), und *`123456789012`* ist die Konto-ID für das Konto.

Wenn Ihre Anfrage erfolgreich ist, gibt Macie eine leere Antwort zurück und die Verknüpfung zwischen Ihrem Konto und dem anderen Konto wird gelöscht. Das zuvor verknüpfte Konto wird aus Ihrem Kontoinventar entfernt.

Überprüfung von Amazon Macie Macie-Konten für eine Organisation, die auf Einladung basiert

Um Ihnen bei der Verwaltung der Konten in Ihrer Organisation zu helfen, bietet Amazon Macie eine Bestandsaufnahme der Konten, die mit Ihrem Macie-Konto verknüpft sind, in allen Ländern, in AWS-Region denen Sie Macie verwenden. Mithilfe dieses Inventars können Sie den Status einzelner Konten sowie Kontostatistiken und -details für Ihre Organisation überprüfen. Sie können auch den Status der Beziehung zwischen Ihrem Konto und einzelnen Konten verwalten.

Um Konten für eine Organisation zu überprüfen, die auf Einladung basiert

Um die Konten in Ihrer Organisation zu überprüfen, können Sie die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden.

Console

Gehen Sie wie folgt vor, um die Konten Ihrer Organisation mithilfe der Amazon Macie Macie-Konsole zu überprüfen.

Um die Konten Ihrer Organisation zu überprüfen

1. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie die Konten Ihrer Organisation überprüfen möchten.
3. Klicken Sie im Navigationsbereich unter Settings auf Accounts.

Die Seite Konten wird geöffnet. Dort werden aggregierte Statistiken und eine Tabelle der Konten angezeigt, die derzeit mit Ihrem Macie-Konto verknüpft sind. AWS-Region

Oben auf der Kontoseite finden Sie die folgenden aggregierten Statistiken.

Über AWS Organizations

Wenn Sie der Macie-Administrator für eine Organisation in sindAWS Organizations, meldet Active die Gesamtzahl der Konten, die mit Ihrem Konto verknüpft sind AWS Organizations und derzeit Macie-Mitgliedskonten in Ihrer Organisation sind. Macie ist für diese Konten aktiviert und Sie sind der Macie-Administrator der Konten.

Alle meldet die Gesamtzahl der Konten, die mit Ihrem Konto verknüpft sindAWS Organizations, einschließlich Konten, bei denen es sich derzeit nicht um Macie-Mitgliedskonten handelt.

Auf Einladung

Aktiv meldet die Gesamtzahl der Konten, bei denen es sich derzeit um Macie-Mitgliedskonten in Ihrer Organisation handelt, die auf Einladung basiert. Macie ist für diese Konten aktiviert und Sie sind der Macie-Administrator der Konten, weil sie eine Mitgliedschaftseinladung von Ihnen angenommen haben.

Alle meldet die Gesamtzahl der Konten, die auf Einladung von Macie mit Ihrem Konto verknüpft wurden, einschließlich Konten, die nicht auf eine Einladung von Ihnen geantwortet haben.

Aktiv/Alle

Aktiv meldet die Gesamtzahl der Konten, die derzeit Macie-Mitgliedskonten für Ihr Konto sind, entweder durch AWS Organizations oder durch Einladung. Macie ist für diese Konten aktiviert und Sie sind der Macie-Administrator der Konten.

Alle meldet die Gesamtzahl der Konten, die entweder durch AWS Organizations oder durch Einladung mit Ihrem Konto verknüpft sind. Dies schließt Konten ein, die keine Einladung zur Macie-Mitgliedschaft von Ihnen angenommen haben. Dies schließt auch Konten ein, die über Macie-Mitgliedskonten mit Ihrem Konto verknüpft sind AWS Organizations und derzeit keine sind.

In der Tabelle finden Sie Einzelheiten zu den einzelnen Konten in der aktuellen Region. Die Tabelle enthält alle Konten, die mit Ihrem Macie-Konto verknüpft sind, entweder auf Einladung von Macie oder über. AWS Organizations

Konto-ID

Die Konto-ID und E-Mail-Adresse für dieAWS-Konto.

Name

Der Kontoname für dieAWS-Konto. Dieser Wert ist in der Regel N/A für Konten, die Ihrem Konto auf Einladung zugeordnet wurden.

Typ

Wie das Konto mit Ihrem Konto verknüpft ist, entweder auf Einladung oder überAWS Organizations.

Status

Der Status der Beziehung zwischen Ihrem Konto und dem Konto. Für ein Konto in einer Organisation, die auf Einladung basiert (Typ ist Auf Einladung) sind folgende Werte möglich:

- Konto gesperrt — Das AWS-Konto ist gesperrt.
- Erstellt (Einladung) — Sie haben das Konto hinzugefügt, ihm aber keine Einladung zur Mitgliedschaft gesendet.
- E-Mail-Überprüfung fehlgeschlagen — Sie haben versucht, eine Einladung zur Mitgliedschaft an das Konto zu senden, aber die angegebene E-Mail-Adresse ist für das Konto nicht gültig.
- E-Mail-Überprüfung läuft — Sie haben eine Einladung zur Mitgliedschaft an das Konto gesendet und Macie bearbeitet die Anfrage.
- Aktiviert — Das Konto ist ein Mitgliedskonto. Macie ist für das Konto aktiviert und Sie sind der Macie-Administrator des Kontos.
- Eingeladen — Sie haben eine Einladung zur Mitgliedschaft an das Konto gesendet und das Konto hat nicht auf Ihre Einladung geantwortet.

- Mitglied hat gekündigt — Das Konto war zuvor ein Mitgliedskonto. Das Konto hat sich jedoch von Ihrer Organisation zurückgezogen, indem es die Verbindung zu Ihrem Konto getrennt hat.
- Pausiert (gesperrt) — Das Konto ist ein Mitgliedskonto, aber Macie ist derzeit für dieses Konto gesperrt.
- Region deaktiviert — Die aktuelle Region ist deaktiviert für. AWS-Konto
- Entfernt (Verbindung aufgehoben) — Das Konto war zuvor ein Mitgliedskonto. Sie haben es jedoch als Mitgliedskonto entfernt, indem Sie es von Ihrem Konto getrennt haben.

Letzte Aktion

Wann Sie oder das zugehörige Konto zuletzt eine Aktion ausgeführt haben, die sich auf die Beziehung zwischen Ihren Konten ausgewirkt hat.

Um die Tabelle nach einem bestimmten Feld zu sortieren, klicken Sie auf die Spaltenüberschrift für das Feld. Um die Sortierreihenfolge zu ändern, klicken Sie erneut auf die Spaltenüberschrift. Um die Tabelle zu filtern, platzieren Sie den Cursor in das Filterfeld und fügen Sie dann eine Filterbedingung für ein Feld hinzu. Um die Ergebnisse weiter zu verfeinern, fügen Sie Filterbedingungen für weitere Felder hinzu.

API

Um die Konten Ihrer Organisation programmgesteuert zu überprüfen, verwenden Sie den ListMembersBetrieb der Amazon Macie Macie-API und geben Sie unbedingt die Region an, für die Ihre Anfrage gilt. Um die Details in weiteren Regionen zu überprüfen, reichen Sie Ihre Anfrage in jeder weiteren Region ein.

Wenn Sie Ihre Anfrage einreichen, verwenden Sie den `onlyAssociated` Parameter, um anzugeben, welche Konten in die Antwort aufgenommen werden sollen. Standardmäßig gibt Macie nur Details zu den Konten zurück, bei denen es sich um Mitgliedskonten in der angegebenen Region handelt, entweder auf Einladung oder überAWS Organizations. Um die Details aller zugehörigen Konten abzurufen, einschließlich Konten, die keine Mitgliedskonten sind, nehmen Sie den `onlyAssociated` Parameter in Ihre Anfrage auf und setzen Sie den Wert des Parameters auf`false`.

Um die Konten Ihrer Organisation mithilfe von AWS Command Line Interface(AWS CLI) zu überprüfen, führen Sie den Befehl list-members aus. Geben Sie für den `only-associated` Parameter an, ob alle zugehörigen Konten oder nur Mitgliedskonten berücksichtigt werden sollen. Um nur Mitgliedskonten einzubeziehen, lassen Sie diesen Parameter weg oder setzen Sie den

Wert des Parameters auf`true`. Um alle Konten einzubeziehen, legen Sie diesen Wert auf `false` fest. Beispiele:

```
C:\> aws macie2 list-members --region us-east-1 --only-associated false
```

Dabei ist *`us-east-1`* die Region, für die sich die Anfrage bezieht, die Region USA Ost (Nord-Virginia).

Wenn Ihre Anfrage erfolgreich ist, gibt Macie ein Array zurück. `members` Das Array enthält ein `member` Objekt für jedes Konto, das die in der Anfrage angegebenen Kriterien erfüllt. In diesem Objekt gibt das `relationshipStatus` Feld den aktuellen Status der Verknüpfung zwischen Ihrem Konto und dem anderen Konto in der angegebenen Region an. Für ein Konto in einer Organisation, die auf Einladung basiert, sind folgende Werte möglich:

- `AccountSuspended`— Das AWS-Konto ist gesperrt.
- `Created`— Sie haben das Konto hinzugefügt, ihm aber keine Einladung zur Mitgliedschaft gesendet.
- `EmailVerificationFailed`— Sie haben versucht, eine Einladung zur Mitgliedschaft an das Konto zu senden, aber die angegebene E-Mail-Adresse ist für das Konto nicht gültig.
- `EmailVerificationInProgress`— Sie haben eine Einladung zur Mitgliedschaft an das Konto gesendet und Macie bearbeitet die Anfrage.
- `Enabled`— Das Konto ist ein Mitgliedskonto. Macie ist für das Konto aktiviert und Sie sind der Macie-Administrator des Kontos.
- `Invited`— Sie haben eine Einladung zur Mitgliedschaft an das Konto gesendet und das Konto hat nicht auf Ihre Einladung geantwortet.
- `Paused`— Das Konto ist ein Mitgliedskonto, aber Macie ist derzeit für das Konto gesperrt (pausiert).
- `RegionDisabled`— Die aktuelle Region ist deaktiviert für. AWS-Konto
- `Removed`— Das Konto war zuvor ein Mitgliedskonto. Sie haben es jedoch als Mitgliedskonto entfernt, indem Sie es von Ihrem Konto getrennt haben.
- `Resigned`— Das Konto war zuvor ein Mitgliedskonto. Das Konto hat sich jedoch von Ihrer Organisation zurückgezogen, indem es die Verbindung zu Ihrem Konto getrennt hat.

Informationen zu anderen Feldern im `member` Objekt finden Sie unter Mitglieder in der Amazon Macie API-Referenz.

Benennen eines anderen Amazon Macie-Administratorkontos für eine Organisation, die auf Einladung basiert

Nachdem Sie eine Organisation auf Einladung erstellt und eingerichtet haben, können Sie das Amazon Macie-Administratorkonto für die Organisation ändern. Zu diesem Zweck sollten Administratoren und Mitglieder der Organisation die folgenden Schritte ausführen:

1. Der aktuelle Macie-Administrator exportiert optional das aktuelle Inventar der aktiven Mitgliedskonten für die Organisation. Dies vereinfacht den Übergang, indem es Ihnen hilft, Mitgliedskonten zu identifizieren, die weiterhin Teil der Organisation sein sollten.
2. Der aktuelle Macie-Administrator entfernt alle Mitgliedskonten aus der aktuellen Organisation. Dadurch werden die Konten vom aktuellen Administratorkonto getrennt, Macie ist jedoch weiterhin für die Konten aktiviert.
3. Der neue Macie-Administrator fügt der neuen Organisation die bisherigen Mitgliedskonten hinzu. Dadurch werden die Konten dem neuen Administratorkonto zugeordnet.
4. Jedes Mitgliedskonto akzeptiert die Einladung, der neuen Organisation beizutreten. Wenn ein Konto die Einladung annimmt, wird das Konto zu einem aktiven Mitgliedskonto in der neuen Organisation. Der neue Macie-Administrator kann dann auf die Macie-Einstellungen, -Daten und -Ressourcen für das Konto zugreifen.

Wenn Ihr Unternehmen Macie in mehreren Fällen verwendetAWS-Regionen, führen Sie die vorherigen Schritte in jeder dieser Regionen durch.

Um den aktuellen Bestand der aktiven Mitgliedskonten zu exportieren, kann der aktuelle Macie-Administrator die Amazon Macie Macie-Konsole oder die Amazon Macie Macie-API verwenden. Mit der Konsole kann der aktuelle Administrator die Daten in eine Datei mit kommagetrennten Werten (CSV) exportieren. Der neue Administrator kann dann die Konsole verwenden, um die CSV-Datei hochzuladen und alle Konten (in großen Mengen) zur neuen Organisation hinzuzufügen.

Um Mitgliedskontendaten mithilfe der Konsole zu exportieren

1. Melden Sie sich AWS Management Console mit dem aktuellen Macie-Administratorkonto an.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in die Sie die Daten exportieren möchten.
3. Öffnen Sie die Amazon Macie Macie-Konsole unter https://console.aws.amazon.com/macie/.
4. Klicken Sie im Navigationsbereich unter Settings auf Accounts.

5. (Optional) Um die Kontentabelle zu filtern und nur die Konten anzuzeigen, die derzeit aktive Macie-Mitgliedskonten in der Organisation sind, verwenden Sie das Filterfeld über der Tabelle, um die folgenden Filterbedingungen hinzuzufügen:

   - Typ = Einladung
   - Status = Aktiviert

6. Aktivieren Sie in der Tabelle Konten das Kontrollkästchen für jedes aktive Mitgliedskonto, das in die exportierten Daten aufgenommen werden soll.
7. Wählen Sie CSV exportieren aus.
8. Geben Sie einen Namen und einen Speicherort für die Datei an.

Mit der Amazon Macie Macie-API kann der aktuelle Macie-Administrator die Daten im JSON-Format abrufen. Der neue Macie-Administrator kann diese Daten dann verwenden, um die Liste der Konto-IDs und E-Mail-Adressen für die Konten zu generieren, die hinzugefügt und zur neuen Organisation eingeladen werden sollen. Verwenden Sie den ListMembersBetrieb der Amazon Macie Macie-API, um die Daten im JSON-Format abzurufen. Wenn der Vorgang erfolgreich ist, gibt Macie ein `members` Array zurück, das Details zu allen Konten enthält, die dem Konto des Administrators zugeordnet sind. Wenn es sich bei einem Konto um ein aktives Macie-Mitgliedskonto in der aktuellen, auf Einladung basierenden Organisation handelt, lautet der Wert für die Kontoeigenschaft `Enabled` und die `relationshipStatus` `invitedAt` Eigenschaft gibt ein Datum und eine Uhrzeit an.

Verwaltung Ihrer Mitgliedschaft in einer Organisation, die auf Einladungen basiert, in Amazon Macie

Wenn Sie eingeladen werden, einer Organisation in Amazon Macie beizutreten, können Sie die Einladung optional annehmen oder ablehnen. In Macie besteht eine Organisation aus einer Reihe von Konten, die zentral als Gruppe verwandter Konten verwaltet werden. Eine Organisation besteht aus einem bestimmten Macie-Administratorkonto und einem oder mehreren zugehörigen Mitgliedskonten.

Wenn Sie eine Einladung annehmen, wird Ihr Konto zu einem Mitgliedskonto in der Organisation. Wenn Sie zustimmen, wird das Konto, das die Einladung gesendet hat, zum Macie-Administratorkonto für Ihr Konto. Sie verknüpfen Ihr Konto mit dem anderen Konto und aktivieren eine Administrator-Mitglieds-Beziehung zwischen den Konten. Das Macie-Administratorkonto kann dann auf bestimmte Macie-Einstellungen, Daten und Ressourcen für Ihr Konto in den

entsprechendenAWS-Region. Weitere Informationen finden Sie unter Die Beziehung zwischen Amazon Macie-Administrator- und Mitgliedskonten verstehen.

Wenn Sie eine Einladung ablehnen, werden der aktuelle Status und die Einstellungen für Ihr Macie-Konto nicht geändert.

Themen

- Beantwortung von Mitgliedschaftseinladungen für Organisationen
- Trennung von einem Amazon Macie-Administratorkonto

Beantwortung von Mitgliedschaftseinladungen für Organisationen

Wenn Sie eine Einladung erhalten, einer Organisation beizutreten, benachrichtigt Amazon Macie Sie auf verschiedene Weise. Standardmäßig sendet Macie die Einladung als E-Mail-Nachricht an Sie. Macie erstellt auch eineAWS HealthVeranstaltung für IhreAWS-Konto. Wenn Sie Macie bereits in derAWS-Regionvon dem aus die Einladung gesendet wurde, zeigt Macie auch eineKontenAbzeichen und Benachrichtigung auf der Macie-Konsole.

Nachdem Sie eine Einladung erhalten haben, können Sie die Einladung optional annehmen oder ablehnen. Bevor Sie antworten, beachten Sie Folgendes:

- Sie können jeweils nur Mitglied einer Organisation sein. Wenn Sie mehrere Einladungen erhalten, können Sie nur eine annehmen. Oder, wenn Sie bereits Mitglied einer Organisation sind, müssen Sie Ihr Konto von dem aktuellen Macie-Administratorkonto trennen, bevor Sie einer anderen Organisation beitreten können.
- Wenn Sie Macie in mehreren Regionen verwenden, muss Ihr Konto in all diesen Regionen über dasselbe Macie-Administratorkonto verfügen. Der Macie-Administrator muss Ihnen Einladungen getrennt von jeder Region senden, und Sie müssen die Einladungen in jeder Region separat annehmen.
- Um eine Einladung anzunehmen oder abzulehnen, musst du Macie in der Region aktivieren, aus der die Einladung gesendet wurde. Das Ablehnen einer Einladung ist optional. Wenn du Macie erlaubst, eine Einladung abzulehnen, kannst dudeaktiviere Macieein der Region, nachdem Sie die Einladung abgelehnt haben. Auf diese Weise können Sie sicherstellen, dass Ihnen für die Nutzung von Macie in der Region keine unnötigen Gebühren entstehen.

Weitere Überlegungen finden Sie unterBeantwortung und Verwaltung von Mitgliedschaftseinladungen.

Um auf eine Einladung zur Mitgliedschaft für eine Organisation zu antworten

Um auf eine Einladung zur Mitgliedschaft zu antworten, können Sie die Amazon Macie-Konsole oder die Amazon Macie-API verwenden.

Console

Gehen Sie wie folgt vor, um mithilfe der Amazon Macie-Konsole auf eine Einladung zur Mitgliedschaft zu antworten.

Um auf eine Einladung zur Mitgliedschaft zu antworten

1. Öffnen Sie die Amazon Macie-Konsole unterhttps://console.aws.amazon.com/macie/.
2. Durch die Verwendung desAWS-RegionWählen Sie in der oberen rechten Ecke der Seite die Region aus, in der Sie die Einladung erhalten haben.
3. Wenn Sie Macie in der Region nicht aktiviert haben, wählen SieFangen Sie an, und wählen Sie dannAktiviere Macie. Sie müssen Macie aktivieren, bevor Sie eine Einladung annehmen oder ablehnen können.
4. Klicken Sie im Navigationsbereich unter Settings auf Accounts.
5. UnterAdministratorkonto, führen Sie einen der folgenden Schritte aus:
   - Um die Einladung anzunehmen, aktivieren SieAkzeptieren(
     neben der Einladung. Dann wähleEinladung annehmenoderAktualisieren, je nachdem, ob Sie zuvor eine andere Einladung angenommen haben.
   - Um die Einladung abzulehnen, wählen SieEinladung ablehnenneben der Einladung, und bestätigen Sie dann, dass Sie die Einladung ablehnen möchten.

Wenn Sie die Einladung in weiteren Regionen erhalten haben und darauf antworten möchten, wiederholen Sie die vorherigen Schritte in jeder weiteren Region.

API

Um programmgesteuert auf eine Einladung zu antworten, verwenden Sie denAcceptInvitationoderDeclineInvitationsBetrieb der Amazon Macie-API, je nachdem, ob Sie die Einladung annehmen oder ablehnen möchten. Wenn Sie Ihre Anfrage einreichen, geben Sie unbedingt die Region an, aus der die Einladung gesendet wurde. Um auf die Einladung in weiteren Regionen zu antworten, reichen Sie Ihre Anfrage in jeder weiteren Region ein.

In einem`AcceptInvitation`anfragen, benutze den`administratorAccountId`Parameter zur Angabe der 12-stelligen Konto-ID fürAWS-Kontodas hat die Einladung gesendet. Benutze die`invitationId`Parameter zur Angabe der eindeutigen ID für die Annahme der Einladung.

In einem`DeclineInvitations`anfragen, benutze den`accountIds`Parameter zur Angabe der 12-stelligen Konto-ID fürAWS-KontoDas war die Einladung, abzulehnen.

Um die IDs abzurufen, können Sie dieListInvitationsBetrieb der Amazon Macie API. Wenn die Operation erfolgreich ist, gibt Macie eine`invitations`Array, das Details zu den Einladungen enthält, die Sie erhalten haben, einschließlich der Konto-ID des Kontos, das jede Einladung gesendet hat, und der eindeutigen ID für jede Einladung. Wenn der Wert für`relationshipStatus`Eigentum einer Einladung ist`Invited`, Sie haben noch nicht auf die Einladung geantwortet.

Um auf eine Einladung zu antworten, verwenden Sie denAWS Command Line Interface(AWS CLI), führe das ausEinladung annehmenoderEinladungen ablehnenBefehl, je nachdem, ob Sie die Einladung annehmen oder ablehnen möchten. Benutze die`region`Parameter zur Angabe der Region, aus der die Einladung gesendet wurde. Beispiele:

```
C:\> aws macie2 accept-invitation --region us-east-1 --administrator-account-
id 123456789012 --invitation-id d8bdad0e203fd1242e0a4721bexample
```

Wo*`us-ost-1`*ist die Region, aus der die Einladung gesendet wurde (Region USA Ost (Nord-Virginia)),*`123456789012`*ist die Konto-ID für das Konto, das die Einladung gesendet hat, und*`d8bdad0e203fd1242e0a4721b Beispiel`*ist die eindeutige ID für die Annahme der Einladung.

Wenn eine Anfrage zur Annahme einer Einladung erfolgreich ist, gibt Macie eine leere Antwort zurück. Wenn eine Anfrage, eine Einladung abzulehnen, erfolgreich ist, gibt Macie ein leeresun`processedAccounts`Reihe.

Nachdem Sie eine Einladung abgelehnt haben, wird die Einladung weiterhin als Ressource für Ihr Macie-Konto verwendet. Sie können es optional löschen, indem Sie denDeleteInvitationsOperation oder, für dieAWS CLI, derEinladungen löschenBefehl.

Trennung von einem Amazon Macie-Administratorkonto

Wenn Sie eine Einladung annehmen, einer Organisation bei Amazon Macie beizutreten, können Sie anschließend aus der Organisation austreten, indem Sie Ihr Konto vom aktuellen Macie-

Administratorkonto trennen. Beachten Sie, dass Sie dies nicht tun können, wenn es sich bei Ihrem Konto um ein Mitgliedskonto in einemAWS OrganizationsOrganisation. Um von einem zurückzutretenAWS OrganizationsOrganisation, arbeiten Sie mit Ihrem Macie-Administrator zusammen, um Ihr Konto als Macie-Mitgliedskonto zu entfernen.

Wenn Sie Ihr Konto von seinem Macie-Administratorkonto trennen, verliert der Macie-Administrator den Zugriff auf alle Einstellungen, Daten und Ressourcen für Ihr Macie-Konto. Dazu gehören Metadaten und Richtlinienergebnisse für Amazon S3-Daten, die Ihnen gehören. Dies bedeutet auch, dass der Administrator Ihre Amazon S3-Daten nicht mehr analysieren kann, indem er die automatische Erkennung vertraulicher Daten durchführt oder Aufgaben zur Erkennung vertraulicher Daten ausführt.

Wenn Sie die Verknüpfung mit Ihrem Konto aufheben, ist Macie weiterhin für Ihr Konto in der entsprechenden Region aktiviert. Ihr Konto wird jedoch zu einem eigenständigen Macie-Konto in der Region. Der Status Ihres Kontos ändert sich zuMitglied ist zurückgetretenim Kontoinventar des Administrators.

So trennen Sie die Verknüpfung mit einem Macie-Administratorkonto

Um Ihr Konto von seinem aktuellen Macie-Administratorkonto zu trennen, können Sie die Amazon Macie-Konsole oder die Amazon Macie-API verwenden.

Console

Gehen Sie wie folgt vor, um Ihr Konto mithilfe der Amazon Macie-Konsole von seinem Macie-Administratorkonto zu trennen.

So trennen Sie die Verknüpfung mit einem Administratorkonto

1. Öffnen Sie die Amazon Macie-Konsole unterhttps://console.aws.amazon.com/macie/.
2. Durch die Verwendung desAWS-RegionWählen Sie in der oberen rechten Ecke der Seite die Region aus, in der Sie Ihr Konto vom Administratorkonto trennen möchten.
3. Klicken Sie im Navigationsbereich unter Settings auf Accounts.
4. UnterAdministratorkonto,
   ausschaltenAkzeptieren(
   neben der Einladung, und wählen Sie dannAktualisieren.

Das Konto erscheint weiterhin auf derKontenSeite. Wenn Sie sich entscheiden, der Organisation erneut beizutreten, können Sie diese Seite verwenden, um die ursprüngliche Einladung erneut

anzunehmen. Alternativ können Sie die Einladung ablehnen und löschen, wodurch auch die Verknüpfung zwischen Ihrem Konto und dem anderen Konto gelöscht wird. Wählen Sie dazuEinladung ablehnen.

Wenn Sie Ihr Konto von seinem Macie-Administratorkonto in weiteren Regionen trennen möchten, wiederholen Sie die vorherigen Schritte in jeder weiteren Region.

API

Um Ihr Konto programmgesteuert von seinem Macie-Administratorkonto zu trennen, verwenden Sie denDisassociateFromAdministratorAccountBetrieb der Amazon Macie API. Wenn Sie Ihre Anfrage einreichen, geben Sie unbedingt die Region an, für die sich die Anfrage bezieht. Um die Verknüpfung mit dem Konto in weiteren Regionen zu trennen, reichen Sie Ihre Anfrage in jeder weiteren Region ein.

Um Ihr Konto von seinem Macie-Administratorkonto zu trennen, verwenden Sie denAWS CLI, führe das ausdisassociate-from-administrator-accountBefehl. Benutze die`region`Parameter zur Angabe der Region, in der die Verknüpfung mit dem Konto getrennt werden soll.

Wenn Ihre Anfrage erfolgreich ist, gibt Macie eine leere Antwort zurück.

Nachdem Sie die Verknüpfung mit dem Konto getrennt haben, bleibt die ursprüngliche Einladung als Ressource für Ihr Macie-Konto erhalten, sofern Sie sie nicht löschen. Wenn Sie sich entscheiden, der Organisation erneut beizutreten, können Sie diese Ressource verwenden, um die ursprüngliche Einladung erneut anzunehmen. Alternativ können Sie die Einladung löschen, indem Sie denDeleteInvitationsOperation oder, für dieAWS CLI, derEinladungen löschenBefehl. Wenn Sie die Einladung löschen, löschen Sie auch die Verknüpfung zwischen Ihrem Konto und dem anderen Konto.

Sicherheit bei Amazon Macie und

Die Sicherheit in der Cloud hat bei AWS höchste Priorität. Als AWS-Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die eingerichtet wurden, um die Anforderungen der anspruchsvollsten Organisationen in puncto Sicherheit zu erfüllen.

Sicherheit ist eine übergreifende Verantwortlichkeit zwischen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud selbst – AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS-Compliance-Programme regelmäßig. Informationen zu den Compliance-Programmen, die für Amazon Macie und gelten, finden Sie unter AWSIm Rahmen des Compliance-Programms .
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Services bestimmt, den Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

In dieser Dokumentation wird erläutert, wie das Modell der geteilten Verantwortung bei der Verwendung von Macie und zum Tragen kommt. Die folgenden Themen zeigen, wie Sie Macie und zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele konfigurieren. Sie erfahren außerdem, wie Sie andere verwendenAWS-Services, mit denen Sie Ihre Macie und schützen können.

Themen

- Datenschutz bei Amazon Macie
- Identitäts- und Zugriffsmanagement für Amazon Macie
- Protokollierung und Überwachung in Amazon Macie
- Konformitätsprüfung für Amazon Macie
- Ausfallsicherheit bei Amazon Macie
- Infrastruktursicherheit in Amazon Macie
- Amazon Macie und VPC-Schnittstellen-Endpunkte () AWS PrivateLink

Datenschutz bei Amazon Macie

Das AWS Modell der gilt für den Datenschutz in Amazon Macie. Wie in diesem Modell beschrieben, ist AWS für den Schutz der globalen Infrastruktur verantwortlich, in der die gesamte AWS Cloud ausgeführt wird. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS-Modell der geteilten Verantwortung und in der DSGVO im AWS-Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, AWS-Konto-Anmeldeinformationen zu schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor Authentifizierung (MFA).
- Verwenden Sie SSL/TLS für die Kommunikation mit AWS-Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit AWS CloudTrail ein.
- Verwenden Sie AWS-Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder über eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Macie oder anderen zusammenarbeiten und die KonsoleAWS CLI, API oder AWS SDKs AWS-Services verwenden. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Verschlüsselung im Ruhezustand

Amazon Macie speichert Ihre Daten sicher im Ruhezustand mithilfe von AWS Verschlüsselungslösungen. Macie verschlüsselt Daten, wie z. B. Ergebnisse, mit einem Von AWS verwalteter Schlüssel From AWS Key Management Service (). AWS KMS

Wenn Sie Macie deaktivieren, werden alle Ressourcen, die es für Sie speichert oder verwaltet, dauerhaft gelöscht, z. B. Erkennungsaufträge für vertrauliche Daten, benutzerdefinierte Datenkennungen und Ergebnisse.

Verschlüsselung während der Übertragung

Macie verschlüsselt alle Daten, die zwischen ihnen übertragen werden. AWS-Services

Amazon Macie analysiert Daten aus Amazon S3 und exportiert die Ergebnisse der Erkennung sensibler Daten in einen S3-Bucket. Nachdem Macie die benötigten Informationen von den S3-Objekten abgerufen hat, werden sie verworfen.

Macie greift über einen VPC-Endpunkt auf Amazon S3 zu, der von betrieben wird. AWS PrivateLink Daher verbleibt der Verkehr zwischen Macie und Amazon S3 im Amazon-Netzwerk und wird nicht über das öffentliche Internet übertragen. Weitere Informationen finden Sie unter AWS PrivateLink.

Identitäts- und Zugriffsmanagement für Amazon Macie

AWS Identity and Access Management (IAM) ist ein AWS-Service, mit dem Administratoren den Zugriff auf AWS-Ressourcen sicher steuern können. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Macie-Ressourcen zu verwenden. IAM ist ein AWS-Service, den Sie ohne zusätzliche Kosten verwenden können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- So arbeitet Amazon Macie mit AWS Identity and Access Management
- Beispiele für Amazon Macie
- Servicebezogene Rollen für Amazon Macie
- AWSverwaltete Richtlinien für Amazon Macie

- Fehlerbehebung für Amazon-Macie-Identität und -Zugriff

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Macie ausführen.

Dienstbenutzer — Wenn Sie den Macie-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr Macie-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Featuresweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie in Macie nicht auf eine Funktion zugreifen können, finden Sie weitere Informationen unter. Fehlerbehebung für Amazon-Macie-Identität und -Zugriff

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die Macie-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Macie. Es ist Ihre Aufgabe, zu bestimmen, auf welche Macie-Funktionen und -Ressourcen Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit Macie verwenden kann, finden Sie unter. So arbeitet Amazon Macie mit AWS Identity and Access Management

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Macie zu verwalten. Beispiele für identitätsbasierte Macie-Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Beispiele für Amazon Macie

Authentifizierung mit Identitäten

Authentifizierung ist die Art, wie Sie sich mit Ihren Anmeldeinformationen bei AWS anmelden. Die Authentifizierung (Anmeldung bei AWS) muss als Root-Benutzer des AWS-Kontos, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle erfolgen.

Sie können sich bei AWS als Verbundidentität mit Anmeldeinformationen anmelden, die über eine Identitätsquelle bereitgestellt werden. Benutzer von AWS IAM Identity Center. (IAM Identity Center), die Single-Sign-on-Authentifizierung Ihres Unternehmens und Anmeldeinformationen für Google oder Facebook sind Beispiele für Verbundidentitäten. Wenn Sie sich als Verbundidentität anmelden, hat

der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie auf AWS mithilfe des Verbunds zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich bei der AWS Management Console oder beim AWS-Zugriffsportal anmelden. Weitere Informationen zum Anmelden bei AWS finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch von AWS-Anmeldung.

Bei programmgesteuerten Zugriff auf AWS bietet AWS ein Software Development Kit (SDK) und eine Command Line Interface (CLI, Befehlszeilenschnittstelle) zum kryptographischen Signieren Ihrer Anforderungen mit Ihren Anmeldeinformationen. Wenn Sie keine AWS-Tools verwenden, müssen Sie Anforderungen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode zum eigenen Signieren von Anforderungen finden Sie unter Signieren von AWS-API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS empfiehlt beispielsweise die Verwendung von Multi-Faktor Authentifizierung (MFA), um die Sicherheit Ihres Kontos zu verbessern. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center-Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS-Konto-Root-Benutzer

Wenn Sie ein AWS-Konto neu erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services und Ressourcen des Kontos hat. Diese Identität wird als AWS-Konto-Root-Benutzer bezeichnet. Für den Zugriff auf den Root-Benutzer müssen Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, die zur Erstellung des Kontos verwendet wurden. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode empfiehlt es sich, menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, aufzufordern, den Verbund mit einem Identitätsanbieter zu verwenden, um auf AWS-Services mit temporären Anmeldeinformationen zuzugreifen.

Eine Verbundidentität ist ein Benutzer aus dem Benutzerverzeichnis Ihres Unternehmens, ein Web Identity Provider, AWS Directory Service, das Identity-Center-Verzeichnis oder jeder Benutzer, der mit Anmeldeinformationen, die über eine Identitätsquelle bereitgestellt werden, auf AWS-Services zugreift. Wenn Verbundidentitäten auf AWS-Konten zugreifen, übernehmen sie Rollen und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen im IAM Identity Center erstellen oder Sie können eine Verbindung mit einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und synchronisieren, um sie in allen AWS-Konten und Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität in Ihrem AWS-Konto mit bestimmten Berechtigungen für eine einzelne Person oder eine einzelne Anwendung. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität in Ihrem AWS-Konto mit spezifischen Berechtigungen. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der AWS Management Console übernehmen, indem Sie Rollen wechseln. Sie können eine Rolle annehmen, indem Sie eine AWS CLI oder AWS-API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center-Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. In einigen AWS-Services können Sie jedoch eine Richtlinie direkt an eine Ressource anfügen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff – Einige AWS-Services verwenden Features in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in Amazon Managed Service for Prometheus verwenden, gelten Sie als Prinzipal. Bei einigen Services

könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS-Service aufruft, in Kombination mit der Anforderung an den AWS-Service, Anforderungen an nachgelagerte Services zu stellen. FAS-Anforderungen werden nur dann gestellt, wenn ein Dienst eine Anforderung erhält, die Interaktionen mit anderen AWS-Services oder Ressourcen erfordert, um abgeschlossen werden zu können. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

- Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
- Serviceverknüpfte Rolle – Eine serviceverknüpfte Rolle ist ein Typ von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverbundene Rollen anzeigen, aber nicht bearbeiten.

- Anwendungen in Amazon EC2 – Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und AWS CLI- oder AWS-API-Anforderungen durchführen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Erstellen Sie ein Instance-Profil, das an die Instance angefügt ist, um eine AWS-Rolle einer EC2-Instance zuzuweisen und die Rolle für sämtliche Anwendungen der Instance bereitzustellen. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Für die Zugriffssteuerung in AWS erstellen Sie Richtlinien und weisen diese den AWS-Identitäten oder -Ressourcen zu. Eine Richtlinie ist ein Objekt in AWS, das, wenn es einer Identität oder Ressource zugeordnet wird, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn

ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anforderung stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Benutzerinformationen über die AWS Management Console, die AWS CLI oder die AWS -API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem AWS-Konto anfügen können. Verwaltete Richtlinien umfassen von AWS verwaltete und von Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services umfassen.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können verwaltete AWS-Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3, AWS WAF und Amazon VPC sind Beispiele für Dienste, die ACLs unterstützen. Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger häufig verwendete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Ein ausdrückliches Ablehnen in einer dieser Richtlinien setzt das Zulassen außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.

- Service-Kontrollrichtlinien (SCPs) – SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OE) in AWS Organizations angeben. AWS Organizations ist ein Dienst für die Gruppierung und zentrale Verwaltung mehrerer AWS-Konten Ihres Unternehmens. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. SCPs schränken Berechtigungen für Entitäten in Mitgliedskonten einschließlich des jeweiligen Root-Benutzer des AWS-Kontos ein. Weitere Informationen zu Organisationen und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations-Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen dazu, wie AWS die Zulässigkeit einer Anforderung ermittelt, wenn mehrere Richtlinientypen beteiligt sind, finden Sie unter Logik für die Richtlinienauswertung im IAM-Benutzerhandbuch.

So arbeitet Amazon Macie mit AWS Identity and Access Management

Bevor Sie AWS Identity and Access Management (IAM) verwenden, um den Zugriff auf Amazon Macie zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen mit Macie verwendet werden können.

IAM-Funktionen, die Sie mit Amazon Macie verwenden können

IAM-Funktion	Macie-Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja

IAM-Funktion	Macie-Unterstützung
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
Zugriffskontrolllisten (ACLs)	Nein
Attributbasierte Zugriffskontrolle (ABAC) — Tags in Richtlinien	Ja
Temporäre Anmeldeinformationen	Ja
Zugriffssitzungen weiterleiten (FAS)	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie Macie und andere mit den meisten IAM-Funktionen AWS-Services funktionierenAWS-Services, finden Sie im IAM-Benutzerhandbuch unter Diese Funktionen mit IAM.

Identitätsbasierte Richtlinien für Amazon Macie

Unterstützt Richtlinien auf Identitätsbasis.	Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet

ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Macie unterstützt identitätsbasierte Richtlinien. Beispiele finden Sie unter Beispiele für Amazon Macie.

Ressourcenbasierte Richtlinien innerhalb von Amazon Macie

Unterstützt ressourcenbasierte Richtlinien	Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services umfassen.

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource in unterschiedlichen AWS-Konten befinden, muss ein IAM-Administrator im vertrauenswürdigen Konto auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden im IAM-Benutzerhandbuch.

Macie unterstützt keine ressourcenbasierten Richtlinien. Das heißt, Sie können eine Richtlinie nicht direkt an eine Macie-Ressource anhängen.

Politische Maßnahmen für Amazon Macie

Unterstützt Richtlinienaktionen	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie die zugehörige AWS-API-Operation. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keine passende API-Operation gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Bei Richtlinienaktionen für Macie wird vor der Aktion das folgende Präfix verwendet:

```
macie2
```

Um beispielsweise jemandem die Erlaubnis zu erteilen, auf Informationen über alle verwalteten Datenkennungen zuzugreifen, die Macie bereitstellt, was eine Aktion ist, die dem `ListManagedDataIdentifiers` Betrieb der Amazon Macie Macie-API entspricht, nehmen Sie die `macie2:ListManagedDataIdentifiers` Aktion in ihre Richtlinie auf:

```
"Action": "macie2:ListManagedDataIdentifiers"
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata: Beispiel:

```
"Action": [
      "macie2:ListManagedDataIdentifiers",
      "macie2:ListCustomDataIdentifiers"
]
```

Sie können auch mehrere Aktionen mittels Platzhaltern (*) angeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `List` beginnen, einschließlich der folgenden Aktion:

```
"Action": "macie2:List*"
```

Als bewährte Methode sollten Sie jedoch Richtlinien erstellen, die dem Prinzip der geringsten Rechte folgen. Mit anderen Worten, Sie sollten Richtlinien erstellen, die nur die Berechtigungen enthalten, die zum Ausführen einer bestimmten Aufgabe erforderlich sind.

Eine Liste der Macie-Aktionen finden Sie unter Von Amazon Macie definierte Aktionen in der Service Authorization Reference. Beispiele für Richtlinien, die Macie-Aktionen spezifizieren, finden Sie unter. Beispiele für Amazon Macie

Richtlinienressourcen für Amazon Macie

Unterstützt Richtlinienressourcen	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Macie definiert die folgenden Ressourcentypen:

- Zulassungsliste
- Benutzerdefinierte Datenkennung
- Filter- oder Unterdrückungsregel, auch Ergebnisfilter genannt
- Mitgliedskonto
- Auftrag zur Erkennung sensibler Daten, auch Klassifizierungsauftrag genannt

Sie können diese Ressourcentypen mithilfe von ARNs in Richtlinien angeben.

Um beispielsweise eine Richtlinie für den Discovery-Job für sensible Daten mit der Job-ID 3ce05dbb7ec5505def334104bexample zu erstellen, können Sie den folgenden ARN verwenden:

```
"Resource": "arn:aws:macie2:*:*:classification-job/3ce05dbb7ec5505def334104bexample"
```

Oder verwenden Sie einen Platzhalter (*), um alle Discovery-Jobs für sensible Daten für ein bestimmtes Konto anzugeben:

```
"Resource": "arn:aws:macie2:*:123456789012:classification-job/*"
```

Dabei ist *123456789012* die Konto-ID für den, der die AWS-Konto Jobs erstellt hat. Es hat sich jedoch bewährt, Richtlinien zu erstellen, die dem Prinzip der geringsten Rechte folgen. Mit anderen Worten, Sie sollten Richtlinien erstellen, die nur die Berechtigungen enthalten, die für die Ausführung einer bestimmten Aufgabe auf einer bestimmten Ressource erforderlich sind.

Einige Macie-Aktionen können für mehrere Ressourcen gelten. Mit der `macie2:BatchGetCustomDataIdentifiers` Aktion können beispielsweise die Details mehrerer benutzerdefinierter Datenbezeichner abgerufen werden. In diesen Fällen muss ein Principal über Berechtigungen für den Zugriff auf alle Ressourcen verfügen, für die sich die Aktion bezieht. Um mehrere Ressourcen in einer einzigen Anweisung anzugeben, trennen Sie die ARNs durch Kommata voneinander:

```
"Resource": [
 "arn:aws:macie2:*:*:custom-data-identifier/12g4aff9-8e22-4f2b-b3fd-3063eexample",
 "arn:aws:macie2:*:*:custom-data-identifier/2d12c96a-8e78-4ca6-b1dc-8fd65example",
 "arn:aws:macie2:*:*:custom-data-identifier/4383a69d-4a1e-4a07-8715-208ddexample"
]
```

Eine Liste der Macie-Ressourcentypen und der jeweiligen ARN-Syntax finden Sie unter Von Amazon Macie definierte Ressourcentypen in der Service Authorization Reference. Informationen darüber, welche Aktionen Sie für jeden Ressourcentyp angeben können, finden Sie unter Von Amazon Macie definierte Aktionen in der Service Authorization Reference. Beispiele für Richtlinien, die Ressourcen spezifizieren, finden Sie unterBeispiele für Amazon Macie.

Schlüssel für Richtlinienbedingungen für Amazon Macie

Unterstützt servicespezifische Richtlinienbedingungsschlüssel	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, wertet AWS die Bedingung mittels einer logischen `OR`-Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und servicespezifische Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter Globale AWS-Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Eine Liste der Macie-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon Macie in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon Macie definierte Aktionen. Beispiele für Richtlinien, die Bedingungsschlüssel verwenden, finden Sie unterBeispiele für Amazon Macie.

Zugriffskontrolllisten (ACLs) in Amazon Macie

Unterstützt ACLs	Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon Simple Storage Service (Amazon S3) ist ein Beispiel für einenAWS-Service, der ACLs unterstützt. Weitere Informationen finden Sie unter Übersicht über die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service-Benutzerhandbuch.

Macie unterstützt keine ACLs. Das heißt, Sie können einer Macie-Ressource keine ACL anhängen.

Attributbasierte Zugriffskontrolle (ABAC) mit Amazon Macie

Unterstützt ABAC (Tags in Richtlinien)	Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und mehrere AWS-Ressourcen anfügen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder `aws:TagKeys`Bedingung verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Was ist ABAC? im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Sie können Tags an Macie-Ressourcen anhängen — Zulassungslisten, benutzerdefinierte Datenkennungen, Filter- und Unterdrückungsregeln, Mitgliedskonten und Aufgaben zur Erkennung sensibler Daten. Sie können den Zugriff auf diese Arten von Ressourcen auch kontrollieren, indem

Sie Tag-Informationen als Element einer Richtlinie angeben. `Condition` Informationen zum Taggen von Macie-Ressourcen finden Sie unter. Kennzeichnen von Amazon Macie-Ressourcen Ein Beispiel für eine identitätsbasierte Richtlinie, die den Zugriff auf eine Ressource anhand von Tags steuert, finden Sie unter. Beispiele für Amazon Macie

Temporäre Anmeldeinformationen mit Amazon Macie verwenden

Unterstützt temporäre Anmeldeinformationen	Ja

Einige AWS-Services Featureieren nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, darunter welche AWS-Services mit temporären Anmeldeinformationen Featureieren, finden Sie unter AWS-Services, die mit IAM Featureieren im IAM-Benutzerhandbuch.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen Methode als einem Benutzernamen und einem Passwort bei der AWS Management Console anmelden. Wenn Sie beispielsweise über den Single Sign-On (SSO)-Link Ihres Unternehmens auf AWS zugreifen, erstellt dieser Prozess automatisch temporäre Anmeldeinformationen. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Sie können mithilfe der AWS CLI- oder AWS-API manuell temporäre Anmeldeinformationen erstellen. Sie können dann diese temporären Anmeldeinformationen verwenden, um auf AWS zuzugreifen. AWS empfiehlt, dass Sie temporäre Anmeldeinformationen dynamisch generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Macie unterstützt die Verwendung temporärer Anmeldeinformationen.

Zugriffssitzungen für Amazon Macie weiterleiten

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion

in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS-Service aufruft, in Kombination mit der Anforderung an den AWS-Service, Anforderungen an nachgelagerte Services zu stellen. FAS-Anforderungen werden nur dann gestellt, wenn ein Dienst eine Anforderung erhält, die Interaktionen mit anderen AWS-Services oder Ressourcen erfordert, um abgeschlossen werden zu können. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Macie stellt FAS-Anfragen an Downstream, AWS-Services wenn Sie die folgenden Aufgaben ausführen:

- Erstellen oder aktualisieren Sie die Macie-Einstellungen für eine Zulassungsliste, die in einem S3-Bucket gespeichert ist.
- Überprüfen Sie den Status einer Zulassungsliste, die in einem S3-Bucket gespeichert ist.
- Rufen Sie mithilfe von IAM-Benutzeranmeldedaten Stichproben vertraulicher Daten von einem betroffenen S3-Objekt ab.
- Verschlüsseln Sie sensible Datenproben, die mit IAM-Benutzeranmeldedaten oder einer IAM-Rolle abgerufen werden.
- Aktivieren Sie Macie für die Integration mit. AWS Organizations
- Geben Sie das delegierte Macie-Administratorkonto für eine Organisation in an. AWS Organizations

Für andere Aufgaben verwendet Macie eine dienstbezogene Rolle, um Aktionen in Ihrem Namen auszuführen. Einzelheiten zu dieser Rolle finden Sie unter. Servicebezogene Rollen für Amazon Macie

Servicerollen für Amazon Macie

Unterstützt Servicerollen	Nein

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

Macie übernimmt oder nutzt keine Servicerollen. Um in Ihrem Namen Aktionen auszuführen, verwendet Macie in erster Linie eine dienstbezogene Rolle. Einzelheiten zu dieser Rolle finden Sie unter. Servicebezogene Rollen für Amazon Macie

Servicebezogene Rollen für Amazon Macie

Unterstützt serviceverknüpfte Rollen	Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverbundene Rollen anzeigen, aber nicht bearbeiten.

Macie verwendet eine dienstbezogene Rolle, um Aktionen in Ihrem Namen auszuführen. Einzelheiten zu dieser Rolle finden Sie unter. Servicebezogene Rollen für Amazon Macie

Beispiele für Amazon Macie

Benutzer und Rollen haben standardmäßig nicht die Berechtigung, Macie-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben über die AWS Management Console, die AWS Command Line Interface (AWS CLI) oder die AWS-API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Einzelheiten zu den von Macie definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Macie in der Service-Authorization-Referenz.

Beheben Sie beim Erstellen einer Richtlinie Sicherheitswarnungen, Fehler, allgemeine Warnungen und Vorschläge von AWS Identity and Access Management Access Analyzer (IAM Access Analyzer), bevor Sie die Richtlinie speichern. IAM Access Analyzer führt Richtlinienprüfungen durch, um eine

Richtlinie anhand der IAM-Richtliniengrammatik und der bewährten Methoden zu validieren. Diese Prüfungen generieren Ergebnisse und bieten umsetzbare Empfehlungen, die Sie beim Erstellen von Richtlinien unterstützen, die funktionsfähig sind und den bewährten Methoden für Sicherheit entsprechen. Informationen zum Validieren von IAM Access Analyzer finden Sie unter Validierung der IAM-Access-Analyzer-Richtlinien im IAM-Benutzerhandbuch. Eine Liste der Warnungen, Fehler und Vorschläge, die IAM Access Analyzer zurückgeben kann, finden Sie unter IAM-Access-Analyzer-Richtlinienprüfungsreferenz im IAM-Benutzerhandbuch.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der Amazon Macie Macie-Konsole
- Beispiel: Benutzern die Berechtigung zur Überprüfung ihrer eigenen Berechtigungen
- Beispiel: Benutzern die Erstellung von Aufträgen zur Erkennung vertraulicher Daten ermöglichen
- Beispiel: Benutzern die Verwaltung einer Aufgabe zur Erkennung vertraulicher Daten
- Beispiel: Benutzern die Berechtigung zum Anzeigen der Ergebnisse
- Beispiel: Benutzern die Überprüfung benutzerdefinierter Datenkennungen auf der Grundlage von Tags ermöglichen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien können festlegen, ob jemand Macie-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS-verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen – Um Ihren Benutzern und Workloads Berechtigungen zu gewähren, verwenden Sie die AWS-verwaltete Richtlinien die Berechtigungen für viele allgemeine Anwendungsfälle gewähren. Sie sind in Ihrem AWS-Konto verfügbar. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie AWS-kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS-verwaltete Richtlinien oder AWS-verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer

Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.

- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Service-Aktionen zu gewähren, wenn diese durch ein bestimmtes AWS-Service, wie beispielsweise AWS CloudFormation, verwendet werden. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Bedarf einer Multi-Faktor-Authentifizierung (MFA) – Wenn Sie ein Szenario haben, das IAM-Benutzer oder Root-Benutzer in Ihrem AWS-Konto erfordert, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der Amazon Macie Macie-Konsole

Um auf die Amazon-Macie-Konsole zugreifen zu können, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen Ihnen das Auflisten und Anzeigen von Details zu Macie-Ressourcen in Ihrem AWS-Konto gestatten. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rolen) mit dieser Richtlinie.

Für Benutzer, die nur Aufrufe an die AWS CLI oder AWS-API durchführen, müssen Sie keine Mindestberechtigungen in der Konsole erteilen. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die den API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die Amazon Macie Macie-Konsole verwenden können, erstellen Sie IAM-Richtlinien, die ihnen Zugriff auf die Konsole gewähren. Weitere Informationen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.

Wenn Sie eine Richtlinie erstellen, die Benutzern oder Rollen die Nutzung der Amazon Macie Macie-Konsole ermöglicht, stellen Sie sicher, dass die Richtlinie die `macie2:GetMacieSession` Aktion zulässt. Andernfalls können diese Benutzer oder Rollen nicht auf Macie-Ressourcen oder -Daten auf der Konsole zugreifen.

Stellen Sie außerdem sicher, dass die Richtlinie die entsprechenden `macie2:List` Aktionen für Ressourcen zulässt, auf die diese Benutzer oder Rollen über die Konsole zugreifen müssen. Andernfalls können sie nicht zu diesen Ressourcen navigieren oder Details zu diesen Ressourcen auf der Konsole anzeigen. Um beispielsweise die Details eines Auftrags zur Erkennung vertraulicher Daten mithilfe der Konsole zu überprüfen, muss ein Benutzer die Möglichkeit haben, die `macie2:DescribeClassificationJob` Aktion für den Job und die `macie2:ListClassificationJobs` Aktion auszuführen. Wenn ein Benutzer die `macie2:ListClassificationJobs` Aktion nicht ausführen darf, kann er keine Liste von Jobs auf der Seite Jobs der Konsole anzeigen und kann daher den Job nicht auswählen, um seine Details anzuzeigen. Damit die Details Informationen über eine benutzerdefinierte Daten-ID enthalten, die der Job verwendet, muss der Benutzer auch berechtigt sein, die `macie2:BatchGetCustomDataIdentifiers` Aktion für die benutzerdefinierte Daten-ID auszuführen.

Beispiel: Benutzern die Berechtigung zur Überprüfung ihrer eigenen Berechtigungen

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie enthält Berechtigungen für die Ausführung dieser Aktion auf der Konsole oder für die programmgesteuerte Ausführung über die AWS CLI oder die AWS-API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Beispiel: Benutzern die Erstellung von Aufträgen zur Erkennung vertraulicher Daten ermöglichen

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen können, die es einem Benutzer erlaubt.

In dem Beispiel gewährt die erste Anweisung dem Benutzer `macie2:CreateClassificationJob` Berechtigungen. Diese Berechtigungen ermöglichen es dem Benutzer, Jobs zu erstellen. Die Erklärung erteilt auch `macie2:DescribeClassificationJob` Genehmigungen. Diese Berechtigungen ermöglichen es dem Benutzer, auf die Details vorhandener Jobs zuzugreifen. Diese Berechtigungen sind zwar nicht erforderlich, um Jobs zu erstellen, aber der Zugriff auf diese Details kann dem Benutzer helfen, Jobs mit individuellen Konfigurationseinstellungen zu erstellen.

Die zweite Anweisung im Beispiel ermöglicht es dem Benutzer, Jobs mithilfe der Amazon Macie Macie-Konsole zu erstellen, zu konfigurieren und zu überprüfen. Die `macie2:ListClassificationJobs` Berechtigungen ermöglichen es dem Benutzer, bestehende Jobs auf der Seite Jobs der Konsole anzuzeigen. Alle anderen Berechtigungen in der Anweisung ermöglichen es dem Benutzer, einen Job zu konfigurieren und zu erstellen, indem er die Seiten „Job erstellen“ in der Konsole verwendet.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndReviewJobs",
            "Effect": "Allow",
            "Action": [
                "macie2:CreateClassificationJob",
                "macie2:DescribeClassificationJob"
            ],
            "Resource": "arn:aws:macie2:*:*:classification-job/*"
        },
        {
            "Sid": "CreateAndReviewJobsOnConsole",
            "Effect": "Allow",
            "Action": [
                "macie2:ListClassificationJobs",
                "macie2:ListAllowLists",
                "macie2:ListCustomDataIdentifiers",
                "macie2:ListManagedDataIdentifiers",
                "macie2:SearchResources",
                "macie2:DescribeBuckets"
            ],
            "Resource": "*"
        }
    ]
}
```

Beispiel: Benutzern die Verwaltung einer Aufgabe zur Erkennung vertraulicher Daten

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen können, die es einem Benutzer erlaubt`3ce05dbb7ec5505def334104bexample`. Das Beispiel ermöglicht es dem Benutzer auch, den Status des Jobs nach Bedarf zu ändern.

Die erste Anweisung im Beispiel gewährt `macie2:DescribeClassificationJob` dem Benutzer `macie2:UpdateClassificationJob` Berechtigungen. Diese Berechtigungen ermöglichen es dem Benutzer, die Details des Jobs abzurufen bzw. den Status des Jobs zu ändern. Die zweite Anweisung gewährt dem Benutzer `macie2:ListClassificationJobs` Berechtigungen, sodass der Benutzer über die Seite Jobs in der Amazon Macie Macie-Konsole auf den Job zugreifen kann.

```
{
   "Version": "2012-10-17",
   "Statement": [
 {
         "Sid": "ManageOneJob",
         "Effect": "Allow",
         "Action": [
            "macie2:DescribeClassificationJob",
            "macie2:UpdateClassificationJob"
         ],
         "Resource": "arn:aws:macie2:*:*:classification-
job/3ce05dbb7ec5505def334104bexample"
 },
 {
         "Sid": "ListJobsOnConsole",
         "Effect": "Allow",
         "Action": "macie2:ListClassificationJobs",
         "Resource": "*"
 }
   ]
}
```

Sie können dem Benutzer auch den Zugriff auf Protokolldaten (Protokollereignisse) gewähren, die Macie für den Job in Amazon CloudWatch Logs veröffentlicht. Dazu können Sie Anweisungen hinzufügen, die Berechtigungen zum Ausführen von CloudWatch Logs (`logs`) -Aktionen für die Protokollgruppe und den Stream für den Job gewähren. Beispiel:

```
"Statement": [
    {
        "Sid": "AccessLogGroupForMacieJobs",
        "Effect": "Allow",
        "Action": [
            "logs:DescribeLogGroups",
            "logs:DescribeLogStreams"
        ],
        "Resource": "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs"
```

```
    },
    {
        "Sid": "AccessLogEventsForOneMacieJob",
        "Effect": "Allow",
        "Action": "logs:GetLogEvents",
        "Resource": [
            "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs/*",
            "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs:log-
stream:3ce05dbb7ec5505def334104bexample"
        ]
    }
]
```

Informationen zur Verwaltung des Zugriffs auf CloudWatch Logs finden Sie unter Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre CloudWatch Logs-Ressourcen im Amazon CloudWatch Logs-Benutzerhandbuch.

Beispiel: Benutzern die Berechtigung zum Anzeigen der Ergebnisse

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen können.

In diesem Beispiel ermöglichen die `macie2:GetFindingStatistics` Berechtigungen `macie2:GetFindings` und dem Benutzer, die Daten mithilfe der Amazon Macie Macie-API oder der Amazon Macie Macie-Konsole abzurufen. Die `macie2:ListFindings` Berechtigungen ermöglichen es dem Benutzer, die Daten mithilfe des Übersichts-Dashboards und der Ergebnisseiten auf der Amazon Macie Macie-Konsole abzurufen und zu überprüfen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "macie2:GetFindings",
                "macie2:GetFindingStatistics",
                "macie2:ListFindings"
            ],
            "Resource": "*"
        }
    ]
}
```

Sie können dem Benutzer auch gestatten, Filter- und Unterdrückungsregeln für Ergebnisse zu erstellen und zu verwalten. Dazu können Sie eine Anweisung hinzufügen, die die folgenden Berechtigungen gewährt: `macie2:CreateFindingsFiltermacie2:GetFindingsFilter`,`macie2:UpdateFindingsFilter`, und`macie2:DeleteFindingsFilter`. Damit der Benutzer die Regeln mithilfe der Amazon Macie Macie-Konsole verwalten kann, sollten Sie auch `macie2:ListFindingsFilters` Berechtigungen in die Richtlinie aufnehmen. Beispiel:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "macie2:GetFindings",
                "macie2:GetFindingStatistics",
                "macie2:ListFindings"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ManageRules",
            "Effect": "Allow",
            "Action": [
                "macie2:GetFindingsFilter",
                "macie2:UpdateFindingsFilter",
                "macie2:CreateFindingsFilter",
                "macie2:DeleteFindingsFilter"
            ],
            "Resource": "arn:aws:macie2:*:*:findings-filter/*"
        },
        {
            "Sid": "ListRulesOnConsole",
            "Effect": "Allow",
            "Action": "macie2:ListFindingsFilters",
            "Resource": "*"
        }
    ]
}
```

Beispiel: Benutzern die Überprüfung benutzerdefinierter Datenkennungen auf der Grundlage von Tags ermöglichen

In identitätsbasierten Richtlinien können Sie Bedingungen für die Steuerung des Zugriffs auf Amazon Macie Macie-Ressourcen auf der Basis von Tags verwenden. In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen können Amazon Macie es einem Amazon Macie. Die Berechtigung wird jedoch nur erteilt, wenn der Wert für das `Owner` Tag der Benutzername des Benutzers ist.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewCustomDataIdentifiersIfOwner",
            "Effect": "Allow",
            "Action": "macie2:GetCustomDataIdentifier",
            "Resource": "arn:aws:macie2:*:*:custom-data-identifier/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        },
        {
            "Sid": "ListCustomDataIdentifiersOnConsoleIfOwner",
            "Effect": "Allow",
            "Action": "macie2:ListCustomDataIdentifiers",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

Wenn in diesem Beispiel ein Benutzer, der den Benutzernamen hat, `richard-roe` versucht, die Details einer benutzerdefinierten Daten-ID zu überprüfen, muss die benutzerdefinierte Daten-ID mit `Owner=richard-roe` oder gekennzeichnet werden`owner=richard-roe`. Andernfalls wird dem Benutzer der Zugriff verweigert. Der Tag-Schlüssel `Owner` stimmt mit beiden überein `Owner` und `owner` weil die Namen von Bedingungsschlüsseln nicht zwischen Groß- und Kleinschreibung unterscheiden. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

Servicebezogene Rollen für Amazon Macie

Amazon Macie verwendet eine AWS Identity and Access Management (IAM) -Serviceverknüpfte Rolle mit dem Namen. `AWSServiceRoleForAmazonMacie` Bei dieser serviceverknüpften Rolle handelt es sich um eine IAM-Rolle, die direkt mit Macie verknüpft ist. Sie ist von Macie vordefiniert und beinhaltet alle Berechtigungen, die Macie benötigt, um andere Personen anzurufen AWS-Services und Ressourcen in Ihrem Namen zu überwachen AWS . Macie verwendet diese dienstbezogene Rolle überall dort, AWS-Regionen wo Macie verfügbar ist.

Eine dienstbezogene Rolle erleichtert die Einrichtung von Macie, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Macie definiert die Berechtigungen dieser dienstbezogenen Rolle, und sofern nicht anders definiert, kann nur Macie die Rolle übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie müssen Berechtigungen konfigurieren, damit eine IAM-Entität (z. B. ein Benutzer oder eine Rolle) eine dienstverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch. Sie können eine dienstverknüpfte Rolle erst löschen, nachdem Sie die zugehörigen Ressourcen gelöscht haben. Dies schützt Ihre -Ressourcen, da Sie nicht versehentlich die Berechtigung für den Zugriff auf die Ressourcen entfernen können.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS-Services , die mit IAM arbeiten. Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie Ja mit einem Link, um die Dokumentation der dienstbezogenen Rolle für diesen Dienst zu lesen.

Themen

- Servicebezogene Rollenberechtigungen für Amazon Macie
- Die serviceverknüpfte Rolle für Amazon Macie erstellen
- Bearbeiten der serviceverknüpften Rolle für Amazon Macie
- Löschen der serviceverknüpften Rolle für Amazon Macie
- Wird AWS-Regionen für die serviceverknüpfte Amazon Macie Macie-Rolle unterstützt

Servicebezogene Rollenberechtigungen für Amazon Macie

Amazon Macie verwendet die mit dem Service verknüpfte Rolle mit dem Namen. `AWSServiceRoleForAmazonMacie` Diese dienstbezogene Rolle vertraut darauf, dass der `macie.amazonaws.com` Service die Rolle übernimmt.

Die Berechtigungsrichtlinie für die Rolle, die diesen Namen trägt`AmazonMacieServiceRolePolicy`, ermöglicht es Macie, Aufgaben wie die folgenden für die angegebenen Ressourcen auszuführen:

- Verwenden Sie Amazon-S3-Aktionen, um Informationen über S3-Buckets und Objekte abzurufen.
- Verwenden Sie Amazon S3 S3-Aktionen, um S3-Objekte abzurufen.
- Verwenden Sie AWS Organizations Aktionen, um Informationen über verknüpfte Konten abzurufen.
- Verwenden Sie Amazon CloudWatch Logs-Aktionen, um Ereignisse für Aufträge zur Erkennung sensibler Daten zu protokollieren.

Die Rolle ist mit der folgenden Berechtigungsrichtlinie konfiguriert.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:ListAccountAliases",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
```

```
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/macie/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/macie/*:log-stream:*"
      ]
    }
  ]
}
```

Einzelheiten zu Aktualisierungen der `AmazonMacieServiceRolePolicy` Richtlinie finden Sie unterAmazon Macie aktualisiert aufAWSverwaltete Richtlinien. Wenn Sie automatische Benachrichtigungen über Änderungen an dieser Richtlinie erhalten möchten, abonnieren Sie den RSS-Feed auf der Macie-Dokumentverlaufsseite.

Sie müssen Berechtigungen konfigurieren, damit eine IAM-Entität (z. B. ein Benutzer oder eine Rolle) eine dienstbezogene Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Die serviceverknüpfte Rolle für Amazon Macie erstellen

Sie müssen die `AWSServiceRoleForAmazonMacie` serviceverknüpfte Rolle für Amazon Macie nicht manuell erstellen. Wenn Sie Macie für Sie aktivieren AWS-Konto, erstellt Macie automatisch die serviceverknüpfte Rolle für Sie.

Wenn Sie die mit dem Dienst verknüpfte Macie-Rolle löschen und sie dann erneut erstellen müssen, können Sie dieselbe Vorgehensweise verwenden, um die Rolle in Ihrem Konto neu zu erstellen. Wenn Sie Macie erneut aktivieren, erstellt Macie die dienstverknüpfte Rolle erneut für Sie.

Bearbeiten der serviceverknüpften Rolle für Amazon Macie

Amazon Macie erlaubt Ihnen nicht, die `AWSServiceRoleForAmazonMacie` serviceverknüpfte Rolle zu bearbeiten. Nachdem eine serviceverknüpfte Rolle erstellt wurde, können Sie den Namen der Rolle nicht mehr ändern, da verschiedene Entitäten möglicherweise auf die Rolle verweisen. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen der serviceverknüpften Rolle für Amazon Macie

Wenn Sie Amazon Macie nicht mehr verwenden müssen, empfehlen wir Ihnen, die `AWSServiceRoleForAmazonMacie` serviceverknüpfte Rolle manuell zu löschen. Wenn Sie Macie deaktivieren, löscht Macie die Rolle nicht für Sie.

Bevor Sie die Rolle löschen, müssen Sie Macie in allen Bereichen deaktivieren, in AWS-Region denen Sie sie aktiviert haben. Außerdem müssen Sie die Ressourcen für die Rolle manuell bereinigen. Um die Rolle zu löschen, können Sie die IAM-Konsole AWS CLI, die oder die AWS API verwenden. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

> **Note**
>
> Wenn Macie die `AWSServiceRoleForAmazonMacie` Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Warten Sie in diesem Fall einige Minuten und führen Sie den Vorgang dann erneut aus.

Wenn Sie die `AWSServiceRoleForAmazonMacie` dienstverknüpfte Rolle löschen und sie erneut erstellen müssen, können Sie sie erneut erstellen, indem Sie Macie für Ihr Konto aktivieren. Wenn Sie Macie erneut aktivieren, erstellt Macie die dienstverknüpfte Rolle erneut für Sie.

Wird AWS-Regionen für die serviceverknüpfte Amazon Macie Macie-Rolle unterstützt

Amazon Macie unterstützt die Verwendung der `AWSServiceRoleForAmazonMacie` serviceverknüpften Rolle überall dort, AWS-Regionen wo Macie verfügbar ist. Eine Liste der Regionen, in denen Macie derzeit verfügbar ist, finden Sie unter Amazon Macie Macie-Endpunkte und Kontingente in der. Allgemeine AWS-Referenz

AWSverwaltete Richtlinien für Amazon Macie

Eine von AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von AWS erstellt und verwaltet wird. Von AWS verwaltete Richtlinien stellen Berechtigungen für viele häufige Anwendungsfälle bereit, damit Sie beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS-verwaltete Richtlinien möglicherweise nicht die geringsten Berechtigungen für Ihre spezifischen Anwendungsfälle gewähren, da sie für alle AWS-Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Die Berechtigungen, die in den von AWS verwalteten Richtlinien definiert sind, können nicht geändert werden. Wenn AWS Berechtigungen aktualisiert, die in einer von AWS verwalteten Richtlinie definiert werden, wirkt sich das Update auf alle Prinzipalidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWSaktualisiert am wahrscheinlichsten eine von AWS verwaltete Richtlinie, wenn ein neuer AWS-Service gestartet wird oder neue API-Operationen für bestehende Services verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

Amazon Macie bietet mehrereAWSverwaltete Richtlinien: die`AmazonMacieFullAccess`Politik, die`AmazonMacieReadOnlyAccess`Politik und die`AmazonMacieServiceRolePolicy`Politik.

Themen

- AWS verwaltete Richtlinie: AmazonMacieFullAccess
- AWS verwaltete Richtlinie: AmazonMacieReadOnlyAccess
- AWS verwaltete Richtlinie: AmazonMacieServiceRolePolicy
- Amazon Macie aktualisiert aufAWSverwaltete Richtlinien

AWS verwaltete Richtlinie: AmazonMacieFullAccess

Sie können das anhängen`AmazonMacieFullAccess`Richtlinie für Ihre IAM-Entitäten.

Diese Richtlinie gewährt vollständige Administratorberechtigungen, die eine IAM-Identität ermöglichen (Schulleiter) um das zu erstellenMit Amazon Macie verbundene Rolleund führen Sie alle Lese- und Schreibaktionen für Amazon Macie aus. Zu den Berechtigungen gehören mutierende Funktionen wie Erstellen, Aktualisieren und Löschen. Wenn diese Richtlinie einem Principal zugeordnet ist, kann der Principal alle Macie-Ressourcen, -Daten und -Einstellungen für sein Konto erstellen, abrufen und auf andere Weise darauf zugreifen.

Diese Richtlinie muss einem Principal zugewiesen werden, bevor der Principal Macie für sein Konto aktivieren kann. Ein Principal muss die Möglichkeit haben, die mit Macie verbundene Rolle zu erstellen, um Macie für sein Konto zu aktivieren.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `macie2`— Ermöglicht es Schulleitern, alle Lese- und Schreibaktionen für Amazon Macie durchzuführen.
- `iam`— Ermöglicht es Schulleitern, dienstverknüpfte Rollen zu erstellen. Der`Resource`Das Element gibt die dienstverknüpfte Rolle für Macie an. Der`Condition`Element verwendet die`iam:AWSServiceName` Zustandsschlüsselund der`StringLike` Zustandsoperatorum die Berechtigungen auf die dienstverknüpfte Rolle für Macie einzuschränken.
- `pricing`— Ermöglicht es Auftraggebern, Preisdaten für ihre AWS-KontovonAWS Billing and Cost Management. Macie verwendet diese Daten, um die geschätzten Kosten zu berechnen und anzuzeigen, die entstehen, wenn Principals Aufgaben zur Erkennung vertraulicher Daten erstellen und konfigurieren.

```
{
```

```
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "macie2:*"
         ],
         "Resource": "*"
      },
      {
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName": "macie.amazonaws.com"
            }
         }
      },
      {
         "Effect": "Allow",
         "Action": "pricing:GetProducts",
         "Resource": "*"
      }
   ]
}
```

AWS verwaltete Richtlinie: AmazonMacieReadOnlyAccess

Sie können das anhängen`AmazonMacieReadOnlyAccess`Richtlinie für Ihre IAM-Entitäten.

Diese Richtlinie gewährt schreibgeschützte Berechtigungen, die eine IAM-Identität zulassen (Schulleiter), um alle Leseaktionen für Amazon Macie auszuführen. Die Berechtigungen beinhalten keine mutierenden Funktionen wie Erstellen, Aktualisieren oder Löschen. Wenn diese Richtlinie einem Principal zugeordnet ist, kann der Principal alle Macie-Ressourcen, -Daten und -Einstellungen für sein Konto abrufen, aber nicht auf andere Weise darauf zugreifen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

`macie2`— Ermöglicht es Schulleitern, alle Leseaktionen für Amazon Macie durchzuführen.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "macie2:Describe*",
            "macie2:Get*",
            "macie2:List*",
            "macie2:BatchGetCustomDataIdentifiers",
            "macie2:SearchResources"
         ],
         "Resource": "*"
      }
   ]
}
```

AWS verwaltete Richtlinie: AmazonMacieServiceRolePolicy

Sie können die `AmazonMacieServiceRolePolicy`-Richtlinie Ihren IAM-Entitäten nicht anfügen. Diese Richtlinie ist mit einer dienstverknüpften Rolle verknüpft, die es Macie ermöglicht, Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter Servicebezogene Rollen für Amazon Macie.

Amazon Macie aktualisiert aufAWSverwaltete Richtlinien

Lesen Sie Einzelheiten zu Updates fürAWSverwaltete Richtlinien für Amazon Macie, seit dieser Service damit begonnen hat, diese Änderungen zu verfolgen. Um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf derGeschichte des Macie-DokumentsSeite.

Änderung	Beschreibung	Datum
AmazonMacieReadOnlyAccess— Eine neue Richtlinie wurde hinzugefügt	Macie hat eine neue Richtlinie hinzugefügt, die`AmazonMacieReadOnlyAccess` Politik. Diese Richtlinie gewährt nur Leserechte, die es Schulleitern ermöglichen, alle Macie-Ressourcen, -Daten und -Einstellungen für ihr Konto abzurufen.	15. Juni 2023
AmazonMacieFullAccess— Eine bestehende Richtlinie wurde aktualisiert	In der`AmazonMacieFullAccess` Richtlinie, Macie hat den Amazon-Ressourcennamen (ARN) der dienstverknüpften Macie-Rolle aktualisiert (`aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`).	30. Juni 2022
AmazonMacieServiceRolePolicy— Eine bestehende Richtlinie wurde aktualisiert	Macie entfernte Aktionen und Ressourcen für Amazon Macie Classic aus dem`AmazonMacieServiceRolePolicy` Politik. Amazon Macie Classic wurde eingestellt und ist nicht mehr verfügbar. Genauer gesagt hat Macie alles entferntAWS CloudTrailAktionen. Macie hat auch alle Amazon S3-Aktionen für die folgenden Ressourcen entfernt:	20. Mai 2022

Änderung	Beschreibung	Datum
	`arn:aws:s3:::awsmacie-*` ,`arn:aws:s3:::awsmacietrail-*` , und`arn:aws:s3:::*-awsmacietrail-*` .	
AmazonMacieFullAccess— Eine bestehende Richtlinie wurde aktualisiert	Macie hat eine hinzugefügtAWS Billing and Cost Management(`pricing`) Aktion an die`AmazonMacieFullAccess` Politik. Diese Aktion ermöglicht es Principals, Preisdaten für ihr Konto abzurufen. Macie verwendet diese Daten, um die geschätzten Kosten zu berechnen und anzuzeigen, die entstehen, wenn Principals Aufgaben zur Erkennung vertraulicher Daten erstellen und konfigurieren. Macie hat auch Amazon Macie Classic entfernt (`macie`) Aktionen von`AmazonMacieFullAccess` Politik.	7. März 2022

Änderung	Beschreibung	Datum
AmazonMacieService RolePolicy— Eine bestehende Richtlinie wurde aktualisiert	Macie hat Amazon hinzugefügtCloudWatchProtokolliert Aktionen auf dem`AmazonMacieServiceRolePolicy` Politik. Diese Aktionen ermöglichen es Macie, Protokollereignisse auf zu veröffentlichenCloudWatchProtokolle für Aufgaben zur Erkennung vertraulicher Daten.	13. April 2021
Macie begann, Änderungen zu verfolgen	Macie begann, Änderungen für seine zu verfolgen AWSverwaltete Richtlinien.	13. April 2021

Fehlerbehebung für Amazon-Macie-Identität und -Zugriff

Die folgenden Informationen helfen Ihnen bei der Diagnose und Behebung häufiger Probleme, die bei der Arbeit mit Amazon Macie und AWS Identity and Access Management (IAM) auftreten können.

Themen

- Ich bin nicht autorisiert, eine Aktion in Amazon Macie auszuführen
- Ich möchte Personen außerhalb meines s Zugriff AWS-Konto auf meine Amazon Macie Macie-Ressourcen gewähren

Ich bin nicht autorisiert, eine Aktion in Amazon Macie auszuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `macie2:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 macie2:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `macie2:GetWidget`-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung benötigen. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen odzur Verfügung gestellt.

Ich möchte Personen außerhalb meines s Zugriff AWS-Konto auf meine Amazon Macie Macie-Ressourcen gewähren

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Services, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob Macie diese Funktionen unterstützt, finden Sie unterSo arbeitet Amazon Macie mit AWS Identity and Access Management.
- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen für alle Ihre AWS-Konten finden Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen Ihrer AWS-Konto im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie AWS-Konten-Drittanbieter Zugriff auf Ihre Ressourcen bereitstellen, finden Sie unter Gewähren des Zugriffs auf AWS-Konten von externen Benutzern im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Protokollierung und Überwachung in Amazon Macie

Amazon Macie kann in AWS CloudTrail integriert werden. AWS CloudTrail zeichnet die Aktionen auf, die von einem Benutzer, einer Rolle oder einem anderen AWS-Service in Macie vorgenommen wurden. Dazu gehören Aktionen über die Amazon-Macie-Konsole und programmatische Aufrufe von Amazon-Macie-API-Vorgängen. Anhand der von CloudTrail gesammelten Informationen können Sie feststellen, welche Anfragen an Macie gestellt wurden. Für jede Anfrage können Sie feststellen, wann sie gestellt wurde, von welcher IP-Adresse aus sie gestellt wurde, wer sie gestellt hat und weitere Details. Weitere Informationen finden Sie unter Protokollieren Amazon Macie Macie-API-Aufrufen mit AWS CloudTrail.

Konformitätsprüfung für Amazon Macie

Informationen darüber, ob ein AWS-Service in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter AWS-Services in Geltungsbereich nach Compliance-Programm. Wählen Sie das Compliance-Programm, das Sie interessiert. Allgemeine Informationen finden Sie unter AWS-Compliance-Programme.

Sie können Auditberichte von Drittanbietern unter AWS Artifact herunterladen. Weitere Informationen finden Sie unter Berichte herunterladen in AWS Artifact.

Ihre Compliance-Verantwortung bei der Verwendung von AWS-Services ist von der Sensibilität Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften abhängig. AWS stellt die folgenden Ressourcen zur Unterstützung der Compliance bereit:

- Kurzanleitungen für Sicherheit und Compliance – In diesen Bereitstellungsleitfäden werden Überlegungen zur Architektur erörtert und Schritte zum Bereitstellen von Basisumgebungen auf AWS zur Verfügung gestellt, die auf Sicherheit und Compliance ausgerichtet sind.
- Erstellung einer Architektur mit HIPAA-konformer Sicherheit und Compliance in Amazon Web Services – In diesem Whitepaper wird beschrieben, wie Unternehmen mithilfe von AWS HIPAA-berechtigte Anwendungen erstellen können.

> **Note**
>
> Nicht alle AWS-Services sind HIPAA-berechtigt. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS-Compliance-Ressourcen – Diese Arbeitsbücher und Leitfäden könnten für Ihre Branche und Ihren Standort relevant sein.
- AWS-Compliance-Leitfäden für Kunden – Verstehen Sie das Modell der geteilten Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Methoden zum Schutz von AWS-Services zusammengefasst und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Auswertung von Ressourcen mit Regeln im AWS ConfigEntwicklerhandbuch – Der AWS Config-Service bewertet, wie gut Ihre Ressourcenkonfigurationen mit internen Praktiken, Branchenrichtlinien und Vorschriften übereinstimmen.
- AWS Security Hub – Dieser AWS-Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus innerhalb von AWS. Security Hub verwendet Sicherheitskontrollen, um Ihre AWS-Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- AWS Audit Manager – Dieser AWS-Service hilft Ihnen, Ihre AWS-Nutzung kontinuierlich zu überprüfen, um den Umgang mit Risiken und die Compliance von Branchenstandards zu vereinfachen.

Ausfallsicherheit bei Amazon Macie

DieAWS globale -Infrastruktur basiert aufAWS-Regionen Availability Zones. Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen über AWS-Regionen und Availability Zones finden Sie unter Globale AWS-Infrastruktur.

Infrastruktursicherheit in Amazon Macie

Als verwalteter Service ist Amazon Macie durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS-Sicherheitsdiensten und wie AWS die Infrastruktur schützt, finden Sie unter AWSCloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS-Umgebung anhand der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz im Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Macie zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Amazon Macie und VPC-Schnittstellen-Endpunkte () AWS PrivateLink

Wenn Sie Amazon Virtual Private Cloud (Amazon VPC) zum Hosten Ihrer AWS Ressourcen verwenden, können Sie eine private Verbindung zwischen Ihrer VPC und Amazon Macie herstellen. Amazon VPC ist eineAWS-Service, mit der Sie AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können. Mit einer VPC haben Sie die Kontrolle über Ihre Netzwerkeinstellungen, wie IP-Adressbereich, Subnetze, Routing-Tabellen und Netzwerk-Gateways.

Um Ihre VPC mit Macie zu verbinden, erstellen Sie einen VPC-Schnittstellen-Endpunkt für Macie. Schnittstellenendpunkte werden von einer Technologie unterstützt AWS PrivateLink, mit der Sie privat auf Amazon Macie Macie-APIs zugreifen können, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder AWS Direct Connect eine Verbindung zu benötigen. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit Amazon Macie Macie-APIs zu kommunizieren. Der Verkehr zwischen Ihrer VPC und Macie verlässt das Amazon-Netzwerk nicht.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere Elastic Network-Schnittstellen in Ihren Subnetzen dargestellt. Weitere Informationen finden Sie unter Zugreifen und AWS-Service Verwenden eines VPC-Endpunkts mit einer Schnittstelle im Amazon VPC-Benutzerhandbuch.

Themen

- Überlegungen zu Amazon Macie VPC-Endpunkten
- Erstellen eines VPC-Schnittstellen-Endpunkts für Amazon Macie

Überlegungen zu Amazon Macie VPC-Endpunkten

Amazon Macie unterstützt VPC-Endpunkte in allen Regionen, in AWS-Regionen denen es derzeit verfügbar ist, mit Ausnahme der Regionen Asien-Pazifik (Osaka) und Israel (Tel Aviv). Eine Liste der Regionen, in denen Macie derzeit verfügbar ist, finden Sie unter Amazon Macie Macie-Endpunkte und Kontingente in der. Allgemeine AWS-Referenz Darüber hinaus unterstützt Macie Aufrufe all seiner API-Aktionen von einer VPC aus.

Wenn Sie einen VPC-Schnittstellen-Endpunkt für Macie erstellen, sollten Sie erwägen, dasselbe für andere zu tunAWS-Services, die VPC-Unterstützung bieten und in Macie integriert sind, z. B. Amazon und. EventBridge AWS Security Hub Macie und diese Dienste können dann VPC-Endpunkte für die Integration verwenden. Wenn Sie beispielsweise einen VPC-Endpunkt für Macie und einen VPC-Endpunkt für Security Hub erstellen, kann Macie seinen VPC-Endpunkt verwenden, wenn es Ergebnisse auf Security Hub veröffentlicht, und Security Hub kann seinen VPC-Endpunkt verwenden, wenn es die Ergebnisse empfängt. Informationen zu Services, die VPC-Endpunkte unterstützen AWS-Services, finden Sie AWS PrivateLink im Amazon VPC-Benutzerhandbuch unter That Integrate with.

Weitere Überlegungen finden Sie unter Zugreifen und AWS-Service Verwenden eines VPC-Endpunkts mit einer Schnittstelle im Amazon VPC-Benutzerhandbuch.

Beachten Sie, dass VPC-Endpunktrichtlinien für Macie nicht unterstützt werden. Standardmäßig ist der vollständige Zugriff auf Macie über den Endpunkt zulässig. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für VPC-Endpunkte und VPC-Endpunktdienste im Amazon VPC-Benutzerhandbuch.

Erstellen eines VPC-Schnittstellen-Endpunkts für Amazon Macie

Sie können einen VPC-Schnittstellen-Endpunkt für den Amazon Macie-Service erstellen, indem Sie entweder die Amazon VPC-Konsole oder die AWS Command Line Interface () verwenden.

AWS CLI Weitere Informationen finden Sie unter Erstellen eines VPC-Endpunkts im Amazon VPC-Benutzerhandbuch.

Wenn Sie einen VPC-Endpunkt für Macie erstellen, verwenden Sie den folgenden Dienstnamen:

- com.amazonaws.*region*.macie2

Wobei *Region* der Regionalcode für den entsprechenden Code ist. AWS-Region

Wenn Sie privates DNS für den Endpunkt aktivieren, können Sie API-Anfragen an Macie stellen, indem Sie dessen Standard-DNS-Namen für die Region verwenden, z. B. `macie2.us-east-1.amazonaws.com` für die Region USA Ost (Nord-Virginia).

Weitere Informationen finden Sie unter Zugreifen und AWS-Service Verwenden eines VPC-Endpunkts mit einer Schnittstelle im Amazon VPC-Benutzerhandbuch.

Protokollieren Amazon Macie Macie-API-Aufrufen mit AWS CloudTrail

Amazon Macie lässt sich integrieren. AWS CloudTrail Dabei handelt es sich um einen Service, der eine Aufzeichnung der Aktionen bereitstellt, die in Macie von einem Benutzer, einer Rolle oder einer anderen Person ausgeführt wurden. AWS-Service CloudTrailerfasst alle API-Aufrufe für Macie als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Amazon Macie Macie-Konsole und programmatische Aufrufe von Amazon Macie Macie-API-Vorgängen.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon Simple Storage Service (Amazon S3) -Bucket aktivieren, einschließlich Ereignissen für Macie. Wenn Sie keinen Trail konfigurieren, können Sie trotzdem die neuesten Ereignisse mithilfe des Ereignisverlaufs auf der AWS CloudTrail Konsole überprüfen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an Macie gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrailBenutzerhandbuch.

Themen

- Informationen zu Amazon Macie in AWS CloudTrail
- Grundlegendes zu Amazon Macie Macie-Protokolldateieinträgen

Informationen zu Amazon Macie in AWS CloudTrail

AWS CloudTrailist für Sie aktiviertAWS-Konto, wenn Sie das Konto erstellen. Wenn in Amazon Macie eine Aktivität auftritt, wird diese Aktivität zusammen mit anderen AWS Ereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS-Konto überprüfen, suchen und herunterladen. Weitere Informationen finden Sie im AWS CloudTrailBenutzerhandbuch unter Arbeiten mit dem CloudTrail Ereignisverlauf.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem SystemAWS-Konto, einschließlich der Ereignisse für Macie, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon Simple Storage Service (Amazon S3) -Bucket. Wenn Sie mit der AWS CloudTrail Konsole einen Trail erstellen, gilt der Trail standardmäßig für alleAWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt

die Protokolldateien für den von Ihnen angegebenen S3 Bucket bereit. Darüber hinaus können Sie andere konfigurieren, AWS-Services um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie in folgenden Themen im AWS CloudTrail-Benutzerhandbuch:

- Erstellen eines Trails für AWS-Konto
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen
- Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle Macie-Aktionen werden von der Amazon Macie API-Referenz protokolliert CloudTrail und sind in dieser dokumentiert. Beispielsweise generieren Aufrufe der `ListFindings` Aktionen `CreateClassificationJobDescribeBuckets`, und Einträge in CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

- Ob die Anfrage mit Stammbenutzer- oder AWS Identity and Access Management (IAM)-Benutzeranmeldeinformationen ausgeführt wurde.
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer ausgeführt wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde.

Weitere Informationen finden Sie unter CloudTrail UserIdentity-Element im AWS CloudTrail Benutzerhandbuch.

Grundlegendes zu Amazon Macie Macie-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3) -Bucket ermöglicht. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und umfasst Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. AWS CloudTrailProtokolldateien enthalten einen oder mehrere Protokolleinträge für Ereignisse. CloudTrail

Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Die folgenden Beispiele zeigen CloudTrail Protokolleinträge, die Ereignisse für Amazon Macie Macie-Aktionen demonstrieren. Einzelheiten zu den Informationen, die ein Protokolleintrag enthalten kann, finden Sie in der Referenz zu CloudTrail Protokollereignissen im AWS CloudTrailBenutzerhandbuch.

Beispiel: Ergebnisse auflisten

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der ein Ereignis für die ListFindingsMacie-Aktion demonstriert. In diesem Beispiel hat ein AWS Identity and Access Management (IAM-) Benutzer (`Mary_Major`) die Amazon Macie Macie-Konsole verwendet, um eine Teilmenge von Informationen über aktuelle Richtlinienfeststellungen für sein Konto abzurufen.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Mary_Major",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary_Major",
        "sessionContext":{
            "attributes": {
                "creationdate": "2023-11-14T15:49:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-14T16:09:56Z",
    "eventSource": "macie2.amazonaws.com",
    "eventName": "ListFindings",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/119.0.0.0 Safari/537.36",
    "requestParameters": {
        "sortCriteria": {
            "attributeName": "updatedAt",
            "orderBy": "DESC"
        },
        "findingCriteria": {
```

```
            "criterion": {
                "archived": {
                    "eq": [
                        "false"
                    ]
                },
                "category": {
                    "eq": [
                        "POLICY"
                    ]
                }
            }
        },
        "maxResults": 25,
        "nextToken": ""
    },
    "responseElements": null,
    "requestID": "d58af6be-1115-4a41-91f8-ace03example",
    "eventID": "ad97fac5-f7cf-4ff9-9cf2-d0676example",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


Beispiel: Stichproben sensibler Daten für ein Ergebnis werden abgerufen

Dieses Beispiel zeigt CloudTrail Protokolleinträge, die Ereignisse beim Abrufen und Aufdecken von Stichproben sensibler Daten veranschaulichen, die Macie in einem Befund gemeldet hat. In diesem Beispiel verwendete ein IAM-Benutzer (`JohnDoe`) die Amazon Macie Macie-Konsole, um sensible Datenproben abzurufen und offenzulegen. Das Macie-Konto des Benutzers ist so konfiguriert, dass es eine IAM-Rolle (`MacieReveal`) übernimmt, um sensible Datenproben abzurufen und offenzulegen.

Das folgende Protokollereignis enthält Details zur Anfrage des Benutzers, Stichproben vertraulicher Daten mithilfe der GetSensitiveDataOccurrencesMacie-Aktion abzurufen und offenzulegen.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
```

```
        "principalId": "UU4MH7OYK5ZCOAEXAMPLE:JohnDoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/JohnDoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "UU4MH7OYK5ZCOAEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-12-12T14:40:23Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-12-12T17:04:47Z",
    "eventSource": "macie2.amazonaws.com",
    "eventName": "GetSensitiveDataOccurrences",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "198.51.100.252",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/119.0.0.0 Safari/537.36",
    "requestParameters": {
        "findingId": "3ad9d8cd61c5c390bede45cd2example"
    },
    "responseElements": null,
    "requestID": "c30cb760-5102-47e7-88d8-ff2e8example",
    "eventID": "baf52d92-f9c3-431a-bfe8-71c81example",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Das nächste Protokollereignis enthält Details darüber, wie Macie dann die angegebene IAM-Rolle (`MacieReveal`) annimmt, indem er die Aktion AWS Security Token Service (AWS STS) ausführt. [AssumeRole](#)

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "reveal-samples.macie.amazonaws.com"
    },
    "eventTime": "2023-12-12T17:04:47Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "AssumeRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "reveal-samples.macie.amazonaws.com",
    "userAgent": "reveal-samples.macie.amazonaws.com",
    "requestParameters": {
        "roleArn": "arn:aws:iam::111122223333:role/MacieReveal",
        "roleSessionName": "RevealCrossAccount"
    },
    "responseElements": {
        "credentials": {
            "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
            "sessionToken": "XXYYaz...
EXAMPLE_SESSION_TOKEN
XXyYaZAz",
            "expiration": "Dec 12, 2023, 6:04:47 PM"
        },
        "assumedRoleUser": {
            "assumedRoleId": "AROAXOTKAROCSNEXAMPLE:RevealCrossAccount",
            "arn": "arn:aws:sts::111122223333:assumed-role/MacieReveal/
RevealCrossAccount"
        }
    },
    "requestID": "d905cea8-2dcb-44c1-948e-19419example",
    "eventID": "74ee4d0c-932d-3332-87aa-8bcf3example",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::IAM::Role",
            "ARN": "arn:aws:iam::111122223333:role/MacieReveal"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
```

```
    "eventCategory": "Management"
}
```

Kennzeichnen von Amazon Macie-Ressourcen

Ein Tag ist eine optionale Bezeichnung, die Sie definieren und AWS Ressourcen zuweisen können, einschließlich bestimmter Arten von Amazon Macie-Ressourcen. Mithilfe von Tags können Sie Ressourcen auf unterschiedliche Weise identifizieren, kategorisieren und verwalten, z. B. nach Zweck, Eigentümer, Umgebung oder anderen Kriterien. Sie können beispielsweise Tags verwenden, um Richtlinien anzuwenden, Kosten zuzuweisen, zwischen Versionen von Ressourcen zu unterscheiden oder Ressourcen zu identifizieren, die bestimmte Compliance-Anforderungen oder Workflows unterstützen.

Sie können den folgenden Arten von Macie-Ressourcen Tags zuweisen: Zulassungslisten, benutzerdefinierte Datenkennungen, Filterregeln und Unterdrückungsregeln für Ergebnisse sowie Aufgaben zur Erkennung vertraulicher Daten. Wenn Sie der Macie-Administrator für eine Organisation sind, können Sie Mitgliedskonten in Ihrer Organisation auch Tags zuweisen.

Themen

- Grundlagen des Taggens
- Verwendung von Tags in IAM-Richtlinien
- Hinzufügen von Tags zu Amazon Macie-Ressourcen
- Überprüfung der Tags für Amazon Macie-Ressourcen
- Tags für Amazon Macie-Ressourcen bearbeiten
- Tags aus Amazon Macie-Ressourcen entfernen

Grundlagen des Taggens

Eine Ressource kann bis zu 50 Tags enthalten. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert. Beides können Sie definieren. Ein Tag-Schlüssel ist eine allgemeine Bezeichnung, die als Kategorie für einen spezifischeren Tag-Wert dient. Ein Tag-Wert dient als Bezeichnung für einen Tag-Schlüssel.

Wenn Sie beispielsweise benutzerdefinierte Datenkennungen und Aufträge zur Erkennung vertraulicher Daten erstellen, um Daten an verschiedenen Stellen in einem Workflow zu analysieren (ein Set für gestaffelte Daten und ein anderes für Produktionsdaten), können Sie diesen Ressourcen einen `Stack` Tag-Schlüssel zuweisen. Der Tag-Wert für diesen Tag-Schlüssel kann `Staging` für

benutzerdefinierte Datenkennungen und Jobs gelten, die für die Analyse von in Stage bereitgestellten Daten konzipiert sind, und `Production` für die anderen.

Beachten Sie beim Definieren und Zuweisen von Tags zu Ressourcen Folgendes:

- Jede Ressource kann maximal 50 Tags haben.
- Für jede Ressource muss jeder Tag-Schlüssel eindeutig sein und er kann nur einen Tag-Wert haben.
- Bei Tag-Schlüsseln und -Werten muss die Groß- und Kleinschreibung beachtet werden. Als bewährte Methode empfehlen wir, eine Strategie für die Großschreibung von Tags zu definieren und diese Strategie in allen Ressourcen einheitlich umzusetzen.
- Ein Tag-Schlüssel kann maximal 128 UTF-8-Zeichen enthalten. Ein Tag-Wert kann maximal 256 UTF-8-Zeichen enthalten. Die Zeichen können Buchstaben, Zahlen, Leerzeichen oder die folgenden Symbole sein: _.:/= + - @
- Das `aws:` Präfix ist für die Verwendung durch reserviertAWS. Sie können es in keinen von Ihnen definierten Tag-Schlüsseln oder -Werten verwenden. Darüber hinaus können Sie Tag-Schlüssel oder -Werte, die dieses Präfix verwenden, nicht ändern oder entfernen. Tags mit diesem Präfix werden beim Kontingent von 50 Tags pro Ressource nicht eingerechnet.
- Alle Tags, die Sie zuweisen, sind nur für Sie AWS-Konto und nur AWS-Region in dem, dem Sie sie zuweisen, verfügbar.
- Wenn Sie eine Ressource löschen, werden alle Tags, die der Ressource zugewiesen sind, ebenfalls gelöscht.

Weitere Einschränkungen, Tipps und bewährte Methoden finden Sie im Tagging AWS Resources User Guide.

> **Important**
>
> Speichern Sie keine vertraulichen oder anderen Arten von sensiblen Daten in Tags. Auf Tags kann von vielen aus zugegriffen werdenAWS-Services, darunterAWS Billing and Cost Management. Sie sind nicht dafür vorgesehen, für sensible Daten verwendet zu werden.

Um Tags für Macie-Ressourcen hinzuzufügen und zu verwalten, können Sie die Amazon Macie-Konsole, die Amazon Macie-API, den Tag-Editor auf der AWS Resource Groups Konsole oder die AWS Resource Groups Tagging-API verwenden. Mit Macie können Sie einer Ressource Tags

hinzufügen, wenn Sie die Ressource erstellen. Sie können auch Tags für einzelne vorhandene Ressourcen hinzufügen und verwalten. Mit Ressourcengruppen können Sie Tags für mehrere vorhandene Ressourcen, einschließlich MacieAWS-Services, auf einmal hinzufügen und verwalten. Weitere Informationen finden Sie im Benutzerhandbuch zur Markierung von AWS-Ressourcen.

Verwendung von Tags in IAM-Richtlinien

Nachdem Sie mit dem Taggen von Ressourcen begonnen haben, können Sie in AWS Identity and Access Management (IAM-) Richtlinien tagbasierte Berechtigungen auf Ressourcenebene definieren. Durch die Verwendung von Tags auf diese Weise können Sie detailliert steuern, welche Benutzer und Rollen in Ihrem Netzwerk die Berechtigung AWS-Konto haben, Ressourcen zu erstellen und zu taggen, und welche Benutzer und Rollen generell berechtigt sind, Tags hinzuzufügen, zu bearbeiten und zu entfernen. Um den Zugriff auf der Grundlage von Tags zu steuern, können Sie tagbezogene Bedingungsschlüssel im Condition-Element der IAM-Richtlinien verwenden.

Sie können beispielsweise eine Richtlinie erstellen, die einem Benutzer vollen Zugriff auf alle Amazon Macie-Ressourcen ermöglicht, wenn das `Owner` Tag für die Ressource seinen Benutzernamen angibt:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "macie2:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

Wenn Sie Tag-basierte Berechtigungen auf Ressourcenebene definieren, werden die Berechtigungen sofort wirksam. Dies bedeutet, dass Ihre Ressourcen besser geschützt sind, sobald sie erstellt wurden, und Sie schnell damit beginnen können, die Verwendung von Tags für neue Ressourcen zu erzwingen. Mithilfe von Berechtigungen auf Ressourcenebene können Sie auch steuern, welche Tag-Schlüssel und -Werte können mit neuen und vorhandenen Ressourcen verknüpft werden können.

Weitere Informationen finden Sie unter Steuern des Zugriffs auf AWS-Ressourcen mithilfe von Tags im IAM-Benutzerhandbuch.

Hinzufügen von Tags zu Amazon Macie-Ressourcen

Um einer einzelnen Amazon Macie-Ressource Tags hinzuzufügen, können Sie die Amazon Macie-Konsole oder die Amazon Macie-API verwenden. Um Tags zu mehreren Macie-Ressourcen gleichzeitig hinzuzufügen, verwenden Sie den Tag-Editor auf der AWS Resource Groups Konsole oder die Tagging-Operationen der AWS Resource GroupsTagging-API.

> **Important**
>
> Das Hinzufügen von Tags zu einer Ressource kann den Zugriff auf die Ressource beeinträchtigen. Bevor Sie einer Ressource ein Tag hinzufügen, überprüfen Sie alle AWS Identity and Access Management (IAM-) Richtlinien, die möglicherweise Tags verwenden, um den Zugriff auf Ressourcen zu steuern.

Console

Wenn Sie eine Zulassungsliste, eine benutzerdefinierte Datenkennzeichnung oder einen Job zur Erkennung vertraulicher Daten erstellen, bietet die Amazon Macie-Konsole Optionen zum Hinzufügen von Tags zur Ressource. Folgen Sie den Anweisungen auf der Konsole, um diesen Ressourcentypen Tags hinzuzufügen, wenn Sie die Ressourcen erstellen. Um Tags zu einer Filter- oder Unterdrückungsregel oder einem Mitgliedskonto in einer Organisation hinzuzufügen, müssen Sie die Ressource erstellen, bevor Sie ihr Tags hinzufügen können.

Gehen Sie folgendermaßen vor, um einer vorhandenen Ressource mithilfe der Amazon Macie-Konsole ein oder mehrere Tags hinzuzufügen.

Um einer Ressource ein Tag hinzuzufügen

1. Öffnen Sie die Amazon Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Gehen Sie je nach Ressourcentyp, zu der Sie ein Tag hinzufügen möchten, einen der folgenden Schritte aus:

   - Wählen Sie für eine Zulassungsliste im Navigationsbereich die Option Zulässige Listen aus.

Aktivieren Sie dann in der Tabelle das Kontrollkästchen für die Liste. Wählen Sie dann im Menü „Aktionen“ die Option „Schlagworte verwalten“.

- Wählen Sie für eine benutzerdefinierte Daten-ID im Navigationsbereich die Option Benutzerdefinierte Datenkennungen aus.

  Aktivieren Sie dann in der Tabelle das Kontrollkästchen für die benutzerdefinierte Daten-ID. Wählen Sie dann im Menü „Aktionen“ die Option „Schlagworte verwalten“.

- Wählen Sie für eine Filter- oder Unterdrückungsregel im Navigationsbereich die Option Ergebnisse aus.

  Wählen Sie dann in der Liste Gespeicherte Regeln das Bearbeitungssymbol () neben der Regel aus. Wählen Sie dann Tags verwalten aus.

- Wählen Sie für ein Mitgliedskonto in Ihrer Organisation im Navigationsbereich Konten aus.

  Aktivieren Sie dann in der Tabelle das Kontrollkästchen für das Konto. Wählen Sie dann im Menü „Aktionen“ die Option „Schlagworte verwalten“.

- Wählen Sie für einen Job zur Erkennung vertraulicher Daten im Navigationsbereich Jobs aus.

  Aktivieren Sie dann in der Tabelle das Kontrollkästchen für den Job. Wählen Sie dann im Menü „Aktionen“ die Option „Schlagworte verwalten“.

Das Fenster „Schlagworte verwalten“ listet alle Tags auf, die der Ressource derzeit zugewiesen sind.

3. Wählen Sie im Fenster „Schlagworte verwalten“ die Option „Schlagworte bearbeiten“.
4. Wählen Sie Add tag.
5. Geben Sie im Feld Schlüssel den Tag-Schlüssel für das Tag ein, das der Ressource hinzugefügt werden soll. Geben Sie dann im Feld Wert optional einen Tag-Wert für den Schlüssel ein.

   Ein Tag-Schlüssel kann bis zu 128 Zeichen enthalten. Ein Tag-Wert kann bis zu 256 Zeichen enthalten. Die Zeichen können Buchstaben, Zahlen, Leerzeichen oder die folgenden Symbole sein: _.:/= + - @

6. (Optional) Um der Ressource ein weiteres Tag hinzuzufügen, wählen Sie Tag hinzufügen aus, und wiederholen Sie dann den vorherigen Schritt. Sie können einer Ressource bis zu 50 Tags zuweisen.
7. Wenn Sie mit dem Hinzufügen von Tags fertig sind, wählen Sie Speichern.

API

Um eine Ressource zu erstellen und ihr programmgesteuert ein oder mehrere Tags hinzuzufügen, verwenden Sie die entsprechende `Create` Operation für den Ressourcentyp, den Sie erstellen möchten:

- Liste zulassen — Verwenden Sie die CreateAllowListOperation oder, falls Sie die AWS Command Line Interface (AWS CLI) verwenden, führen Sie den create-allow-listBefehl aus.
- Benutzerdefinierter Datenbezeichner — Verwenden Sie den CreateCustomDataIdentifierVorgang oder, falls Sie den verwendenAWS CLI, führen Sie den create-custom-data-identifierBefehl aus.
- Filter- oder Unterdrückungsregel — Verwenden Sie die CreateFindingsFilterOperation oder, falls Sie die verwendenAWS CLI, führen Sie den create-findings-filterBefehl aus.
- Mitgliedskonto — Verwenden Sie den CreateMemberVorgang oder, falls Sie den verwendenAWS CLI, führen Sie den Befehl create-member aus.
- Aufgabe zur Erkennung vertraulicher Daten — Verwenden Sie den CreateClassificationJobVorgang oder, falls Sie den verwendenAWS CLI, führen Sie den create-classification-jobBefehl aus.

Verwenden Sie in Ihrer Anfrage den `tags` Parameter, um den Tag-Schlüssel (`key`) und den optionalen Tag-Wert (`value`) für jedes Tag anzugeben, das der Ressource hinzugefügt werden soll. Der `tags` Parameter gibt eine string-to-string Übersicht von Tag-Schlüsseln und den zugehörigen Tag-Werten an.

Um einer vorhandenen Ressource ein oder mehrere Tags hinzuzufügen, verwenden Sie die TagResourceAmazon Macie-API oder, falls Sie die verwenden, führen Sie den Befehl AWS CLI tag-resource aus. Geben Sie in Ihrer Anfrage den Amazon-Ressourcennamen (ARN) der Ressource an, der Sie ein Tag hinzufügen möchten. Verwenden Sie den `tags` Parameter, um den Tag-Schlüssel (`key`) und den optionalen Tag-Wert (`value`) für jedes Tag anzugeben, das der Ressource hinzugefügt werden soll. Wie bei `Create` Operationen und Befehlen gibt der `tags`

Parameter eine string-to-string Zuordnung von Tag-Schlüsseln und den zugehörigen Tag-Werten an.

Beispielsweise fügt der folgende AWS CLI Befehl dem angegebenen Job einen `Stack` Tag-Schlüssel mit einem `Production` Tag-Wert hinzu. Dieses Beispiel ist für Microsoft Windows formatiert und verwendet das Caret-Zeichen (^) zur Zeilenfortsetzung, um die Lesbarkeit zu verbessern.

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"Production\"}
```

Wobei gilt:

- `resource-arn`gibt den ARN des Jobs an, zu dem ein Tag hinzugefügt werden soll.
- *`Stack`*ist der Tag-Schlüssel des Tags, das dem Job hinzugefügt werden soll.
- *`Production`*ist der Tag-Wert für den angegebenen Tag-Schlüssel (*`Stack`*).

Im folgenden Beispiel fügt der Befehl dem Job mehrere Tags hinzu:

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"Production\",\"CostCenter\":\"12345\",\"Owner\":\"jane-doe\"}
```

Für jedes Tag in einer `tags` Map sind `key` sowohl die Argumente als auch die `value` Argumente erforderlich. Der Wert für das `value` Argument kann jedoch eine leere Zeichenfolge sein. Wenn Sie keinen Tag-Wert mit einem Tag-Schlüssel verknüpfen möchten, geben Sie keinen Wert für das `value` Argument an. Der folgende AWS CLI Befehl fügt beispielsweise einen `Owner` Tag-Schlüssel ohne zugehörigen Tag-Wert hinzu:

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Owner\":\"\"}
```

Wenn ein Tagging-Vorgang erfolgreich ist, gibt Macie eine leere HTTP 204-Antwort zurück. Andernfalls gibt Macie eine HTTP 4 xx - oder 500-Antwort zurück, die angibt, warum der Vorgang fehlgeschlagen ist.

Überprüfung der Tags für Amazon Macie-Ressourcen

Sie können die Tags (sowohl Tag-Schlüssel als auch Tag-Werte) für eine Amazon Macie-Ressource überprüfen, indem Sie die Amazon Macie-Konsole oder die Amazon Macie-API verwenden. Wenn Sie dies lieber für mehrere Macie-Ressourcen gleichzeitig tun möchten, können Sie den Tag-Editor auf der AWS Resource Groups Konsole oder die Tagging-Operationen der AWS Resource GroupsTagging-API verwenden.

Console

Gehen Sie wie folgt vor, um die Tags einer Ressource mithilfe der Amazon Macie-Konsole zu überprüfen.

Um die Tags für eine Ressource zu überprüfen

1. Öffnen Sie die Amazon Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Führen Sie je nach Art der Ressource, deren Tags Sie überprüfen möchten, einen der folgenden Schritte aus:

   - Wählen Sie für eine Zulassungsliste im Navigationsbereich die Option Zulässige Listen aus.

     Aktivieren Sie dann in der Tabelle das Kontrollkästchen für die Liste. Wählen Sie dann im Menü „Aktionen“ die Option „Schlagworte verwalten“.
   - Wählen Sie für eine benutzerdefinierte Daten-ID im Navigationsbereich die Option Benutzerdefinierte Datenkennungen aus.

     Aktivieren Sie dann in der Tabelle das Kontrollkästchen für die benutzerdefinierte Daten-ID. Wählen Sie dann im Menü „Aktionen“ die Option „Schlagworte verwalten“.
   - Wählen Sie für eine Filter- oder Unterdrückungsregel im Navigationsbereich die Option Ergebnisse aus.

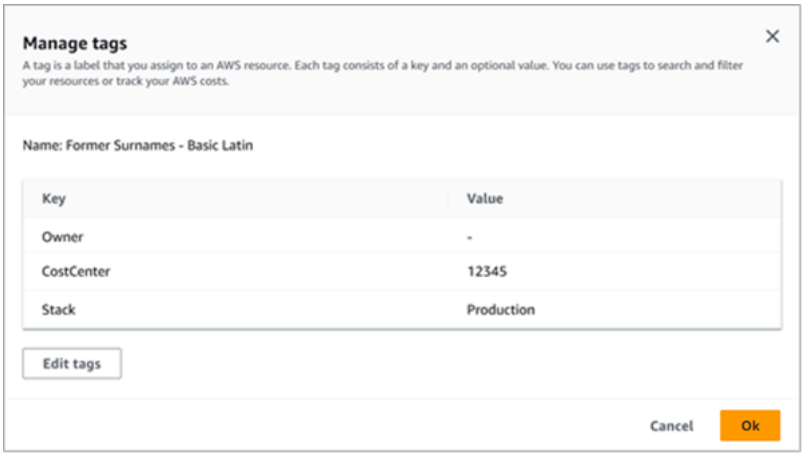
     Wählen Sie dann in der Liste Gespeicherte Regeln das Bearbeitungssymbol () neben der Regel aus. Wählen Sie dann Tags verwalten aus.

- Wählen Sie für ein Mitgliedskonto in Ihrer Organisation im Navigationsbereich Konten aus.

  Aktivieren Sie dann in der Tabelle das Kontrollkästchen für das Konto. Wählen Sie dann im Menü „Aktionen“ die Option „Schlagworte verwalten“.
- Wählen Sie für einen Job zur Erkennung vertraulicher Daten im Navigationsbereich Jobs aus.

  Aktivieren Sie dann in der Tabelle das Kontrollkästchen für den Job. Wählen Sie dann im Menü „Aktionen“ die Option „Schlagworte verwalten“.

Das Fenster „Schlagworte verwalten“ listet alle Tags auf, die der Ressource derzeit zugewiesen sind. Die folgende Abbildung zeigt beispielsweise die Tags, die einer benutzerdefinierten Daten-ID zugewiesen sind.



In diesem Beispiel werden der benutzerdefinierten Daten-ID drei Tags zugewiesen: der Owner-Tag-Schlüssel ohne zugehörigen Tag-Wert, der CostCenterTag-Schlüssel mit 12345 als zugeordnetem Tag-Wert und der Stack-Tag-Schlüssel mit Production als zugeordnetem Tag-Wert.

3. Wenn Sie mit der Überprüfung der Tags fertig sind, wählen Sie Abbrechen, um das Fenster zu schließen.

API

Um die Tags für eine vorhandene Ressource programmgesteuert abzurufen und zu überprüfen, können Sie den entsprechenden `Get` oder `Describe` Vorgang für den Ressourcentyp verwenden, für den Sie die Tags überprüfen möchten. Wenn Sie beispielsweise die GetCustomDataIdentifierOperation verwenden oder den get-custom-data-identifierBefehl von

AWS Command Line Interface (AWS CLI) aus ausführen, enthält die Antwort ein `tags` Objekt. Das Objekt listet alle Tags (sowohl Tag-Schlüssel als auch Tag-Werte) auf, die der Ressource derzeit zugewiesen sind.

Sie können auch den ListTagsForResourceBetrieb der Amazon Macie API verwenden. Verwenden Sie in Ihrer Anfrage den `resourceArn` Parameter, um den Amazon-Ressourcennamen (ARN) der Ressource anzugeben. Wenn Sie den verwendenAWS CLI, führen Sie den list-tags-for-resourceBefehl aus und geben Sie mit dem `resource-arn` Parameter den ARN der Ressource an. Beispiele:

```
C:\> aws macie2 list-tags-for-resource --resource-arn arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample
```

Im vorherigen Beispiel ist *`arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104beexample`* der ARN eines vorhandenen Auftrags zur Erkennung vertraulicher Daten.

Wenn der Vorgang erfolgreich ist, gibt Macie ein `tags` Objekt zurück, das alle Tags (sowohl Tag-Schlüssel als auch Tag-Werte) auflistet, die der Ressource derzeit zugewiesen sind. Beispiele:

```
{
    "tags": {
        "Stack": "Production",
        "CostCenter": "12345",
        "Owner": ""
    }
}
```

Wo`Stack`,`CostCenter`, und `Owner` sind die Tag-Schlüssel, die der Ressource zugewiesen sind. `Production`ist der Tag-Wert, der dem `Stack` Tag-Schlüssel zugeordnet ist. `12345`ist der Tag-Wert, der dem `CostCenter` Tag-Schlüssel zugeordnet ist. Dem `Owner` Tag-Schlüssel ist kein Tag-Wert zugeordnet.

Verwenden Sie den GetResourcesVorgang der AWS Resource Groups Tagging-API, um eine Liste aller Macie-Ressourcen mit Tags und aller Tags abzurufen, die jeder dieser Ressourcen zugewiesen sind. Stellen Sie in Ihrer Anfrage den Wert für den `ResourceTypeFilters` Parameter auf ein`macie2`. Führen Sie dazu den AWS CLI Befehl get-resources aus und setzen Sie den Wert für den `resource-type-filters` Parameter auf`macie2`. Beispiele:

```
C:\> aws resourcegroupstaggingapi get-resources --resource-type-filters "macie2"
```

Wenn der Vorgang erfolgreich ist, gibt Resource Groups ein `ResourceTagMappingList` Array zurück, das die ARNs aller Macie-Ressourcen mit Tags sowie die Tag-Schlüssel und Werte enthält, die jeder dieser Ressourcen zugewiesen sind.

Tags für Amazon Macie-Ressourcen bearbeiten

Um die Tags (Tag-Schlüssel oder Tag-Werte) für eine Amazon Macie-Ressource zu bearbeiten, können Sie die Amazon Macie-Konsole oder die Amazon Macie-API verwenden. Um dies für mehrere Macie-Ressourcen gleichzeitig zu tun, verwenden Sie den Tag-Editor auf der AWS Resource Groups Konsole oder die Tagging-Operationen der AWS Resource GroupsTagging-API.

> **Important**
>
> Das Bearbeiten der Tags für eine Ressource kann sich auf den Zugriff auf die Ressource auswirken. Bevor Sie einen Tag-Schlüssel oder -Wert für eine Ressource bearbeiten, überprüfen Sie alle AWS Identity and Access Management (IAM-) Richtlinien, die das Tag möglicherweise verwenden, um den Zugriff auf Ressourcen zu steuern.

Console

Gehen Sie wie folgt vor, um die Tags einer Ressource mithilfe der Amazon Macie-Konsole zu bearbeiten.

Um die Tags für eine Ressource zu bearbeiten

1. Öffnen Sie die Amazon Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Führen Sie je nach Ressourcentyp, deren Tags Sie bearbeiten möchten, einen der folgenden Schritte aus:

   - Wählen Sie für eine Zulassungsliste im Navigationsbereich die Option Zulässige Listen aus.

     Aktivieren Sie dann in der Tabelle das Kontrollkästchen für die Liste. Wählen Sie dann im Menü „Aktionen“ die Option „Schlagworte verwalten“.
   - Wählen Sie für eine benutzerdefinierte Daten-ID im Navigationsbereich die Option Benutzerdefinierte Datenkennungen aus.

Aktivieren Sie dann in der Tabelle das Kontrollkästchen für die benutzerdefinierte Daten-ID. Wählen Sie dann im Menü „Aktionen“ die Option „Schlagworte verwalten“.

- Wählen Sie für eine Filter- oder Unterdrückungsregel im Navigationsbereich die Option Ergebnisse aus.

  Wählen Sie dann in der Liste Gespeicherte Regeln das Bearbeitungssymbol () neben der Regel aus. Wählen Sie dann Tags verwalten aus.

- Wählen Sie für ein Mitgliedskonto in Ihrer Organisation im Navigationsbereich Konten aus.

  Aktivieren Sie dann in der Tabelle das Kontrollkästchen für das Konto. Wählen Sie dann im Menü „Aktionen“ die Option „Schlagworte verwalten“.

- Wählen Sie für einen Job zur Erkennung vertraulicher Daten im Navigationsbereich Jobs aus.

  Aktivieren Sie dann in der Tabelle das Kontrollkästchen für den Job. Wählen Sie dann im Menü „Aktionen“ die Option „Schlagworte verwalten“.

Das Fenster „Schlagworte verwalten“ listet alle Tags auf, die der Ressource derzeit zugewiesen sind.

3. Wählen Sie im Fenster „Schlagworte verwalten“ die Option „Schlagworte bearbeiten“.
4. Führen Sie eine der folgenden Aktionen aus:

   - Um einem Tag-Schlüssel einen Tag-Wert hinzuzufügen, geben Sie den Wert in das Feld Wert neben dem Tag-Schlüssel ein.
   - Um einen vorhandenen Tag-Schlüssel zu ändern, wählen Sie neben dem Tag die Option Entfernen aus. Wählen Sie dann Tag hinzufügen. Geben Sie in das angezeigte Schlüsselfeld den neuen Tag-Schlüssel ein. Geben Sie optional einen zugehörigen Tag-Wert in das Feld Wert ein.
   - Um einen vorhandenen Tag-Wert zu ändern, wählen Sie X im Feld Wert, das den Wert enthält. Geben Sie dann den neuen Tag-Wert in das Feld Wert ein.
   - Um einen vorhandenen Tag-Wert zu entfernen, wählen Sie X im Feld Wert, das den Wert enthält.
   - Um ein vorhandenes Tag (sowohl den Tag-Schlüssel als auch den Tag-Wert) zu entfernen, wählen Sie neben dem Tag die Option Entfernen aus.

Eine Ressource kann bis zu 50 Tags enthalten. Ein Tag-Schlüssel kann bis zu 128 Zeichen enthalten. Ein Tag-Wert kann bis zu 256 Zeichen enthalten. Die Zeichen können Buchstaben, Zahlen, Leerzeichen oder die folgenden Symbole sein: _.:/= + - @

5. Wenn Sie mit der Bearbeitung der Tags fertig sind, wählen Sie Speichern.

API

Wenn Sie ein Tag für eine Ressource programmgesteuert bearbeiten, überschreiben Sie das vorhandene Tag mit neuen Werten. Daher hängt die beste Methode zum Bearbeiten eines Tags davon ab, ob Sie einen Tag-Schlüssel, einen Tag-Wert oder beides bearbeiten möchten. Um einen Tag-Schlüssel zu bearbeiten, entfernen Sie das aktuelle Tag und fügen Sie ein neues Tag hinzu.

Um nur den Tag-Wert zu bearbeiten oder zu entfernen, der mit einem Tag-Schlüssel verknüpft ist, überschreiben Sie den vorhandenen Wert, indem Sie den TagResourceVorgang der Amazon Macie-API verwenden oder, falls Sie die AWS Command Line Interface (AWS CLI) verwenden, den Befehl tag-resource ausführen. Geben Sie in Ihrer Anfrage den Amazon-Ressourcennamen (ARN) der Ressource an, deren Tag-Wert Sie bearbeiten oder entfernen möchten.

Um einen Tag-Wert für einen Tag-Schlüssel zu bearbeiten, geben Sie mit dem `tags` Parameter den Tag-Schlüssel an, dessen Tag-Wert Sie ändern möchten, und geben Sie den neuen Tag-Wert für den Schlüssel an. Mit dem folgenden Befehl wird beispielsweise der Tag-Wert `Staging` für den Tag-Schlüssel, der `Stack` dem angegebenen Auftrag zur Erkennung vertraulicher Daten zugewiesen ist, von `Production` in geändert. Dieses Beispiel ist für Microsoft Windows formatiert und verwendet das Caret-Zeichen (^) zur Zeilenfortsetzung, um die Lesbarkeit zu verbessern.

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"Staging\"}
```

Wobei gilt:

- `resource-arn`gibt den ARN des Jobs an.
- *`Stack`*ist der Tag-Schlüssel, der dem zu ändernden Tag-Wert zugeordnet ist.
- *`Staging`*ist der neue Tag-Wert für den angegebenen Tag-Schlüssel (*`Stack`*).

Um einen Tag-Wert aus einem Tag-Schlüssel zu entfernen, geben Sie keinen Wert für das `value` Argument im `tags` Parameter an. Beispiele:

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"\"}
```

Wenn die Operation erfolgreich ist, gibt Macie eine leere HTTP 204-Antwort zurück. Andernfalls gibt Macie eine HTTP 4 xx - oder 500-Antwort zurück, die angibt, warum der Vorgang fehlgeschlagen ist.

Tags aus Amazon Macie-Ressourcen entfernen

Um Tags aus einer Amazon Macie-Ressource zu entfernen, können Sie die Amazon Macie-Konsole oder die Amazon Macie-API verwenden. Um dies für mehrere Macie-Ressourcen gleichzeitig zu tun, verwenden Sie den Tag-Editor auf der AWS Resource Groups Konsole oder die Tagging-Operationen der AWS Resource GroupsTagging-API.

> **Important**
>
> Das Entfernen von Tags aus einer Ressource kann den Zugriff auf die Ressource beeinträchtigen. Bevor Sie ein Tag entfernen, überprüfen Sie alle AWS Identity and Access Management (IAM-) Richtlinien, die das Tag möglicherweise verwenden, um den Zugriff auf Ressourcen zu steuern.

Console

Gehen Sie wie folgt vor, um mithilfe der Amazon Macie-Konsole ein oder mehrere Tags aus einer Ressource zu entfernen.

Um ein Tag aus einer Ressource zu entfernen

1. Öffnen Sie die Amazon Macie-Konsole unter https://console.aws.amazon.com/macie/.
2. Gehen Sie je nach Ressourcentyp, aus der Sie ein Tag entfernen möchten, einen der folgenden Schritte aus:

   - Wählen Sie für eine Zulassungsliste im Navigationsbereich die Option Zulässige Listen aus.

Aktivieren Sie dann in der Tabelle das Kontrollkästchen für die Liste. Wählen Sie dann im Menü „Aktionen“ die Option „Schlagworte verwalten“.

- Wählen Sie für eine benutzerdefinierte Daten-ID im Navigationsbereich die Option Benutzerdefinierte Datenkennungen aus.

  Aktivieren Sie dann in der Tabelle das Kontrollkästchen für die benutzerdefinierte Daten-ID. Wählen Sie dann im Menü „Aktionen“ die Option „Schlagworte verwalten“.

- Wählen Sie für eine Filter- oder Unterdrückungsregel im Navigationsbereich die Option Ergebnisse aus.

  Wählen Sie dann in der Liste Gespeicherte Regeln das Bearbeitungssymbol () neben der Regel aus. Wählen Sie dann Tags verwalten aus.

- Wählen Sie für ein Mitgliedskonto in Ihrer Organisation im Navigationsbereich Konten aus.

  Aktivieren Sie dann in der Tabelle das Kontrollkästchen für das Konto. Wählen Sie dann im Menü „Aktionen“ die Option „Schlagworte verwalten“.

- Wählen Sie für einen Job zur Erkennung vertraulicher Daten im Navigationsbereich Jobs aus.

  Aktivieren Sie dann in der Tabelle das Kontrollkästchen für den Job. Wählen Sie dann im Menü „Aktionen“ die Option „Schlagworte verwalten“.

Das Fenster „Schlagworte verwalten“ listet alle Tags auf, die der Ressource derzeit zugewiesen sind.

3. Wählen Sie im Fenster „Schlagworte verwalten“ die Option „Schlagworte bearbeiten“.
4. Führen Sie eine der folgenden Aktionen aus:

   - Um nur den Tag-Wert für ein Tag zu entfernen, wählen Sie X im Feld Wert, das den zu entfernenden Wert enthält.
   - Um sowohl den Tag-Schlüssel als auch den Tag-Wert (als Paar) für ein Tag zu entfernen, wählen Sie neben dem zu entfernenden Tag die Option Entfernen aus.

5. (Optional) Um weitere Tags aus der Ressource zu entfernen, wiederholen Sie den vorherigen Schritt für jedes weitere zu entfernende Tag.
6. Wenn Sie mit dem Entfernen von Tags fertig sind, wählen Sie Speichern.

API

Um ein oder mehrere Tags programmgesteuert aus einer Ressource zu entfernen, verwenden Sie den UntagResourceVorgang der Amazon Macie-API. Verwenden Sie in Ihrer Anfrage den `resourceArn` Parameter, um den Amazon-Ressourcennamen (ARN) der Ressource anzugeben, aus der ein Tag entfernt werden soll. Verwenden Sie den `tagKeys` Parameter, um den Tag-Schlüssel des zu entfernenden Tags anzugeben. Um nur einen bestimmten Tag-Wert (keinen Tag-Schlüssel) aus einer Ressource zu entfernen, bearbeiten Sie das Tag, anstatt das Tag zu entfernen.

Wenn Sie AWS Command Line Interface (AWS CLI) verwenden, führen Sie den Befehl untag-resource aus und geben Sie mit dem `resource-arn` Parameter den ARN der Ressource an, aus der ein Tag entfernt werden soll. Verwenden Sie den `tag-keys` Parameter, um den Tag-Schlüssel des zu entfernenden Tags anzugeben. Der folgende Befehl entfernt beispielsweise das `Stack` Tag (sowohl den Tag-Schlüssel als auch den Tag-Wert) aus dem angegebenen Job zur Erkennung vertraulicher Daten:

```
C:\> aws macie2 untag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tag-keys Stack
```

Wo `resource-arn` gibt den ARN des Jobs an, aus dem ein Tag entfernt werden soll, und *`Stack`* ist der Tag-Schlüssel des zu entfernenden Tags.

Um mehrere Tags aus einer Ressource zu entfernen, fügen Sie jeden zusätzlichen Tag-Schlüssel als Argument für den `tag-keys` Parameter hinzu. Beispiele:

```
C:\> aws macie2 untag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tag-keys Stack Owner
```

Wo `resource-arn` gibt den ARN des Jobs an, aus dem Tags entfernt werden sollen, *`Stack`* und *`Owner`* sind die Tag-Schlüssel der zu entfernenden Tags.

Wenn die Operation erfolgreich ist, gibt Macie eine leere HTTP 204-Antwort zurück. Andernfalls gibt Macie eine HTTP 4 xx - oder 500-Antwort zurück, die angibt, warum der Vorgang fehlgeschlagen ist.

Amazon Macie Macie-Ressourcen erstellen mit AWS CloudFormation

Amazon Macie ist in integriert. Dies ist ein ServiceAWS CloudFormation, der Ihnen hilft, Ihre AWS -Ressourcen zu modellieren und einzurichten, so dass Sie weniger Zeit für die Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur aufwenden müssen. Sie erstellen eine Vorlage, in der alle gewünschten AWS -Ressourcen (z. B. benutzerdefinierte Datenkennungen) beschrieben werden. übernimmt dann die AWS CloudFormation Bereitstellung und Konfiguration dieser Ressourcen für Sie.

Wenn Sie verwendenAWS CloudFormation, können Sie Ihre Vorlage wiederverwenden, um Ihre Macie-Ressourcen einheitlich und wiederholt einzurichten. Sie beschreiben Ihre Ressourcen dann einmal und stellen Sie dann dieselben Ressourcen immer wieder in mehreren AWS-Konten und bereitAWS-Regionen.

Themen

- Amazon Macie und Vorlagen AWS CloudFormation
- Weitere Informationen zu AWS CloudFormation

Amazon Macie und Vorlagen AWS CloudFormation

Um Ressourcen für Amazon Macie und verwandte Dienstleistungen bereitzustellen und zu konfigurieren, müssen Sie AWS CloudFormation-Vorlagen kennen und verstehen. Vorlagen sind Textdateien im JSON- oder YAML-Format. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren AWS CloudFormation-Stacks bereitstellen möchten.

Wenn Sie noch keine Erfahrungen mit JSON oder YAML haben, können Sie AWS CloudFormation Designer, ein Grafiktool zum Erstellen und Ändern AWS CloudFormation von Vorlagen, verwenden. Mit Designer können Sie Ihre Vorlagenressourcen über eine drag-and-drop Oberfläche schematisch darstellen und dann die Details mithilfe des integrierten JSON- und YAML-Editors bearbeiten. Weitere Informationen finden Sie unter Was ist AWS CloudFormation-Designer? im AWS CloudFormation-Benutzerhandbuch.

Sie können AWS CloudFormation Vorlagen für die folgenden Arten von Macie-Ressourcen erstellen:

- Listen zulassen

- Benutzerdefinierte Datenbezeichner
- Filterregeln und Unterdrückungsregeln für Ergebnisse, auch als Ergebnisfilter bezeichnet

Weitere Informationen, einschließlich Beispiele für JSON- und YAML-Vorlagen für diese Art von Ressourcen, finden Sie in der Amazon Macie Macie-Referenz zum Ressourcentyp im AWS CloudFormation-Benutzerhandbuch.

Weitere Informationen zu AWS CloudFormation

Weitere Informationen AWS CloudFormation zu finden Sie in den folgenden Ressourcen.

- AWS CloudFormation
- AWS CloudFormation-Benutzerhandbuch
- AWS CloudFormation API Referenz
- AWS CloudFormation-Benutzerhandbuch für die Befehlszeilenschnittstelle

Amazon Macie aussetzen oder deaktivieren

Sie können Amazon Macie in einem bestimmten Bereich sperren oder deaktivierenAWS-Regionindem Sie die Amazon Macie-Konsole oder die Amazon Macie-API verwenden. Macie beendet dann die Ausführung aller Aktivitäten für Ihr Konto in dieser Region. Die Nutzung von Macie in der Region wird Ihnen nicht in Rechnung gestellt, solange es gesperrt oder deaktiviert ist.

Wenn du Macie aussetzt oder deaktivierst, kannst du es zu einem späteren Zeitpunkt wieder aktivieren.

Themen

- Amazon Macie sperren
- Amazon Macie deaktivieren

Amazon Macie sperren

Wenn Sie Amazon Macie sperren, behält Macie die Sitzungskennung, die Einstellungen und Ressourcen für Ihr Konto in den entsprechendenAWS-Region. Ihre vorhandenen Ergebnisse bleiben beispielsweise erhalten und werden bis zu 90 Tage lang aufbewahrt. Wenn Sie Macie jedoch sperren, werden alle Aktivitäten für Ihr Konto in der entsprechenden Region nicht mehr ausgeführt. Dazu gehören die Überwachung Ihrer Amazon Simple Storage Service (Amazon S3) - Daten, die automatische Erkennung vertraulicher Daten und die Ausführung aller derzeit laufenden Aufgaben zur Erkennung vertraulicher Daten. Macie storniert auch alle Ihre Aufträge zur Entdeckung vertraulicher Daten in der Region.

Nachdem Sie Macie gesperrt haben, können Sie es wieder aktivieren. Sie erhalten dann wieder Zugriff auf Ihre Einstellungen und Ressourcen in der entsprechenden Region, und Macie nimmt die Aktivitäten für Ihr Konto in dieser Region wieder auf. Dazu gehören die Aktualisierung des S3-Bucket-Inventars für Ihr Konto und die Überwachung der Buckets auf Sicherheits- und Zugriffskontrolle. Dies beinhaltet nicht die Wiederaufnahme oder den Neustart Ihrer Aufgaben zur Erkennung vertraulicher Daten. Aufträge zur Erkennung vertraulicher Daten können nicht wieder aufgenommen oder neu gestartet werden, nachdem sie storniert wurden.

In diesem Thema wird erklärt, wie Sie Macie mithilfe der Amazon Macie-Konsole sperren können. Wenn Sie dies lieber programmgesteuert tun möchten, können Sie denUpdateMacieSessionBetrieb der Amazon Macie API.

> **Note**
>
> Wenn Sie der Macie-Administrator einer Organisation sind, müssen Sie alle Mitgliedskonten entfernen, die mit Ihrem Konto verknüpft sind, bevor Sie Macie für Ihr Konto sperren. Weitere Informationen finden Sie unter Verwalten mehrerer Konten.

Um Macie zu suspendieren

1. Öffnen Sie die Amazon Macie-Konsole unterhttps://console.aws.amazon.com/macie/.
2. Durch die Verwendung desAWS-RegionWählen Sie in der oberen rechten Ecke der Seite die Region aus, in der Sie Macie sperren möchten.
3. Wählen Sie im Navigationsbereich Settings (Einstellungen).
4. Wählen SieMacie aussetzen.
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie**Suspend**, und wählen Sie dannAussetzen.

Um Macie in weiteren Regionen auszusetzen, wiederholen Sie die vorherigen Schritte in jeder weiteren Region.

Amazon Macie deaktivieren

Wenn Sie Amazon Macie deaktivieren, beendet Macie die Ausführung aller Aktivitäten für Ihr Konto in der entsprechendenAWS-Region. Dazu gehören die Überwachung Ihrer Amazon Simple Storage Service (Amazon S3) -Daten, die automatische Erkennung vertraulicher Daten und die Ausführung aller derzeit laufenden Aufgaben zur Erkennung vertraulicher Daten. Macie löscht außerdem alle vorhandenen Einstellungen und Ressourcen, die es für Ihr Konto in der entsprechenden Region speichert oder verwaltet, einschließlich Ihrer Ergebnisse und Aufgaben zur Erkennung vertraulicher Daten. Daten, die Sie gespeichert oder für andere veröffentlicht habenAWS-Servicesbleibt intakt und ist nicht betroffen — zum Beispiel führt die Erkennung vertraulicher Daten zu Amazon S3 und das Auffinden von Ereignissen in AmazonEventBridge.

> **Warning**
>
> Wenn Sie Macie deaktivieren, löschen Sie auch dauerhaft alle Ihre vorhandenen Ergebnisse, Aufträge zur Erkennung vertraulicher Daten, benutzerdefinierte Datenkennungen und andere

Ressourcen, die Macie für Ihr Konto in der entsprechenden Region speichert oder verwaltet. Diese Ressourcen können nicht wiederhergestellt werden, nachdem sie gelöscht wurden. Um die Ressourcen zu behalten und nur Ihre Nutzung von Macie zu unterbrechen, sperren Sie Macie, anstatt ihn zu deaktivieren.

In diesem Thema wird erklärt, wie Macie mithilfe der Amazon Macie-Konsole deaktiviert wird. Wenn Sie dies lieber programmgesteuert tun möchten, können Sie denDisableMacieBetrieb der Amazon Macie API.

Note

Wenn Ihr Konto Teil einer Organisation ist, die mehrere Macie-Konten zentral verwaltet, müssen Sie Folgendes tun, bevor Sie Macie deaktivieren:

- Wenn es sich bei Ihrem Konto um ein Macie-Mitgliedskonto handelt, wenden Sie sich an Ihren Macie-Administrator, um Ihr Konto als Mitgliedskonto zu entfernen.
- Wenn es sich bei Ihrem Konto um ein Macie-Administratorkonto handelt, entfernen Sie alle Mitgliedskonten, die mit Ihrem Konto verknüpft sind, und löschen Sie die Verknüpfungen zwischen Ihrem Konto und diesen Konten.

Wie Sie die vorherigen Aufgaben ausführen, hängt davon ab, ob Ihr Macie-Konto mit anderen Konten verknüpft istAWS Organizationsoder auf Einladung. Weitere Informationen finden Sie unter Verwalten mehrerer Konten.

Um Macie zu deaktivieren

1. Öffnen Sie die Amazon Macie-Konsole unterhttps://console.aws.amazon.com/macie/.
2. Durch die Verwendung desAWS-RegionWählen Sie in der oberen rechten Ecke der Seite die Region aus, in der Sie Macie deaktivieren möchten.
3. Wählen Sie im Navigationsbereich Settings (Einstellungen).
4. Wählen SieDeaktiviere Macie.
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie**`Disable`**, und wählen Sie dannDeaktiviere.

Um Macie in weiteren Regionen zu deaktivieren, wiederholen Sie die vorherigen Schritte in jeder weiteren Region.

Amazon Macie Macie-Kontingente

Bei Ihnen AWS-Konto gibt es jeweils AWS-Service bestimmte Standardkontingente, die früher als Limits bezeichnet wurden. Diese Kontingente sind die maximale Anzahl von Serviceressourcen oder Vorgängen für Ihr Konto. In diesem Thema sind die Kontingente aufgeführt, die für Amazon Macie Macie-Ressourcen und -Vorgänge für Ihr Konto gelten. Sofern nicht anders angegeben, gilt jedes Kontingent jeweils AWS-Region für Ihr Konto.

Einige Kontingente können erhöht werden, andere dagegen nicht. Verwenden Sie die Service Quotas-Konsole, um eine Erhöhung eines Kontingents anzufordern. Informationen dazu, wie Sie eine Erhöhung beantragen können, finden Sie unter Eine Erhöhung des Kontingents beantragen im Service Quotas Quota-Benutzerhandbuch. Wenn ein Kontingent in der Service-Kontingents-Konsole nicht verfügbar ist, verwenden Sie das Formular zur Erhöhung des Servicelimits auf derAWS Support Center Console, um eine Erhöhung des Kontingents zu beantragen.

Konten

- Mitgliedskonten auf Einladung: 1.000
- Mitgliedskonten bisAWS Organizations: 10.000

Funde

- Filter- und Unterdrückungsregeln pro Konto: 1.000
- Ergebnisse pro Ausführung eines Discovery-Jobs für sensible Daten: 100.000 + 5% aller verbleibenden Ergebnisse, die den Schwellenwert von 100.000 überschreiten, werden erreicht

  Dieses Kontingent gilt nur für die Amazon Macie Macie-Konsole und die Amazon Macie Macie-API. Es gibt kein Kontingent für die Anzahl der Findereignisse, die Macie auf Amazon veröffentlicht, EventBridge oder für die Anzahl der Discovery-Ergebnisse vertraulicher Daten, die Macie für jeden Lauf eines Jobs erstellt.
- Erkennungsorte pro gefundenem Ergebnis vertraulicher Daten: 15
- Anfragen zum Abrufen und Offenlegen sensibler Datenproben aus einem Amazon S3 S3-Objekt: 100 pro Tag

  Dieses Kontingent wird alle 24 Stunden um 00:00:01 UTC+0 zurückgesetzt.
- Größe eines Amazon S3 S3-Objekts, aus dem sensible Datenproben abgerufen und angezeigt werden sollen:

- Apache Avro-Objektcontainerdatei (.avro): 70 MB
- Apache Parquet-Datei (.parquet): 100 MB
- CSV-Datei (.csv): 255 MB
- GNU-Zip-komprimierte Archivdatei (.gz oder .gzip): 90 MB
- JSON- oder JSON-Zeilendatei (.json oder .jsonl): 25 MB
- Microsoft Excel-Arbeitsmappendatei (.xlsx): 20 MB
- Nicht-binäre Textdatei (text/plain): 100 MB
- TSV-Datei (.tsv): 75 MB
- ZIP-komprimierte Archivdatei (.zip): 355 MB

Wenn ein Ergebnis auf eine Archivdatei zutrifft, die mehrere .gz-Dateien für die entsprechenden Ergebnisse der Erkennung sensibler Daten generiert, können keine Stichproben sensibler Daten aus der Archivdatei abgerufen und offengelegt werden.

Erkennung sensibler Daten

- Monatliche Analyse pro Konto nach Aufträgen zur Erkennung sensibler Daten: 5 TB

  Dieses Kontingent gilt nur für Aufträge zur Erkennung sensibler Daten. Verwenden Sie die Service Quotas Quotas-Konsole, um das Kontingent auf bis zu 1.000 TB (1 PB) zu erhöhen. Um eine Erhöhung für mehr als 1 PB zu beantragen, verwenden Sie das Formular zur Erhöhung des Service-Limits auf der. AWS Support Center Console
- Benutzerdefinierte Datenkennungen pro Konto: 10.000
- Zulassungslisten pro Konto: 10, 1—5 Zulassungslisten, die vordefinierten Text angeben, und 1—5 Zulassungslisten, die reguläre Ausdrücke angeben

  Zusätzliche Kontingente gelten für eine Zulassungsliste, die vordefinierten Text enthält. Die Liste darf nicht mehr als 100.000 Einträge enthalten und die Speichergröße der Liste darf 35 MB nicht überschreiten.
- S3-Buckets, die von der automatisierten Erkennung sensibler Daten ausgeschlossen werden sollen: 1.000

  Wenn es sich bei Ihrem Konto um das Macie-Administratorkonto für eine Organisation handelt, gilt dieses Kontingent für Ihre gesamte Organisation.
- S3-Buckets pro Auftrag zur Erkennung sensibler Daten: 1.000

Dieses Kontingent gilt nicht für Jobs, die anhand von Runtime-Bucket-Kriterien bestimmen, welche Buckets analysiert werden sollen. Es gilt nur für einen Job, wenn Sie den Job so konfigurieren, dass er bestimmte Buckets analysiert, die Sie auswählen. Wenn es sich bei Ihrem Konto um das Macie-Administratorkonto für eine Organisation handelt, können Sie bis zu 1.000 Buckets auswählen, die bis zu 1.000 Konten in Ihrer Organisation umfassen.

- Benutzerdefinierte Datenkennungen pro Auftrag zur Erkennung sensibler Daten: 30
- Zulässige Listen pro Discovery-Job für sensible Daten: 10, 1—5 Zulassungslisten, die vordefinierten Text angeben, und 1—5 Zulassungslisten, die reguläre Ausdrücke angeben
- CreateClassificationJobVorgang: 0,1 Anfragen pro Sekunde
- Zeit für die Analyse einer einzelnen Datei: 10 Stunden
- Größe einer einzelnen zu analysierenden Datei:
  - Datei im Adobe Portable Document Format (.pdf): 1.024 MB
  - Apache Avro-Objektcontainerdatei (.avro): 8 GB
  - Apache Parquet-Datei (.parquet): 8 GB
  - E-Mail-Nachrichtendatei (.eml): 20 GB
  - GNU-Zip-komprimierte Archivdatei (.gz oder .gzip): 8 GB
  - Microsoft Excel-Arbeitsmappendatei (.xls oder .xlsx): 512 MB
  - Microsoft Word-Dokumentdatei (.doc oder .docx): 512 MB
  - Nicht-binäre Textdatei: 20 GB
  - TAR-Archivdatei (.tar): 20 GB
  - ZIP-komprimierte Archivdatei (.zip): 8 GB

  Wenn eine Datei das geltende Kontingent überschreitet, analysiert Macie keine Daten in der Datei.
- Extraktion und Analyse von Daten in einer komprimierten Datei oder Archivdatei:
  - Speichergröße (komprimiert): 8 GB für eine komprimierte GNU Zip-Archivdatei (.gz oder .gzip) oder eine ZIP-komprimierte Archivdatei (.zip); 20 GB für eine TAR-Archivdatei (.tar)
  - Tiefe des verschachtelten Archivs: 10 Stufen
  - Extrahierte Dateien: 1.000.000
  - Extrahierte Byte: Insgesamt 10 GB unkomprimierter Daten. 3 GB unkomprimierter Daten für jede extrahierte Datei, die einen unterstützten Dateityp oder ein unterstütztes Speicherformat verwendet.

Wenn die Metadaten für eine komprimierte Datei oder Archivdatei darauf hinweisen, dass die Datei mehr als 10 verschachtelte Ebenen enthält oder das geltende Kontingent für Speichergröße oder extrahierte Byte überschreitet, extrahiert oder analysiert Macie keine Daten in der Datei. Wenn Macie mit dem Extrahieren und Analysieren von Daten in einer komprimierten Datei oder Archivdatei beginnt und anschließend feststellt, dass die Datei mehr als 1.000.000 Dateien enthält oder das Kontingent für extrahierte Byte überschreitet, beendet Macie die Analyse der Daten in der Datei und erstellt Ergebnisse vertraulicher Daten und Ermittlungsergebnisse nur für die Daten, die verarbeitet wurden.

- Analyse verschachtelter Elemente in strukturierten Daten: 256 Ebenen pro Datei

  Dieses Kontingent gilt nur für JSON- (.json) - und JSON Lines- (.jsonl) -Dateien. Wenn die verschachtelte Tiefe eines der Dateitypen dieses Kontingent überschreitet, analysiert Macie keine Daten in der Datei.
- Erkennungsorte pro Erkennungsergebnis für sensible Daten: 1.000 pro Erkennungstyp für sensible Daten
- Erkennung vollständiger Namen: 1.000 pro Datei, einschließlich Archivdateien

  Nachdem Macie die ersten 1.000 Vorkommen vollständiger Namen in einer Datei erkannt hat, hört Macie auf, die Anzahl zu erhöhen und die Standortdaten für vollständige Namen zu melden.
- Erkennung von Postanschriften: 1.000 pro Datei, einschließlich Archivdateien

  Nachdem Macie die ersten 1.000 Vorkommen von Postanschriften in einer Datei erkannt hat, hört Macie auf, die Anzahl zu erhöhen und die Standortdaten für Postanschriften zu melden.

Dokumentverlauf für das Amazon Macie-Benutzerhandbuch

In der folgenden Tabelle werden die wichtigen Änderungen an der Dokumentation seit der letzten Version von Amazon Macie beschrieben. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

Letzte Aktualisierung der Dokumentation: 20. Februar 2024

Änderung	Beschreibung	Datum
Neue Funktionalität	AWS Security Hub bietet jetzt Sicherheitskontrollen, die den Status von Macie und die automatische Erkennung sensibler Daten für Konten überprüfen. Wenn diese Kontrollen aktiviert sind, führt Security Hub regelmäßig Sicherheitsprüfungen durch, um festzustellen, ob Macie für ein aktiviert ist AWS-Konto (Macie.1-Kontrolle) und ob die automatische Erkennung sensibler Daten für ein Macie-Konto aktiviert ist (Macie.2-Kontrolle).	20. Februar 2024
Neue Funktionalität	Macie kann jetzt Amazon S3-Objekte analysieren, die mit serverseitiger Dual-Layer-Verschlüsselung mit AWS KMS keys (DSSE-KMS) verschlüsselt sind. Diese Objekte können jetzt analysiert werden, wenn Macie eine automatische Erkennung sensibler Daten	17. Januar 2024

	durchführt oder Sie Aufträge zur Erkennung sensibler Daten ausführen. Darüber hinaus sind S3-Buckets und -Objekte, die DSSE-KMS-Verschlüs selung verwenden, jetzt in Statistiken und Metadaten enthalten, die Macie über Ihre Amazon S3-Daten bereitstellt.	
Neues Feature	Sie können Macie jetzt so konfigurieren, dass eine AWS Identity and Access Management (IAM)-Rolle angenommen wird, wenn Sie sich dafür entscheiden, Beispiele für sensible Daten abzurufen und preiszugeben, die Macie in Ergebnissen meldet. Die Beispiele können Ihnen helfen, die Art der sensiblen Daten zu überprüfe n, die Macie gefunden hat, und Ihre Untersuchung eines betroffenen Amazon S3-Objekt s und -Buckets anzupassen.	16. November 2023

Neue Funktionalität	Macie stellt jetzt verwaltete Datenkennungen bereit, die darauf ausgelegt sind, Internationale Bankkontonummern (IBANs) für 47 zusätzliche Länder und Regionen zu erkennen. Sie können Macie jetzt verwenden, um IBANs für mehr als 50 Länder und Regionen zu erkennen und zu melden.	1. November 2023
Neue Funktionalität	Macie stellt jetzt verwaltete Datenkennungen bereit, die darauf ausgelegt sind, die folgenden Arten sensibler Daten zu erkennen: Google-Cloud-API-Schlüssel, Stripe-API-Schlüssel und AadSpeed-Nummern, Permanent Account Numbers (PANs) und Führerschein-Identifikationsnummern für Indien.	25. September 2023

Neue Kontingente	Um Ihnen zu helfen, die Art der sensiblen Daten zu überprüfen, die durch Erkenntnisse gemeldet werden, haben wir die Größenkontingente für das Abrufen und Aufdecken sensibler Daten aus Amazon S3-Objekten erhöht. Sie können jetzt Beispiele von S3-Objekten abrufen und preisgeben, deren Speicherg rößе 10 MB überschre itet. Eine Liste der neuen Kontingente finden Sie unter Amazon Macie-Kontingente.	07. September 2023
Regionale Verfügbarkeit	Macie ist jetzt in der Region Israel (Tel Aviv) verfügbar. Eine vollständige Liste der , AWS-Regionen in denen Macie derzeit verfügbar ist, finden Sie unter Endpunkte und Kontingente von Amazon Macie im Allgemeine AWS-Referenz.	28. August 2023

Aktualisierte Funktionalität	Wir haben einen neuen, dynamischen Satz verwaltet er Standarddatenkennungen für die automatische Erkennung sensibler Daten implementiert. Der Standardsatz enthält die verwalteten Datenkennungen, die wir für die automatische Erkennung sensibler Daten empfehlen. Es wurde entwickelt, um allgemeine Kategorien und Arten sensibler Daten zu erkennen und gleichzeitig Ihre automatisierten Ergebnisse der Erkennung sensibler Daten zu optimieren.	02. August 2023
Aktualisierte Funktionalität	Um Ihnen zu helfen, Vorkommen sensibler Daten zu finden, die Macie in Ergebnissen zur Erkennung sensibler Daten und sensibler Daten meldet, haben wir das Zeichenlimit für die Namen von JSON-Pfadelementen in `Record` Objekten von 20 auf 240 geändert. Diese Änderung wirkt sich auf neue Erkenntnisse zu sensiblen Daten und Erkennungsergebnisse für Apache Avro-Objektcontainer, Apache Parquet-Dateien, JSON-Dateien und JSON Lines-Dateien aus.	24. Juli 2023

Aktualisierte Funktionalität	Wenn Sie der delegierte Macie-Administrator für eine Organisation in sind AWS Organizations, können Sie Macie jetzt für bis zu 10.000 Konten in Ihrer Organisation verwalten.	30. Juni 2023
Neues Feature	Sie können jetzt Aufträge zur Erkennung vertraulicher Daten erstellen und konfigurieren, um automatisch die von uns für Aufträge empfohlenen verwalteten Datenkennungen zu verwenden. Dieser empfohlene Satz verwalteter Datenkennungen ist darauf ausgelegt, allgemeine Kategorien und Arten sensibler Daten zu erkennen und gleichzeitig Ihre Auftragsergebnisse zu optimieren.	28. Juni 2023
Neue Richtlinie	Wir haben eine neue AWS verwaltete Richtlinie hinzugefügt, die `-AmazonMacieReadOnlyAccess` Richtlinie. Diese Richtlinie gewährt schreibgeschützte Berechtigungen, die es einer IAM-Identität (Prinzipal) ermöglichen, alle Macie-Ressourcen, -Daten und -Einstellungen für ihr Konto abzurufen.	15. Juni 2023

Neues Feature	Um Ihnen bei der Bewertung und Überwachung der automatisierten Abdeckung Ihrer Amazon-S3-Daten zur Erkennung sensibler Daten zu helfen, enthält die Macie-Konsole jetzt eine Seite Ressourcenabdeckung. Amazon S3 Die Seite bietet eine einheitliche Ansicht der Abdeckungsstatistiken und Daten für alle Ihre S3-Buckets, einschließlich einer Zusammenfassung der Analyseprobleme (falls vorhanden), die kürzlich für jeden Bucket aufgetreten sind. Wenn Probleme aufgetreten sind, enthält die Seite auch Anleitungen zur Behebung.	15. Mai 2023

Neues Feature	Macie lässt sich in integrieren AWS-Benutzerbenachrichtigungen. Dabei handelt es sich um einen neuen AWS-Service , der als zentraler Ort für Ihre AWS Benachrichtigungen auf der dient AWS Managemen t Console. Mit können Sie benutzerdefinierte Regeln und Benutzerbenachrich tigungenÜbermittlungskanäle zum Generieren und Senden von Benachrichtigungen über Amazon- EventBridge Ereignisse konfigurieren, die Macie für Richtlinien und Ergebnisse sensibler Daten veröffentlicht. https://docs.aws.amazon.com/macie/latest/user/findings-monitor-events-uno.html	5. Mai 2023

Aktualisierter Inhalt	Aktualisierte Beschreibungen von Statistiken und Metadaten, die Macie über Standardverschlüsselungseinstellungen für S3-Buckets bereitstellt. Außerdem wurde die Beschreibung der Policy:IAMUser/S3BucketEncryptionDisabled Richtlinienerkenntnis aktualisiert. Amazon S3 wendet jetzt automatisch die serverseitige Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3) als Basisverschlüsselungsstufe für Objekte an, die neuen und vorhandenen Buckets hinzugefügt werden. Informationen zu dieser Änderung in Amazon S3 finden Sie unter Festlegen des serverseitigen Verschlüsselungsverhaltens für S3-Buckets im Benutzerhandbuch für Amazon Simple Storage Service.	27. Februar 2023

Neue Funktionalität	Macie kann jetzt eine zusätzliche Art von Richtlinienerkenntnis für einen S3-Bucket generieren: `Policy:IAMUser/S3BucketSharedWithCloudFront` . Diese Art von Erkenntnis weist darauf hin, dass die Richtlinie eines Buckets geändert wurde, um die Freigabe des Buckets für eine Amazon-CloudFront Ursprungszugriffsidentität (Origin Access Identity, OAI), eine CloudFront Ursprungszugriffssteuerung (Origin Access Control, OAC) oder beides zu ermöglichen. Darüber hinaus gelten Buckets, die mit CloudFront OAIs oder OACs geteilt werden, jetzt als extern in Statistiken und Metadaten, die Macie über Ihre Amazon S3-Daten bereitstellt.	24. Februar 2023

Neue Funktionalität	Macie unterstützt jetzt die Speicherklasse Amazon S3 Glacier Instant Retrieval für die Erkennung sensibler Daten. S3-Objekte, die diese Speicherklasse verwenden, können jetzt analysiert werden, wenn Macie eine automatische Erkennung sensibler Daten durchführt oder Sie Aufträge zur Erkennung sensibler Daten ausführen. Sie gelten auch als klassifizierbare Objekte in Statistiken und Metadaten, die Macie über Ihre Amazon S3-Daten bereitstellt.	21. Dezember 2022

Neues Feature	Sie können Macie jetzt so konfigurieren, dass automatische Erkennung sensibler Daten für Ihr Konto oder Ihre Organisation durchgeführt wird. Mit der automatisierten Erkennung sensibler Daten wertet Macie Ihre Amazon S3-Daten kontinuierlich aus und verwendet Sampling-Techniken, um repräsentative Objekte in Ihren S3-Buckets zu identifizieren, auszuwählen und zu analysieren, wobei die Objekte auf sensible Daten überprüft werden. Sie können die Ergebnisse von Analysen in Statistiken, Erkenntnissen und anderen Informationen auswerten, die Macie über Ihre Amazon S3-Daten bereitstellt.	28. November 2022

Neues Feature	Sie können jetzt Zulassung slisten erstellen und verwenden, um Text und Textmuster anzugeben, die Macie ignorieren soll, wenn es Amazon S3-Objekt e auf sensible Daten prüft. Durch die Verwendung von Zulassungslisten können Sie Ausnahmen für sensible Daten für Ihre bestimmten Szenarien oder Umgebunge n definieren, z. B. die Namen öffentlicher Verantwor tlichen für Ihre Organisation, bestimmte Telefonnummern oder Beispieldaten, die Ihre Organisation zum Testen verwendet.	30. August 2022
Neues Feature	Um die Art der sensiblen Daten zu überprüfen, die Macie in S3-Objekten findet, können Sie jetzt Macie konfigurieren und verwenden , um Stichproben sensibler Daten abzurufen, die von Ergebnissen gemeldet werden.	26. Juli 2022

Aktualisierte Funktionalität	In der AmazonMacieFullAccess Richtlinie haben wir den Amazon-Ressourcennamen (ARN) der serviceverknüpften Macie-Rolle () aktualisiertaws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie .	30. Juni 2022
Aktualisierte Funktionalität	Wir haben die AmazonMacieServiceRolePolicy Richtlinie aktualisiert. Dabei handelt es sich um die Richtlinie, die der serviceverknüpften Macie-Rolle () zugeordnet istAWSServiceRoleForAmazonMacie . Die Richtlinie legt keine Aktionen und Ressourcen mehr für Amazon Macie Classic fest. Amazon Macie Classic wurde eingestellt und ist nicht mehr verfügbar.	20. Mai 2022
Neue Funktionalität	Macie nimmt nun das `OriginType` Feld in Erkenntnisse zu sensiblen Daten auf, die es in veröffentlicht AWS Security Hub. Das `OriginType` Feld gibt an, wie Macie die sensiblen Daten gefunden hat, die zu einem Ergebnis geführt haben.	11. Mai 2022

Aktualisierter Inhalt	Es wurde klargestellt, wie Schlüsselwort- und maximale Abstandseinstellungen für benutzerdefinierte Datenkennungen funktionieren.	22. April 2022
Neue Funktionalität	Macie stellt jetzt verwaltete Datenkennungen bereit, die darauf ausgelegt sind, HTTP Basic Authorization-Header, HTTP-Cookies und JSON-Web-Token zu erkennen.	21. April 2022
Neuer Inhalt	Beschreibungen und Definitionen der wichtigsten Konzepte und Begriffe für Macie hinzugefügt.	16. März 2022
Neue Funktionalität	Um die geschätzten Kosten zu berechnen und anzuzeigen, wenn Sie Aufträge zur Erkennung sensibler Daten erstellen und konfigurieren, ruft Macie jetzt Preisdaten für Ihr AWS-Konto von ab AWS Billing and Cost Management. Um diese Funktionalität zu unterstützen, haben wir der AmazonMacieFullAccess Richtlinie eine Aktion für Fakturierung und Kostenmanagement hinzugefügt.	7. März 2022

Neue Funktionalität	Macie nimmt nun das `Sample` Feld in Erkenntnisse auf, die es in veröffentlicht AWS Security Hub. Das `Sample` Feld gibt an, ob ein Ergebnis ein Beispielergebnis ist.	24. Februar 2022
Neuer Inhalt	Es wurden Informationen zur Verwendung von Amazon Virtual Private Cloud hinzugefügt, um eine private Verbindung zwischen Ihrer VPC und Macie herzustellen.	19. Januar 2022
Neue Funktionalität	Sie können jetzt die Amazon Macie-Konsole verwenden, um Tags für benutzerdefinierte Datenkennungen zuzuweisen und zu verwalten, Regeln für Erkenntnisse zu filtern und zu unterdrücken, Aufträge zur Erkennung vertraulicher Daten zu erkennen und, wenn Sie der Macie-Administrator für eine Organisation sind, Mitgliedskonten in Ihrer Organisation. Ein Tag ist eine Bezeichnung, die Sie optional definieren und bestimmten Arten von AWS Ressourcen zuweisen.	12. Januar 2022
Neuer Inhalt	Es wurden Informationen zur Verwendung von AWS Identity and Access Management zur Verwaltung des Zugriffs auf Macie hinzugefügt.	20. Dezember 2021

Neues Feature	Wenn Sie eine benutzerdefinierte Datenkennung erstellen, können Sie jetzt Schweregradeinstellungen für Ergebnisse sensibler Daten definieren, die sie erzeugt. Mit diesen Einstellungen können Sie angeben, welcher Schweregrad einer Erkenntnis zugewiesen werden soll, basierend auf der Anzahl der Textereignisse, die den Erkennungskriterien der benutzerdefinierten Datenkennung entsprechen.	4. November 2021
Neue Funktionalität	Um mehr über die verschiedenen Arten von Erkenntnissen zu erfahren, die Macie bereitstellt, können Sie Beispielergebnisse generieren. Beispielerkenntnisse verwenden Beispieldaten und Platzhalterwerte, um die Arten von Informationen zu demonstrieren, die Macie in jede Art von Erkenntnissen einbeziehen könnte.	28. Oktober 2021

Neue Funktionalität	Macie nimmt nun das `OwnerAccountId` Feld in Erkenntnisse auf, die es in veröffentlicht AWS Security Hub. Dieses Feld gibt die Konto-ID für das an AWS-Konto , dem der betroffene S3-Bucket gehört.	27. Oktober 2021
Neuer Inhalt	Es wurden Informationen zur zentralen Verwaltung mehrerer Macie-Konten hinzugefügt. Sie können dies auf zwei Arten tun, indem Sie Macie in integrieren AWS Organizations oder Mitgliedschaftseinladungen von Macie senden.	13. Oktober 2021
Neue Funktionalität	Ihr S3-Bucket-Bestand gibt jetzt an, ob die Berechtigungseinstellungen eines Buckets Macie daran hindern, Informationen über den Bucket oder die Objekte des Buckets abzurufen und die Sicherheit und den Datenschutz der Daten des Buckets zu bewerten und zu überwachen. Darüber hinaus haben wir die Verweise auf AWS KMS keys und vom Kunden verwaltete Schlüssel aktualisiert, um die aktuelle Terminologie widerzuspiegeln.	5. Oktober 2021

Neue Funktionalität	Macie speichert jetzt Ergebnisse zu Richtlinien und sensiblen Daten 90 Tage lang statt 30 Tage. Wenn Macie am oder nach dem 31. August 2021 ein Ergebnis erstellt oder aktualisiert hat, können Sie über die Macie-Konsole oder die Macie-API bis zu 90 Tage auf das Ergebnis zugreifen . In bestimmten begann Macie AWS-Regionenmit der Aufbewahrung der Ergebnisse 90 Tage lang, und zwar bereits am 27. September 2021.	1. Oktober 2021
Neues Feature	Wenn Sie einen Auftrag zur Erkennung vertraulicher Daten erstellen, können Sie jetzt angeben, welche verwaltet en Datenkennungen der Auftrag bei der Analyse von S3-Objekten verwenden soll. Mit dieser Funktion können Sie die Analyse eines Auftrags anpassen, um sich auf bestimmte Arten sensibler Daten zu konzentrieren.	17. September 2021
Neue Funktionalität	Ergebnisse zu sensiblen Daten enthalten jetzt zusätzlic he Informationen, mit denen Sie sensible Daten in JSON- und JSON-Lines-Dateien finden können.	6. Juli 2021

Aktualisierte Funktionalität	Macie verwendet jetzt den `AwsS3Bucket` Ressourcentyp in Erkenntnissen, die es in veröffentlicht AWS Security Hub. (Macie hat diesen Wert zuvor auf festgeleg t`AWS::S3::Bucket` .) `AwsS3Bucket` ist der Ressourcentypwert, der für S3-Buckets im AWS Security Finding Format (ASFF) verwendet wird.	28. Juni 2021
Neues Feature	Wenn Sie einen Auftrag zur Erkennung vertraulicher Daten erstellen, können Sie jetzt Laufzeitkriterien definieren, die bestimmen, welche S3-Buckets der Auftrag analysier t. Mit dieser Funktion kann sich der Umfang der Analyse eines Auftrags dynamisch an Änderungen an Ihrem Bucket-Bestand anpassen.	15. Mai 2021

Neue Funktionalität	Ihr S3-Bucket-Bestand und das Übersichts-Dashboard enthalten jetzt Verschlüsselungsmetadaten und Statistiken, die angeben, ob Bucket-Richtlinien eine serverseitige Verschlüsselung neuer Objekte erfordern. Darüber hinaus können Sie jetzt On-Demand-Aktualisierungen von Objektmetadaten für einzelne Buckets in Ihrem Bucket-Bestand durchführen.	30. April 2021
Neues Feature	Sie können jetzt Amazon CloudWatch Logs verwenden, um Ereignisse zu überwachen und zu analysieren, die auftreten, wenn Sie Aufträge zur Erkennung sensibler Daten ausführen. Um dieses Feature zu unterstützen, haben wir der AWS verwalteten Richtlinie für die serviceverknüpfte Macie-Rolle - CloudWatch Protokollaktionen hinzugefügt.	14. April 2021
Regionale Verfügbarkeit	Macie ist jetzt in der Region AWS Asien-Pazifik (Osaka) verfügbar.	05. April 2021
Neues Feature	Sie können Macie jetzt so konfigurieren, dass vertrauliche Datenergebnisse in veröffentlicht werden AWS Security Hub.	22. März 2021

Neuer Inhalt	Es wurden Informationen zur Überwachung und Prognose der Macie-Kosten und zur Teilnahme an der kostenlosen Testversion hinzugefügt.	26. Februar 2021
Aktualisierter Inhalt	Wir haben den Begriff Masterkonto durch den Begriff Administratorkonto ersetzt. Ein Administratorkonto wird verwendet, um mehrere Konten zentral zu verwalten.	12. Februar 2021
Neue Funktionalität	Sie können jetzt den Umfang von Erkennungsaufträgen für sensible Daten verfeinern, indem Sie S3-Objekt präfixe in benutzerdefinierten Ein- und Ausschlusskriterien verwenden.	2. Februar 2021
Aktualisierter Inhalt	Macie hält sich jetzt an die Erkenntnistyp-Tastatur des AWS Security Finding Format (ASFF), wenn es Richtlini energebnisse in veröffentlicht AWS Security Hub.	28. Januar 2021
Neuer Inhalt	Es wurden Informationen zur Überwachung von Amazon S3-Daten und zur Bewertung der Sicherheit und des Datenschutzes dieser Daten hinzugefügt.	08. Januar 2021

Regionale Verfügbarkeit	Macie ist jetzt in den Regionen AWS AWS Afrika (Kapstadt), Europa (Mailand) und AWS Naher Osten (Bahrain) verfügbar.	21. Dezember 2020
Neue Funktionalität	Wenn Ihr Konto ein Macie-Administratorkonto ist, können Sie jetzt Aufträge zur Erkennung sensibler Daten erstellen und ausführen, die Daten für bis zu 1 000 Buckets mit bis zu 1 000 Konten in Ihrer Organisation analysieren.	25. November 2020
Neue Funktionalität	Ihr S3-Bucket-Bestand gibt jetzt an, ob Sie einmalige oder regelmäßige Erkennung saufträge für sensible Daten zur Analyse von Daten in einem Bucket konfiguriert haben. Wenn Sie dies tun, enthält es auch Details zu dem Auftrag, der zuletzt ausgeführt wurde.	23. November 2020
Neuer Inhalt	Es wurden Informationen zum Filtern von Ergebnissen hinzugefügt.	12. November 2020

Neue Funktionalität	Ergebnisse zu sensiblen Daten enthalten jetzt zusätzliche Informationen, mit denen Sie sensible Daten in Apache Avro-Objektcontainern, Apache Parquet-Dateien und Microsoft Excel-Arbeitsmappen finden können.	9. November 2020
Neues Feature	Sie können jetzt Ergebnisse zu sensiblen Daten verwenden, um einzelne Vorkommen sensibler Daten in S3-Objekten zu finden. S3	22. Oktober 2020
Neues Feature	Sie können jetzt Aufträge zur Erkennung sensibler Daten anhalten und fortsetzen.	16. Oktober 2020
Neuer Inhalt	Es wurden Details zum Schweregradbewertungssystem für Richtlinienergebnisse und Ergebnisse zu sensiblen Daten hinzugefügt.	6. Oktober 2020
Neue Features	Sie können jetzt Statistiken anzeigen, die angeben, wie viele Daten Macie in einzelnen S3-Buckets analysieren kann, wenn Sie einen Erkennungsauftrag für sensible Daten ausführen. Darüber hinaus können Sie jetzt die geschätzten Kosten eines Auftrags anzeigen, wenn Sie einen Auftrag erstellen.	3. September 2020

Neuer Inhalt	Es wurden Informationen zum Konfigurieren, Ausführen und Verwalten von Aufträgen zur Erkennung sensibler Daten hinzugefügt.	31. August 2020
Neue Funktionalität	Verwaltete Datenkennungen können jetzt bestimmte Arten von persönlich identifizierbaren Informationen für Brasilien erkennen.	31. Juli 2020
Aktualisierter Inhalt	Es wurden Informationen zur unterstützten Syntax für reguläre Ausdrücke in benutzerdefinierten Datenkennungen hinzugefügt.	30. Juli 2020
Aktualisierter Inhalt	Hinzufügung von Schlüsselwortanforderungen für verwaltete Datenkennungen und Erhöhung des Kontingents für die Anzahl der Erkenntnisse, die jeder Erkennungsauftrag für sensible Daten erzeugen kann.	17. Juli 2020

Neuer Inhalt	Es wurden Informationen zur Verwendung von Amazon EventBridge und AWS Security Hub zur Überwachung und Verarbeitung von Erkenntnissen hinzugefügt. Dazu gehören das EventBridge Ereignisschema für Erkenntnisse und Ereignisbeispiele für Erkenntnisse aus Richtlinien und sensiblen Daten.	22. Juni 2020
Neuer Inhalt	Es wurden Informationen zum Analysieren und Unterdrücken von Erkenntnissen hinzugefügt.	17. Juni 2020
Neuer Inhalt	Anweisungen zum Konfigurieren von Macie zum Speichern detaillierter Erkennungsergebnisse in einem S3-Bucket hinzugefügt.	2. Juni 2020
Neuer Inhalt	Es wurden Informationen zu den Arten sensibler Daten hinzugefügt, die Macie erkennen kann, sowie zu den Verschlüsselungsanforderungen für die Erkennung sensibler Daten in Amazon S3-Objekten.	28. Mai 2020
Allgemeine Verfügbarkeit	Dies ist die erste öffentliche Version des Amazon Macie-Benutzerhandbuchs.	13. Mai 2020

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.