Leitfaden zur Partnerintegration

AWS Security Hub

AWS Security Hub: Leitfaden zur Partnerintegration

Table of Contents

Überblick über die Integration von Drittanbietern mitAWS Security Hub

Dieser Leitfaden ist gedacht fürAWSPartner Network (APN) Partner, die eine Integration mitAWS Security Hubaus.

Als APN-Partner können Sie auf eine oder mehrere der folgenden Arten in den Security Hub integrieren.

- Senden Sie Ergebnisse an den Security Hub
- Verwenden von Ergebnissen aus dem Security Hub
- Beide senden Erkenntnisse an Security Hub und konsumieren Ergebnisse aus dem Security Hub
- Verwenden Sie Security Hub als Zentrum eines Angebots für Managed Security Service Provider (MSSP)
- Konsultieren Sie mitAWSKunden zur Bereitstellung und Verwendung von Security Hub

Dieser Onboarding-Leitfaden konzentriert sich hauptsächlich auf Partner, die Ergebnisse an den Security Hub senden.

Themen

Warum integrieren mitAWS Security Hub?

AWS Security HubBietet einen umfassenden Überblick über Sicherheitswarnungen und den Sicherheitsstatus von Security Hub -Konten mit hoher Priorität. Security Hub ermöglicht es Partnern wie Ihnen, Sicherheitsergebnisse an Security Hub zu senden, um Ihren Kunden einen Einblick in die von Ihnen generierten Sicherheitsergebnisse zu geben.

Eine Integration mit Security Hub kann auf folgende Weise einen Mehrwert schaffen.

- Befriedigt Ihre Kunden, die eine Security Hub Hub-Integration angefordert haben

- Bietet Ihren Kunden eine einzige Ansicht ihrerAWSsicherheitsbezogene Ergebnisse
- Ermöglicht es neuen Kunden, Ihre Lösung zu finden, wenn sie nach Partnern suchen, die Erkenntnisse zu bestimmten Arten von Sicherheitsereignissen liefern

Bevor Sie eine Integration mit Security Hub aufbauen, prüfen Sie Ihre Gründe für die Integration. Eine Integration ist wahrscheinlicher erfolgreich, wenn Ihre Kunden eine Security Hub Hub-Integration mit Ihrem Produkt wünschen. Sie können eine Integration ausschließlich aus Marketinggründen aufbauen oder neue Kunden gewinnen. Wenn Sie die Integration jedoch ohne aktuellen Kundeneintrag aufbauen und die Bedürfnisse Ihrer Kunden nicht berücksichtigen, führt die Integration möglicherweise nicht zu den erwarteten Ergebnissen.

Senden von Ergebnissen anAWS Security Hub

Als APN-Partner können Sie keine Informationen für Ihre Kunden an Security Hub senden, bis das Security Hub Hub-Team Sie als Suchanbieter ermöglicht. Um als Finding-Provider aktiviert zu sein, müssen Sie die folgenden Onboarding-Schritte ausführen. Dies gewährleistet ein positives Erlebnis Security Hub für Sie und Ihre Kunden.

Befolgen Sie beim Abschließen der Onboarding-Schritte unbedingt die Richtlinien unterthe section called “Grundsätze zur Erstellung und Aktualisierung von Erkenntnissen”,the section called “Richtlinien für ASFFFF-Zuordnung”, undthe section called “Richtlinien für die Verwendung von`BatchImportFindings`API”aus.

1. Ordnen Sie Ihre Sicherheitsergebnisse demAWSSecurity Finding Format (ASFF)
2. Bauen Sie Ihre Integrationsarchitektur auf, um die Ergebnisse an den richtigen regionalen Security Hub Hub-Endpunkt zu bringen. Um dies zu tun, definieren Sie, ob Sie Ergebnisse von Ihren eigenen sendenAWSKonto oder aus den Konten Ihres Kunden heraus.
3. Lassen Sie Ihre Kunden das Produkt für ihr Konto abonnieren. Verwenden Sie dazu die - Konsole oder den`EnableImportFindingsForProduct`API-Operation. Siehe .Verwalten von Produktintegrationenim AWS Security Hub-Benutzerhandbuchaus.

   Sie können das Produkt auch für sie abonnieren. Verwenden Sie dazu eine kontoübergreifende -Rolle für den Zugriff auf`EnableImportFindingsForProduct`API-Operation im Auftrag des Kunden

   In diesem Schritt werden die Ressourcenrichtlinien festgelegt, die erforderlich sind, um Ergebnisse dieses Produkts für dieses Konto zu akzeptieren.

In den folgenden Blogbeiträgen werden einige der bestehenden Partnerintegrationen mit Security Hub behandelt.

- Ankündigung der Cloud Custodian-Integration mitAWS Security Hub
- Verwenden vonAWS Fargateund Prowler senden Erkenntnisse zur Sicherheitskonfiguration überAWSServices für Security Hub
- So importieren SieAWS ConfigRegelbewertungen als Ergebnisse im Security Hub

Vorbereitung auf den Erhalt von Ergebnissen vonAWS Security Hub

Um Ergebnisse zu erhalten vonAWS Security Hubverwenden Sie eine der folgenden Optionen:

- Lassen Sie Ihre Kunden automatisch alle Ergebnisse senden anCloudWatchEreignisse. Ein Kunde kann bestimmte erstellenCloudWatchEreignisregeln, um Ergebnisse an bestimmte Ziele zu senden, z. B. einen SIEM oder einen S3-Bucket.
- Lassen Sie Ihre Kunden bestimmte Ergebnisse oder Ergebnisgruppen aus der Security Hub Hub-Konsole auswählen und dann Maßnahmen ergreifen.

Ihre Kunden können beispielsweise Ergebnisse an ein SIEM, ein Ticketsystem, eine Chat-Plattform oder einen Behebungs-Workflow senden. Dies wäre Teil eines Workflows für Warn-Triage, den ein Kunde in Security Hub durchführt.

Diese werden als benutzerdefinierte Aktionen bezeichnet. Wenn ein Benutzer eine benutzerdefinierte Aktion durchführt, wird einCloudWatch-Ereignis wird für diese spezifischen Erkenntnisse erstellt. Als Partner können Sie diese Fähigkeit nutzen und aufbauenCloudWatchEreignisregeln oder -ziele, die ein Kunde im Rahmen einer benutzerdefinierten Aktion verwenden kann. Beachten Sie, dass diese Funktion nicht automatisch alle Ergebnisse eines bestimmten Typs oder einer bestimmten Klasse an sendetCloudWatchEreignisse. Mit dieser Funktion kann ein Benutzer Maßnahmen zu bestimmten Erkenntnissen ergreifen.

In den folgenden Blogbeiträgen werden Lösungen beschrieben, die die Integration mit Security Hub undCloudWatchEreignisse für benutzerdefinierte Aktionen.

- IntegrierenAWS Security HubBenutzerdefinierte Aktionen mitPagerDuty
- Aktivieren von benutzerdefinierten Aktionen inAWS Security Hub

- So importieren SieAWS ConfigRegelbewertungen als Ergebnisse im Security Hub

Ressourcen zum Lernen vonAWS Security Hub

Die folgenden Materialien können Ihnen helfen, dieAWS Security Hub-Lösung und wieAWSKunden können den Service nutzen.

- Einführung inAWS Security HubVideo
- Security Hub Hub-Benutzerhandbuch
- Security Hub Hub-API-Referenz
- Onboarding-Webinar

Wir empfehlen Ihnen auch, Security Hub in einem IhrerAWSKonten und sammeln Sie praktische Erfahrungen mit dem Service.

Partnervoraussetzungen

Bevor Sie eine Integration mit beginnen könnenAWS Security Hubmüssen Sie mindestens eines der folgenden Kriterien erfüllen:

- Du bist einAWSWählen Sie Tierpartner oder höher aus.
- Du bist dem beigetretenAWSISV-Partnerpfad, und das Produkt, das Sie für die Security Hub Hub-Integration verwenden, hat eineAWSGrundlegender technischer Review (FTR)aus. Dem Produkt wird dann ein „Reviewt vonAWS„Badge.

Sie müssen auch eine gegenseitige Geheimhaltungsvereinbarung mitAWSaus.

Anwendungsfälle für die Integration und erforderliche Berechtigungen

AWS Security HuberlaubtAWSKunden, um Ergebnisse von APN-Partnern zu erhalten. Die Produkte des Partners laufen möglicherweise innerhalb oder außerhalb des KundenAWSKonto. Die Berechtigungskonfiguration im Konto des Kunden unterscheidet sich je nach Modell, das das Partnerprodukt verwendet.

In Security Hub kontrolliert der Kunde immer, welche Partner Ergebnisse an das Konto des Kunden senden können. Kunden können Berechtigungen eines Partners jederzeit widerrufen.

Damit ein Partner Sicherheitsergebnisse an sein Konto senden kann, abonniert der Kunde zunächst das Partnerprodukt in Security Hub. Der Abonnementschritt ist für alle unten aufgeführten Anwendungsfälle erforderlich. Weitere Informationen darüber, wie Kunden Produktintegrationen verwalten, finden Sie unterVerwalten von ProduktintegrationenimAWS Security Hub-Benutzerhandbuchaus.

Nachdem ein Kunde ein Partnerprodukt abonniert hat, erstellt Security Hub automatisch eine Richtlinie für verwaltete Ressourcen. Die Richtlinie erteilt dem Partnerprodukt die Berechtigung zur Verwendung des`BatchImportFindings`-Operation, um Erkenntnisse für das Kundenkonto an den Security Hub zu senden.

Hier sind die häufigsten Fälle für Partnerprodukte, die in Security Hub integriert werden. Die Informationen enthalten die zusätzlichen Berechtigungen, die für jeden Anwendungsfall erforderlich sind.

Partner gehostet: Ergebnisse aus dem Partnerkonto

Dieser Anwendungsfall deckt Partner ab, die ein Produkt selbst hostenAWSKonto. So senden Sie Sicherheitsergebnisse für eineAWSKunde, der Partner ruft die`BatchImportFindings`-Operation vom Partnerproduktkonto aus.

Für diesen Anwendungsfall benötigt das Kundenkonto nur die Berechtigungen, die festgelegt werden, wenn der Kunde das Partnerprodukt abonniert.

Im Partnerkonto ruft der IAM-Prinzipal, der die`BatchImportFindings`Die API-Operation muss eine IAM-Richtlinie haben, die es dem Prinzipal ermöglicht, aufzurufen`BatchImportFindings`aus.

Es ist ein zweistufiger Prozess, dem ein Partnerprodukt Ergebnisse an den Kunden Security Hub senden, ist ein zweistufiger Prozess:

1. Der Kunde erstellt ein Abonnement für ein Partnerprodukt in Security Hub.
2. Security Hub generiert die richtige Richtlinie für verwaltete Ressourcen mit der Bestätigung des Kunden.

Um Sicherheitsergebnisse im Zusammenhang mit dem Konto des Kunden zu senden, verwendet das Partnerprodukt seine eigenen Anmeldeinformationen, um die`BatchImportFindings`API-Operation.

Hier ist ein Beispiel für eine IAM-Richtlinie, die dem Prinzipal im Partnerkonto die erforderlichen Security Hub Hub-Berechtigungen gewährt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "securityhub:BatchImportFindings",
            "Resource": "arn:aws:securityhub:us-west-1:*:product-subscription/company-
name/product-name"
        }
    ]
}
```

Partner gehostet: Ergebnisse aus dem Kundenkonto

Dieser Anwendungsfall deckt Partner ab, die ein Produkt selbst hostenAWS-Konto, verwenden Sie jedoch eine kontoübergreifende Rolle, um auf das Konto des Kunden zuzugreifen. Sie rufen auf`BatchImportFindings`-API-Operation vom Kundenkonto aus.

Für diesen Anwendungsfall rufen Sie die`BatchImportFindings`API-Betrieb, das Partnerkonto übernimmt eine vom Kunden verwaltete IAM-Rolle im Kundenkonto.

Dieser Anruf wird vom Konto des Kunden aus getätigt. Daher muss die Richtlinie für verwaltete Ressourcen zulassen, dass der ARN des Produkts für das Partnerprodukt im Anruf verwendet werden kann. Die Richtlinie für verwaltete Ressourcen von Security Hub gewährt die Berechtigung für das Partnerproduktkonto und den ARN des Partnerprodukts. Das Produkt ARN ist die eindeutige

Kennung des Partners als Anbieter. Da der Anruf nicht vom Partnerproduktkonto stammt, muss der Kunde dem Partnerprodukt ausdrücklich die Erlaubnis erteilen, Ergebnisse an Security Hub zu senden.

Die beste Vorgehensweise für kontoübergreifende Rollen zwischen Partner- und Kundenkonten besteht darin, eine externe Kennung zu verwenden, die der Partner bereitstellt. Diese externe Kennung ist Teil der kontoübergreifenden Richtliniendefinition im Konto des Kunden. Der Partner muss die Kennung angeben, wenn er die Rolle übernimmt. Eine externe Kennung sorgt für eine zusätzliche Sicherheitsebene beim GewährenAWS-Kontozugriff auf einen Partner. Die eindeutige Kennung stellt sicher, dass der Partner das richtige Kundenkonto verwendet.

Die Möglichkeit, dass ein Partnerprodukt Ergebnisse in Security Hub mit einer kontoübergreifenden Rolle an den Kunden senden kann, erfolgt in vier Schritten:

1. Der Kunde oder Partner, der kontoübergreifende Rollen verwendet, die im Auftrag des Kunden arbeiten, startet das Abonnement für ein Produkt in Security Hub.
2. Security Hub generiert die richtige Richtlinie für verwaltete Ressourcen mit der Bestätigung des Kunden.
3. Der Kunde konfiguriert die kontoübergreifenden Rolle entweder manuell oder mitAWS CloudFormationaus. Weitere Informationen zu kontoübergreifenden Rollen finden Sie unterGewähren von Zugriff aufAWS-Konten von DrittenimIAM User Guideaus.
4. Das Produkt speichert die Kundenrolle und die externe ID sicher.

Als Nächstes sendet das Produkt Erkenntnisse an den Security Hub:

1. Das Produkt nenntAWS Security Token Service(AWS STS) um die Kundenrolle zu übernehmen.
2. Das Produkt nenntBatchImportFindingsAPI-Vorgang im Security Hub mit den temporären Anmeldeinformationen der angenommenen Rolle.

Hier finden Sie ein Beispiel für eine IAM-Richtlinie, die die erforderlichen Security Hub Hub-Berechtigungen für die kontoübergreifenden Rolle des Partners gewährt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
```

```
            "Action": "securityhub:BatchImportFindings",
            "Resource": "arn:aws:securityhub:us-west-1:111122223333:product-
subscription/company-name/product-name"
        }
    ]
}
```

Die`Resource`in der Richtlinie wird das spezifische Produktabonnement identifiziert. Dies stellt sicher, dass der Partner nur Ergebnisse für das Partnerprodukt senden kann, das der Kunde abonniert hat.

Kunde gehostet: Ergebnisse aus dem Kundenkonto

Dieser Anwendungsfall deckt Partner ab, die ein Produkt haben, das im Kunden eingesetzt wirdAWSKonto. Die`BatchImportFindings`Die API wird von der Lösung aufgerufen, die im Kundenkonto ausgeführt wird.

Für diesen Anwendungsfall müssen dem Partnerprodukt zusätzliche Berechtigungen erteilt werden, um die`BatchImportFindings`API. Wie diese Berechtigung erteilt wird, hängt von der Partnerlösung und der Konfiguration im Kundenkonto ab.

Ein Beispiel für diesen Ansatz ist ein Partnerprodukt, das auf einer EC2-Instanz im Kundenkonto läuft. Diese EC2-Instanz muss eine EC2-Instanzrolle angehängt haben, die dieser Instanz die Möglichkeit gibt,`BatchImportFindings`API-Operation. Dies ermöglicht es der EC2-Instanz, Sicherheitsergebnisse an das Konto des Kunden zu senden.

Dieser Anwendungsfall entspricht funktional einem Szenario, in dem ein Kunde Erkenntnisse für ein Produkt, das er besitzt, in sein Konto lädt.

Der Kunde ermöglicht es dem Partnerprodukt, Ergebnisse aus dem Kundenkonto an den Kunden im Security Hub zu senden:

1. Der Kunde setzt das Partnerprodukt in seinemAWSKonto manuell mitAWS CloudFormationoder ein anderes Bereitstellungstool.
2. Der Kunde definiert die notwendige IAM-Richtlinie, die das Partnerprodukt verwenden kann, wenn es Ergebnisse an Security Hub sendet.
3. Der Kunde hängt die Richtlinie an die erforderlichen Komponenten des Partnerprodukts an, z. B. eine EC2-Instanz, einen Container oder eine Lambda-Funktion.

Jetzt kann das Produkt Ergebnisse an den Security Hub senden:

1. Das Partnerprodukt verwendet dieAWSSDK oderAWS CLIrufen Sie aufBatchImportFindings-Operation im Security Hub. Es führt den Anruf von der Komponente im Konto des Kunden aus, an der die Richtlinie angehängt ist.
2. Während des API-Aufrufs werden die erforderlichen temporären Anmeldeinformationen generiert, um dieBatchImportFindingsrufen Sie auf, erfolgreich zu sein.

Hier ist ein Beispiel für eine IAM-Richtlinie, die dem Partnerprodukt im Kundenkonto die erforderlichen Security Hub Hub-Berechtigungen gewährt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "securityhub:BatchImportFindings",
            "Resource": "arn:aws:securityhub:us-west-2:111122223333:product-
subscription/company-name/product-name"
        }
    ]
}
```

Partner-Onboarding-Prozess

Als Partner können Sie damit rechnen, mehrere High-Level-Schritte im Rahmen Ihres Onboarding-Prozesses durchzuführen. Sie müssen diese Schritte ausführen, bevor Sie Sicherheitsergebnisse an senden könnenAWS Security Hubaus.

1. Sie initiieren eine Zusammenarbeit mit dem APN-Partnerteam oder dem Security Hub-Team und bekunden Interesse daran, Partner mit Security Hub zu werden. Sie identifizieren die E-Mail-Adressen, die zu Security Hub-Kommunikationskanälen hinzugefügt werden sollen.
2. AWSgibt Ihnen die Onboarding-Materialien des Security Hub Hub-Partners.
3. Du bist zum Security Hub Hub-Partner-Slack-Channel eingeladen, wo du Fragen zu deiner Integration stellen kannst.
4. Sie stellen APN-Partnerkontakten einen Entwurf eines Produktintegrationsmanifests zur Überprüfung zur Verfügung.

   Das Produktintegrationsmanifest enthält Informationen, die verwendet werden, um das Partnerprodukt zu erstellen Amazon Resource Name (ARN) für die Integration mitAWS Security Hubaus.

   Es stellt dem Security Hub Hub-Team Informationen bereit, die auf der Seite des Partneranbieters in der Security Hub Hub-Konsole angezeigt werden. Es wird auch verwendet, um neue verwaltete Erkenntnisse im Zusammenhang mit der Integration vorzuschlagen, die zur Security Hub Insight Library hinzugefügt werden können.

   Diese erste Version des Produktintegrationsmanifests muss nicht die vollständigen Details enthalten. Es sollte jedoch zumindest den Anwendungsfall und die Datensatzinformationen enthalten.

   Weitere Informationen zum Manifest und den erforderlichen Informationen finden Sie unterManifestdateien zur Produktintegrationaus.
5. Das Security Hub Hub-Team gibt Ihnen einen Produkt-ARN für Ihr Produkt. Mit dem ARN senden Sie Erkenntnisse an den Security Hub.
6. Sie bauen Ihre Integration auf, um Ergebnisse an Security Hub zu senden oder Ergebnisse von Security Hub zu erhalten.

Abbildung der Ergebnisse auf ASFF

Um Ergebnisse an Security Hub zu senden, müssen Sie Ihre Ergebnisse demAWSSecurity Finding Format (ASFF)

Der ASFF bietet eine konsistente Beschreibung der Ergebnisse, die geteilt werden könnenAWSSicherheitsdienste, Partner und Kundensicherheitssysteme. Dies reduziert die Integrationsbemühungen, fördert eine gemeinsame Sprache und bietet Implementierern einen Entwurf.

ASFF ist das erforderliche Drahtprotokollformat zum Senden von Ergebnissen anAWS Security Hubaus. Ergebnisse werden als JSON-Dokumente dargestellt, die dem ASFF JSON-Schema und dem RFC-7493 The I-JSON-Nachrichtenformat entsprechen. Einzelheiten zum ASFF-Schema finden Sie unterAWSSecurity Finding Format (ASFF)imAWS Security Hub-Benutzerhandbuchaus.

Siehe the section called “Richtlinien für ASFFFF-Zuordnung”.

Aufbau und Testen der Integration

Sie können alle Tests für Ihre Integration mit einemAWSKonto, das Sie besitzen. Auf diese Weise erhalten Sie einen vollständigen Überblick darüber, wie die Ergebnisse im Security Hub erscheinen. Es hilft Ihnen auch, die Erfahrung des Kunden mit Ihren Sicherheitsergebnissen zu verstehen.

Sie benutzen das`BatchImportFindings`API-Vorgang, um neue und aktualisierte Erkenntnisse an den Security Hub zu senden.

Während des Aufbaus einer Security Hub Hub-IntegrationAWSermutigt Sie, Ihre APN-Partner-Kontakte über den Fortschritt Ihrer Integration auf dem Laufenden zu halten. Sie können auch Ihre APN-Partner-Kontakte um Hilfe bei Integrationsfragen fragen.

Siehe the section called “Richtlinien für die Verwendung von`BatchImportFindings`API”.

7. Sie demonstrieren die Integration in das Security Hub Hub-Produktteam. Diese Integration muss mithilfe eines Kontos nachgewiesen werden, das dem Security Hub Hub-Team gehört.

   Wenn sie mit der Integration vertraut sind, gibt das Security Hub Hub-Team die Genehmigung, Sie als Anbieter aufzulisten.

8. Sie stellen zur VerfügungAWSmit einem endgültigen Manifest zur Überprüfung.

9. Das Security Hub Hub-Team erstellt die Anbieterintegration in die Security Hub Hub-Konsole. Kunden können dann die Integration entdecken und aktivieren.
10. (Optional) Sie unternehmen zusätzliche Marketingmaßnahmen, um Ihre Security Hub Hub-Integration zu fördern. Siehe Go-to-marketAktivitäten.

    Security Hub empfiehlt mindestens, die folgenden Assets bereitzustellen.

    - Ein Demonstrationsvideo (höchstens 3 Minuten) der Arbeitsintegration. Das Video wird für Marketingzwecke verwendet und wird auf derAWS YouTube-Kanal.
    - Ein Ein-Dia-Architekturdiagramm, das zum ersten Aufruf des Security Hub hinzugefügt werden soll.

Go-to-marketAktivitäten

Partner können sich auch an optionalen Marketingaktivitäten beteiligen, um ihreAWS Security Hub-Integration

Wenn Sie Ihre eigenen Marketing-Inhalte im Zusammenhang mit Security Hub erstellen möchten, senden Sie vor der Veröffentlichung des Inhalts einen Entwurf an Ihren APN-Partnermanager zur Überprüfung und Genehmigung. Dies stellt sicher, dass jeder auf Messaging ausgerichtet ist.

AWSPartner Network (APN) -Partner können APN Partner Marketing Central und das MDF-Programm (Market Development Funds) nutzen, um Kampagnen zu erstellen und Finanzierungsunterstützung zu erhalten. Weitere Informationen zu diesen Programmen erhalten Sie von Ihrem Partnermanager.

Eintrag auf der Security Hub Hub-Partnerseite

Nachdem Sie als Security Hub Hub-Partner zugelassen wurden, kann Ihre Lösung auf derAWS Security HubPartnerseiteaus.

Um auf dieser Seite aufgeführt zu werden, geben Sie Ihren APN-Partnerkontakten die folgenden Details an. Dies könnte Ihr Partner Development Manager (PDM), Partner Solution Architect (PSA) oder eine E-Mail an sein<securityhub-pms@amazon.com>aus.

- Eine kurze Beschreibung Ihrer Lösung, deren Integration in Security Hub und den Wert, den die Integration mit Security Hub den Kunden bietet. Diese Beschreibung ist auf 700 Zeichen einschließlich Leerzeichen begrenzt.
- Die URL zu einer Seite, die Ihre Lösung beschreibt. Diese Seite sollte spezifisch für IhreAWSIntegration und insbesondere Ihre Security Hub Hub-Integration. Es sollte sich auf das Kundenerlebnis und den Wert konzentrieren, den Kunden bei der Nutzung der Integration erhalten.
- Eine hochauflösende Kopie Ihres Logos mit 600 x 300 Pixel. Einzelheiten zu den Anforderungen für dieses Logo finden Sie unterthe section called “Logo für Partnerseite”aus.

Pressemitteilung

Als anerkannter Partner können Sie optional eine Pressemitteilung auf Ihrer Website und in den Öffentlichkeitsarbeit veröffentlichen. Die Pressemitteilung muss vonAWSaus.

Bevor Sie die Pressemitteilung veröffentlichen, müssen Sie sie anAWSzur Überprüfung durch APN-Partnermarketing, Security Hub Hub-Führung undAWSExterne Sicherheitsdienste (ESS). Die Pressemitteilung kann ein vorgeschlagenes Zitat für den VP von ESS enthalten.

Um diesen Prozess einzuleiten, arbeiten Sie mit Ihrem PDM. Wir haben einen Service Level Agreement (SLA) von 10 Werktagen, um Pressemitteilungen zu überprüfen.

AWSBlog des Partnernetzwerks (APN)

Wir können Ihnen auch dabei helfen, einen Blogeintrag zu veröffentlichen, den Sie im APN-Blog verfassen. Der Blogeintrag muss sich auf eine Kundengeschichte und einen Anwendungsfall konzentrieren. Es kann nicht nur darin positioniert werden, ein Partner für die Einführung der Integration zu sein.

Wenden Sie sich bei Interesse an Ihr PDM oder PSA, um den Vorgang zu beginnen. APN-Blogs können 8 Wochen oder länger dauern, bis sie endgültig genehmigt und veröffentlicht werden.

Wichtigste Dinge, die Sie über den APN-Blog wissen sollten

Beachten Sie beim Erstellen eines Blog-Beitrags die folgenden Elemente.

Was geht in einen Blogbeitrag?

- Partnerbeiträge sollten lehrreich sein und fundiertes Fachwissen zu einem fürAWSKunden.
- Die ideale Länge beträgt nicht mehr als 1.500 Wörter. Leser schätzen tiefe, pädagogische Inhalte, die ihnen beibringen, was möglich istAWSaus.
- Der Inhalt sollte originell für den APN-Blog sein. Verwenden Sie keine Inhalte aus Quellen wie vorhandenen Blogbeiträgen oder Whitepapern.

Welche anderen Grenzen gibt es beim Posten im APN-Blog?

- Nur Advanced- oder Premier-Tier-Partner können im APN-Blog posten. Es gibt Ausnahmen für Select-Partner, die über eine APN-Programmbezeichnung wie Service Delivery verfügen.
- Jeder Partner ist auf drei Posts pro Jahr begrenzt. Mit Zehntausenden von APN-PartnernAWSmuss in seiner Deckung gerecht sein.
- Jeder Beitrag muss einen technischen Sponsor haben, der die Lösung oder den Anwendungsfall validieren kann.

Wie lange dauert es, einen Blogbeitrag zu bearbeiten, bevor er veröffentlicht wird?

> Nachdem Sie den ersten Entwurf des Blogbeitrags in voller Länge eingereicht haben, dauert die Bearbeitung vier bis sechs Wochen.

Warum für den APN-Blog schreiben?

Ein APN-Blogbeitrag kann die folgenden Vorteile bieten.

- Glaubwürdigkeit— Für APN-Partner, eine Geschichte veröffentlicht vonAWSkann Kunden weltweit beeinflussen.
- Sichtbarkeit— Der APN-Blog ist einer der meistgelesenen Blogs unterAWSmit 1,79 Millionen Seitenaufrufen im Jahr 2019, einschließlich beeinflusstem Traffic.
- Geschäft- APN-Partner-Beiträge verfügen über Connect-Schaltflächen, die Leads über das APN Customer Engagements (ACE) -Programm generieren können.

Welche Art von Inhalt passt am besten?

Die folgenden Arten von Inhalten eignen sich am besten für einen APN-Blogbeitrag.

- Technischer Inhalt ist die beliebteste Art von Geschichte. Dies beinhaltet Lösungsstrahler und Anleitungen. Über 75% der Leser schauen sich diese technischen Inhalte an.
- Kunden schätzen Geschichten der Stufe 200 oder höher, die zeigen, wie etwas funktioniertAWSoder wie ein APN-Partner ein Geschäftsproblem für Kunden gelöst hat.
- Beiträge, die von technischen Experten oder Fachexperten verfasst wurden, schneiden bei weitem das Beste ab.

Glattes Blatt oder Marketingblatt

Ein glattes Blatt ist ein einseitiges Dokument, das Ihr Produkt, seine Integrationsarchitektur und gemeinsame Kunden-Anwendungsfälle umreißt.

Wenn Sie ein glattes Blatt für Ihre Integration erstellen, senden Sie eine Kopie an das Security Hub Hub-Team. Sie werden es zur Partnerseite hinzufügen.

Whitepaper oder eBook

Wenn Sie ein Whitepaper oder E-Book erstellen, in dem Ihr Produkt, seine Integrationsarchitektur und gemeinsame Kunden-Anwendungsfälle beschrieben werden, senden Sie eine Kopie an das Security Hub Hub-Team. Sie werden es zur Security Hub Hub-Partnerseite hinzufügen.

– Webinar

Wenn Sie ein Webinar über Ihre Integration durchführen, senden Sie eine Aufzeichnung des Webinars an das Security Hub Hub-Team. Das Team wird von der Partnerseite aus darauf verlinken.

Das Team kann auch einen Fachexperten für Security Hub zur Verfügung stellen, der an Ihrem Webinar teilnehmen kann.

Demo-Video

Zu Marketingzwecken können Sie ein Demovideo der Arbeitsintegration erstellen. Posten Sie ein solches Video auf Ihrem Videoplattform-Konto, und das Security Hub Hub-Team verlinkt von der Partnerseite aus darauf.

Manifestdateien zur Produktintegration

JederAWS Security Hub Integrationspartner muss ein Produktintegrationsmanifest ausfüllen, das die erforderlichen Details für die vorgeschlagene Integration enthält.

Das Security Hub-Team verwendet diese Informationen auf verschiedene Weise:

- Um Ihren Website-Eintrag zu erstellen
- So erstellen Sie die Produktkarte für die Security Hub-Konsole
- Um das Produktteam über Ihren Anwendungsfall zu informieren.

Um die Qualität der vorgeschlagenen Integration und der bereitgestellten Informationen zu bewerten, verwendet das Security Hub-Team diethe section called “Checkliste für die Produktbereitschaft”. Diese Checkliste bestimmt, ob Ihre Integration bereit ist, gestartet zu werden.

Alle technischen Informationen, die Sie angeben, müssen auch in Ihrer Dokumentation enthalten sein.

Sie können eine PDF-Version des Produktintegrationsmanifests im Bereich Ressourcen auf derAWS Security Hub Partnerseite herunterladen. Beachten Sie, dass die Partnerseite in den Regionen China (Peking) und China (Ningxia) nicht verfügbar ist.

Inhalt

- Logos für die Security Hub-Konsole
- Typen finden
- Hotline
- Bestimmung des Herzschlags
- AWS Security HubInformationen zur Konsole
  - Informationen zum Unternehmen
  - Produktinformationen

Anwendungsfall und Marketinginformationen

Die folgenden Anwendungsfälle können Ihnen bei der KonfigurationAWS Security Hub für verschiedene Zwecke helfen.

Anwendungsbeispiel für die Suche nach Anbietern und Verbrauchern

Erforderlich für unabhängige Softwareanbieter (ISV).

Um Ihren Anwendungsfall rund um Ihre Integration mit zu beschreibenAWS Security Hub, beantworten Sie die folgenden Fragen. Wenn Sie nicht vorhaben, Ergebnisse zu senden oder zu empfangen, beachten Sie dies in diesem Abschnitt und führen Sie dann den nächsten Abschnitt aus.

Die folgenden Informationen müssen in Ihrer Dokumentation enthalten sein.

- Senden Sie Ergebnisse, erhalten Sie Ergebnisse oder beides?
- Welche Art von Ergebnissen werden Sie senden, wenn Sie planen, Ergebnisse zu senden? Senden Sie alle Ergebnisse oder eine bestimmte Teilmenge der Ergebnisse?
- Was werden Sie mit diesen Ergebnissen tun, wenn Sie planen, Ergebnisse zu erhalten? Welche Art von Befunden werden Sie erhalten? Erhalten Sie beispielsweise alle Ergebnisse, Ergebnisse eines bestimmten Typs oder nur bestimmte Ergebnisse, die ein Kunde auswählt?
- Haben Sie vor, die Ergebnisse zu aktualisieren? Wenn ja, welche Felder werden Sie aktualisieren? Security Hub empfiehlt, dass Sie die Ergebnisse aktualisieren, anstatt ständig neue zu erstellen. Die Aktualisierung vorhandener Ergebnisse trägt dazu bei, das Suchgeräusch für Kunden zu verringern.

  Um einen Befund zu aktualisieren, senden Sie einen Befund mit einer Find-ID, die einem Befund zugeordnet ist, den Sie bereits gesendet haben.

Um frühzeitig Feedback zu Ihrem Anwendungsfall und Ihren Datensätzen zu erhalten, wenden Sie sich an den APN-Partner oder das Security Hub-Team.

Anwendungsfall Beratungspartner (CP)

Erforderlich, wenn Sie ein Security Hub-Beratungspartner sind.

Geben Sie zwei Kundenanwendungsfälle für Ihre Arbeit mit Security Hub an. Dies können private Anwendungsfälle sein. Das Security Hub-Team bewirbt sie nirgends. Sie sollten eine oder beide der folgenden Aktionen beschreiben.

- Wie helfen Sie Kunden beim Bootstrap Security Hub? Haben Sie beispielsweise Kunden dabei geholfen, professionelle Services, ein Terraform-Modul oder eineAWS CloudFormation Vorlage zu verwenden?
- Wie unterstützen Sie Kunden bei der Operationalisierung und Erweiterung von Security Hub? Haben Sie beispielsweise Vorlagen für Reaktionen oder Abhilfemaßnahmen bereitgestellt, benutzerdefinierte Integrationen erstellt oder Business Intelligence-Tools verwendet, um ein Dashboard für Führungskräfte einzurichten?

Datensätze

Erforderlich, wenn Sie Ergebnisse an den Security Hub senden.

Geben Sie für die Ergebnisse, die Sie an Security Hub senden, die folgenden Informationen an.

- Die Ergebnisse in ihrem nativen Format wie JSON oder XML
- Ein Beispiel dafür, wie Sie die Ergebnisse in dasAWS Security Finding Format (ASFF) konvertieren

Teilen Sie dem Security Hub-Team mit, ob Sie Updates für den ASFF benötigen, um Ihre Integration zu unterstützen.

Architektur

Erforderlich, wenn Sie Ergebnisse an den Security Hub senden oder Ergebnisse vom Security Hub erhalten haben.

Beschreiben Sie, wie Sie sich in Security Hub integrieren werden. Diese Informationen müssen auch in Ihrer Dokumentation enthalten sein.

Sie müssen Architekturdiagramme bereitstellen. Wenn Sie Ihre Architekturdiagramme erstellen, beachten Sie Folgendes:

- WelcheAWS Dienste, Betriebssystemagenten usw. werden Sie verwenden?
- Wenn Sie Ergebnisse an Security Hub senden, senden Sie die Ergebnisse dann vomAWS Kundenkonto oder von Ihrem eigenenAWS Konto aus?
- Wie werden Sie die CloudWatch Events-Integration verwenden, falls Sie Ergebnisse erhalten?
- Wie werden Sie die Ergebnisse in ASFF umwandeln?
- Wie werden Sie Ergebnisse stapeln, den Status der Ergebnisse verfolgen und Drosselungsgrenzen vermeiden?

Konfiguration

Erforderlich, wenn Sie Ergebnisse an den Security Hub senden oder Ergebnisse vom Security Hub erhalten haben.

Beschreiben Sie, wie ein Kunde Ihre Integration mit Security Hub konfigurieren wird.

Sie müssen mindestensAWS CloudFormation Vorlagen oder eine ähnliche Infrastruktur wie Codevorlagen verwenden. Einige Partner haben eine Benutzeroberfläche bereitgestellt, um die Integration mit einem Klick zu unterstützen.

Die Konfiguration sollte nicht länger als 15 Minuten dauern. Ihre Produktdokumentation muss auch Konfigurationshinweise für Ihre Integration enthalten.

Durchschnittliche Ergebnisse pro Tag pro Kunde

Erforderlich, wenn Sie Ergebnisse an den Security Hub senden.

Wie viele Finding-Updates pro Monat (Durchschnitt und Maximum) erwarten Sie in Ihrem Kundenstamm an Security Hub zu senden? Schätzungen in Größenordnungen sind akzeptabel.

Latency

Erforderlich, wenn Sie Ergebnisse an den Security Hub senden.

Wie schnell werden Ergebnisse stapeln und an den Security Hub senden? Mit anderen Worten, wie hoch ist die Latenz von der Erstellung des Befundes in Ihrem Produkt bis zum Senden an Security Hub?

Diese Informationen müssen in Ihrer Produktdokumentation für Ihre Integration enthalten sein. Dies ist eine häufig gestellte Frage von Kunden.

Unternehmens- und Produktbeschreibung

Erforderlich für alle Integrationen mit Security Hub.

Beschreiben Sie kurz Ihr Unternehmen und Ihr Produkt, wobei der Schwerpunkt auf der Art Ihrer Security Hub-Integration liegt. Wir verwenden dies auf unserer Security Hub-Partnerseite.

Wenn Sie mehrere Produkte in Security Hub integrieren, können Sie für jedes Produkt eine separate Beschreibung angeben. Wir kombinieren sie jedoch zu einem einzigen Eintrag auf der Partnerseite.

Jede Beschreibung darf nicht mehr als 700 Zeichen mit Leerzeichen enthalten.

Inhalte der Partnerwebsite

Erforderlich für alle Integrationen mit Security Hub.

Sie müssen mindestens eine URL angeben, die Sie für den Hyperlink Weitere Informationen auf der Security Hub-Partnerseite verwenden können. Es sollte eine Marketing-Landingpage sein, die die Integration zwischen Ihrem Produkt und Security Hub beschreibt.

Wenn Sie mehrere Produkte in Security Hub integrieren, können Sie eine einzige Landingpage für sie einrichten. Security Hub empfiehlt, dass diese Landingpage einen Link zu Ihren Konfigurationsanweisungen enthält.

Sie können auch Links zu anderen Ressourcen wie Blogs, Webinaren, Demovideos oder Whitepapers bereitstellen. Security Hub wird auch Links zu denen von der Partnerseite aus erstellen.

Logo für Partnerseite

Erforderlich für alle Security Hub-Integrationen.

Geben Sie eine URL zu einem Logo an, das auf der Security Hub-Partnerseite angezeigt werden soll. Das Logo muss folgende Kriterien erfüllen:

- Größe: 600 x 300 Pixel
- Schnitt: eng anliegend ohne Polsterung
- Hintergrund: transparent
- Format: PNG

Logos für die Security Hub-Konsole

Für alle Integrationen erforderlich.

Geben Sie URLs für die Logos für den hellen Modus und den dunklen Modus an, die auf der Security Hub-Konsole angezeigt werden sollen.

Die Logos müssen folgende Kriterien erfüllen:

- Format: SVG
- Größe: 175 x 40 Pixel. Wenn es größer ist, sollte das Bild dieses Verhältnis verwenden.
- Schnitt: eng, ohne Polsterung
- Hintergrund: transparent

Detaillierte Richtlinien für das kleine Logo finden Sie unterthe section called “Richtlinien für das Konsolenlogo”.

Typen finden

Erforderlich, wenn Sie Ergebnisse an den Security Hub senden.

Stellen Sie eine Tabelle bereit, in der die von Ihnen verwendeten Suchtypen im ASFF-Format und deren Ausrichtung auf Ihre systemeigenen Findungstypen dokumentiert sind. Einzelheiten zum Suchen von Typen in ASFF finden Sie unter Typtaxonomie für ASFF im AWS Security HubBenutzerhandbuch.

Zudem empfehlen wir die Aufnahme dieser Informationen in Ihre Produktdokumentation.

Hotline

Erforderlich für alle Integrationen mit Security Hub.

Geben Sie eine E-Mail-Adresse und eine Telefonnummer oder Pager-Nummer für einen technischen Ansprechpartner an. Security Hub wird sich mit diesem Ansprechpartner in Verbindung setzen, wenn technische Probleme auftreten, z. B. wenn eine Integration nicht mehr funktioniert.

Stellen Sie außerdem einen rund um die Uhr verfügbaren Ansprechpartner für schwerwiegende technische Probleme bereit.

Bestimmung des Herzschlags

Wird empfohlen, wenn Ergebnisse an den Security Hub senden.

Können Sie Security Hub alle fünf Minuten einen „Heartbeat“ -Befund senden, der darauf hinweist, dass Ihre Integration mit Security Hub funktioniert?

Wenn Sie können, verwenden Sie dazu den Suchtyp`Heartbeat`.

AWS Security HubInformationen zur Konsole

Stellen Sie demAWS Security Hub Team einen JSON-Text zur Verfügung, der die folgenden Informationen enthält. Security Hub verwendet diese Informationen, um Ihren Produkt-ARN zu erstellen, die Anbieterliste in der Konsole anzuzeigen und Ihre vorgeschlagenen Managed Insights in die Security Hub Insight-Bibliothek aufzunehmen.

Informationen zum Unternehmen

Die Unternehmensinformationen enthalten Informationen über Ihr Unternehmen. Ein Beispiel:

```
{
    "id": "example",
    "name": "Example Corp",
    "description": "Example Corp is a network security company that monitors your
 network for vulnerabilities.",
}
```

Die Unternehmensinformationen enthalten die folgenden Felder:

Feld	Erforderlich	Beschreibung
`id`	Ja	Die eindeutige Kennung des Unternehm ens. Die Unternehmens-ID muss unternehm ensübergreifend eindeutig sein. Dies ist wahrscheinlich dasselbe oder ähnlich wie`name`. Typ: Zeichenfolge

Feld	Erforderlich	Beschreibung
		Mindestlänge: 5 Zeichen Maximale Länge: 24 Zeichen Erlaubte Zeichen: Kleinbuchstaben, Zahlen und Bindestriche Muss mit einem Kleinbuchstaben beginnen. Muss mit einem Kleinbuchstaben oder einer Zahl beginnen.
`name`	Ja	Der Name des Unternehmens des Anbieters , der auf der Security Hub-Konsole angezeigt werden soll. Typ: Zeichenfolge Maximale Länge: 16 Zeichen
`description`	Ja	Die Beschreibung des Unternehmens des Anbieters, die auf der Security Hub-Konsole angezeigt werden soll. Typ: Zeichenfolge Maximale Länge: 200 Zeichen

Produktinformationen

In diesem Abschnitt finden Sie Informationen zu Ihrem Produkt. Ein Beispiel:

```
{
    "IntegrationTypes": ["SEND_FINDINGS_TO_SECURITY_HUB"],
    "id": "example-corp-network-defender",
    "regionsNotSupported": "us-west-1",
    "commercialAccountNumber": "111122223333",
    "govcloudAccountNumber": "444455556666",
    "chinaAccountNumber": "777788889999",
    "name": "Example Corp Product",
```

```
    "description": "Example Corp Product is a managed threat detection service.",
    "importType": "BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT",
    "category": "Intrusion Detection Systems (IDS)",
    "marketplaceUrl": "marketplace_url",
    "configurationUrl": "configuration_url"
}
```

Die Produktinformationen enthalten die folgenden Felder.

Feld	Erforderlich	Beschreibung
`IntegrationType`	Ja	Gibt an, ob Ihr Produkt Ergebnisse an Security Hub sendet, Ergebnisse von Security Hub empfängt oder ob sowohl Ergebnisse gesendet als auch empfangen werden. Lassen Sie dieses Feld leer, wenn Sie ein Beratungspartner sind. Typ: Zeichenfolge-Array Zulässige Werte: `SEND_FINDINGS_TO_SECURITY_HUB` | `RECEIVE_FINDINGS_FROM_SECURITY_HUB`
`id`	Ja	Die eindeutige Kennung des Produkts. Diese müssen innerhalb eines Unternehmens eindeutig sein. Sie müssen nicht unternehm ensübergreifend eindeutig sein. Dies ist wahrscheinlich dasselbe oder ähnlich wie`name`. Typ: Zeichenfolge Mindestlänge: 5 Zeichen Maximale Länge: 24 Zeichen Erlaubte Zeichen: Kleinbuchstaben, Zahlen und Bindestriche

Feld	Erforderlich	Beschreibung
		Muss mit einem Kleinbuchstaben beginnen. Muss mit einem Kleinbuchstaben oder einer Zahl beginnen.
`regionsNotSupported`	Ja	Welche der folgendenAWS Regionen unterstützen Sie nicht? Mit anderen Worten, in welchen Regionen sollte Security Hub Sie nicht als Option auf unserer Partnerseite in der Security Hub-Konsole anzeigen? Typ: Zeichenfolge Geben Sie nur den Regionalcode ein. Zum Beispiel `us-west-1` . Eine Liste der Regionen finden Sie unter Regionale Endpunkte in der Allgemeine AWS-Referenz. Die Regionscodes fürAWS GovCloud (US) lauten`us-gov-west-1` (fürAWS GovCloud (US-West)) und`us-gov-east-1` (fürAWS GovCloud (US-Ost)). Die Regionalcodes für die chinesischen Regionen lauten`cn-north-1` (für China (Peking)) und`cn-northwest-1` (für China (Ningxia)).

Feld	Erforderlich	Beschreibung
`commercialAccountNumber`	Ja	Die primäreAWS Kontonummer für das Produkt für dieAWS Regionen. Wenn Sie Ergebnisse an Security Hub senden, hängt das von Ihnen angegebene Konto davon ab, von wo Sie die Ergebnisse senden. • Von deinemAWS Konto. Geben Sie in diesem Fall die Kontonummer an, die Sie für die Einreichung der Ergebnisse verwendet haben. • Aus demAWS Konto des Kunden. In diesem Fall empfiehlt Security Hub, dass Sie die primäre Kontonummer angeben, die Sie zum Testen der Integration verwenden. Idealerweise verwenden Sie dasselbe Konto für alle Ihre Produkte in allen Regionen. Wenn dies nicht möglich ist, wenden Sie sich an das Security Hub-Team. Wenn Sie nur Ergebnisse von Security Hub erhalten, ist diese Kontonummer nicht erforderlich. Typ: Zeichenfolge

Feld	Erforderlich	Beschreibung
`govcloudAccountNumber`	Nein	Die primäreAWS Kontonummer für das Produkt fürAWS GovCloud (US) Regionen (falls Ihr Produkt in den Regionen verfügbar istAWS GovCloud (US)). Wenn Sie Ergebnisse an Security Hub senden, hängt das von Ihnen angegebene Konto davon ab, von wo Sie die Ergebnisse senden. • Von deinemAWS Konto. Geben Sie in diesem Fall die Kontonummer an, die Sie für die Einreichung der Ergebnisse verwendet haben. • Aus demAWS Konto des Kunden. In diesem Fall empfiehlt Security Hub, dass Sie die primäre Kontonummer angeben, die Sie zum Testen der Integration verwenden. Idealerweise verwenden Sie dasselbe Konto für alle Ihre Produkte in allenAWS GovCloud (US) Regionen. Wenn dies nicht möglich ist, wenden Sie sich an das Security Hub-Team. Wenn Sie nur Ergebnisse von Security Hub erhalten, ist diese Kontonummer nicht erforderlich. Typ: Zeichenfolge

Feld	Erforderlich	Beschreibung
`chinaAccountNumber`	Nein	Die primäreAWS Kontonummer für das Produkt für die Regionen China (wenn Ihr Produkt in den chinesischen Regionen verfügbar ist). Wenn Sie Ergebnisse an Security Hub senden, hängt das von Ihnen angegebene Konto davon ab, von wo Sie die Ergebnisse senden. • Von deinemAWS Konto. Geben Sie in diesem Fall die Kontonummer an, die Sie für die Einreichung der Ergebnisse verwendet haben. • Aus demAWS Konto des Kunden. In diesem Fall empfiehlt Security Hub, dass Sie die primäre Kontonummer angeben, die Sie zum Testen der Produktintegration verwenden. Idealerweise verwenden Sie dasselbe Konto für alle Ihre Produkte in allen Regionen Chinas. Wenn dies nicht möglich ist, wenden Sie sich an das Security Hub-Team. Wenn Sie nur Ergebnisse von Security Hub erhalten, kann dies jedes Konto sein, das Sie in einer Region in China besitzen. Typ: Zeichenfolge
`name`	Ja	Der Name des Produkts des Anbieters, der auf der Security Hub-Konsole angezeigt werden soll. Typ: Zeichenfolge Maximale Länge: 24 Zeichen

Feld	Erforderlich	Beschreibung
`description`	Ja	Die Beschreibung des Produkts des Anbieters , die auf der Security Hub-Konsole angezeigt werden soll. Typ: Zeichenfolge Maximale Länge: 200 Zeichen
`importType`	Ja	Die Art der Ressourcenrichtlinie für den Partner. Während des Partner-Onboarding-Prozesse s können Sie eine der folgenden Ressource nrichtlinien angeben oder angeben`NEITHER`. • Mit`BATCH_IMPORT_FINDINGS_FROM_ PRODUCT_ACCOUNT` können Sie Ergebniss e nur von dem Konto aus, das in Ihrem Produkt-ARN aufgeführt ist, an Security Hub senden. • Mit`BATCH_IMPORT_FINDINGS_FROM_ CUSTOMER_ACCOUNT` können Sie nur Befunde von dem Kundenkonto senden, das Sie abonniert hat. Typ: Zeichenfolge Gültige Werte: `BATCH_IMPORT_FINDI NGS_FROM_PRODUCT_ACCOUNT` `|BATCH_IMPORT_FINDINGS_FROM_ CUSTOMER_ACCOUNT |` `NEITHER`

Feld	Erforderlich	Beschreibung
`category`	Ja	Die Kategorien, die Ihr Produkt definieren. Ihre Auswahl wird auf der Security Hub-Konsole angezeigt. Wählen Sie bis zu drei Kategorien. Benutzerdefinierte Auswahlen sind nicht zulässig. Wenn Sie der Meinung sind, dass Ihre Kategorie fehlt, wenden Sie sich an das Security Hub-Team. Typ: Array Verfügbare Kategorien: • `API Firewall` • `Asset Management` • `AV Scanning and Sandboxing` • `Backup and Disaster Recovery` • `Breach and Attack Simulation` • `Bug Bounty Platform` • `Certificate Management` • `Cloud Access Security Broker` • `Cloud Security Posture Management` • `Configuration and Patch Management` • `Configuration Management Database (CMDB)` • `Consulting Partner` • `Container Security` • `Cyber Range` • `Data Access Management`

Feld	Erforderlich	Beschreibung
		• Data Classification • Data Loss Prevention • Data Masking and Tokenization • Database Activity Monitoring • DDoS Protection • Deception • Device Control • Dynamic Application Security Testing • Data Encryption • Email Gateway • Encrypted Search • Endpoint Detection and Response (EDR) • Endpoint Forensics • Forensics Toolkit • Fraud Detection • Governance, Risk, and Compliance (GRC) • Host-based Intrusion Detection (HIDs) • Human Resources Information System • Interactive Application Security Testing (IAST) • Instant Messaging • IoT Security • IT Security Training • IT Ticketing and Incident Management

Feld	Erforderlich	Beschreibung
		• `Managed Security Service Provider (MSSP)` • `Micro-Segmentation` • `Multi-Cloud Management` • `Multi-Factor Authentication` • `Network Access Control (NAC)` • `Network Firewall` • `Network Forensics` • `Network Intrusion Detection Systems (IDS)` • `Network Intrusion Prevention Systems (IPS)` • `Phishing Simulation and Training` • `Privacy Operations` • `Privileged Access Management` • `Rogue Device Detection` • `Runtime Application Self-Protection (RASP)` • `Secure Web Gateway`
`marketplaceUrl`	Nein	Die URL zu IhremAWS Marketplace Produktziel. Die URL wird in der Security Hub-Konsole angezeigt. Typ: Zeichenfolge Dies muss eineAWS Marketplace URL sein. Lassen Sie dieses Feld leer, wenn Sie keinAWS Marketplace Angebot haben.

Feld	Erforderlich	Beschreibung
`configurationUrl`	Ja	Die URL zu Ihrer Produktdokumentation zur Integration mit Security Hub. Dieser Inhalt wird auf Ihrer Website oder auf einer von Ihnen verwalteten Webseite, z. B. einer GitHub Seite, gehostet. Typ: Zeichenfolge Ihre Dokumentation sollte die folgenden Informationen enthalten. • Anweisungen zur Konfiguration • Links zuAWS CloudFormation Vorlagen (falls erforderlich) • Informationen zu Ihrem Anwendungsfall für die Integration • Latency • ASFF-Zuweisung • Folgende Ergebnisarten • Architektur

Richtlinien und Checklisten

Wenn Sie die benötigten Materialien für Ihre vorbereitenAWS Security HubIntegration, verwenden Sie diese Richtlinien.

Die Bereitschaftscheckliste wird verwendet, um eine abschließende Überprüfung der Integration durchzuführen, bevor Security Hub sie Security Hub Hub-Kunden zur Verfügung stellt.

Themen

Richtlinien für das Logo, das auf derAWS Security HubKonsole

Damit das Logo auf derAWS Security HubConsole, befolgen Sie diese Richtlinien.

Hell- und Dunkel-Modi

Sie müssen sowohl einen Lichtmodus als auch eine Dunkelmodus-Version des Logos angeben.

Format

SVG-Dateiformat

Hintergrundfarbe

Transparent

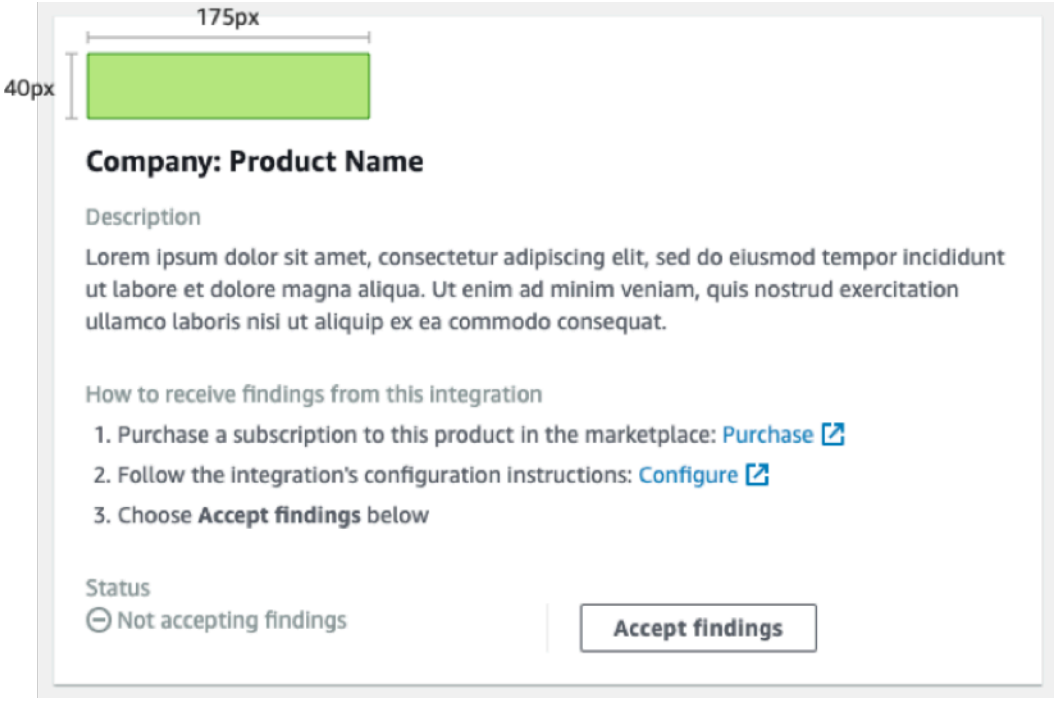
Größe

Das ideale Verhältnis ist 175 px breit und 40 px hoch.

Die Mindesthöhe beträgt 40 px.

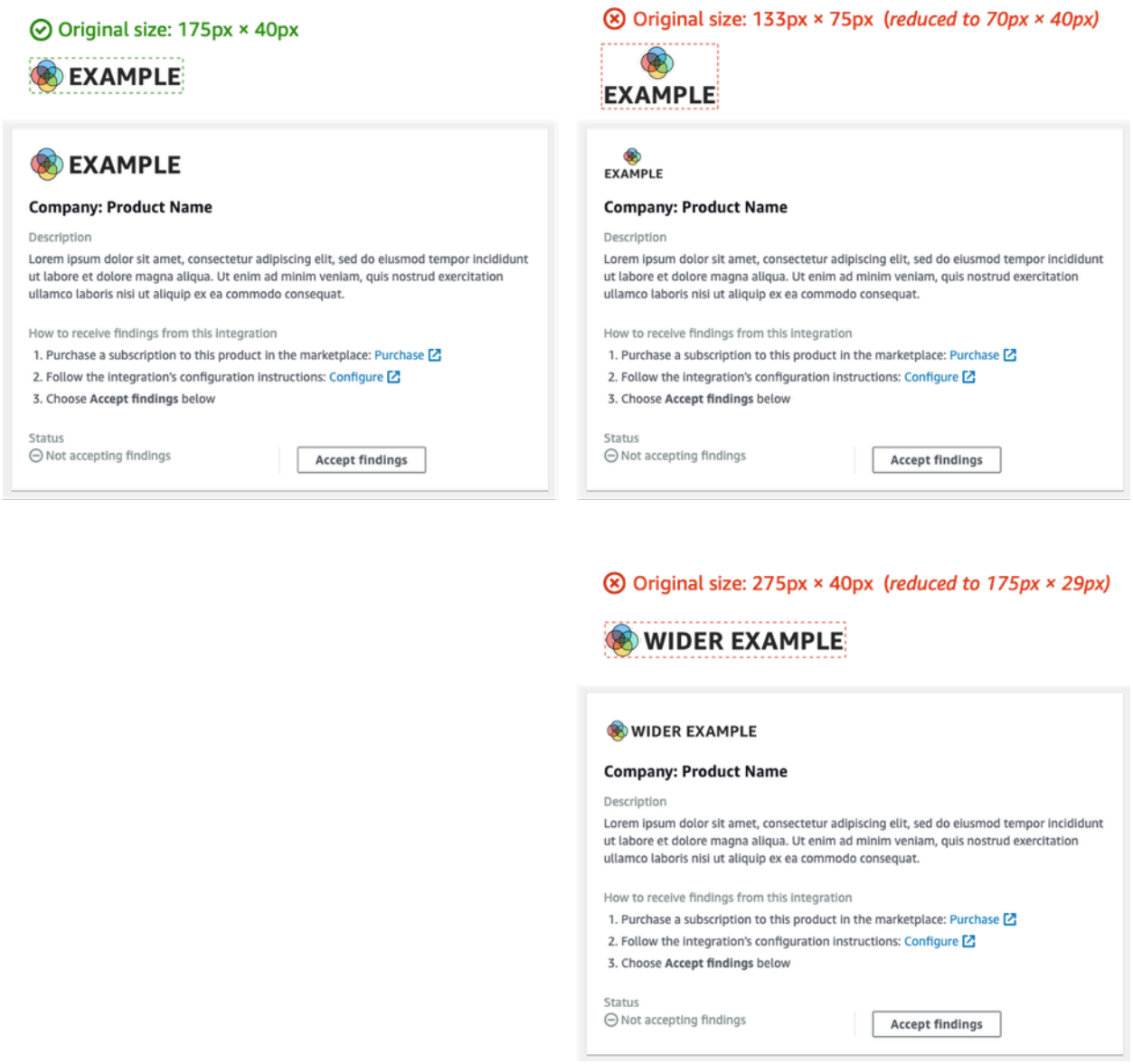
Rechteckige Logos funktionieren am besten.

Die folgende Abbildung zeigt, wie ein ideales Logo auf der Security Hub Hub-Konsole angezeigt wird.



Wenn Ihr Logo nicht mit diesen Abmessungen übereinstimmt, reduziert Security Hub die Größe auf eine maximale Höhe von 40 px und eine maximale Breite von 175 px. Dies wirkt sich darauf aus, wie das Logo auf der Security Hub Hub-Konsole angezeigt wird.

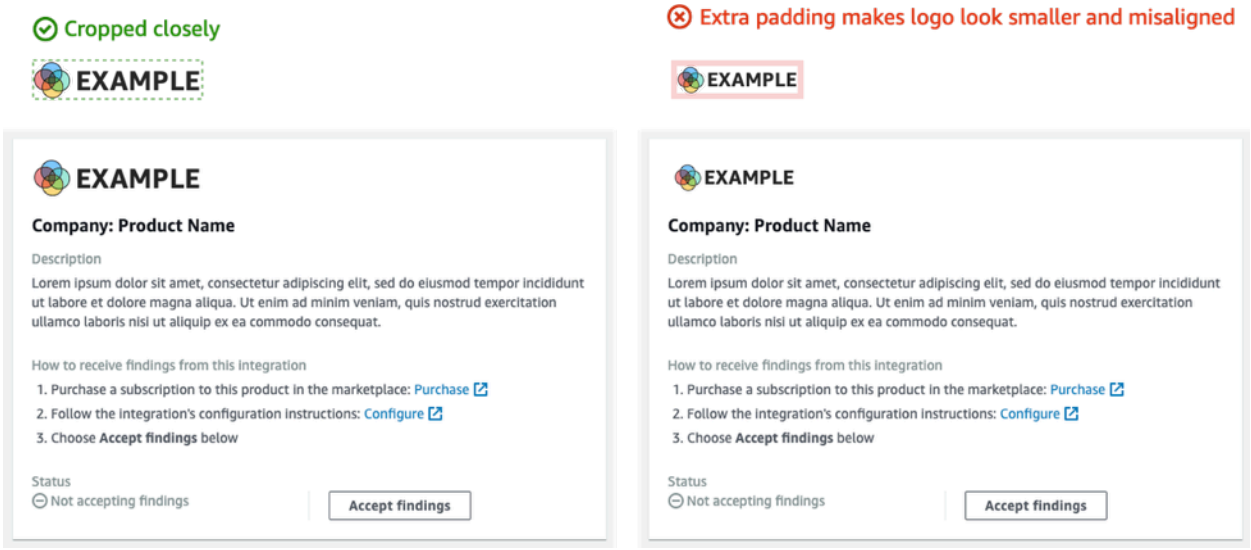
Das folgende Bild vergleicht die Anzeige eines Logos, das die ideale Größe verwendete, mit Logos, die breiter oder größer waren.



Zuschneiden

Beschneiden Sie das Logo-Bild so nah wie möglich. Stellen Sie keine zusätzliche Polsterung bereit.

Die folgende Abbildung zeigt den Unterschied zwischen einem eng abgeschnittenen Logo und einem Logo mit zusätzlicher Polsterung.



Grundsätze zur Erstellung und Aktualisierung von Erkenntnissen

Wie Sie planen, wie Sie Ergebnisse in erstellen und aktualisieren.AWS Security HubBeachten Sie die folgenden Grundsätze.

Machen Sie Ergebnisse spezifisch, damit Kunden leicht Maßnahmen ergreifen können.

Kunden möchten Reaktions- und Behebungsmaßnahmen automatisieren und Ergebnisse mit anderen Ergebnissen korrelieren. Um dies zu unterstützen, sollten Ergebnisse folgende Merkmale aufweisen:

- Sie sollten sich im Allgemeinen mit einer einzelnen oder primären Ressource befassen.
- Sie sollten einen einzigen Findetyp haben.
- Sie sollten sich mit einem einzigen Sicherheitsereignis befassen.

Wenn ein Befund Daten für mehrere Sicherheitsereignisse enthält, ist es für Kunden schwieriger, Maßnahmen bei der Suche zu ergreifen.

Ordnen Sie alle Ihre Suchfelder demAWSSecurity Finding Format (ASFF) Erlauben Sie Kunden, sich auf Security Hub als Quelle der Wahrheit zu verlassen.

Kunden erwarten, dass jedes Feld, das in Ihrem nativen Suchformat vorliegt, auch im Security Hub ASFF dargestellt wird.

Kunden möchten, dass alle Daten in der Security Hub Hub-Version des Ergebnisses vorhanden sind. Fehlende Daten führen dazu, dass sie das Vertrauen in Security Hub als zentrale Quelle für Sicherheitsinformationen verlieren.

Minimieren Sie Redundanz bei Ergebnissen. Überwältigen Sie Kunden nicht damit, Volumen zu finden.

Security Hub ist kein allgemeines Tool zur Protokollverwaltung. Sie sollten Erkenntnisse an Security Hub senden, die sehr umsetzbar sind und dass Kunden direkt auf andere Ergebnisse reagieren, beheben oder mit ihnen korrelieren können.

Wenn die Suche nur geringfügig geändert wird, aktualisieren Sie die Suche, anstatt eine neue Erkenntnis zu erstellen.

Wenn es eine größere Änderung des Ergebnisses gibt, z. B. am Schweregrad oder der Ressourcenkennung, erstellen Sie eine neue Erkenntnis.

Beispielsweise ist es nicht sehr umsetzbar, Erkenntnisse für einzelne Portscans in Echtzeit zu erstellen. Da das Scannen von Ports kontinuierlich erfolgen kann, würde es zu einer großen Menge an Erkenntnissen führen. Es ist weitaus überzeugender und präziser, einfach die letzte Scanzeit zu aktualisieren und die Scan-Zählung auf einen einzigen Befund für einen Port-Scan an einem MongoDB-Port von einem TOR-Knoten aus zu zählen.

Ermöglichen Sie Kunden, ihre Ergebnisse anzupassen, um sie aussagekräftiger zu machen.

Kunden möchten in der Lage sein, bestimmte Suchfelder anzupassen, um sie für ihre Umgebung oder Anforderungen relevanter zu machen.

Kunden möchten z. B. in der Lage sein, Notizen und Tags hinzuzufügen und Schweregradwerte basierend auf dem Kontotyp oder dem Typ der Ressource, mit der die Suche verknüpft ist, anzupassen.

Richtlinien für die Abbildung von Ergebnissen in dieAWSSecurity Finding Format (ASFF)

Beachten Sie die folgenden Richtlinien, um Ihre Ergebnisse dem ASFF zuzuordnen. Ausführliche Beschreibungen jedes ASFF-Feldes und -Objekts finden Sie unterAWSSecurity Finding Format (ASFF)imAWS Security Hub-Benutzerhandbuchaus.

Identifizieren von Informationen

`SchemaVersion` ist immer `2018-10-08`.

`ProductArn`ist der ARNAWS Security Hubweist dir zu.

`Id`ist der Wert, den Security Hub verwendet, um Ergebnisse zu indizieren. Die Erkennungskennung muss eindeutig sein, um sicherzustellen, dass andere Ergebnisse nicht überschrieben werden. Um eine Suche zu aktualisieren, übermitteln Sie die Suche erneut mit demselben Bezeichner.

`GeneratorId`kann das gleiche sein wie`Id`oder kann sich auf eine diskrete Logikeinheit beziehen, z. B.GuardDutyDetektor-ID,AWS ConfigRekorder-ID oder IAM Access Analyzer-ID.

Title und Description

`Title`sollte einige Informationen über die betroffene Ressource enthalten.`Title`Dies ist auf 256 Zeichen beschränkt, einschließlich Leerzeichen.

Fügen Sie längere detaillierte Informationen hinzu`Description`aus.`Description`Dies ist auf 1024 Zeichen beschränkt, einschließlich Leerzeichen. Sie können erwägen, Beschreibungen zu Kürzen hinzuzufügen. Ein Beispiel:

```
"Title": "Instance i-12345678901 is vulnerable to CVE-2019-1234",
"Description": "Instance i-12345678901 is vulnerable to CVE-2019-1234. This
 vulnerability affects version 1.0.1 of widget-1 and earlier, and can lead to buffer
 overflow when someone sends a ping.",
```

Typen finden

Sie geben Ihre Informationen über den Suchtyp in`FindingProviderFields.Types`aus.

`Types`sollte mit der übereinstimmenTaxonomie der ASFFaus.

Bei Bedarf können Sie einen benutzerdefinierten Klassifikator (den dritten Namespace) angeben.

Zeitstempel

Das ASFF-Format enthält ein paar verschiedene Zeitstempel.

`CreatedAt` und **`UpdatedAt`**

Sie müssen einreichen`CreatedAt`und`UpdatedAt`jedes Mal wenn Sie anrufen`BatchImportFindings`für jeden Befund.

Die Werte müssen mit dem ISO8601-Format in Python 3.8 übereinstimmen.

```
datetime.datetime.utcnow().replace(tzinfo=datetime.timezone.utc).isoformat()
```

`FirstObservedAt` und `LastObservedAt`

`FirstObservedAt`und`LastObservedAt`muss übereinstimmen, wenn Ihr System den Befund beobachtet hat. Wenn Sie diese Informationen nicht aufzeichnen, müssen Sie diese Zeitstempel nicht einreichen.

Die Werte entsprechen dem ISO8601-Format in Python 3.8.

```
datetime.datetime.utcnow().replace(tzinfo=datetime.timezone.utc).isoformat()
```

Severity

Sie geben Informationen zum Schweregrad im`FindingProviderFields.Severity`-Objekt, das die folgenden Felder enthält.

`Original`

Der Schweregrad Ihres Systems.`Original`kann eine beliebige Zeichenfolge sein, um das von Ihnen verwendete System aufzunehmen.

`Label`

Der erforderliche Security Hub Hub-Indikator für den Schweregrad der Ermittlung. Die zulässigen Werte lauten wie folgt.

- `INFORMATIONAL`- Es wurde kein Problem gefunden.
- `LOW`— Das Problem erfordert keine eigenen Maßnahmen.
- `MEDIUM`— Das Problem muss angegangen werden, aber nicht dringend.
- `HIGH`— Das Problem muss vorrangig behandelt werden.
- `CRITICAL`— Das Problem muss sofort behoben werden, um weitere Schäden zu vermeiden.

Ergebnisse, die konform sind, sollten immer haben`Label`Stellen Sie auf`INFORMATIONAL`aus. Beispiele für`INFORMATIONAL`Ergebnisse sind Ergebnisse aus Sicherheitsüberprüfungen, die bestanden haben undAWS Firewall ManagerErgebnisse, die behoben werden.

Kunden sortieren die Ergebnisse oft nach ihrem Schweregrad, um ihren Sicherheitsoperationsteams eine Aufgabenliste zu geben. Seien Sie konservativ, wenn Sie den Schweregrad der Suche`HIGH`oder`CRITICAL`aus.

Ihre Integrationsdokumentation muss Ihre Mapping-Begründung enthalten.

Remediation

`Remediation`hat zwei Elemente. Diese Elemente werden auf der Security Hub Hub-Konsole kombiniert.

`Remediation.Recommendation.Text`Die Datei befindet sich imAbhilfeAbschnitt der Erkennungsdetails. Es ist mit dem Wert von verknüpft`Remediation.Recommendation.Url`aus.

Derzeit zeigen nur Erkenntnisse aus Security Hub Hub-Standards, IAM Access Analyzer und Firewall Manager Hyperlinks zur Dokumentation zur Behebung des Findens an.

SourceUrl

Verwenden Sie nur`SourceUrl`wenn Sie Ihrer Konsole eine vertiefte URL für diese spezifische Befund bereitstellen können. Andernfalls lassen Sie es aus dem Mapping aus.

Security Hub unterstützt keine Hyperlinks aus diesem Feld, ist jedoch auf der Security Hub Hub-Konsole verfügbar.

Malware, Network, Process, ThreatIntelIndicators

Verwenden Sie gegebenenfalls`Malware`,`Network`,`Process`, oder`ThreatIntelIndicators`aus. Jedes dieser Objekte wird in der Security Hub Hub-Konsole verfügbar gemacht. Verwenden Sie diese Objekte im Kontext des Ergebnisses, das Sie senden.

Wenn Sie beispielsweise Malware erkennen, die eine ausgehende Verbindung zu einem bekannten Befehls- und Steuerknoten herstellt, geben Sie die Details für die EC2-Instanz in`Resource.Details.AwsEc2Instance`aus. Geben Sie das relevante`Malware`,`Network`, und`ThreatIntelIndicator`-Objekte für diese EC2-Instance.

Malware

`Malware`ist eine Liste, die bis zu fünf Arrays von Malware-Informationen akzeptiert. Machen Sie die Malware-Einträge für die Ressource und den Befund relevant.

Jeder Eintrag enthält die folgenden Felder.

`Name`

Der Name der Malware. Der Wert besteht aus einer Zeichenfolge mit bis zu 64 Zeichen.

`Name`sollte aus einer geprüften Bedrohungsinformationen oder Forscherquelle stammen.

`Path`

Der Pfad zur Malware. Der Wert besteht aus einer Zeichenfolge mit bis zu 512 Zeichen.`Path`sollte ein Linux- oder Windows-Systemdateipfad sein, außer in den folgenden Fällen.

- Wenn Sie Objekte in einem S3-Bucket oder einer EFS-Freigabe mit YARA-Regeln scannen, dann`Path`ist der S3://oder HTTPS-Objektpfad.
- Wenn Sie Dateien in einem Git-Repository scannen, dann`Path`ist die Git-URL oder der Klonpfad.

`State`

Der Status der Malware. Die zulässigen Werte lauten`OBSERVED`| `REMOVAL_FAILED`|`REMOVED`aus.

Stellen Sie im Titel und in der Beschreibung der Suche sicher, dass Sie Kontext für das bereitstellen, was mit der Malware passiert ist.

Zum Beispiel, wenn`Malware.State`ist`REMOVED`, dann sollten der Suchtitel und die Beschreibung widerspiegeln, dass Ihr Produkt die Malware entfernt hat, die sich auf dem Pfad befindet.

Wenn`Malware.State`ist`OBSERVED`, dann sollten der Suchtitel und die Beschreibung widerspiegeln, dass Ihr Produkt auf diese Malware gestoßen ist, die sich auf dem Pfad befindet.

`Type`

Gibt die Art der Malware an. Die zulässigen Werte lauten`ADWARE`|`BLENDED_THREAT`|`BOTNET_AGENT`|`COIN_MINER`|`EXPLOIT_KIT`|`KEYLOGGER`|`MACRO`|`POT`

Wenn Sie einen zusätzlichen Wert für benötigen`Type`, wenden Sie sich an das Security Hub Hub-Team.

Network

`Network`ist ein einzelnes Objekt. Sie können nicht mehrere netzwerkbezogene Details hinzufügen. Beachten Sie bei der Zuordnung der Felder die folgenden Richtlinien.

Ziel- und Quellinformationen

Ziel und Quelle sind TCP- oder VPC Flow Logs oder WAF-Protokolle einfach zuzuordnen. Sie sind schwieriger zu verwenden, wenn Sie Netzwerkinformationen für eine Feststellung über einen Angriff beschreiben.

In der Regel ist die Quelle der Ort, woher der Angriff stammt, aber er könnte andere Quellen haben, wie unten aufgeführt. Sie sollten die Quelle in Ihrer Dokumentation erläutern und sie auch im Suchtitel und in der Beschreibung beschreiben.

- Für einen DDoS-Angriff auf eine EC2-Instance ist die Quelle der Angreifer, obwohl ein echter DDoS-Angriff Millionen von Hosts verwenden kann. Das Ziel ist die öffentliche IPv4-Adresse der EC2-Instance.`Direction`ist IN.
- Bei Malware, die beobachtet wird, die von einer EC2-Instanz zu einem bekannten Befehls- und Steuerknoten kommuniziert, ist die Quelle die IPV4-Adresse der EC2-Instanz. Das Ziel ist der Befehl- und Steuerknoten.`Direction`ist0UTaus. Sie würden auch zur Verfügung stellen`Malware`und`ThreatIntelIndicators`aus.

`Protocol`

`Protocol`wird immer einem registrierten Namen der Internet Assigned Numbers Authority (IANA) zugeordnet, es sei denn, Sie können ein bestimmtes Protokoll angeben. Sie sollten dies immer verwenden und die Portinformationen angeben.

`Protocol`ist unabhängig von den Quell- und Zielinformationen. Stellen Sie es nur bereit, wenn es sinnvoll ist, dies zu tun.

`Direction`

`Direction`ist immer relativ zumAWSNetzwerkgrenzen.

- `IN`bedeutet, dass es eintrittAWS(VPC, Dienst).
- 0UTbedeutet, dass es dieAWSNetzwerkgrenzen.

Process

`Process`ist ein einzelnes Objekt. Sie können nicht mehrere prozessbezogene Details hinzufügen. Beachten Sie bei der Zuordnung der Felder die folgenden Richtlinien.

`Name`

`Name`sollte dem Namen der ausführbaren Datei entsprechen. Er akzeptiert bis zu 64 Zeichen.

`Path`

`Path`Ist der Dateisystempfad zur ausführbaren Datei für den Prozess. Es akzeptiert bis zu 512 Zeichen.

`Pid`, **`ParentPid`**

`Pid`und`ParentPid`sollte mit der Linux-Prozesskennung (PID) oder der Windows-Ereignis-ID übereinstimmen. Um zu unterscheiden, verwenden Sie EC2 Amazon Machine Images (AMI), um die Informationen bereitzustellen. Kunden können wahrscheinlich zwischen Windows und Linux unterscheiden.

Zeitstempel (**`LaunchedAt`**und**`TerminatedAt`**)

Wenn Sie diese Informationen nicht zuverlässig abrufen können und sie auf die Millisekunde nicht korrekt sind, geben Sie sie nicht an.

Wenn ein Kunde für die forensische Untersuchung auf Zeitstempel angewiesen ist, ist es besser, keinen Zeitstempel zu haben, als den falschen Zeitstempel zu haben.

ThreatIntelIndicators

`ThreatIntelIndicators`Akzeptiert eine Reihe von bis zu fünf Bedrohungsinformationsobjekten.

Für jeden Eintrag`Type`steht im Zusammenhang mit der spezifischen Bedrohung. Die zulässigen Werte lauten`DOMAIN|EMAIL_ADDRESS|HASH_MD5|HASH_SHA1|HASH_SHA256|HASH_SHA512|IPV4_ADDRESS|IPV`

Hier finden Sie einige Beispiele, wie Sie Bedrohungsinformationsindikatoren abbilden können:

- Sie haben einen Prozess gefunden, von dem Sie wissen, dass er mit Cobalt Strike verbunden ist. Das hast du gelernt vonFireEyes -Blog.

  Setzen Sie `Type` auf `PROCESS`. Erstellen Sie auch ein`Process`Objekt für den Prozess.
- Ihr E-Mail-Filter hat jemanden gefunden, der ein bekanntes Hash-Paket von einer bekannten bösartigen Domäne gesendet hat.

  Erstellen von zwei`ThreatIntelIndicator`-Objekte. Ein Objekt ist für die`DOMAIN`aus. Die andere ist für die`HASH_SHA1`aus.
- Du hast Malware mit einer Yara-Regel gefunden (Loki, Fenrir, Awss3VirusScan,BinaryAlert) enthalten.

Erstellen von zweiThreatIntelIndicator-Objekte. Eine davon ist für die Malware. Die andere ist für dieHASH_SHA1aus.

Resources

FürResourcesverwenden Sie nach Möglichkeit unsere bereitgestellten Ressourcentypen und Detailfelder. Security Hub fügt dem ASFF ständig neue Ressourcen hinzu. Um ein monatliches Protokoll der Änderungen an ASFF zu erhalten, wenden Sie sich an<securityhub-partners@amazon.com>aus.

Wenn Sie die Informationen nicht in die Detailfelder für einen modellierten Ressourcentyp einfügen können, ordnen Sie die restlichen Details zuDetails.Otheraus.

Für eine Ressource, die nicht in ASFF modelliert ist, setzen SieTypezuOtheraus. Verwenden Sie für die detaillierten InformationenDetails.Otheraus.

Sie können auch dieOtherRessourcentyp für nicht-AWSErgebnisse.

ProductFields

Verwenden Sie nurProductFieldswenn Sie kein anderes kuratiertes Feld für verwenden könnenResourcesoder ein beschreibendes Objekt wieThreatIntelIndicators,Network, oderMalwareaus.

Wenn du es benutztProductFields, müssen Sie eine strikte Begründung für diese Entscheidung angeben.

Compliance

Verwenden Sie nurCompliancewenn Ihre Ergebnisse mit der Compliance zusammenhängen.

Security Hub verwendetCompliancefür die Ergebnisse, die es basierend auf Kontrollen generiert.

Firewall Manager verwendetCompliancefür seine Ergebnisse, weil sie konformitätsbezogen sind.

Felder, die eingeschränkt sind

Diese Felder sind für Kunden bestimmt, um ihre Untersuchung einer Feststellung im Auge zu behalten.

Ordnen Sie diesen Feldern oder Objekten nicht zu.

- `Note`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Ordnen Sie für diese Felder den Feldern zu, die sich im`FindingProviderFields`-Objekt. Ordnen Sie nicht den Feldern der obersten Ebene zu.

- `Confidence`- Fügen Sie einen Konfidenzwert (0-99) nur ein, wenn Ihr Service über eine ähnliche Funktionalität verfügt oder wenn Sie zu 100% zu Ihrer Erkenntnis stehen.
- `Criticality`— Der Kritikalitätswert (0-99) soll die Bedeutung der mit dem Befund verbundenen Ressource zum Ausdruck bringen.
- `RelatedFindings`— Geben Sie verwandte Ergebnisse nur an, wenn Sie Ergebnisse im Zusammenhang mit derselben Ressource oder demselben Suchtyp verfolgen können. Um eine verwandte Befund zu identifizieren, müssen Sie sich auf die Erkennungskennung eines Ergebnisses beziehen, das sich bereits im Security Hub befindet.

Richtlinien für die Verwendung von**`BatchImportFindings`**API

Bei Verwendung von`BatchImportFindings`API-Operation zum Senden von Ergebnissen anAWS Security Hubverwenden Sie die folgenden Richtlinien.

- Du musst anrufen`BatchImportFindings`unter Verwendung des Kontos, das mit den Ergebnissen verknüpft ist. Die Kennung des verknüpften Kontos ist der Wert des`AwsAccountId`-Attribut für den Befund.
- Senden Sie den größten Stapel, den Sie können. Security Hub akzeptiert bis zu 100 Ergebnisse pro Charge, bis zu 240 KB pro Befund und bis zu 6 MB pro Stapel.
- Das Drosselzinslimit beträgt 10 TPS pro Konto und Region mit einem Ausbruch von 30 TPS.
- Sie müssen einen Mechanismus implementieren, um den Stand der Ergebnisse beizubehalten, wenn Drosselungs- oder Netzwerkprobleme auftreten. Sie benötigen auch den Suchstatus, damit Sie die Suche nach Updates einreichen können, wenn ein Ergebnis ein- und aus der Compliance hinein- und ausgeht.
- Weitere Informationen zu den maximalen Längen von Strings und anderen Einschränkungen finden Sie unterAWSSecurity Finding Format (ASFF)imAWS Security Hub-Benutzerhandbuchaus.

Checkliste für die Produktbereitschaft

DieAWS Security Hubund APN-Partnerteams verwenden diese Checkliste, um zu überprüfen, dass die Integration startbereit ist.

ASFFFF-Zuordnung

Diese Fragen beziehen sich auf die Abbildung Ihres Ergebnisses auf dieAWSSecurity Finding Format (ASFF)

Werden alle Erkennungsdaten des Partners in ASFF abgebildet?

- Ordnen Sie alle Ihre Ergebnisse auf irgendeine Weise dem ASFF zu.
- Verwenden Sie kuratierte Felder wie modellierte Ressourcentypen,`Network`,`Malware`, oder`ThreatIntelIndicators`aus.
- Ordnen Sie alles andere in`Resource.Details.Other`oder`ProductFields`entsprechend.

Verwendet der Partner**`Resource.Details`**Felder, wie**`AwsEc2instance`**,**`AwsS3Bucket`**, und**`Container`**? Verwendet der Partner**`Resource.Details.Other`**um Ressourcendetails zu definieren, die nicht im ASFF modelliert sind?

- Verwenden Sie nach Möglichkeit die bereitgestellten Felder für kuratierte Ressourcen wie EC2-Instances, S3-Buckets und Sicherheitsgruppen in Ihren Ergebnissen.
- Ordnen Sie andere Informationen in Bezug auf Ressourcen zu`Resource.Details.Other`nur wenn es keine direkte Übereinstimmung gibt.

Ordnet der Partner Werte zu**`UserDefinedFields`**?

- Verwenden Sie nicht `UserDefinedFields`.
- Erwägen Sie, ein anderes kuratiertes Feld zu verwenden, z.`Resource.Details.Other`oder`ProductFields`aus.

Ordnet der Partner Informationen in**`ProductFields`**das könnte anderen ASFF-Feldern zugeordnet werden?

- Verwenden Sie nur`ProductFields`für produktspezifische Informationen wie Versionsinformationen, produktspezifische Schweregrade oder andere Informationen, die nicht in ein kuratiertes Feld abgebildet werden können oder`Resources.Details.Other`aus.

Importiert der Partner seine eigenen Zeitstempel für**`FirstObservedAt`**?

DieFirstObservedAttimestamp soll den Zeitpunkt aufzeichnen, zu dem ein Befund im Produkt beobachtet wurde. Ordnen Sie dieses Feld wenn möglich zu.

Stellt der Partner eindeutige Werte zur Verfügung, die für jeden Finding-Bezeichner generiert wurden, mit Ausnahme von Ergebnissen, die er aktualisieren möchte?

Alle Ergebnisse im Security Hub werden auf den Finding-Bezeichner (Id-Attribut). Dieser Wert muss immer eindeutig sein, um sicherzustellen, dass die Ergebnisse nicht versehentlich aktualisiert werden.

Sie sollten auch den Bezeichnungsstatus für die Suche beibehalten, um die Ergebnisse zu aktualisieren.

Bietet der Partner einen Wert, der Ergebnisse einer Generator-ID zuordnet?

GeneratorIDsollte nicht den gleichen Wert wie die Finden-ID haben.

GeneratorIDsollte in der Lage sein, Ergebnisse logisch mit dem zu verknüpfen, was sie generiert hat.

Dies kann eine Unterkomponente innerhalb eines Produkts (Produkt A - Vulnerability vs Produkt A - EDR) oder etwas ähnliches sein.

Verwendet der Partner die erforderlichen Suchtypen Namespaces auf eine Weise, die für sein Produkt relevant ist? Verwendet der Partner die empfohlenen Suchtypkategorien oder Klassifikatoren in seinen Suchtypen?

Die Taxonomie des Erkennungstyps sollte den Ergebnissen, die das Produkt generiert, genau abbilden.

Die Namespaces der ersten Ebene, die imAWSSecurity Finding-Format ist erforderlich.

Sie können benutzerdefinierte Werte für die Namespaces der zweiten und dritten Ebene (Kategorien oder Klassifizierer) verwenden.

Erfasst der Partner Informationen zum Netzwerkfluss im**`Network`**Felder, wenn sie Netzwerkdaten haben?

Wenn Ihr Produkt erfasstNetFlowInformationen, ordnen Sie es demNetworkfield.

Erfasst der Partner Informationen (PID) im**`Process`**Felder, wenn sie Prozessdaten haben?

Wenn Ihr Produkt Prozessinformationen erfasst, ordnen Sie es demProcessfield.

Erfasst der Partner Malware-Informationen im**`Malware`**-Feldern, wenn sie Malware-Daten haben?

Wenn Ihr Produkt Malware-Informationen erfasst, ordnen Sie es dem`Malware`field.

Erfasst der Partner Threat Intelligence-Informationen im**`ThreatIntelIndicators`**Felder, wenn sie Threat Intelligence-Daten haben?

Wenn Ihr Produkt Informationen über Bedrohungsinformationen erfasst, ordnen Sie es dem`ThreatIntelIndicators`field.

Gibt der Partner eine Vertrauensbewertung für Ergebnisse an? Wenn ja, wird eine Begründung gegeben?

Wenn Sie dieses Feld verwenden, geben Sie eine Begründung in Ihrer Dokumentation und Ihrem Manifest an.

Verwendet der Partner eine kanonische ID oder einen ARN für die Ressourcen-ID bei der Suche?

Bei der IdentifizierungAWS-Ressourcen ist es am besten, den ARN zu verwenden. Wenn kein ARN verfügbar ist, verwenden Sie die kanonische Ressourcen-ID.

Einrichtung und Funktion der Integration

Diese Fragen beziehen sich auf das Setup undday-to-dayFunktion der Integration.

Bietet der Partner eineinfrastructure-as-code(iAC) -Vorlage zur Bereitstellung der Integration mit Security Hub, wie Terraform,AWS CloudFormation, oderAWS Cloud Development Kit (AWS CDK)?

Für Integrationen, die Ergebnisse aus dem Kundenkonto senden oder verwendenCloudWatchEreignisse, um Ergebnisse zu konsumieren, ist eine Form von iAC-Vorlage erforderlich.

AWS CloudFormationwird bevorzugt, aberAWS CDKoder Terraform kann auch verwendet werden.

Hat das Partnerprodukt ein Ein-Klick-Setup auf seiner Konsole für die Integration mit Security Hub?

Einige Partnerprodukte verwenden einen Toggle oder einen ähnlichen Mechanismus in ihrem Produkt, um die Integration zu aktivieren. Dies kann zur automatischen Bereitstellung von Ressourcen und Berechtigungen führen. Wenn Sie Ergebnisse aus einem Produktkonto senden, ist die Einrichtung mit einem Klick die bevorzugte Methode.

Sendet der Partner nur Wertfindungen?

Im Allgemeinen sollten Sie nur Erkenntnisse mit Sicherheitswert an Security Hub Hub-Kunden senden.

Security Hub ist kein allgemeines Tool zur Protokollverwaltung. Sie sollten nicht jedes mögliche Protokoll an Security Hub senden.

Hat der Partner eine Schätzung abgegeben, wie viele Erkenntnisse er pro Tag pro Kunde und mit welcher Häufigkeit (Durchschnitt und Burst) senden wird?

Zur Berechnung der Belastung des Security Hub wird eine Anzahl eindeutiger Ergebnisse verwendet. Ein eindeutiger Befund ist definiert als ein Ergebnis mit einer anderen ASFF-Zuordnung als einer anderen Erkenntnis.

Wenn zum Beispiel nur eine Befund aufgefüllt ist`ThreatIntelIndicators`und ein anderer bevölkerte nur`Resources.Details.AWSEc2Instance`, das sind zwei einzigartige Erkenntnisse.

Hat der Partner eine anmutige Art, 4xx- und 5xx-Fehler so zu behandeln, dass sie nicht gedrosselt werden und alle Ergebnisse zu einem späteren Zeitpunkt gesendet werden können?

Derzeit gibt es eine Burst-Rate von 30 bis 50 TPS auf der`BatchImportFindings`API-Operation. Wenn 4xx- oder 5xx-Fehler zurückgegeben werden, müssen Sie den Status dieser fehlgeschlagenen Ergebnisse beibehalten, damit Sie sie später vollständig wiederholen können. Sie können dies durch eine Warteschlange für tote Briefe oder eine andere tunAWSMessaging-Services wie Amazon SNS oder Amazon SQS.

Behält der Partner den Stand seiner Ergebnisse bei, damit er weiß, dass er Erkenntnisse archiviert, die nicht mehr vorhanden sind?

Wenn Sie vorhaben, die Ergebnisse durch Überschreiben der ursprünglichen Finding-ID zu aktualisieren, müssen Sie über einen Mechanismus verfügen, um den Status beizubehalten, damit die richtigen Informationen für die korrekte Suche aktualisiert werden.

Wenn Sie Ergebnisse angeben, verwenden Sie nicht die`BatchUpdateFindings`Operation, um Ergebnisse zu aktualisieren. Dieser Vorgang sollte nur von Kunden genutzt werden. Du benutzt nur`BatchUpdateFindings`wenn Sie Ergebnisse untersuchen und Maßnahmen ergreifen.

Behandelt der Partner Wiederholungen auf eine Weise, die keine Kompromisse eingeht, die zuvor erfolgreiche Ergebnisse gesendet wurden?

Sie sollten über einen Mechanismus verfügen, um die ursprünglichen Find-IDs im Fehlerfall beizubehalten, damit Sie erfolgreiche Ergebnisse nicht fälschlicherweise duplizieren oder überschreiben.

Aktualisiert der Partner die Ergebnisse durch Aufruf der**`BatchImportFindings`**Betrieb mit der Finding-ID der bestehenden Findings?

Um eine Suche zu aktualisieren, müssen Sie die vorhandene Suche überschreiben, indem Sie dieselbe Suchkennung übermitteln.

Die`BatchUpdateFindings`-Betrieb sollte nur von Kunden genutzt werden.

Aktualisiert der Partner Ergebnisse mit dem**`BatchUpdateFindings`**API?

Wenn Sie Maßnahmen zu Ergebnissen ergreifen, können Sie die`BatchUpdateFindings`Operation, um bestimmte Felder zu aktualisieren.

Gibt der Partner Informationen über die Latenzzeit zwischen dem Zeitpunkt der Erstellung eines Findens und dem Zeitpunkt, an dem er von seinem Produkt an Security Hub gesendet wird?

Sie sollten die Latenz minimieren, um sicherzustellen, dass Kunden die Ergebnisse im Security Hub so schnell wie möglich sehen.

Diese Informationen sind im Manifest erforderlich.

Wenn die Architektur des Partners Ergebnisse von einem Kundenkonto an Security Hub senden soll, haben sie dies erfolgreich demonstriert? Wenn die Architektur des Partners Ergebnisse von ihrem eigenen Konto an Security Hub senden soll, haben sie dies erfolgreich demonstriert?

Während des Tests müssen die Ergebnisse erfolgreich von einem Konto gesendet werden, das sich von dem Konto unterscheidet, das sich von dem für das Produkt ARN bereitgestellten Konto unterscheidet.

Das Senden eines Ergebnisses aus dem Konto des ARN-Eigentümers des Produkts kann bestimmte Fehlerausnahmen von den API-Vorgängen umgehen.

Bietet der Partner Security Hub eine Heartbeat-Findung?

Um zu zeigen, dass Ihre Integration ordnungsgemäß funktioniert, sollten Sie eine Heartbeat-Findung senden. Die Heartbeat-Findung wird alle fünf Minuten gesendet und verwendet den Findetyp`Heartbeat`aus.

Dies ist wichtig, wenn Sie Ergebnisse von einem Produktkonto senden.

Hat sich der Partner während des Tests in das Konto des Security Hub Hub-Produktteams integriert?

Während der Validierung vor der Produktion sollten Sie Suchbeispiele an das Security Hub Hub-Produktteams sendenAWSKonto. Diese Beispiele zeigen, dass die Ergebnisse korrekt gesendet und abgebildet werden.

Dokumentation

Diese Fragen beziehen sich auf die Dokumentation der von Ihnen bereitgestellten Integration.

Hostet der Partner seine Dokumentation auf einer dedizierten Website?

Die Dokumentation sollte auf Ihrer Website als statische Webseite, Wiki, Lesen Sie die Dokumente oder ein anderes dediziertes Format gehostet werden.

Hosting von Dokumentation aufGitHuberfüllt nicht die Anforderung der dedizierten Website.

Enthält die Partnerdokumentation Anweisungen zum Einrichten der Security Hub Hub-Integration?

Sie können die Integration entweder mit einer iAC-Vorlage oder einer konsolenbasierten „Ein-Klick“ -Integration einrichten.

Liefert die Partnerdokumentation eine Beschreibung ihres Anwendungsfalls?

Der Anwendungsfall, den Sie im Manifest angeben, sollte ebenfalls in der Dokumentation beschrieben werden

Bietet die Partnerdokumentation eine Begründung für die Ergebnisse, die sie senden?

Sie sollten die Gründe für die Arten von Ergebnissen angeben, die Sie senden.

Beispielsweise kann Ihr Produkt Ergebnisse für Schwachstellen, Malware und Antivirenprogramme erzeugen, aber Sie senden nur Schwachstellen- und Malware-Erkenntnisse an Security Hub. In diesem Fall müssen Sie eine Begründung dafür angeben, warum Sie keine Antivirus-Ergebnisse senden.

Bietet die Partnerdokumentation eine Begründung dafür, wie der Partner seine Ergebnisse dem ASFF zuordnet?

Sie sollten die Begründung für die Zuordnung des nativen Ergebnisses eines Produkts zu ASFF angeben. Kunden möchten wissen, wo sie nach bestimmten Produktinformationen suchen müssen.

Gibt die Partnerdokumentation Anleitungen dazu, wie der Partner die Ergebnisse aktualisiert, wenn er die Ergebnisse aktualisiert?

Geben Sie Kunden Informationen darüber, wie Sie den Staat behalten, Idempotenz sicherstellen und Ergebnisse überschreibenup-to-date-Informationen.

Beschreibt die Partnerdokumentation die Suche nach Latenz?

Minimieren Sie die Latenz, um sicherzustellen, dass Kunden die Ergebnisse im Security Hub so schnell wie möglich sehen.

Diese Informationen sind im Manifest erforderlich.

Beschreibt die Partnerdokumentation, wie sich ihr Schweregrad dem Schweregrad von ASFF entspricht?

Geben Sie Informationen darüber an, wie Sie kartieren`Severity.Original`zu`Severity.Label`aus.

Wenn Ihr Schweregrad beispielsweise eine Buchstabennote (A, B, C) ist, sollten Sie Informationen darüber angeben, wie Sie die Buchstabennote dem Schweregrad zuordnen.

Bietet die Partnerdokumentation eine Begründung für Vertrauensbewertungen?

Wenn Sie Konfidenzwerte angeben, sollten diese Punktzahlen eingestuft werden.

Wenn Sie statisch ausgefüllte Konfidenzwerte oder Mappings verwenden, die sich aus künstlicher Intelligenz oder maschinellem Lernen ergeben, sollten Sie zusätzlichen Kontext bereitstellen.

Notiert die Partnerdokumentation, welche Regionen der Partner unterstützt und nicht?

Hinweis: Regionen, die unterstützt werden oder nicht, damit Kunden wissen, in welchen Regionen sie keine Integration versuchen sollen.

-Produktkarteninformationen

Diese Fragen beziehen sich auf die Karte für das Produkt, das auf derIntegrationenSeite der Security Hub Hub-Konsole.

Ist das zur Verfügung gestelltAWSKonto-ID gültig und enthält 12 Ziffern?

Kontokennungen sind 12 Ziffern lang. Wenn eine Konto-ID weniger als 12 Ziffern enthält, ist der ARN des Produkts nicht gültig.

Enthält die Produktbeschreibung 200 oder weniger Zeichen?

Die im JSON im Manifest angegebene Produktbeschreibung sollte nicht länger als 200 Zeichen einschließlich Leerzeichen enthalten.

Führt der Konfigurationslink zur Dokumentation für die Integration?

Der Konfigurationslink sollte zu Ihrer Online-Dokumentation führen. Es sollte nicht zu Ihrer Hauptwebsite oder zu Marketingseiten führen.

Führt der Kauflink (falls vorhanden) zumAWS MarketplaceAuflistung für das Produkt?

Wenn Sie einen Kauflink angeben, muss dieser für einenAWS Marketplace-Eintrag. Security Hub akzeptiert keine Kauflinks, die nicht von gehostet werdenAWSaus.

Beschreiben die Produktkategorien das Produkt richtig?

Im Manifest können Sie bis zu drei Produktkategorien angeben. Diese sollten mit dem JSON übereinstimmen und können nicht benutzerdefiniert sein. Sie können nicht mehr als drei Produktkategorien angeben.

Sind die Firmen- und Produktnamen gültig und korrekt?

Der Firmenname muss 16 oder weniger Zeichen lang sein.

Der Produktname muss 24 oder weniger Zeichen lang sein.

Der Produktname in der Produktkarte JSON muss mit dem Namen im Manifest übereinstimmen.

Marketing-Informationen

Diese Fragen beziehen sich auf das Marketing für die Integration.

Liegt die Produktbeschreibung für die Security Hub Hub-Partnerseite innerhalb von 700 Zeichen, einschließlich Leerzeichen?

Die Seite Security Hub Hub-Partner akzeptiert nur bis zu 700 Zeichen, einschließlich Leerzeichen.

Das Team bearbeitet längere Beschreibungen.

Ist das Logo der Security Hub Hub-Partnerseite nicht größer als 600 x 300 px?

Geben Sie eine öffentlich zugängliche URL mit einem Firmenlogo in PNG oder JPG an, das nicht größer als 600 x 300 Pixel ist.

Führt der Hyperlink Weitere Informationen auf der Security Hub Hub-Partnerseite zur dedizierten Webseite des Partners über die Integration?

DieWeitere InformationenLink sollte nicht zur Hauptwebsite des Partners oder zu den Dokumentationsinformationen führen.

Dieser Link sollte immer auf eine dedizierte Webseite mit Marketinginformationen über die Integration gehen.

Bietet der Partner eine Demo oder ein Anleitungsvideo zur Verwendung seiner Integration an?

Eine Demo- oder Integrations-Walkthrough-Video ist optional, wird jedoch empfohlen.

Ist einAWSDer Blogbeitrag des Partnernetzwerks wird mit dem Partner und seinem Partner Development Manager oder Partner Development Vertreter veröffentlicht?

AWSBlogbeiträge des Partnernetzwerks sollten im Voraus mit dem Partner Development Manager oder Vertreter der Partnerentwicklung koordiniert werden.

Diese sind getrennt von jedem Blogbeitrag, den Sie selbst erstellen.

Lassen Sie 4 bis 6 Wochen Vorbereitungs- und Anlaufzeit einwirken. Dieser Aufwand sollte begonnen werden, nachdem das Testen mit dem privaten Produkt ARN abgeschlossen ist.

Wird eine von Partnern geleitete Pressemitteilung veröffentlicht?

Sie können mit Ihrem Partner Development Manager oder Partner Development Vertreter zusammenarbeiten, um ein Angebot vom VP External Security Services zu erhalten. Dieses Angebot können Sie in Ihrer Pressemitteilung verwenden.

Wird ein von Partnern geleiteter Blogbeitrag veröffentlicht?

Sie können Ihre eigenen Blogbeiträge erstellen, um die Integration außerhalb desAWS-Blog des Partnernetzwerks.

Wird ein von Partnern geleitetes Webinar veröffentlicht?

Sie können eigene Webinare erstellen, um die Integration zu präsentieren.

Wenn Sie Unterstützung vom Security Hub Hub-Team benötigen, arbeiten Sie mit dem Produktteam zusammen, nachdem Sie die Tests mit dem privaten Produkt ARN abgeschlossen haben.

Hat der Partner Social-Media-Unterstützung vonAWS?

Nach Ihrer Veröffentlichung können Sie mit derAWSSicherheitsmarketing führt zur VerwendungAWSoffizielle Social-Media-Kanäle, um Details zu Ihren Webinaren zu teilen.

AWS Security HubPartner — Häufig gestellte Fragen

Im Folgenden werden häufig gestellte Fragen zum Einrichten und Aufrechterhalten einer Integration mitAWS Security Hubaus.

1. Was sind die Vorteile der Security Hub Hub-Integration?
   - Zufriedenheit der Kunden— Der wichtigste Grund für die Integration in Security Hub ist, dass Sie Kundenanfragen dazu haben.

     Security Hub ist das Sicherheits- und Compliance-Zentrum fürAWSKunden. Es ist als erste Station konzipiert, woAWSSicherheits- und Compliance-Experten verstehen jeden Tag ihren Sicherheits- und Compliance-Zustand.

     Hören Sie Ihren Kunden zu. Sie werden Ihnen sagen, ob sie Ihre Ergebnisse im Security Hub sehen möchten.
   - Erkennungsmöglichkeiten— Wir fördern Partner mit zertifizierten Integrationen innerhalb der Security Hub Hub-Konsole, einschließlich Links zu derenAWS MarketplaceInserate. Dies ist eine großartige Möglichkeit für Kunden, neue Sicherheitsprodukte zu entdecken.
   - Marketing-Möglichkeiten— Anbieter mit genehmigten Integrationen können an Webinaren teilnehmen, Pressemitteilungen veröffentlichen, glatte Blätter erstellen und ihre Integrationen demonstrierenAWSKunden.
2. Welche Arten von Partnern gibt es?
   - Partner, die Ergebnisse an den Security Hub senden
   - Partner, die Ergebnisse vom Security Hub erhalten
   - Partner, die Ergebnisse sowohl senden als auch empfangen
   - Beratungspartner, die Kunden beim Einrichten, Anpassen und Verwenden von Security Hub in ihrer Umgebung unterstützen
3. Wie funktioniert eine Partnerintegration mit Security Hub auf hohem Niveau?

   Sie sammeln Ergebnisse aus einem Kundenkonto oder von Ihrem eigenenAWSerfassen und transformieren Sie das Format der Ergebnisse in dieAWS-Security-Finding-Format (ASFF) Sie bringen diese Ergebnisse dann an den entsprechenden regionalen Endpunkt Security Hub.

   Sie können auchCloudWatchEreignisse, die Ergebnisse vom Security Hub erhalten werden.
4. Was sind die grundlegenden Schritte zum Abschluss einer Integration mit Security Hub?

a. Senden Sie die Manifest-Informationen Ihres Partners ein.
b. Erhalten Sie Produkt-ARNs zur Verwendung mit Security Hub, wenn Sie Ergebnisse an Security Hub senden.
c. Ordnen Sie Ihre Ergebnisse ASFF zu. Siehe the section called “Richtlinien für ASFFFF-Zuordnung”.
d. Definieren Sie Ihre Architektur für das Senden von Erkenntnissen an Security Hub und Empfangen von Ergebnissen. Folgen Sie den unterthe section called “Grundsätze zur Erstellung und Aktualisierung von Erkenntnissen”aus.
e. Erstellen Sie ein Bereitstellungs-Framework für Kunden. Beispiel,AWS CloudFormationSkripte können diesem Zweck dienen.
f. Dokumentieren Sie Ihre Einrichtung und geben Sie Konfigurationsanweisungen für Kunden an.
g. Definieren Sie alle benutzerdefinierten Erkenntnisse (Korrelationsregeln), die Kunden mit Ihrem Produkt verwenden können.
h. Demonstrieren Sie Ihre Integration in das Security Hub Hub-Team.
i. Reichen Sie Marketinginformationen zur Genehmigung ein (Sprache der Website, Pressemitteilung, Architekturfolie, Video, glattes Blatt).

5. Wie ist der Vorgang zur Einreichung des Partnermanifests? Und fürAWS-Services zum Senden von Ergebnissen an den Security Hub?

   Um die Manifestinformationen an das Security Hub Hub-Team zu übermitteln, verwenden Sie`<securityhub-partners@amazon.com>`aus.

   Sie erhalten innerhalb von sieben Kalendertagen Produkt-ARNs.

6. Welche Arten von Ergebnissen sollte ich an Security Hub senden?

   Die Preise für Security Hub basieren teilweise auf der Anzahl der aufgenommenen Ergebnisse. Aus diesem Grund sollten Sie davon absehen, Erkenntnisse zu senden, die den Kunden keinen Mehrwert bieten.

   Beispielsweise senden einige Anbieter von Schwachstellenmanagement nur Ergebnisse mit einem CVSS (Common Vulnerability Scoring System) von 3 oder höher von möglichen 10 Punkten.

7. Was sind die verschiedenen Ansätze für mich, Ergebnisse an Security Hub zu senden?

   Dies sind die primären Ansätze:

   - Sie senden Erkenntnisse von ihren eigenen BezeichnetenAWSKonto mit dem`BatchImportFindings`verwenden.

- Sie senden Ergebnisse aus dem Kundenkonto über die`BatchImportFindings`verwenden. Sie könnten Ansätze für Annahmen verwenden, aber diese Ansätze sind nicht erforderlich.

Für allgemeine Richtlinien zur Verwendung`BatchImportFindings`, finden Sie unterthe section called “Richtlinien für die Verwendung von`BatchImportFindings`API”aus.

8. Wie sammle ich meine Ergebnisse und bringe sie an einen regionalen Endpunkt des Security Hub?

   Partner haben hierfür verschiedene Ansätze verwendet, da sie stark von der Architektur Ihrer Lösung abhängen.

   Einige Partner erstellen beispielsweise eine Python-App, die alsAWS CloudFormation-Skript. Das Skript sammelt die Ergebnisse des Partners aus der Kundenumgebung, wandelt sie in ASFF um und sendet sie an den regionalen Endpunkt des Security Hub.

   Andere Partner erstellen einen vollständigen Assistenten, der dem Kunden ein einmaliges Klick-Erlebnis bietet, um Ergebnisse an Security Hub weiterzuleiten.

9. Woran erkenne ich, wann ich Ergebnisse an den Security Hub senden muss?

   Security Hub unterstützt die teilweise Batch-Autorisierung für den`BatchImportFindings`API-Betrieb, damit Sie alle Ihre Ergebnisse für alle Ihre Kunden an Security Hub senden können.

   Wenn einige Ihrer Kunden Security Hub noch nicht abonniert haben, nimmt Security Hub diese Ergebnisse nicht auf. Es nimmt nur autorisierte Befunde auf, die sich in der Charge befinden.

10. Welche Schritte muss ich ausführen, um Ergebnisse an die Security Hub Hub-Instanz eines Kunden zu senden?

    a. Stellen Sie sicher, dass die richtigen IAM-Richtlinien vorhanden sind.

    b. Aktivieren Sie ein Produktabonnement (Ressourcenrichtlinien) für die Konten. Benutze entweder das`EnableImportFindingsForProduct`Die API-Operation oder dieIntegrationenangezeigten. Der Kunde kann dies tun oder Sie können kontoübergreifende Rollen verwenden, um im Namen des Kunden zu handeln.

    c. Stellen Sie sicher, dass die`ProductArn`des Ergebnisses ist der öffentliche ARN Ihres Produkts.

    d. Stellen Sie sicher, dass die`AwsAccountId`Die -Erkenntnis ist die Konto-ID des Kunden.

    e. Stellen Sie sicher, dass Ihre Ergebnisse keine fehlerhaften Daten enthalten, gemäß derAWS-Security-Finding-Format (ASFF) Beispielsweise werden Pflichtfelder ausgefüllt, und es gibt keine ungültigen Werte.

f. Senden Sie die Ergebnisse in Chargen an den richtigen regionalen Endpunkt.

11. Welche IAM-Berechtigungen müssen vorhanden sein, damit ich Ergebnisse senden kann?

IAM-Richtlinien müssen für den IAM-Benutzer oder die Rolle konfiguriert sein, die aufruft`BatchImportFindings`oder andere API-Aufrufe.

Der einfachste Test besteht darin, dies von einem Administratorkonto aus zu tun. Sie können diese beschränken auf`action: 'securityhub:BatchImportFindings'`und`resource: <productArn and/or productSubscriptionArn>`aus.

Ressourcen im selben Konto können mit IAM-Richtlinien konfiguriert werden, ohne dass Ressourcenrichtlinien erforderlich sind.

So schließen Sie Probleme mit IAM-Richtlinien vom Anrufer von`BatchImportFindings`, legen Sie die IAM-Richtlinie für den Aufrufer wie folgt fest:

```
{
    Action: 'securityhub:*',
    Effect: 'Allow',
    Resource: '*'
}
```

Stellen Sie sicher, dass es keine gibt`Deny`Richtlinien für den Aufrufer. Nachdem Sie damit arbeiten können, können Sie die Richtlinie auf Folgendes beschränken:

```
{
    Action: 'securityhub:BatchImportFindings',
    Effect: 'Allow',
    Resource: 'arn:aws:securityhub:<region>:<account>:product/mycompany/myproduct'
},
{
    Action: 'securityhub:BatchImportFindings',
    Effect: 'Allow',
    Resource: 'arn:aws:securityhub:<region>:*:product-subscription/mycompany/
myproduct'
}
```

12. Was ist ein Produktabonnement?

Um Ergebnisse von einem bestimmten Partnerprodukt zu erhalten, muss der Kunde (oder der Partner mit kontoübergreifenden Rollen, die im Auftrag des Kunden arbeiten)

ein Produktabonnement einrichten. Um dies über die -Konsole zu tun, verwenden sie dieIntegrationenangezeigten. Um dies von der API aus zu tun, verwenden sie die`EnableImportFindingsForProduct`API-Operation.

Das Produktabonnement erstellt eine Ressourcenrichtlinie, die die Ergebnisse des Partners autorisiert, vom Kunden empfangen oder gesendet zu werden. Details hierzu finden Sie unter Anwendungsfälle und -berechtigungen.

Security Hub verfügt über die folgenden Arten von Ressourcenrichtlinien für Partner:

- `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`
- `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`

Während des Partner-Onboarding-Prozesses können Sie eine oder beide Arten von Richtlinien anfordern.

mit`BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`können Sie Ergebnisse nur von dem in Ihrem Produkt ARN aufgeführten Konto an Security Hub senden.

mit`BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`können Sie nur Ergebnisse aus dem Kundenkonto senden, das Sie abonniert hat.

13. Angenommen, ein Kunde hat ein Administratorkonto erstellt und einige Mitgliedskonten hinzugefügt. Muss der Kunde jedes Mitgliedskonto bei mir abonnieren? Oder abonniert der Kunde nur das Administratorkonto und ich kann dann Ergebnisse gegen Ressourcen in allen Mitgliedskonten senden?

    Diese Frage fragt, ob die Berechtigungen für alle Mitgliedskonten basierend auf der Registrierung des Administratorkontos erstellt werden.

    Der Kunde muss für jedes Konto ein Produktabonnement erstellen. Sie können dies programmgesteuert über die API tun.

14. Was ist mein Produkt ARN?

    Ihr Produkt ARN ist Ihre eindeutige Kennung, die Security Hub für Sie generiert und mit der Sie Ergebnisse einreichen. Sie erhalten einen Produkt-ARN für jedes Produkt, das Sie in Security Hub integrieren. Der richtige Produkt-ARN muss Teil jeder Erkenntnis sein, die Sie an Security Hub senden. Ergebnisse ohne das Produkt ARN werden fallen gelassen. Das Produkt ARN verwendet das folgende Format:

`arn:aws:securityhub:[region code]:[account ID]:product/[company name]/[product name]`

Ein Beispiel:

`arn:aws:securityhub:us-west-2:222222222222:product/generico/secure-pro`

Sie erhalten einen Produkt-ARN für jede Region, in der Security Hub bereitgestellt wird. Die Konto-ID, die Unternehmens- und Produktnamen werden von Ihren Partnermanifest-Einreichungen bestimmt. Sie ändern niemals eine der Informationen, die mit Ihrem Produkt ARN verknüpft sind, mit Ausnahme des Regionalcodes. Der Regionalcode muss mit der Region übereinstimmen, für die Sie Ergebnisse einreichen.

Ein häufiger Fehler besteht darin, die Konto-ID so zu ändern, dass sie mit dem Konto übereinstimmt, von dem aus Sie gerade arbeiten. Die Konto-ID ändert sich nicht. Sie reichen im Rahmen der Manifestübermittlung eine „Home“ -Konto-ID ein. Diese Konto-ID ist in Ihrem Produkt-ARN gesperrt.

Wenn Security Hub in neuen Regionen eingeführt wird, verwendet er automatisch die Standardregions-Codes, um Ihre Produkt-ARNs für diese Regionen zu generieren.

Jedes Konto wird auch automatisch mit einem ARN für private Produkte bereitgestellt. Sie können diesen ARN verwenden, um den Import von Ergebnissen in Ihrem eigenen Entwicklungskonto zu testen, bevor Sie Ihr offizielles öffentliches Produkt ARN erhalten.

15. Welches Format sollte verwendet werden, um Ergebnisse an den Security Hub zu senden?

    Ergebnisse müssen in derAWS-Security-Finding-Format (ASFF) Details dazu finden Sie unter .AWSSecurity Finding Format (ASFF)imAWS Security Hub-Benutzerhandbuchaus.

    Es wird erwartet, dass sich alle Informationen in Ihren nativen Ergebnissen vollständig im ASFF widerspiegeln. Benutzerdefinierte Felder wie`ProductFields`und`Resource.Details.Other`ermöglichen es Ihnen, Daten zuzuordnen, die nicht ordentlich in die vordefinierten Felder passen.

16. Was ist der richtige regionale Endpunkt zu verwenden?

    Sie müssen Ergebnisse an den regionalen Endpunkt des Security Hub senden, der mit dem Kundenkonto verknüpft ist.

17. Wo finde ich die Liste der regionalen Endpunkte?

Sehen Sie dieSecurity Hub Hub-Endpunktelisteaus.

18. Kann ich regionsübergreifende Ergebnisse einreichen?

    Security Hub unterstützt die regionsübergreifende Einreichung von Ergebnissen für den nativenAWSDienstleistungen wie AmazonGuardDuty, Amazon Macie und Amazon Inspector. Wenn Ihr Kunde dies zulässt, hindert Security Hub Sie nicht daran, Ergebnisse aus verschiedenen Regionen einzureichen.

    In diesem Sinne können Sie von überall aus einen regionalen Endpunkt aufrufen, und die Ressourceninformationen des ASFF müssen nicht mit der Region des Endpunkts übereinstimmen. Allerdings`ProductArn`muss mit der Region des Endpunkts übereinstimmen.

19. Wie lauten die Regeln und Richtlinien für den Versand von Befundenchargen?

    Sie können bis zu 100 Befunde oder 240 KB in einem einzigen Aufruf von`BatchImportFindings`aus. Stellen Sie eine Warteschlange und stapeln Sie so viele Ergebnisse wie möglich bis zu diesem Limit.

    Sie können eine Reihe von Ergebnissen aus verschiedenen Konten stapeln. Wenn jedoch eines der Konten im Stapel nicht bei Security Hub abonniert ist, schlägt der gesamte Stapel fehl. Dies ist eine Einschränkung des API Gateway Gateway-Baseline-Autorisierungsmodells.

    Siehe the section called “Richtlinien für die Verwendung von`BatchImportFindings`API”.

20. Kann ich Updates zu den von mir erstellten Erkenntnissen senden?

    Ja, wenn Sie einen Befund mit demselben Produkt-ARN und derselben Find-ID einreichen, überschreibt er die vorherigen Daten für diesen Befund. Beachten Sie, dass alle Daten überschrieben werden, daher sollten Sie eine vollständige Suche einreichen.

    Kunden werden sowohl neue Erkenntnisse als auch für die Suche nach Updates bewertet und in Rechnung gestellt.

21. Kann ich Updates zu Erkenntnissen senden, die jemand anderes erstellt hat?

    Ja, wenn der Kunde Ihnen Zugriff auf die`BatchUpdateFindings`API-Betrieb können Sie bestimmte Felder mit diesem Vorgang aktualisieren. Dieser Vorgang wurde entwickelt, um von Kunden, SIEMs, Ticketsystemen und Plattformen für Sicherheitsorchestrierung, Automatisierung und Reaktion (SOAR) verwendet zu werden.

22. Wie sind die Ergebnisse abgebaut?

Security Hub altert Ergebnisse 90 Tage nach der letzten Aktualisierung aus. Nach dieser Zeit werden die ausgesetzten Ergebnisse aus dem Security Hub gelöschtOpenSearch-Cluster.

Wenn Sie eine Suche mit derselben Finding-ID aktualisieren und diese abgelagert wurde, wird im Security Hub eine neue Erkenntnis erstellt.

Kunden können verwendenCloudWatchEreignisse zum Verschieben von Erkenntnissen aus dem Security Hub. Dadurch können alle Ergebnisse an Ziele der Wahl des Kunden gesendet werden.

Im Allgemeinen empfiehlt Security Hub, alle 90 Tage neue Erkenntnisse zu erstellen und die Ergebnisse nicht für immer zu aktualisieren.

23. Welche Drosseln hat Security Hub eingeführt?

Drosseln des Security Hub`GetFindings`API-Aufrufe, da der empfohlene Ansatz für den Zugriff auf Ergebnisse verwendet wirdCloudWatchEreignisse.

Security Hub implementiert keine andere Drosselung für interne Dienste, Partner oder Kunden darüber hinaus, die durch API Gateway- und Lambda-Aufrufe durchgesetzt werden.

24. Was sind die Aktualität oder Latenz-SLAs oder Erwartungen für Erkenntnisse, die von Quelldiensten an Security Hub gesendet werden?

Ziel ist es, sowohl für erste Erkenntnisse als auch für Aktualisierungen der Ergebnisse so nahezu in Echtzeit wie möglich zu sein. Sie sollten Ergebnisse innerhalb von fünf Minuten nach ihrer Erstellung an Security Hub senden.

25. Wie kann ich Ergebnisse vom Security Hub erhalten?

Verwenden Sie zum Erhalt von Erkenntnissen eine der folgenden Methoden.

- Alle Ergebnisse werden automatisch an gesendetCloudWatchEreignisse. Ein Kunde kann bestimmte erstellenCloudWatchEreignisregeln, um Ergebnisse an bestimmte Ziele zu senden, z. B. einen SIEM oder einen S3-Bucket. Diese Fähigkeit ersetzte das Vermächtnis`GetFindings`API-Operation.
- Verwenden vonCloudWatchEreignisse für benutzerdefinierte Aktionen. Mit Security Hub können Kunden bestimmte Ergebnisse oder Gruppen von Erkenntnissen innerhalb der Konsole auswählen und Maßnahmen gegen diese ergreifen. Sie können beispielsweise Ergebnisse an ein SIEM, ein Ticketsystem, eine Chat-Plattform oder einen Behebungsworkflow senden. Dies wäre Teil eines Workflows für Warn-Triage, den ein Kunde in Security Hub durchführt. Diese werden als benutzerdefinierte Aktionen bezeichnet.

Wenn ein Benutzer eine benutzerdefinierte Aktion auswählt, wird einCloudWatch-Ereignis wird für diese spezifischen Erkenntnisse erstellt. Sie könnten diese Fähigkeit nutzen und aufbauenCloudWatchEreignisregeln und Ziele, die ein Kunde im Rahmen einer benutzerdefinierten Aktion verwenden kann. Beachten Sie, dass diese Funktion nicht dazu verwendet wird, alle Ergebnisse eines bestimmten Typs oder einer bestimmten Klasse automatisch anCloudWatchEreignisse. Es ist Sache eines Benutzers, Maßnahmen zu bestimmten Erkenntnissen zu ergreifen.

Sie können die API-Vorgänge für benutzerdefinierte Aktionen verwenden, z.`CreateActionTarget`, um automatisch verfügbare Aktionen für Ihr Produkt zu erstellen (z. B.AWS CloudFormation-Vorlagen). Du würdest auch benutzenCloudWatchEreignisse regeln API-Operationen zum Erstellen entsprechenderCloudWatchEreignisregeln, die mit der benutzerdefinierten Aktion verknüpft sind. benutzenAWS CloudFormationVorlagen können Sie auch erstellenCloudWatchEreignisregeln, um alle Ergebnisse oder alle Erkenntnisse mit bestimmten Merkmalen aus Security Hub automatisch aufzunehmen.

26. Was sind die Anforderungen für einen Managed Security Service Provider (MSSP), um Security Hub Hub-Partner zu werden?

    Sie müssen demonstrieren, wie Security Hub im Rahmen Ihrer Servicebereitstellung an Kunden verwendet wird.

    Sie sollten eine Benutzerdokumentation haben, die Ihre Verwendung von Security Hub erklärt.

    Wenn der MSSP ein Suchanbieter ist, muss er nachweisen, dass er Ergebnisse an Security Hub sendet.

    Wenn der MSSP nur Ergebnisse vom Security Hub erhält, muss er mindestens einAWS CloudFormation-Vorlage zum Einrichten der entsprechendenCloudWatchEreignisregeln.

27. Was sind die Voraussetzungen, damit ein APN-Beratungspartner außerhalb von MSSP ein Security Hub Hub-Partner wird?

    Wenn Sie APN Consulting Partner sind, können Sie Security Hub Hub-Partner werden. Sie sollten zwei private Fallstudien einreichen, wie Sie einem bestimmten Kunden geholfen haben, Folgendes zu tun.

    - Richten Sie Security Hub mit IAM-Berechtigungen ein, die der Kunde benötigt.

- Helfen Sie, bereits integrierte Lösungen für unabhängige Softwarehersteller (ISV) mit Security Hub zu verbinden, indem Sie die Konfigurationsanweisungen auf der Partnerseite in der Konsole verwenden.
- Helfen Sie Kunden bei benutzerdefinierten Produktintegrationen.
- Erstellen Sie benutzerdefinierte Erkenntnisse, die für die Kundenbedürfnisse und -datensätze relevant sind.
- Erstellen Sie benutzerdefinierte Aktionen.
- Erstellen Sie Wiederherstellungs-Playbooks.
- Erstellen Sie Quickstarts, die sich an den Sicherheitshub-Compliance-Standards anpassen. Diese müssen vom Security Hub Hub-Team validiert werden.

Fallstudien müssen nicht öffentlich teilbar sein.

28. Was sind die Anforderungen, wie ich meine Integration mit Security Hub bei meinen Kunden bereitstelle?

    Integrationsarchitekturen zwischen Security Hub und Partnerprodukten variieren von Partner zu Partner in Bezug auf den Betrieb der Lösung dieses Partners. Sie sollten sicherstellen, dass der Einrichtungsprozess für die Integration nicht länger als 15 Minuten dauert.

    Wenn Sie Integrationssoftware in den Kunden bereitstellenAWSUmgebung sollten Sie nutzenAWS CloudFormationVorlagen zur Vereinfachung der Integration. Einige Partner haben eine Ein-Klick-Integration geschaffen, die dringend empfohlen wird.

29. Was sind meine Dokumentationsanforderungen?

    Sie müssen einen Link zur Dokumentation bereitstellen, die den Integrations- und Einrichtungsprozess zwischen Ihrem Produkt und Security Hub beschreibt, einschließlich Ihrer Verwendung vonAWS CloudFormation-Vorlagen.

    Diese Dokumentation sollte auch Informationen über Ihre Verwendung von ASFF enthalten. Insbesondere sollte dies die ASFF-Findungstypen auflisten, die Sie für Ihre verschiedenen Ergebnisse verwenden. Wenn Sie Standard-Insight-Definitionen haben, sollten Sie diese ebenfalls hier einbeziehen.

    Berücksichtigen Sie, andere potenzielle Informationen einzubeziehen

    - Ihr Anwendungsfall für die Integration mit Security Hub
    - Durchschnittliches Volumen der gesendeten Ergebnisse

- Ihre Integrationsarchitektur
- Die Regionen, die Sie unterstützen und die Sie nicht unterstützen
- Latenz zwischen dem Zeitpunkt, wann Ergebnisse erstellt werden und wann sie an Security Hub gesendet werden
- Ob Sie Ergebnisse aktualisieren

30. Was sind benutzerdefinierte Erkenntnisse?

    Sie werden aufgefordert, benutzerdefinierte Erkenntnisse für Ihre Ergebnisse zu definieren. Erkenntnisse sind leichte Korrelationsregeln, die einem Kunden dabei helfen, zu priorisieren, welche Erkenntnisse und Ressourcen am meisten Aufmerksamkeit und Handeln erfordern.

    Security Hub hat einen`CreateInsight`API-Operation. Sie können benutzerdefinierte Erkenntnisse in einem Kundenkonto als Teil IhresAWS CloudFormation-Vorlage. Diese Erkenntnisse werden auf der Kundenkonsole angezeigt.

31. Kann ich Dashboard-Widgets einreichen?

    Nein, derzeit nicht. Sie können nur verwaltete Erkenntnisse erstellen.

32. Was ist Ihr Preismodell?

    Sehen Sie diePreisinformationen des Security Hubaus.

33. Wie übertrage ich Ergebnisse im Rahmen des endgültigen Genehmigungsprozesses für meine Integration an das Security Hub Hub-Demokonto?

    Senden Sie Ergebnisse mit Ihrem bereitgestellten Produkt-ARN an das Security Hub Hub-Demokonto mit`us-west-2`wie die Region. Die Ergebnisse sollten die Demo-Kontonummer im`AwsAccountId`Bereich von ASFF. Wenden Sie sich an das Security Hub Hub-Team, um die Demo-Kontonummer zu erhalten.

    Senden Sie uns keine sensiblen Daten oder personenbezogenen Daten. Diese Daten werden für öffentliche Demos verwendet. Wenn Sie uns diese Daten senden, ermächtigen Sie uns, sie in Demos zu verwenden.

34. Welche Fehler- oder Erfolgsmeldungen haben**`BatchImportFindings`**Stellen Sie bereit?

    Security Hub gibt eine Antwort auf Autorisierung und eine Antwort auf`BatchImportFindings`aus. Knackigere Erfolge, Misserfolg und Fehlermeldungen befinden sich in der Entwicklung.

35. Für welche Fehlerbehandlung ist der Quelldienst verantwortlich?

Quelldienste sind für die gesamte Fehlerbehandlung verantwortlich. Sie müssen mit Fehlermeldungen, Wiederholungen, Drosselung und Alarmierung umgehen. Sie müssen auch Feedback oder Fehlermeldungen behandeln, die über den Security Hub Feedback-Mechanismus gesendet werden.

36. Was sind einige Lösungen für häufige Probleme?

Importieren in &S3;`AuthorizerConfigurationException`wird entweder durch eine Fehlformierung verursacht`AwsAccountId`oder`ProductArn`aus.

Beachten Sie bei der Fehlerbehebung Folgendes:

- `AwsAccountId`muss genau 12 Ziffern haben.
- `ProductArn`muss das folgende Format haben: arn:aws:securityhub:*<us-west-2 or us-east-1>*:*<accountId>*:produkt/*<company-id>*/*<product-id>*

  Die Konto-ID ändert sich nicht von der, die das Security Hub Hub-Team in den Produkt-ARNs aufgenommen hat, die es Ihnen zur Verfügung gestellt hat.

`AccessDeniedException`wird verursacht, wenn ein Befund an oder von dem falschen Konto gesendet wird oder wenn das Konto kein`ProductSubscription`aus. Die Fehlermeldung enthält einen ARN mit einem Ressourcentyp von`product`oder`product-subscription`aus. Dieser Fehler tritt nur bei kontoübergreifenden Anrufen auf. Wenn du anrufst`BatchImportFindings`mit Ihrem eigenen Konto für dasselbe Konto in`AwsAccountId`und`ProductArn`, Die Operation verwendet IAM-Richtlinien und hat nichts mit zu tun`ProductSubscriptions`aus.

Stellen Sie sicher, dass das Kundenkonto und das Produktkonto, das Sie verwenden, die tatsächlich registrierten Konten sind. Einige Partner haben eine Kontonummer für das Produkt aus dem Produkt ARN verwendet, versuchen jedoch, ein völlig anderes Konto zu verwenden, um anzurufen`BatchImportFindings`aus. In anderen Fällen haben sie erstellt`ProductSubscriptions`für andere Kundenkonten oder sogar für ein eigenes Produktkonto. Sie haben nicht erstellt`ProductSubscriptions`für das Kundenkonto, in das sie Ergebnisse importieren wollten.

37. Wohin schicke ich Fragen, Kommentare und Bugs?

`<securityhub-partners@amazon.com>`

38. In welche Region sende ich Ergebnisse für Artikel im Zusammenhang mit GlobalAWSdienstleistungen? Wo sende ich zum Beispiel IAM-bezogene Ergebnisse?

Senden Sie Ergebnisse in dieselbe Region, in der der Befund entdeckt wurde. Für einen Dienst wie IAM wird Ihre Lösung wahrscheinlich das gleiche IAM-Problem in mehreren Regionen finden. In diesem Fall wird der Befund an jede Region gesendet, in der das Problem erkannt wurde.

Wenn der Kunde Security Hub in drei Regionen ausführt und das gleiche IAM-Problem in allen drei Regionen festgestellt wird, senden Sie die Suche an alle drei Regionen.

Wenn ein Problem behoben ist, senden Sie das Update an die Suche an alle Regionen, in denen Sie die ursprüngliche Suche gesendet haben.

Dokumentverlauf für Partner Integration Guide

Die folgende Tabelle beschreibt die Dokumentation für diese Anleitung

Änderung	Beschreibung	Datum
Aktualisierte Anforderungen für das Konsolenlogo	Das Partnermanifest und die Logo-Richtlinien wurden aktualisiert, um darauf hinzuweisen, dass Partner sowohl eine Version des Logos im hellen Modus als auch eine Dunkelmodus-Version für die Anzeige auf der Security Hub Hub-Konsole bereitstellen müssen. Die Logos müssen im SVG-Format vorliegen.	10 Mai 2021
Die Voraussetzungen für neue Integrationspartner wurden aktualisiert	Security Hub ermöglicht jetzt auch Partnern, die demAWSISV-Partnerpfad und wer ein Integrationsprodukt verwendet, das eineAWSGrundlegende technische Überprüfung (FTR). Bisher mussten alle IntegrationspartnerAWSWählen Sie Partnerstufe aus.	29. April 2021
neu`FindingProviderFields` -Objekt in ASFF	Die Informationen zur Zuordnung der Ergebnisse zur ASFF wurden aktualisiert. Für`Confidence` ,`Criticality` ,`RelatedFindings` ,`Severity`,	18. März 2021

	und`Types`ordnen Partner ihre Werte den Feldern in`FindingProviderFields` .	
Neue Grundsätze für die Erstellung und Aktualisierung von Erkenntnissen	Es wurden neue Richtlinien für die Erstellung neuer Erkenntnisse und die Aktualisierung vorhandener Ergebnisse im Security Hub hinzugefügt.	4. Dezember 2020
Erstversion dieses Handbuchs	DasLeitfaden zur -PartnerintegrationbietetAWSPartner mit Informationen darüber, wie eine Integration hergestellt werden kannAWS Security Hub.	23. Juni 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.