Crawl, Walk, Run: Schnellere Sicherheitsreife in der AWS Cloud

AWS Prescriptive Guidance

AWS Prescriptive Guidance: Crawl, Walk, Run: Schnellere Sicherheitsreife in der AWS Cloud

Table of Contents

Einführung 1
Crawl 3
Plan 3
Umfang der Sicherheit 4
Sicherheitsmodell 7
Modell für Geschäftsziele 12
Entwicklung 13
Bewerten 15
Prowler 16
AWS Security Hub CSPM 16
Walk 17
Operationalisieren 17
AWS Framework für die Cloud-Einführung 17
Erwartete Ergebnisse 19
Reif 20
Prozesse 20
Tools 22
Risk 25
Beispiele 25
Ausführen 29
Optimieren 29
Schlussfolgerung 32
Ressourcen 35
Frameworks und Modelle 35
AWS-Services 35
Andere Ressourcen AWS 35
Mitwirkende 36
Verfassen 36
Überprüfend 36
Technisches Schreiben 36
Dokumentverlauf 37
..... xxxviii

Crawl, Walk, Run: Schnellere Sicherheitsreife in der AWS Cloud

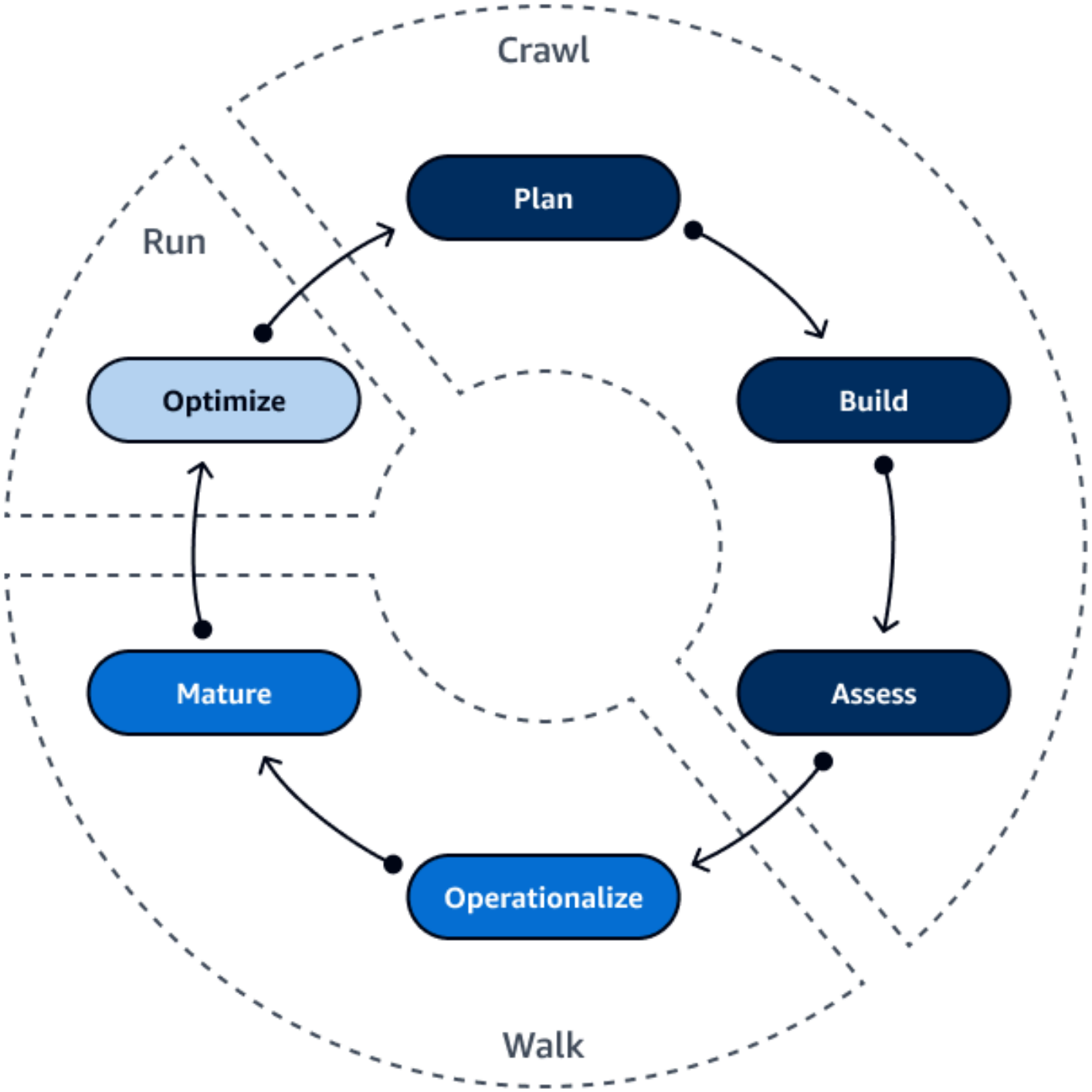
Amazon Web Services (Mitwirkende)

Dezember 2023 (Dokumentverlauf)

Für viele Unternehmen ist Sicherheit die oberste Priorität und Überlegung bei der Migration in die Cloud. Die Implementierung von Cloud-Sicherheitsfunktionen und -kontrollen ist keine einmalige Aktivität, sondern ein iteratives Modell. Sie erhöhen schrittweise Ihr Sicherheitsniveau und Ihren Reifegrad, während Sie den Cloud-Betrieb ausbauen. Sie könnten beispielsweise mit AWS verwalteten Richtlinien beginnen und dann, wenn Ihr Unternehmen bereit ist, benutzerdefinierte Richtlinien implementieren, die dem Prinzip der geringsten Rechte folgen.

Dieser Leitfaden bietet einen Leitfaden für die Anwendung einer Crawling-Walk-Run-Methode, mit der Sie Ihr Unternehmen im Bereich Cloud-Sicherheit schneller voranbringen können. Es definiert einen schrittweisen Ansatz zur Automatisierung von Sicherheitsfunktionen. Es wird auch pragmatisch erklärt, wie Sie die Funktionalität AWS-Services und die Funktionen optimal nutzen können. Dieser Leitfaden hilft Ihnen dabei, die Herausforderungen und Chancen der Cloud zu verstehen und zu erfahren, wie Sie schnell vorankommen und erfolgreich sein können. AWS

Eine Reise in die Cloud erfordert den Aufbau von Frameworks, die Verwaltung und Weiterentwicklung von Abläufen und die Optimierung von Prozessen. Die folgende Abbildung zeigt die einzelnen Phasen der Crawl-, Walk- und Run-Methode: Planung, Aufbau, Bewertung, Operationalisierung, Weiterentwicklung und Optimierung.



Die Crawl-Phase besteht aus der Planung, dem Aufbau der Grundlage und der Bewertung Ihres aktuellen Sicherheitsstatus. In der Walk-Phase implementieren Sie Ihre Mitarbeiter, Prozesse und Technologien und entwickeln anschließend Ihre Betriebsabläufe durch Optimierung und Messung weiter. Die Startphase besteht aus der Optimierung durch Bewertung und Automatisierung.

Crawl-Phase: Planung, Aufbau und Bewertung

Die Crawl-Phase beginnt mit der Planung. Die Planung umfasst die Festlegung des Sicherheitsbereichs und die Auswahl des Modells, das am besten zu Ihrem Unternehmen passt. Nachdem Sie den Plan erstellt haben, können Sie mit dem Aufbau einer Grundlage beginnen. Darauf folgt die Bewertung Ihrer aktuellen Sicherheitslage und die Festlegung einer Disziplin, sobald Sie die Sicherheitsinfrastruktur aufgebaut haben. Die Crawl-Phase ist iterativ. Die Iteration in der Cloud ist schneller als die Iteration in einer lokalen Umgebung. Mit zunehmender Weiterentwicklung Ihrer Cloud-Funktionen beschleunigt sich der Iterationsprozess.

Die Crawl-Phase umfasst die folgenden Phasen:

- Plan— Wie ermitteln Sie Ihren Anwendungsbereich und wählen ein Modell aus?
- Entwicklung— Wie werden Sie den Rahmen festlegen?
- Bewerten— Wie ist Ihr derzeitiger Sicherheitsstatus?

Plan: Festlegung Ihres Sicherheitsumfangs und -modells

Die Planung ist ein iterativer Prozess, während Sie Ihr Sicherheitsmodell weiterentwickeln. Zu den wichtigsten Schritten des Planungsprozesses gehören:

- Den Sicherheitsumfang verstehen— Der Sicherheitsumfang variiert und hängt davon ab, wie die Cloud genutzt wird.
- Auswahl eines Sicherheitsmodells— Identifizieren Sie das am besten geeignete Sicherheitsmodell für Ihren Sicherheitsanwendungsfall.
- Erstellung eines Geschäftszielmodells— Definieren Sie klare Ziele und Mechanismen zur Erfolgsmessung.

Beachten Sie bei der Entwicklung Ihres Plans Folgendes:

- Seien Sie bereit, es zu wiederholen. Die Iteration ist in der Cloud konstant. Die Iteration hilft Ihnen dabei, Lücken im Plan zu identifizieren.

- Fangen Sie nicht mit Dienstleistungen an. Beginnen Sie mit Ihrem Plan, anstatt herauszufinden, welche Dienste Sie benötigen. Dies trägt dazu bei, dass Ihr Unternehmen die angestrebten Ergebnisse erzielt.

Den Sicherheitsumfang verstehen

Das Modell der AWS gemeinsamen Verantwortung definiert, wie Sie gemeinsam die Verantwortung AWS für Sicherheit und Compliance in der Cloud übernehmen. AWS sichert die Infrastruktur, auf der alle in der angebotenen Dienste ausgeführt werden AWS Cloud, und Sie sind dafür verantwortlich, Ihre Nutzung dieser Dienste, z. B. Ihrer Daten und Anwendungen, zu sichern.

Dieses gemeinsame Modell kann Ihnen dabei helfen, die Einhaltung von Vorschriften und den betrieblichen Aufwand zu verringern, da viele Komponenten AWS betrieben, verwaltet und kontrolliert werden, angefangen beim Host-Betriebssystem und der Virtualisierungsebene bis hin zur physischen Sicherheit der Einrichtungen, in denen der Service betrieben wird. Managed Services helfen Ihnen dabei, Ihre Sicherheits- und Compliance-Verpflichtungen AWS zu reduzieren, indem sie die Verwaltung einiger Sicherheitsaufgaben wie Patches und Schwachstellenmanagement ermöglichen. Die Verwendung von Managed Services ist eine bewährte Methode im AWS Well-Architected Framework. Im Allgemeinen wird mit der Modernisierung der Infrastruktur mehr Verantwortung auf den Dienstanbieter verlagert.

Im Folgenden finden Sie drei verschiedene Servicebeispiele, die Ihnen helfen sollen, zu verstehen, wie sich Ihr Sicherheitsumfang je nachdem, für welche Dienste Sie sich entscheiden, ändert:

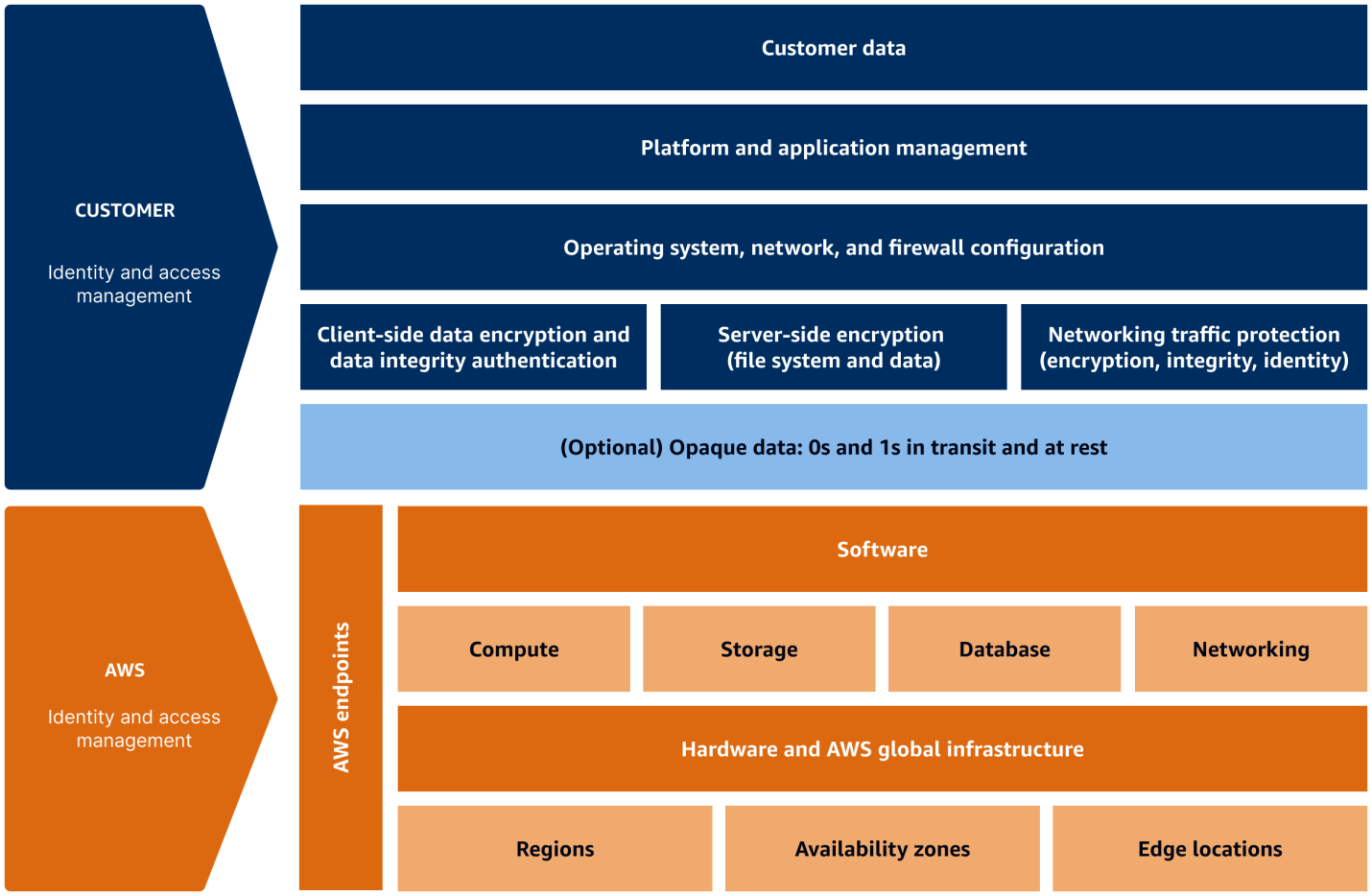
- Infrastrukturdienste
- Container-Services
- Serverlose Dienste

Ihre Verantwortung für die Sicherheit ist nicht statisch und ändert sich je nach Art der Architektur, die Sie auswählen. Ihre Zeit, Ihr Aufwand und Ihre Kosten hängen von der von Ihnen gewählten Cloud-Architektur ab.

Infrastrukturdienste

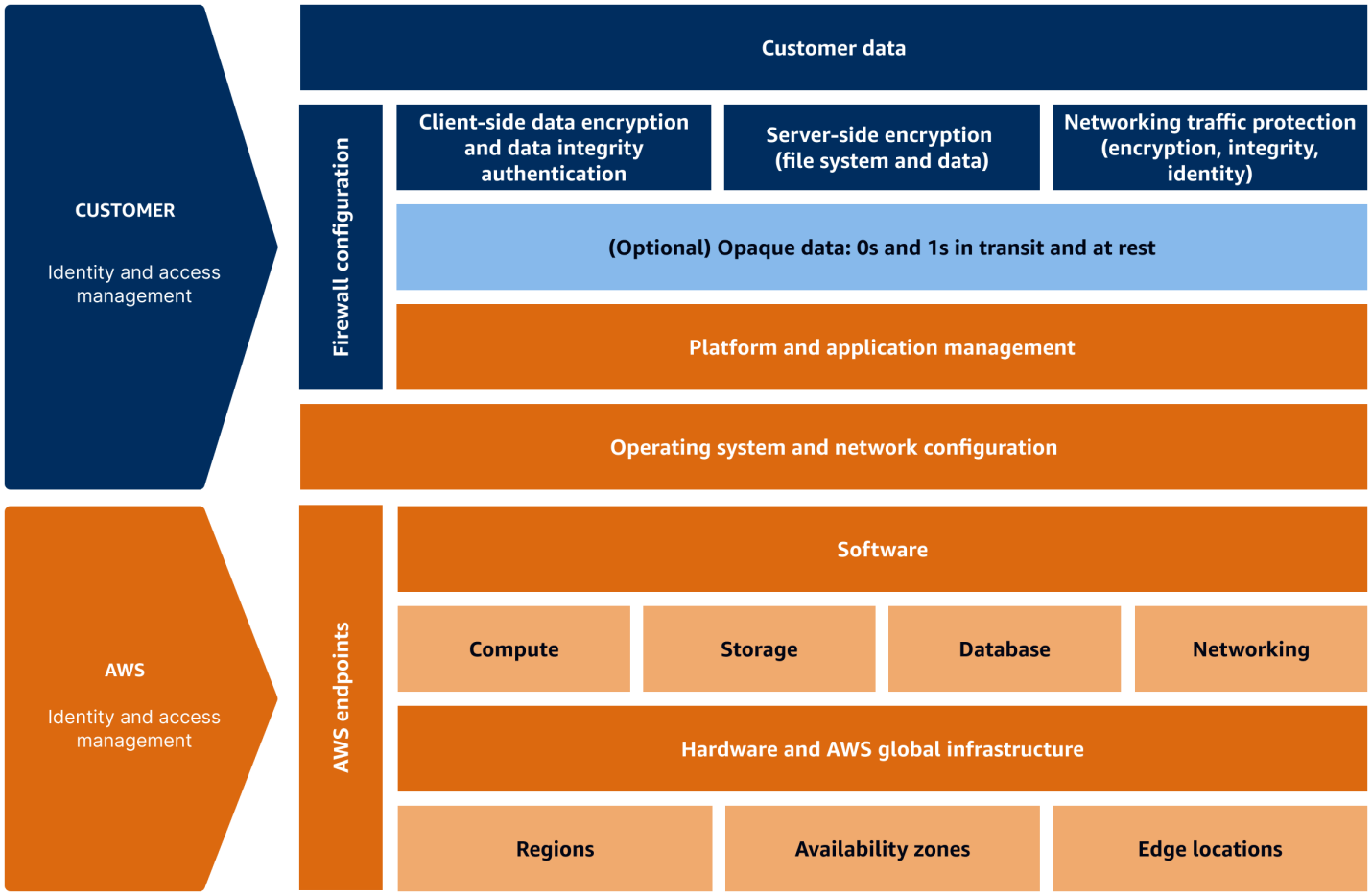
AWS Konzentriert sich bei Infrastrukturdiensten auf die Sicherung der zugrunde liegenden Infrastruktur. Bei Infrastrukturdienstleistungen ist der Umfang für den Kunden größer, da er sich im Vergleich zu den anderen Modellen mit Plattformsicherheit, Betriebssystem-Patching und

Anwendungsmanagement befassen muss. Amazon Elastic Compute Cloud (Amazon EC2) ist ein Beispiel für einen gemeinsamen Infrastrukturservice.



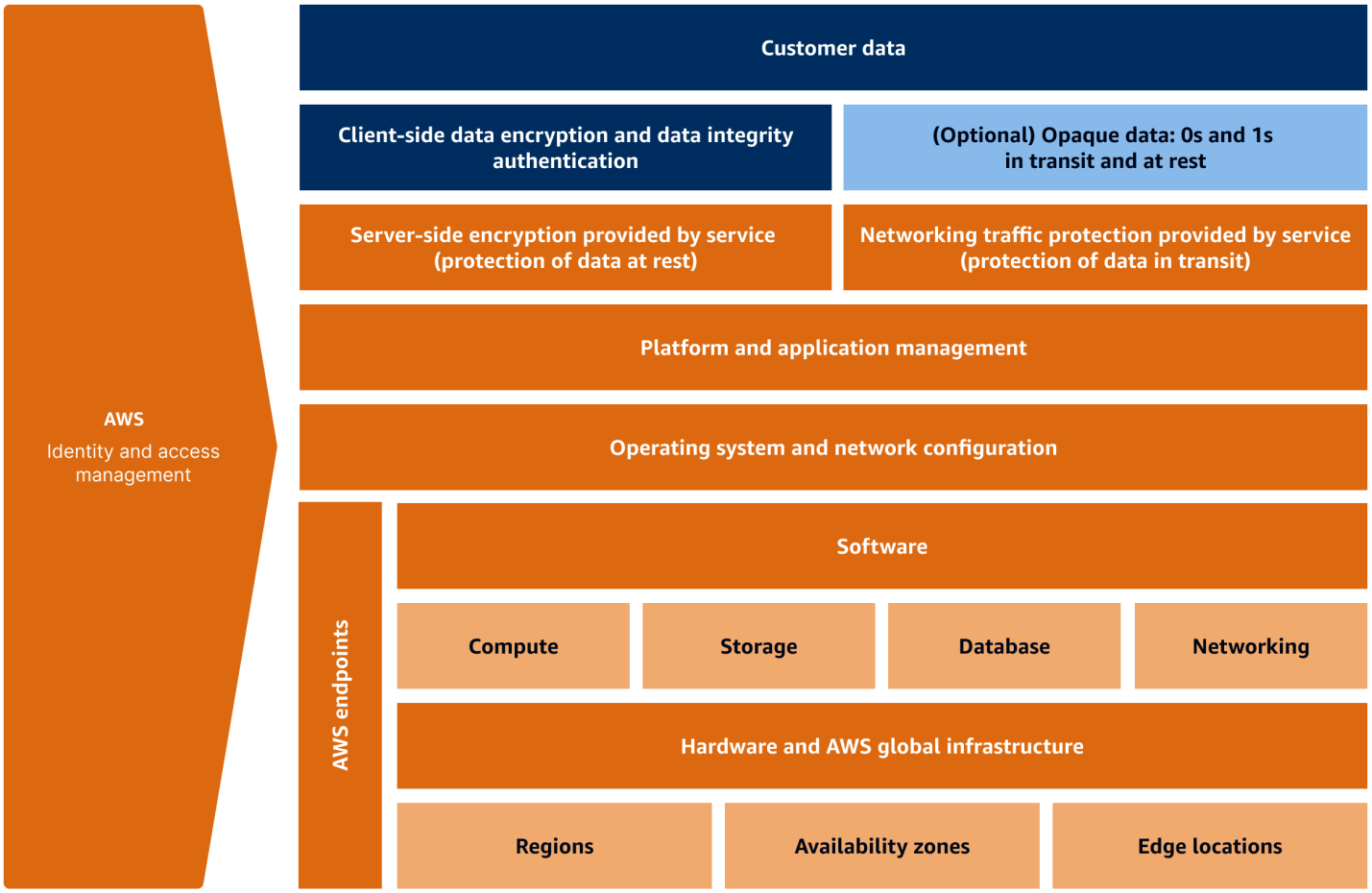
Container-Services

Je abstrahierter und modernisierter die Infrastruktur wird, desto geringer wird der Platzbedarf. Ihr Anwendungsbereich schrumpft, weil sich die Verantwortung für einige Sicherheitselemente auf verlagert. AWS Containerdienste sind ein Beispiel, auf das sich einige der Backend-Verantwortlichkeiten zurückverlagern. AWS AWS Wird beispielsweise für die Konfiguration des Betriebssystems (OS), die Netzwerkkonfiguration, das Plattformmanagement und das Anwendungsmanagement verantwortlich. Beispiele für gängige Container-Services sind Amazon Elastic Kubernetes Service (Amazon EKS), Amazon Elastic Container Registry (Amazon ECR), Amazon Elastic Container Service (Amazon ECS) und. AWS Fargate



Serverlose Dienste

Bei der Nutzung serverloser Dienste liegt fast die gesamte Verantwortung für die Sicherheit bei. AWS Der Umfang Ihrer Verantwortung ist minimal. Mit einer verwalteten serverlosen Datenbank (DB) müssen Sie beispielsweise das Netzwerk, die Hardware und das Betriebssystem nicht mehr sichern. Das gesamte Betriebssystem- und DB-Patching wird von abgedeckt. AWS Ihr einziges Anliegen ist die Sicherung des Zugriffs auf die Daten durch Verschlüsselung und Authentifizierung.



Auswahl eines Sicherheitsmodells

Sie können aus verschiedenen Sicherheitsmodellen oder -ansätzen für wählen AWS. Die Wahl des Ansatzes und des am besten geeigneten Modells hängt von Ihrer Zielgruppe, den angestrebten Geschäftsergebnissen und dem gesamten Geschäftsprozess ab. Es ist möglich, eine Mischung aus mehreren Modellen zu verwenden.

Im Folgenden sind einige gängige Modelle aufgeführt:

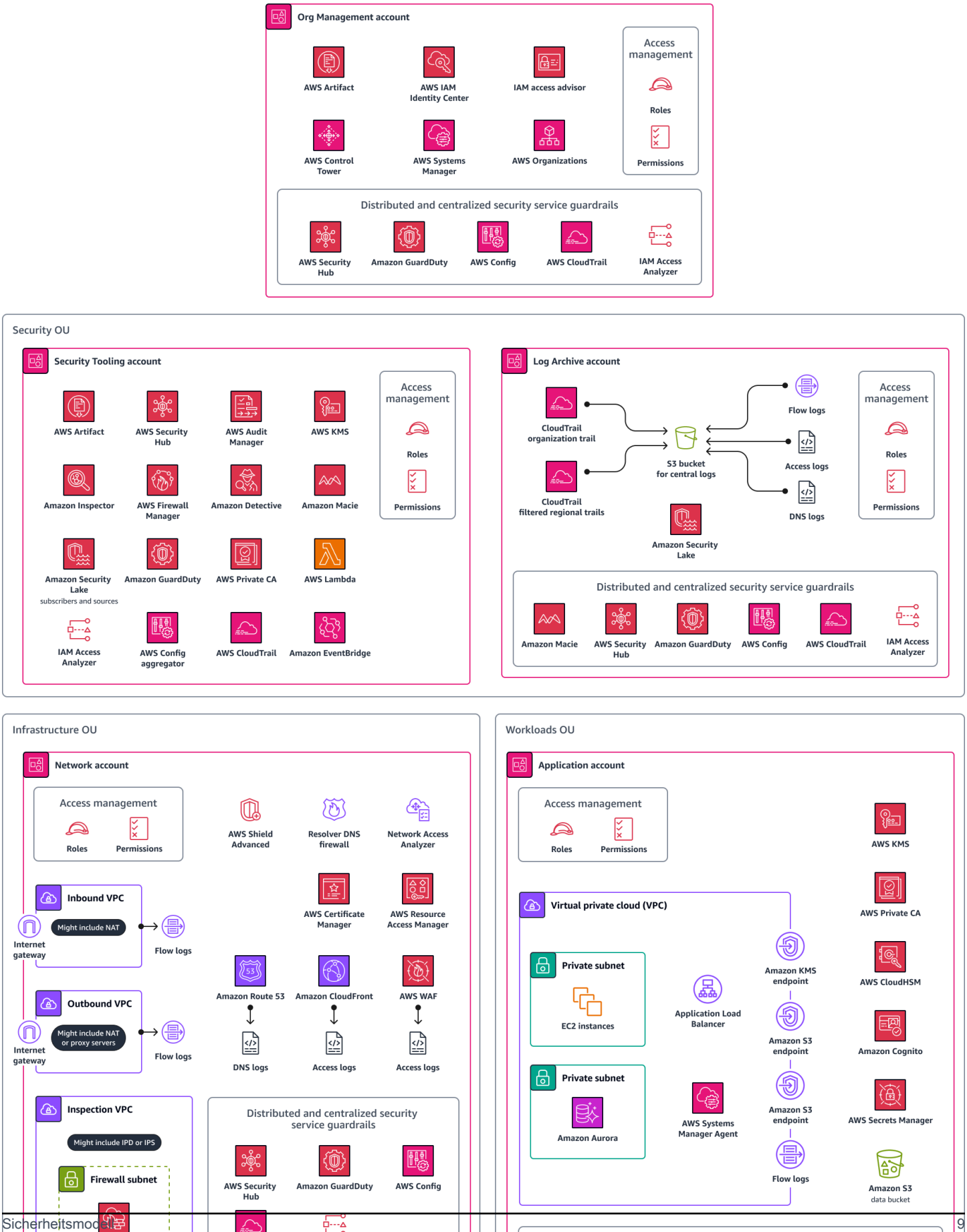
- Architektonisches Modell
- Reifegradmodell
- Modell der Unternehmensführung

Jedes Modell hat seine eigenen Vor- und Nachteile. Es ist wichtig zu überlegen, welcher Ansatz für Ihr Unternehmen am besten geeignet ist. Binden Sie Sicherheitsexperten frühzeitig in den Prozess der Modernisierung Ihrer Infrastruktur und der Einführung von Cloud-Strategien ein. Das von Ihnen

gewählte Modell hat erhebliche Auswirkungen auf die Rollen und Verantwortlichkeiten innerhalb Ihres Unternehmens.

Architektonisches Modell

Die folgende Abbildung zeigt die AWS Sicherheitsreferenzarchitektur. Dieser architektonische Ansatz bietet eine Blaupause für ein Sicherheitsmodell. Dieser Ansatz eignet sich am besten, wenn Sie mit technischen Teams innerhalb Ihres Unternehmens zusammenarbeiten. Es hilft dabei, ein ideales zukünftiges Staatsziel festzulegen. Es entspricht auch vielen Compliance- und AWS Frameworks.


Org Management account
AWS Artifact
AWS IAM Identity Center
IAM access advisor
AWS Control Tower
AWS Systems Manager
AWS Organizations
Access management
Roles
Permissions
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Security OU
Security Tooling account
AWS Artifact
AWS Security Hub
AWS Audit Manager
AWS KMS
Amazon Inspector
AWS Firewall Manager
Amazon Detective
Amazon Macie
Amazon Security Lake
subscribers and sources
Amazon GuardDuty
AWS Private CA
AWS Lambda
IAM Access Analyzer
AWS Config aggregator
AWS CloudTrail
Amazon EventBridge
Access management
Roles
Permissions
Log Archive account
CloudTrail organization trail
CloudTrail filtered regional trails
S3 bucket for central logs
Flow logs
Access logs
DNS logs
Amazon Security Lake
Access management
Roles
Permissions
Distributed and centralized security service guardrails
Amazon Macie
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Infrastructure OU
Network account
Access management
Roles
Permissions
AWS Shield Advanced
Resolver DNS firewall
Network Access Analyzer
AWS Certificate Manager
AWS Resource Access Manager
Inbound VPC
Might include NAT
Internet gateway
Flow logs
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
Amazon Route 53
Amazon CloudFront
AWS WAF
DNS logs
Access logs
Access logs
Inspection VPC
Might include IPD or IPS
Firewall subnet
AWS Network Firewall
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Shared Services account
Workloads OU
Application account
Access management
Roles
Permissions
Virtual private cloud (VPC)
Private subnet
EC2 instances
Private subnet
Amazon Aurora
Application Load Balancer
AWS Systems Manager Agent
Amazon KMS endpoint
Amazon S3 endpoint
Amazon S3 endpoint
Flow logs
AWS KMS
AWS Private CA
AWS CloudHSM
Amazon Cognito
AWS Secrets Manager
Amazon S3
data bucket
Distributed and centralized security service guardrails
Amazon Macie
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer

Vorteile des Architekturmodells:

- Entspricht den Anforderungen des Health Insurance Portability and Accountability Act (HIPAA) und des Health Information Trust Alliance Common Security Framework (HITRUST CSF)
- Bietet eine architektonische Perspektive
- Passt sich den Cloud-Strategien und -Leitlinien für große Unternehmen an
- Stimmt mit dem AWS Cloud Adoption Framework (AWSCAF) überein
- Stimmt mit dem Framework überein AWS Well-Architected

Nachteil des Architekturmodells:

- Ist eher technologieorientiert als geschäftsorientiert

Reifegradmodell

Der Ansatz des AWS Security Maturity Model konzentriert sich auf die Verwaltung und Reduzierung von Risiken, indem der Implementierung von Sicherheitsmaßnahmen Priorität eingeräumt wird. Dieser Ansatz eignet sich gut für Sicherheitsleiter und CISOs, ist jedoch nicht geschäftsorientiert.

Vorteile des Reifegradmodells:

- Ist Sicherheit im Mittelpunkt
- Ist ein Modell, das sich auf die Verwendung eines agilen Implementierungsansatzes konzentriert
- Hilft Ihnen, Risiken schnell zu reduzieren
- Stimmt mit dem AWS Cloud Adoption Framework (AWS CAF) überein

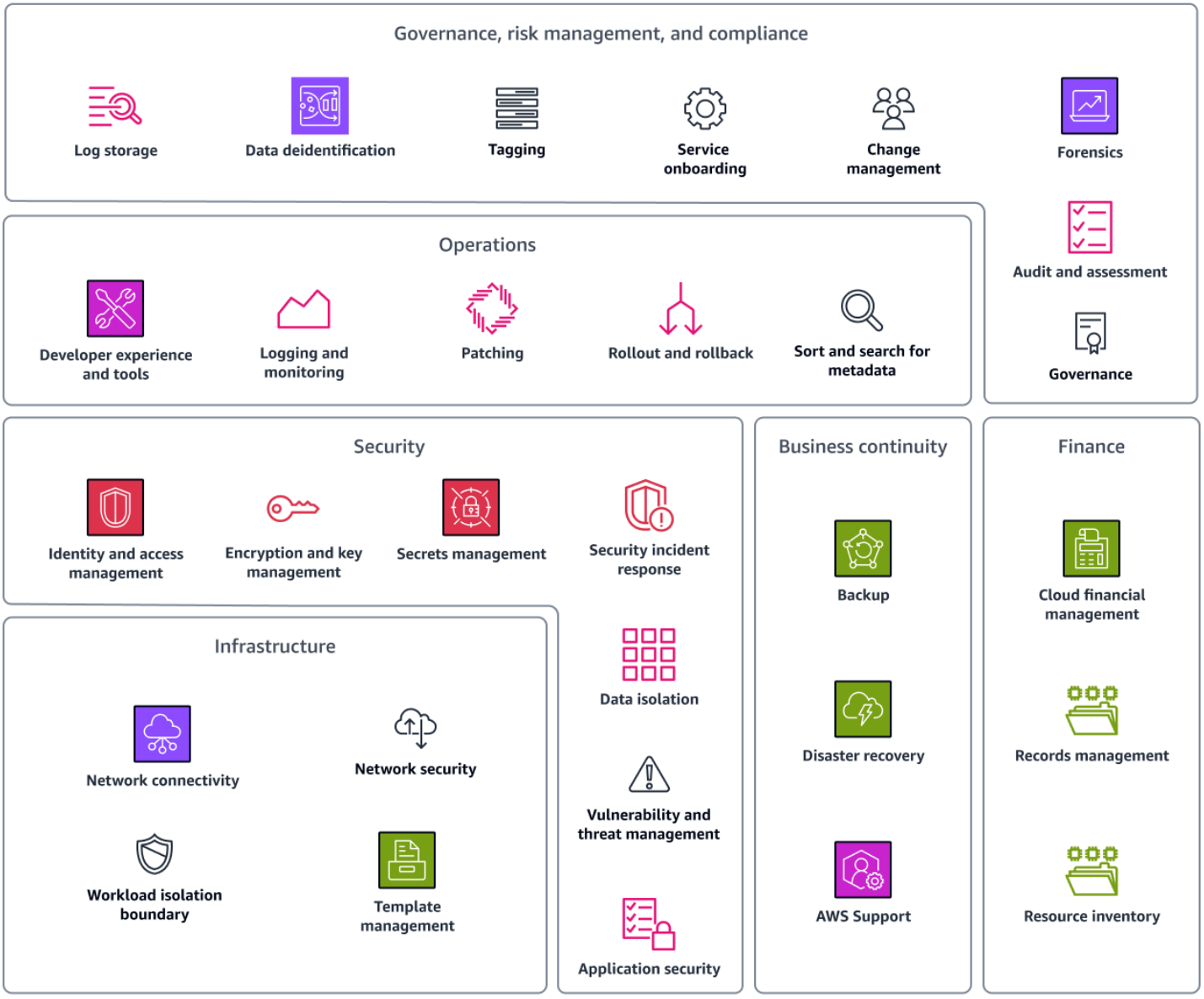
Nachteile des Reifegradmodells:

- Ist eher technologieorientiert als geschäftsorientiert

Modell der Unternehmensführung

Das AWS Cloud-Foundation-On-Modell verwendet einen GRC-Ansatz (Governance, Risikomanagement und Compliance), um Unternehmen bei der Erfüllung von Sicherheits- und Compliance-Anforderungen zu unterstützen. Es definiert die allgemeinen Richtlinien, denen Ihre

Cloud-Umgebung folgen sollte. Die Funktionen dieses Modells helfen Ihnen dabei, Aktionspunkte zu definieren, Ihre Risikobereitschaft zu definieren und interne Richtlinien aufeinander abzustimmen.



Das Cloud Foundation-Modell ist ein Leitfaden für Funktionen und Governance, der Sie beim Aufbau und der Weiterentwicklung Ihrer AWS Cloud Umgebung unterstützt. Es basiert auf einer Reihe von Definitionen, Szenarien, Anleitungen und Automatisierungen. Der Leitfaden umfasst die personellen, prozessualen und technologischen Aspekte der Einrichtung einer AWS Cloud Umgebung. Er deckt sechs Kategorien von Funktionen ab, die für eine Cloud-Grundlage unerlässlich sind:

- Unternehmensführung, Risikomanagement und Compliance
- Operationen

- Sicherheit
- Geschäftskontinuität
- Finanzen
- Infrastruktur

Der Leitfaden enthält außerdem Beispiele, Zeitpläne und weiterführende Informationen zu den einzelnen Funktionen.

Vorteile des Governance-Modells:

- Hat einen breiten Technologiefokus
- Ist auf Zuverlässigkeit ausgelegt
- Verwendet einen operativen Ansatz

Nachteil des Governance-Modells:

- Ist eher technologieorientiert als geschäftsorientiert

Erstellung eines Geschäftszielmodells

Das Geschäftszielmodell beinhaltet die Definition von Geschäftsergebnissen. Es ähnelt dem AWS Cloud Adoption Framework und dem AWS Well-Architected Framework. Dieser Ansatz konzentriert sich auf das, woran das Unternehmen interessiert ist, indem er die angestrebten Geschäftsergebnisse interpretiert. Der Vorteil dieses Ansatzes besteht darin, dass es einfach ist, Geschäftsziele mit Sicherheitszielen zu verknüpfen. Ein Beispiel für ein Geschäftsziel ist: „Ermöglichen Sie sichere externe Verbindungen und eine beschleunigte Bereitstellung neuer Benutzer und Umgebungen, indem Sie die Transparenz automatisieren und anhand bewährter Verfahren messen, um Risiken kontinuierlich zu senken.“ Sie legen Technologieziele fest, die Ihnen helfen, die entsprechenden Geschäftsergebnisse zu erreichen. Das Modell der Geschäftsziele knüpft an Sicherheitsziele an, wie z. B. die Aufrechterhaltung der Transparenz. Anschließend implementieren Sie ein technisches Ziel, wie z. B. bewährte AWS Identity and Access Management (IAM-) Sicherheitsverfahren, um das Sicherheitsrisiko zu reduzieren.

Vorteile des Geschäftszielansatzes:

- Beinhaltet eine Begründung der Kosten

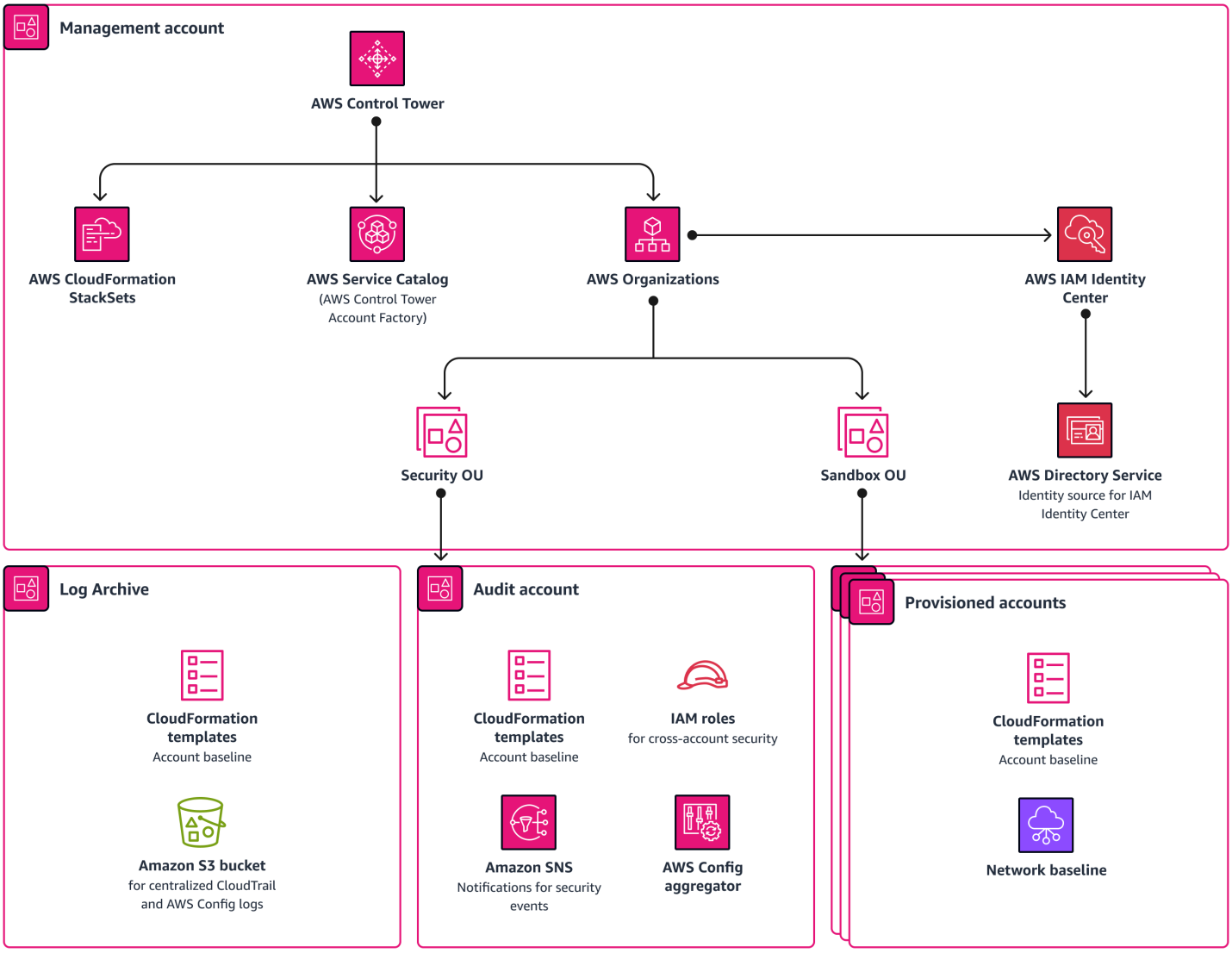
- Bietet eine klare, auf das Geschäft ausgerichtete Sicherheitsausrichtung
- Definiert Erfolgsmessungen anhand der Erreichung von Geschäftsergebnissen

Nachteile des Geschäftszielansatzes:

- Kann zeitaufwändig sein, da Sie herausfinden müssen, was das Unternehmen will
- Ist eher geschäftsorientiert als technologieorientiert

Aufbau: Den Grundstein für eine starke Cloud-Sicherheitsbasis legen

Jetzt, wo Sie einen Plan haben, besteht der nächste Schritt darin, die Grundlagen zu legen. In diesem Schritt wird gezeigt, wie Sie eine erste Cloud-Grundlage aufbauen können AWS , die sicher, belastbar, skalierbar und für mehrere Konten automatisiert ist. Die Grundsteinlegung kann speziell auf Ihre Geschäftsziele zugeschnitten und angepasst werden. Sie können die Steuerung an eine neue landing zone anpassen oder sie in eine bestehende landing zone integrieren.
Die darin enthaltenen Automatisierungen AWS Control Towerkönnen Ihnen dabei helfen, die Sicherheitsgrundlagen in der zu legen. AWS Cloud Das folgende Bild zeigt eine landing zone, die durch eingerichtet ist AWS Control Tower.



AWS Control Tower orchestriert mehrere AWS-Services in Ihrem Namen, z. B. AWS Organizations AWS Service Catalog, und AWS IAM Identity Center. Sie können innerhalb einer Stunde eine neue landing zone einrichten, und diese landing zone ist so konzipiert, dass sie Ihren Sicherheits- und Compliance-Anforderungen entspricht. AWS Control Tower richtet Ihre landing zone gemäß den vorgeschriebenen Best Practices für die Sicherheit ein. AWS Control Tower hilft Ihnen bei der Verwaltung der Cloud-Bereitstellung, indem es die Transparenz und Kontrolle über Konten und Endbenutzer verbessert. Es unterstützt Administratoren dabei, Rechenressourcen effizient zuzuweisen und zu überwachen, eine rollenbasierte Zugriffskontrolle zu implementieren, die Leistung mithilfe von Protokollierungs- und Überwachungstools zu überwachen, Kosten effektiv zu verwalten, Bereitstellungsprozesse zu automatisieren, Sicherheitsmaßnahmen durchzusetzen und die Einhaltung von Industriestandards sicherzustellen.

AWS Control Tower ist der schnellste Weg, eine sichere, konforme AWS Umgebung mit mehreren Konten einzurichten und zu verwalten, die auf bewährten Verfahren basiert. Weitere Informationen zum Umgang mit AWS Control Tower und zu den darin beschriebenen bewährten Verfahren finden Sie unter Strategie für AWS mehrere Konten:AWS Leitfaden für bewährte Verfahren.

Das AWS Control Tower ist zwar der schnellste Ansatz, aber nicht der einzige. Der wichtige Teil ist, dass Sie eine landing zone einrichten, die mindestens Folgendes bietet:

- Multi-account Verwaltung
- Identitäts- und Verbundzugriffsmanagement
- Ein zentrales Archiv für Protokolle
- Cross-account Zugriff prüfen
- End-user Kontobereitstellung
- Zentralisierte Überwachung und Benachrichtigungen

Bewertung: Bewertung Ihrer aktuellen Cloud-Sicherheitslage

Bevor Sie etwas in der landing zone einsetzen, überprüfen Sie Ihre landing zone, um sicherzustellen, dass sie Ihren Anforderungen entspricht, und legen Sie eine Ausgangsbasis fest. Diese Vorgehensweise wird als Bewertung der Cloud-Position bezeichnet. Es hilft Ihnen, Risiken in Ihrer gesamten Cloud-Infrastruktur zu identifizieren und zu beheben. Durch die Bewertung Ihres Cloud-Sicherheitsstatus erhalten Sie einen Überblick über die relevanten Sicherheitskontrollen in der Cloud-Umgebung.

Im Folgenden sind die Vorteile einer Bewertung des Cloud-Status aufgeführt:

- Es hilft Ihnen dabei, Ihren aktuellen Sicherheitsstatus zu verstehen und Empfehlungen zur Reduzierung Ihres Risikoprofils, zur Behebung vorhandener Sicherheitslücken oder zur Korrektur von Fehlkonfigurationen zu erhalten.
- Es hilft Ihnen dabei, bewährte Sicherheitsmethoden zu identifizieren, sodass Sie Fehltritte vermeiden und Geschäftsrisiken reduzieren können.
- Es bietet Kennzahlen, anhand derer Sie Verbesserungen verfolgen und den Erfolg messen können.

In diesem Abschnitt werden Dienste und Tools AWS Security Hub CSPM sowie Tools beschriebenProwler, mit denen Sie eine Bewertung des Cloud-Status in Ihrer Umgebung durchführen können.

Prowler

Prowlerist ein Open-Source-Befehlszeilentool, mit dem Sie Ihre Konten bewerten, prüfen und überwachen können, um sicherzustellen, dass sie bewährte AWS Sicherheitsmethoden und andere Sicherheitsrahmen und -standards einhalten. Es überprüft Ihre Konfiguration und identifiziert Sicherheitsprobleme. Sie können es Prowler in Umgebungen mit mehreren Konten verwenden, und Drittanbieter können es auch verwenden, um die Sicherheit Ihrer AWS Umgebung zu bewerten.

Im Folgenden sind die Vorteile von Prowler aufgeführt:

- Es ist kostenlos und Open Source.
- Es verfügt über flexible Bereitstellungsoptionen und ist skalierbar.
- Es führt Konformitätsprüfungen durch, z. B. für Center for Internet Security (CIS) Benchmark for AWS, General Data Protection Regulation (GDPR) und HIPAA.
- Es hilft Ihnen bei der Erstellung von Snapshots und Baselines.

AWS Security Hub CSPM

AWS Security Hub CSPMbietet einen umfassenden Überblick über Ihren Sicherheitsstatus in. AWS Es hilft Ihnen auch dabei, Ihre Umgebung anhand der Sicherheitsstandards und bewährten Verfahren der Branche zu überprüfen. Es ist integriert, AWS Control Tower sodass Sie die Security Hub CSPM-Detektivkontrollen über den AWS Control Tower Dienst konfigurieren können. Das Ziel, die Sicherheitsreife zu erhöhen, besteht darin, den Bewertungsprozess von einer einmaligen Momentaufnahme zu einem kontinuierlichen Prozess zur Fortschrittsüberwachung weiterzuentwickeln.

Im Folgenden sind die Vorteile von Security Hub CSPM aufgeführt:

- Es bietet ein einheitliches Dashboard, das den aktuellen Status der Umgebung anzeigt und Ihnen hilft, Probleme zu identifizieren und zu beheben.
- Es führt kontinuierliche Bewertungen mit automatisierten Prüfungen durch.

Gehphase: Operationalisierung und Reifung

Die Walk-Phase konzentriert sich auf die Operationalisierung. In dieser Phase muss Ihr Unternehmen sein aktuelles Betriebsmodell bewerten, festlegen, wie es an die Cloud angepasst werden sollte, diese Änderungen implementieren und dann die Fortschritte messen. Dazu gehört auch die Berücksichtigung von Fähigkeiten, Betriebsprozessen und Technologien. Die Optimierung der Cloud-Implementierung und die Messung der Fortschritte sind während der gesamten Startphase von entscheidender Bedeutung, um den Erfolg zu bestätigen.

In der Walk-Phase sind die folgenden Phasen aufgeführt:

- Operationalisieren— Wie bereiten Sie Ihre Mitarbeiter, Technologien und Prozesse auf die Cloud vor?
- Reif— Wie messen Sie Fortschritt und Erfolg?

Operationalisieren: Bereiten Sie Ihr Unternehmen auf eine ausgereifte Cloud-Sicherheit vor

Um den Prozess der Bereitstellung betrieblicher Lasten in der Cloud voranzutreiben, ist es wichtig, sich auf die Abstimmung von Mitarbeitern, Prozessen und Technologien zu konzentrieren. Dies ist in der Cloud-Umgebung besonders wichtig, da sich Prozesse und Fähigkeiten wahrscheinlich von denen vor Ort unterscheiden. In diesem Abschnitt verwenden Sie ein Framework, um Ihre Mitarbeiter, Prozesse und Technologien aufeinander abzustimmen. Anschließend bestätigen Sie, dass das Framework Ihnen geholfen hat, die erwarteten Ergebnisse zu erzielen.

AWS Framework für die Cloud-Einführung

Das AWS Cloud Adoption Framework (AWS CAF) hilft Ihnen dabei, Ihre Geschäftsergebnisse durch innovative Nutzung AWS-Services und Funktionen zu beschleunigen. AWS CAF identifiziert sechs

spezifische Unternehmensperspektiven, die erfolgreiche Cloud-Transformationen untermauern: Unternehmen, Mitarbeiter, Unternehmensführung, Plattform, Sicherheit und Betrieb. Jede Perspektive enthält Funktionen, die Ihre Cloud-Bereitschaft verbessern und Ihnen helfen können, Ihre Cloud-Transformation zu beschleunigen.

Die folgende Abbildung zeigt die sechs Perspektiven in der AWS CAF und die Funktionen in den einzelnen Perspektiven. Weitere Informationen finden Sie unter Grundlegende Funktionen im Überblick über das AWS Cloud Adoption Framework.

Erwartete Ergebnisse

Wenn Sie AWS CAF verwenden, um Ihre Mitarbeiter, Prozesse und Technologien aufeinander abzustimmen, können Sie davon ausgehen, dass Sie die folgenden Ergebnisse erzielen werden:

- DevSecOps Pipeline und Prozess — Die Implementierung einer DevOps Pipeline mit integrierten Sicherheitstools kann Ihnen helfen, Infrastructure as a Code (IaC) sicherer einzusetzen. Sie können Code-Scans und Sicherheitsüberprüfungen im Pipeline-Prozess implementieren, wie z. B. cfn_nag (GitHub), ein statischer Open-Source-Codeanalysator.
- Tagging und Asset Management — Mithilfe von Tags können Sie Ressourcen in der Cloud effizienter und einheitlicher verwalten. Weitere Informationen finden Sie unter Markieren Ihrer AWS -Ressourcen. Es ist wichtig, eine dynamische Vermögensverwaltungsstrategie zu entwickeln, die sich an die sich ständig ändernde Natur der Cloud anpassen kann. AWS Systems Manager Inventar hilft Ihnen beim Zuweisen von Tags, sodass Sie Ihre Ressourcen schnell suchen, verwalten und identifizieren können.
- Integration von Überwachung und Erkennung — Es ist wichtig, eine Methode für das Senden von Warnmeldungen aus der Cloud an lokale Security Operations Center (SOCs) und SIEM-Systeme (Security Information and Event Management) zu entwickeln. Amazon GuardDuty ist ein Dienst zur kontinuierlichen Sicherheitsüberwachung, der Protokolle analysiert und verarbeitet, um unerwartete und potenziell nicht autorisierte Aktivitäten in Ihrer AWS Umgebung zu identifizieren. Es lässt sich auch in viele Tools von Drittanbietern integrieren.
- Plan und Programm zur Reaktion auf Cloud-Vorfälle — Es ist wichtig sicherzustellen, dass die Mitarbeiter, die für die Bearbeitung der Cloud-Benachrichtigungen verantwortlich sind, mit dem Prozess der Erfassung dieser Warnmeldungen vertraut sind und wissen, wie auf Cloud-Warnungen zu reagieren ist, im Gegensatz zu lokalen Warnungen. Um die Reaktionsfähigkeit auf Vorfälle zu verbessern, schulen Sie das Personal darin, Amazon Detective für die Protokollanalyse zu verwenden. Amazon Detective unterstützt Sie bei der Analyse, Untersuchung und Identifizierung der Hauptursache von Sicherheitsfeststellungen oder verdächtigen Aktivitäten. Amazon Detective sollte Teil eines Notfallplans sein.
- Cloud-Schwachstellenmanagement — Der Prozess der Verwaltung von Sicherheitslücken in der Cloud unterscheidet sich von lokalen Umgebungen. Neben dem herkömmlichen Schwachstellenmanagement müssen Sie auch die Codeebene der Infrastruktur bewerten. Amazon Inspector ist ein automatisierter Schwachstellen-Management-Service, der Ihre Ressourcen kontinuierlich auf Schwachstellen und unbeabsichtigte Netzwerkbedrohungen überprüft.
- Verwaltung des Cloud-Status — Wie im Abschnitt Assess beschrieben, ist die Verwaltung des Cloud-Status ein wichtiger Aspekt der Cloud-Sicherheit. Sie können AWS Security Hub CSPM

damit die Überprüfung bewährter Sicherheitsverfahren automatisieren und Ihren gesamten Cloud-Status in allen Bereichen bewerten AWS-Konten.

- Schulungen zur Cloud-Sicherheit — Es ist wichtig, dass die Mitarbeiter angemessen geschult werden, damit sie sich mit Cloud-Sicherheit auskennen. Dazu gehören der Zugang zu Ressourcen und die Bereitstellung von Zeit für die Mitarbeiter, um sich die erforderlichen Kenntnisse und Fähigkeiten anzueignen. AWS bietet zahlreiche Schulungsressourcen zur Weiterbildung und Weiterbildung, wie z. B.AWS Skill Builder.

Ausgereift: Optimierung und Messung von Prozessen, Tools und Risiken

In der Reifephase des Cloud-Sicherheitsmodells liegt der Schwerpunkt darauf, die Sicherheitsteams auf die Sicherheitsfunktionen des AWS Cloud Adoption Framework (AWS CAF) auszurichten und agile Prozesse einzuführen. Diese Abstimmung hilft spezialisierten Teams, Innovationen in kurzen Sprints zu beschleunigen und gleichzeitig Roadmaps und langfristige Planungen zu berücksichtigen. In der Reifephase liegt der Schwerpunkt auf der Zusammenarbeit mit dem IT-Betrieb und dem Ausbau fundierter, spezialisierter Cloud-Fähigkeiten. Jede Sicherheitsfunktion implementiert wichtige Tools und Prozesse zur Steigerung von Effizienz und Wirkung. Hinzu kommt die Entwicklung von Metriken und Berichtsmechanismen zur Messung inkrementeller Änderungen und der Gesamtauswirkungen.

In dieser Phase müssen Sie:

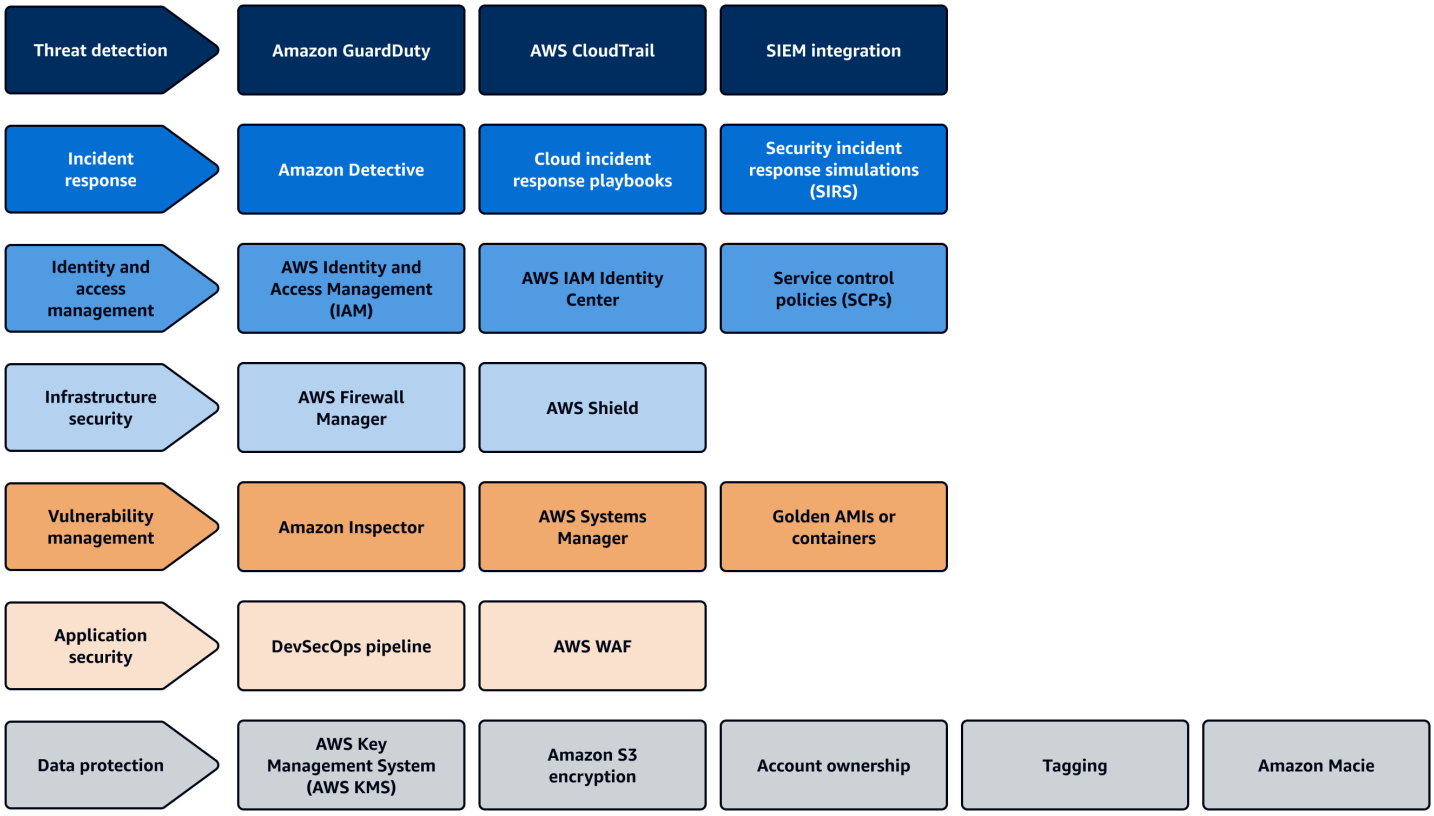
- Prozesse abstimmen und messen
- Tools abstimmen und messen
- Optimieren und messen Sie das Risiko
- Sehen Sie sich Beispiele für Anwendungsfälle in der Reifephase an

Prozesse abstimmen und messen

Der agile Ansatz bietet mehr Flexibilität und Innovation und kann Ihnen helfen, neue Ideen schnell zu testen und umzusetzen. Teilen Sie Ihre Sicherheitsteams in spezialisierte Rollen auf, z. B. Incident Responder und Vulnerability Manager. Die Rollen sollten den Kategorien in der folgenden Abbildung entsprechen, die den Funktionen des AWS Cloud Adoption Framework (AWS CAF) entsprechen. Der agile Ansatz ermutigt Teams, groß zu denken, zu erfinden, zu vereinfachen und potenzielle

Sicherheitslücken zu identifizieren. Dies führt zur Erstellung eines Backlogs an User Stories oder Roadmaps für future Verbesserungen.

Ein agiler Prozess ermöglicht dynamischere und anpassungsfähigere Lösungen, anstatt sich ausschließlich auf die Fähigkeiten eines bestimmten Tools zu verlassen. Fail Fast ist eine Philosophie, die häufige und inkrementelle Tests verwendet, um den Entwicklungslebenszyklus zu verkürzen, und sie ist ein wichtiger Bestandteil eines agilen Ansatzes. Nehmen Sie eine Änderung vor, testen Sie sie und entscheiden Sie dann, ob Sie den aktuellen Ansatz beibehalten oder zu einem anderen wechseln möchten. Wenn die Teams in diesem Zyklus arbeiten, hilft das Ihrem Unternehmen, mit der schnelllebigen Natur der Cloud Schritt zu halten. Gezielte Schulungen sind ebenfalls von entscheidender Bedeutung, und Sie sollten Schulungen anbieten, die speziell auf einen bestimmten Bereich der Cloud-Sicherheit zugeschnitten sind.



> **Note**
>
> Dieses Bild enthält nicht die Funktionen zur Gewährleistung der Sicherheit und zur Sicherheitssteuerung im AWS CAF. Dieser Leitfaden konzentriert sich auf Sicherheitsoperationen, und Sicherheit und Verwaltung fallen nicht in den Geltungsbereich

dieses Leitfadens. Weitere Informationen zur Sicherheitsgarantie finden Sie unter AWS re:INforce 2023 — Scaling Compliance with on. AWS Control Tower YouTube

Verwenden Sie in Ihrer Organisation einen agilen Ansatz, der Ihrem Unternehmen hilft, mit den schnellen Entwicklungen und Veränderungen in der Cloud Schritt zu halten. Im Folgenden finden Sie einige Möglichkeiten, wie Sie mit dem Experimentieren und Iterieren in Ihrer Cloud-Umgebung beginnen können:

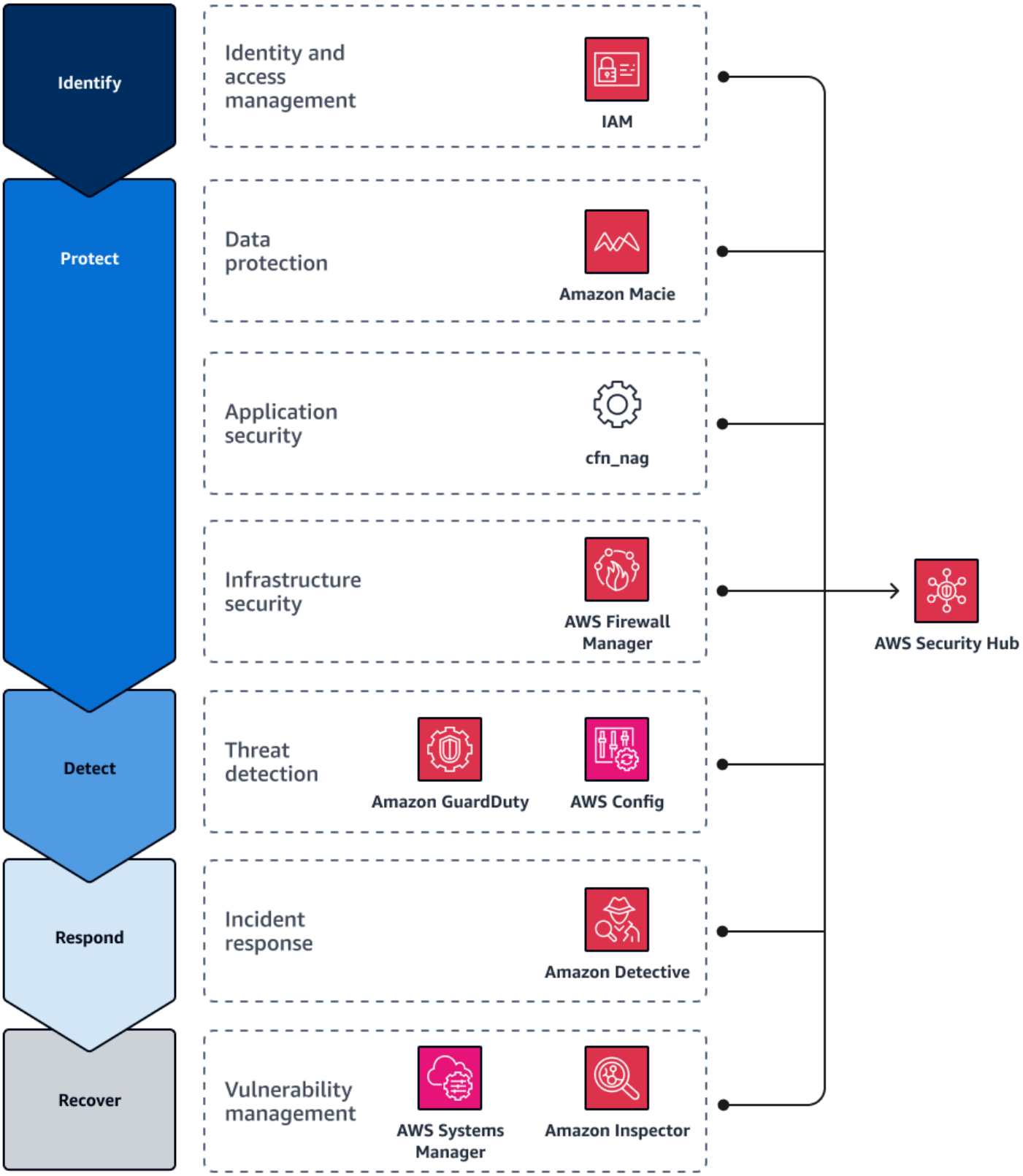
- Spezialisieren Sie sich auf die in AWS CAF definierten Kategorien, wie im vorherigen Bild gezeigt.
- Um dynamischer zu sein, sollten Sie sich auf Innovationen statt auf Betriebsabläufe konzentrieren.
- Gehen Sie schnell in Sprints vor, indem Sie es Mitarbeitern ermöglichen, schnell zu testen, zu scheitern und schnell zu implementieren. Setzen Sie diesen Zyklus fort, um mit dem Geschäft Schritt zu halten.
- Um einen kontinuierlichen Betrieb zu unterstützen, sollten Sie die Prozesse nach Möglichkeit auf cloudbasierte und lokale Umgebungen abstimmen.
- Bieten Sie gezielte Schulungen anstelle von breit gefächerten Schulungen an, um Einzelpersonen dabei zu helfen, sich auf einen Bereich zu konzentrieren.
- Ermutigen Sie die Mitarbeiter, in großen Maßstäben zu denken, zu untersuchen, „Was wäre wenn“ zu untersuchen und Rückstände zu schaffen (z. B. Roadmaps oder Lücken).

Tools abstimmen und messen

Nachdem Sie spezialisierte Teams für verschiedene Sicherheitsbereiche eingerichtet haben, stimmen Sie die Teams aufeinander ab. AWS Security Hub CSPMkann Ihnen dabei helfen, dies zu erreichen. Security Hub CSPM bietet ein zentralisiertes, einheitliches Dashboard zur Überwachung der Fortschritte anhand von Frameworks. Es integriert auch viele Tools von Drittanbietern in AWS Sicherheitsdienste.

Das Cybersicherheits-Framework des National Institute of Standards and Technology (NIST) auf der NIST-Website umfasst fünf Funktionen: Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen. Die folgende Abbildung zeigt, wie Sie AWS-Services bei jeder Funktion unterschiedliche Dienste verwenden und diese dann so konfigurieren können, dass ihre Ergebnisse zur konsolidierten Berichterstattung an Security Hub CSPM gesendet werden. Wenn Sie andere Tools verwenden möchten, können Sie die Security Hub CSPM-API () und das AWS Security Finding Format AWS Command Line Interface (ASFF AWS CLI) verwenden, um benutzerdefinierte

Integrationen zu erstellen. Weitere Informationen zu Security Hub CSPM-Integrationen mit anderen Diensten finden Sie unter Produktintegrationen AWS Security Hub CSPM in der Security Hub CSPM-Dokumentation.



Security Hub CSPM lässt sich in all diese Dienste und Tools integrieren und bietet Folgendes:

- Bietet ein einheitliches Dashboard, das Updates anzeigt und Teams hilft, vor Ort zu iterieren
- Automatische Integration mit AWS Sicherheitsdiensten wie Amazon Macie GuardDuty, Amazon und Amazon Detective
- Unterstützt die Integration mit Tools von Drittanbietern wie und Prowlercfn_nag
- Unterstützt benutzerdefinierte Integrationen mit Tools wie der Security Hub CSPM API und dem AWS Security Finding Format (ASFF) AWS CLI

Optimieren und messen Sie das Risiko

In der Reifephase der Walk-Phase können Sie AWS Security Hub CSPM das Sicherheitsrisiko kontinuierlich anpassen und messen. Security Hub CSPM bewertet kontinuierlich den Sicherheitsstatus eines Unternehmens und ergreift Maßnahmen zur Behebung identifizierter Probleme. Security Hub CSPM zentralisiert und priorisiert Sicherheitsergebnisse von Across AWS-Konten, Services und unterstützten Drittanbietern. Auf diese Weise können Sie Sicherheitstrends analysieren und Sicherheitsprobleme mit hoher Priorität identifizieren.

Security Hub CSPM führt Hunderte von Sicherheitsprüfungen durch und klassifiziert sie anhand des Risikos für Ihre Umgebung. AWS Sie können Ihren Punktestand bei den Sicherheitskontrollen in einem einheitlichen Dashboard in der Security Hub CSPM-Konsole einsehen. Weitere Informationen finden Sie unter Ermitteln von Sicherheitsbewertungen in der Security Hub CSPM-Dokumentation. Über dieses Dashboard kann die DevSecOps Funktion schnell erkennen, welche Prüfungen fehlgeschlagen sind, welchen Schweregrad das Sicherheitsproblem hat AWS-Region und welche Ressource betroffen ist. Nach der Identifizierung kann das DevSecOps Team das Problem priorisieren und beheben. Sobald Probleme behoben sind, aktualisiert Security Hub CSPM den Status automatisch.

Sehen Sie sich Beispiele für Anwendungsfälle in der Reifephase an

Im Folgenden finden Sie Beispiele für die Reifephase. Diese Beispiele befassen sich auf praktischer Ebene eingehender mit den Modellen, Tools und Prozessen für verschiedene Geschäftsziele.

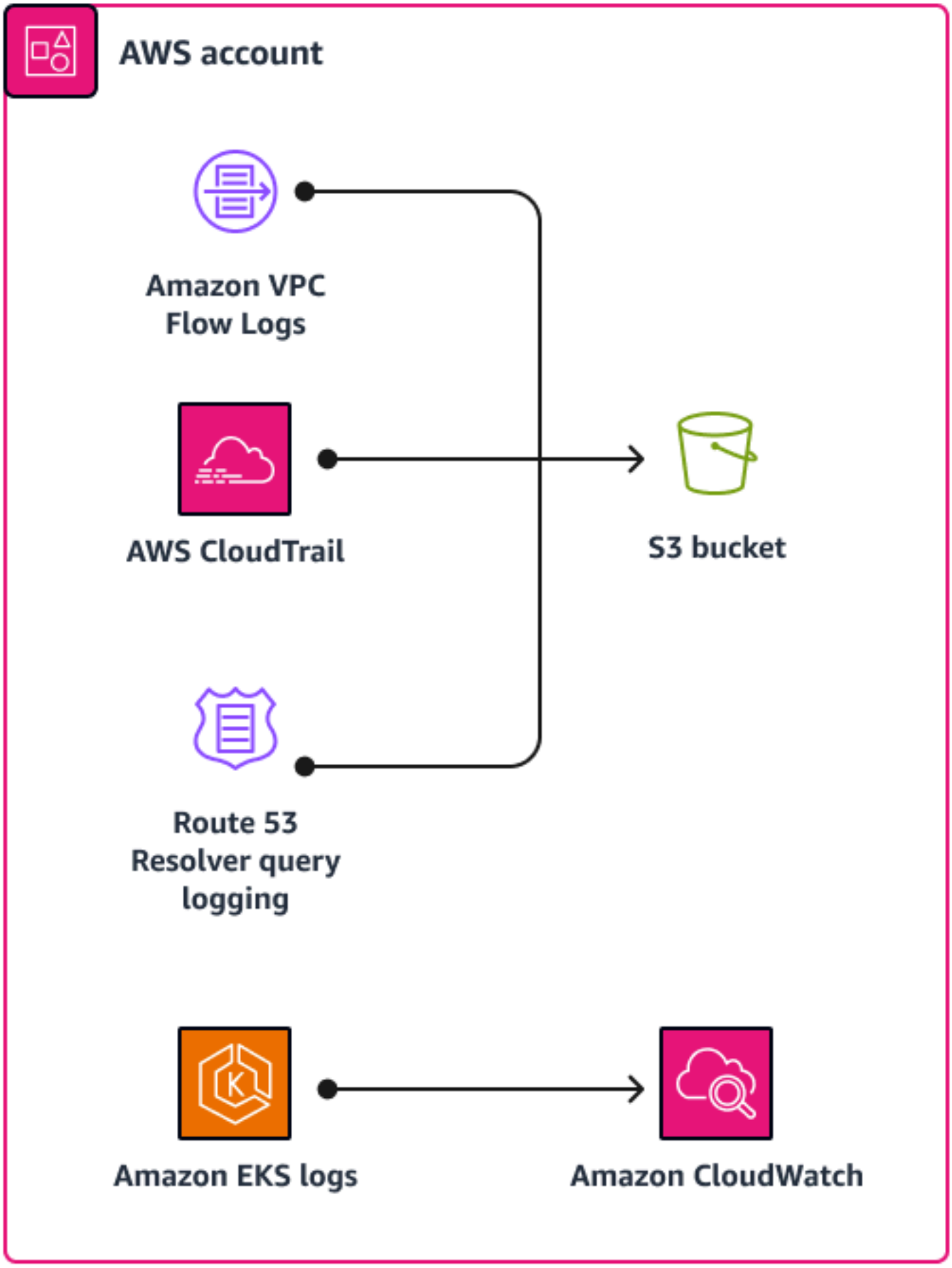
Ausgereift: Beispiel für die Erkennung von Bedrohungen

Geschäftsergebnis für detektive Kontrollen: Erhöhen Sie die Transparenz und Geschwindigkeit der Erkennung von Cloud-Vorfällen, um das Risiko zu senken und eine schnellere Nutzung und Entwicklung von Cloud-Ressourcen zu ermöglichen.

Tool: Assisted Log Enabler for AWS(GitHub) ist ein Open-Source-Tool, mit dem Sie die Protokollierung während eines Sicherheitsvorfalls aktivieren können. Es kann Ihre Sichtbarkeit eines Vorfalls schnell erhöhen.

Beispiel für einen Anwendungsfall: Stellen Sie sich den im folgenden Diagramm dargestellten Anwendungsfall für ein einzelnes Konto vor. Es gibt Ereignisse, die einer weiteren Untersuchung bedürfen. Sie sind sich nicht sicher, ob die Protokollierung aktiviert ist. In diesem Fall ist es am besten, einen Probelauf mit dem durchzuführen, Assisted Log Enabler um zu sehen, welche Dienste aktiviert oder deaktiviert sind. Assisted Log Enablersucht nach AWS CloudTrail Trails, DNS-Abfrageprotokollen, VPC-Flow-Protokollen und anderen Protokollen. Wenn sie nicht aktiviert sind, werden sie Assisted Log Enabler aktiviert. Assisted Log Enablerkann die Protokollierung für alle überprüfen und aktivieren AWS-Regionen.

Sie können auch nach Assisted Log Enabler oben oder unten drosseln. Nachdem Sie Ihren Probelauf abgeschlossen, das Event geschlossen und das Problem behoben haben, stellen Sie fest, dass Sie diese Protokollierungsstufe nicht mehr benötigen. Sie können die Bereitstellung schnell bereinigen, um die Protokollierung zu beenden. Diese Funktion ermöglicht die Verwendung Assisted Log Enabler als Triage-Tool.


AWS account
Amazon VPC Flow Logs
AWS CloudTrail
S3 bucket
Route 53 Resolver query logging
Amazon EKS logs
Amazon CloudWatch

Im Folgenden sind die wichtigsten Funktionen von aufgeführtAssisted Log Enabler for AWS:

- Sie können es in einer Umgebung mit einem oder mehreren Konten ausführen.
- Sie können es verwenden, um eine Grundlage für die Anmeldung in Ihrer Umgebung festzulegen.
- Sie können die Probelauffunktion verwenden, um den aktuellen Status zu überprüfen und festzustellen, für welche Dienste die Protokollierung aktiviert ist.
- Sie können auswählen, für welche Dienste Sie die Protokollierung aktivieren möchten.
- Sie können je nach Anwendungsfall die Assisted Log Enabler Drosselung erhöhen oder verringern.

Ausgereift: Beispiel für IAM

Geschäftsergebnis mit IAM: Automatisieren Sie die Transparenz und messen Sie anhand von Best Practices, um Risiken kontinuierlich zu reduzieren, sichere externe Verbindungen zu ermöglichen und schnell neue Benutzer und Umgebungen bereitzustellen

Tool:AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) hilft Ihnen dabei, Ressourcen zu identifizieren, die mit einer externen Entität gemeinsam genutzt werden, überprüft IAM-Richtlinien anhand der Richtliniengrammatik und der Best Practices und generiert IAM-Richtlinien auf der Grundlage historischer Zugriffsaktivitäten. Wir empfehlen dringend, IAM Access Analyzer sowohl auf Konto- als auch auf Organisationsebene zu aktivieren.

Servicevorteile: IAM Access Analyzer bietet eine Fülle aufschlussreicher Erkenntnisse. Es kann die Ressourcen und Konten Ihres Unternehmens identifizieren, die mit einer externen Entität gemeinsam genutzt werden. Es kann Ressourcen wie einen öffentlichen S3-Bucket, ein mit einem anderen Konto AWS KMS key geteiltes Konto oder eine Rolle, die mit einem externen Konto geteilt wird, erkennen und bietet Ihnen so einen hervorragenden Einblick in die Identifizierung von Ressourcen, die nicht unter der Kontrolle Ihrer Organisation stehen. Es validiert nicht nur IAM-Richtlinien, sondern kann sie auch für Sie generieren.

Run-Phase: Optimierung Ihrer Cloud-Sicherheitsabläufe

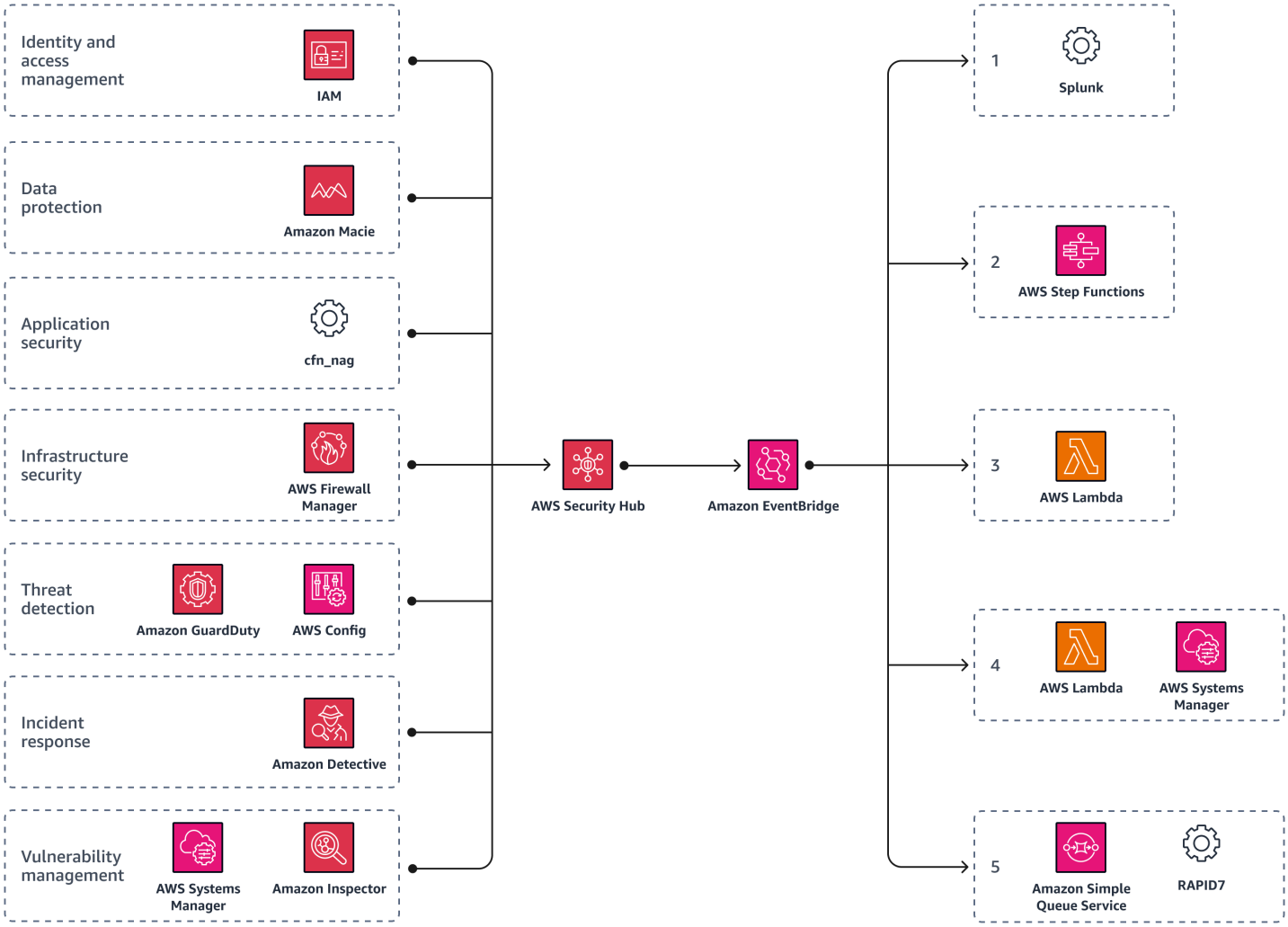
Nachdem Sie einen Basiswert in der Laufphase implementiert haben, geht Ihre Organisation zur Laufphase über. Diese Phase konzentriert sich auf die Demonstration der in der Cloud verfügbaren Cybersicherheitsfunktionen, von denen viele mit lokalen Lösungen nicht oder nur sehr schwer zu implementieren sind. In dieser Phase werden verschiedene Sicherheitskomponenten zusammengeführt und Prozesse automatisiert. Durch Automatisierungen werden Ihre Ressourcen freigesetzt, sodass sie sich auf hochwertige Aufgaben konzentrieren können.

Die folgende Phase ist die einzige Phase in der Ausführungsphase:

- Optimieren— Wie verbessere ich diesen Prozess und füge Automatisierung hinzu?

Optimieren: Automatisieren und iterieren Sie Ihre Cloud-Sicherheitsabläufe

In der Optimierungsphase automatisieren Sie Ihre Sicherheitsabläufe. Wie die Crawl- und Walk-Phasen können Sie auch AWS Security Hub CSPM während der Run-Phase verwenden, um Automatisierung und Iteration zu erreichen. Die folgende Abbildung zeigt, wie Security Hub CSPM eine benutzerdefinierte EventBridgeAmazon-Regel auslösen kann, die automatische Aktionen definiert, die gegen bestimmte Ergebnisse und Erkenntnisse ergriffen werden sollen. Weitere Informationen finden Sie unter Automatisierungen in der Security Hub CSPM-Dokumentation.



Wenn Sie Security Hub CSPM als zentralen Automatisierungs-Hub verwenden, können Sie Aktivitäten auch an weiterleiten. Splunk Splunkkann dann diejenigen erkennen, die anomal sind, und entsprechende Aktionen in auslösen. EventBridge Dies hilft Ihnen, sich wiederholende Aufgaben zu automatisieren, und gibt qualifizierten Teammitgliedern mehr Zeit, sich auf wichtigere Aktivitäten zu konzentrieren. Sie können AWS Step Functionsdamit auch Protokolle sammeln, forensische Schnappschüsse erstellen, kompromittierte Server unter Quarantäne stellen und sie durch ein goldenes Image ersetzen. Darüber hinaus können Sie eine AWS LambdaFunktion verwenden, die Sicherheitslücken in der gesamten Umgebung behebt und eine Amazon Simple Queue Service (Amazon SQS) -Funktion verwendet, um die Sicherheit der Systeme zu überprüfen. AWS Systems Manager Mit diesem Ansatz ist es möglich, Sicherheitsvorfälle schnell einzudämmen und zu beheben, ohne den normalen Geschäftsbetrieb zu beeinträchtigen.

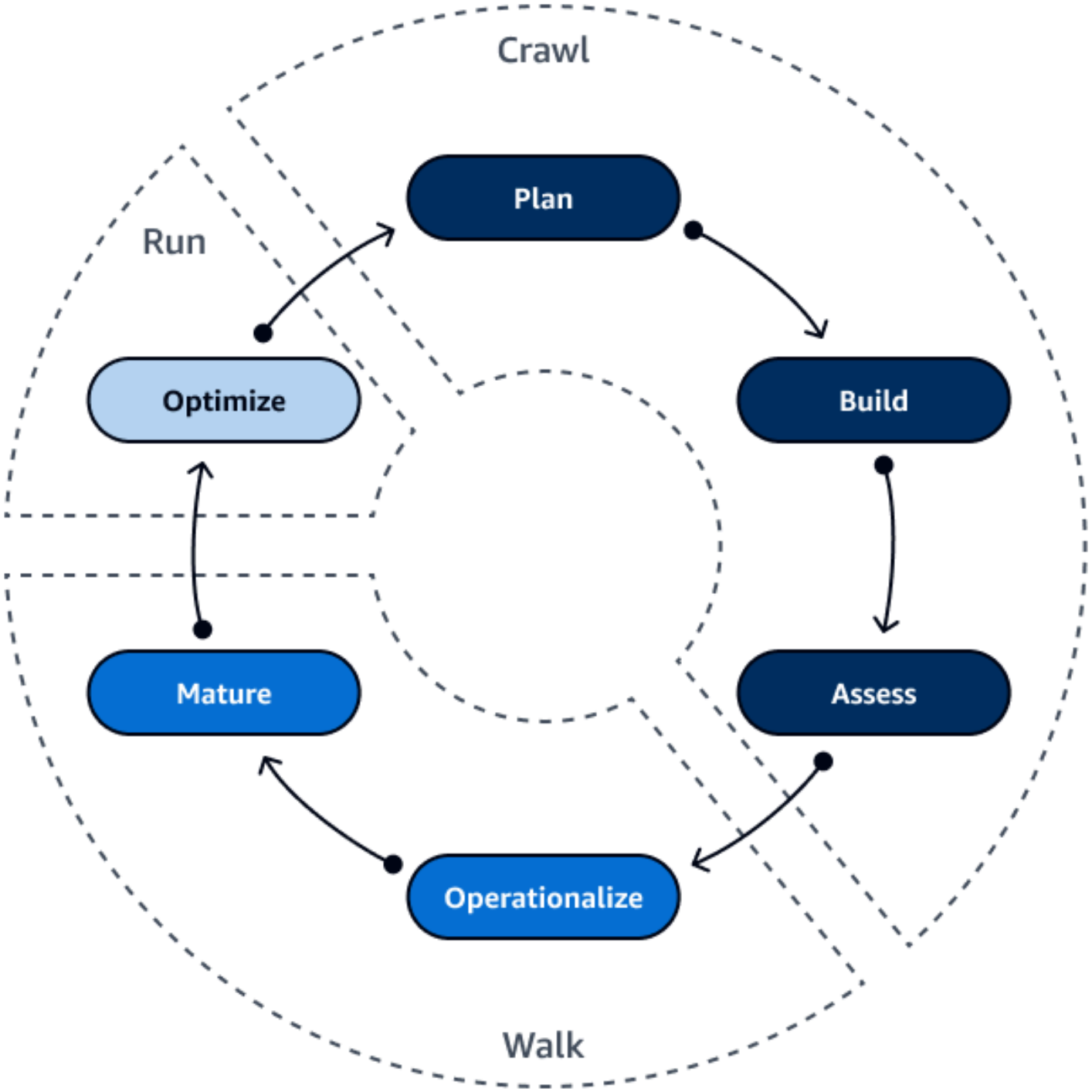
Im Folgenden finden Sie ein Beispiel für wiederholte automatisierte Aktionen, wie im vorherigen Bild dargestellt:

1. Wird verwendetSplunk, um fragwürdige Aktivitäten zu erkennen.
2. Verwenden Sie Step Functions, um Protokolle zu sammeln, den Zugriff zu widerrufen, unter Quarantäne zu stellen und forensische Schnappschüsse zu erstellen.
3. Verwenden Sie eine EventBridge Regel, um eine Lambda-Funktion zu starten, die unter Quarantäne gestellt, forensische Snapshots erstellt und kompromittierte Server durch ein Golden Image ersetzt.
4. Starten Sie eine Lambda-Funktion, die Systems Manager verwendet, um Patches zu korrigieren und in der gesamten Umgebung anzuwenden.
5. Starten Sie eine Amazon SQS SQS-Nachricht, die den Rapid7-Scanner verwendet, um zu scannen und zu überprüfen, ob die AWS Ressource sicher ist.

Weitere Informationen finden Sie unter So automatisieren Sie die Reaktion auf Vorfälle im Sicherheitsblog AWS Cloud für EC2-Instances. AWS

Fazit: Krabbeln, laufen, rennen, dann fliegen!

Zusammenfassend lässt sich sagen, dass das Crawl, Walk, Run-Modell ein Framework ist, das Ihnen hilft, Ihre Sicherheitslage schrittweise zu verbessern und bewährte Methoden für den Schutz AWS der Infrastruktur einzuführen. Dieser Prozess entwickelt sich ständig weiter, wenn neue Technologien und Geschäftsanforderungen auftauchen. Wenn Sie diesem Framework folgen und die von bereitgestellten Ressourcen nutzen AWS, können Sie eine solide Grundlage für Cloud-Sicherheit schaffen, Sicherheitsrisiken effektiv managen, die Sicherheitsreife beschleunigen und Innovationen vorantreiben.



In der Crawl-Phase legen Sie den Grundstein. Sie definieren Ihren Sicherheitsplan, verwenden eine definierte Architektur mit bewährten Sicherheitsmethoden und führen eine kontinuierliche Bewertung der Geschäftsziele Ihres Unternehmens durch.

In der Gehphase machen Sie die ersten Schritte. Sie schauen sich Richtlinien an, erstellen Playbooks, schulen Mitarbeiter und stimmen Strategien ab. In dieser Phase erfahren Sie, wie Sie Innovationen nutzen können, um mit den Technologien in der Cloud Schritt zu halten.

In der Anfangsphase denken Sie groß. Sie nutzen Automatisierung und platzieren Ihre Fachkräfte strategisch an der richtigen Stelle. Sie implementieren Automatisierung, um eine kontinuierliche Bewertung der Geschäftsziele Ihres Unternehmens voranzutreiben.

Jetzt ist es Zeit für dich zu fliegen. Verwenden Sie die Empfehlungen in diesem Leitfaden, um Ihre Sicherheitsreife in der zu beschleunigen AWS Cloud.

Ressourcen

Frameworks und Modelle

- AWS Framework für die Cloud-Einführung (AWS CAF)
- AWS Well-Architected Framework
- AWS Sicherheitsreferenzarchitektur (SRA)AWS
- AWS Modell des Sicherheitsreifegrads
- HIPAA-Referenzarchitektur
- HITRUST-Referenzarchitektur

AWS-Services

- AWS Control Tower
- AWS Identity and Access Management Access Analyzer
- AWS Security Hub CSPM

Andere Ressourcen AWS

- Automatisierte Sicherheitsreaktion AWS in der AWS Lösungsbibliothek
- Automatisieren Sie Ihren IT-Betrieb mithilfe von AWS Step Functions Amazon CloudWatch Events in the AWS Compute Blog
- So automatisieren Sie die Reaktion auf Vorfälle in AWS Cloud den EC2 vier Instanzen im AWS Sicherheits-Blog
- Informationen zur automatisierten Reaktion auf Vorfälle in einer Umgebung mit mehreren Konten finden Sie im AWS Sicherheitsblog
- AWS Re:inForce 2022 — Crawl, Walk, Run: Schnellere Sicherheitsreife — Video auf YouTube
- AWS Präsentation „Re:inForce 2022 — Crawl, Walk, Run: Accelerating security maturating security maturity“ (Anlage) PowerPoint

Mitwirkende

Die folgenden Personen haben zu diesem Leitfaden beigetragen.

Verfassen

- Tschad Lorenc, Leiter der Sicherheitspraxis, AWS
- Ivy Gin, Beraterin für Sicherheit, AWS
- Sayali Paseband, Sicherheitsberaterin, AWS

Überprüfend

- Deeps Baisya, leitender Sicherheitsarchitekt, AWS
- Mike LaRue, leitender Sicherheitsberater, AWS
- Raul Radu, leitender Sicherheitsingenieur, AWS

Technisches Schreiben

- Lilly AbouHarb, leitende technische Redakteurin, AWS

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen in diesem Leitfaden beschrieben. Um Benachrichtigungen über zukünftige Aktualisierungen zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Erste Veröffentlichung	—	20. Dezember 2023

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.