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

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: Crawl, Walk, Run: Beschleunigung der Sicherheitsreife in der AWS Cloud

Table of Contents

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

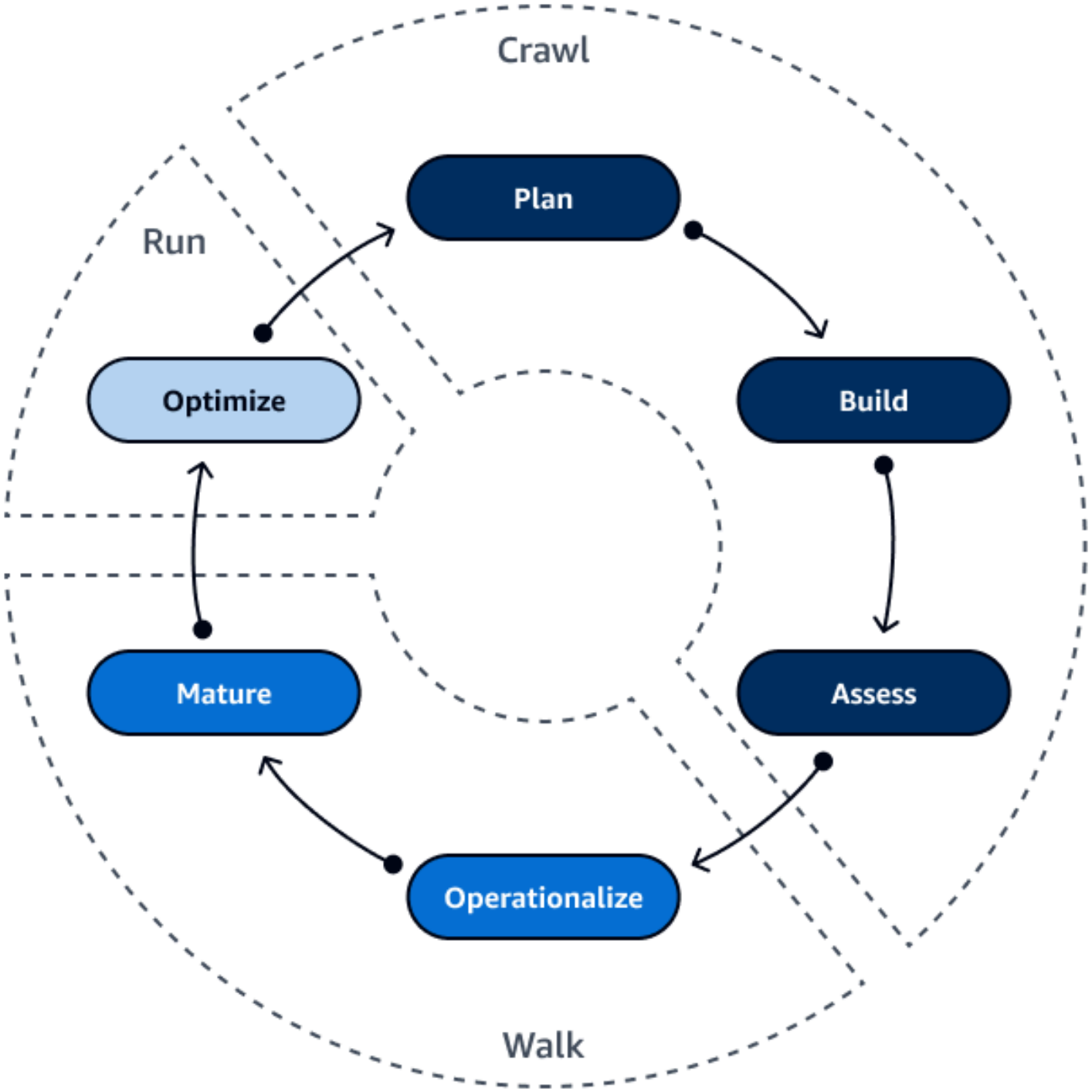
Amazon Web Services (Mitwirkende)

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 step-by-step Ansatz zur Automatisierung von Sicherheitsfunktionen. Außerdem wird pragmatisch erklärt, wie die Funktionalität AWS-Services und die Funktionen optimal genutzt werden 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 Sicherheitsbereich 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 gewünschten Ergebnisse erzielt.

Den Sicherheitsbereich 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.

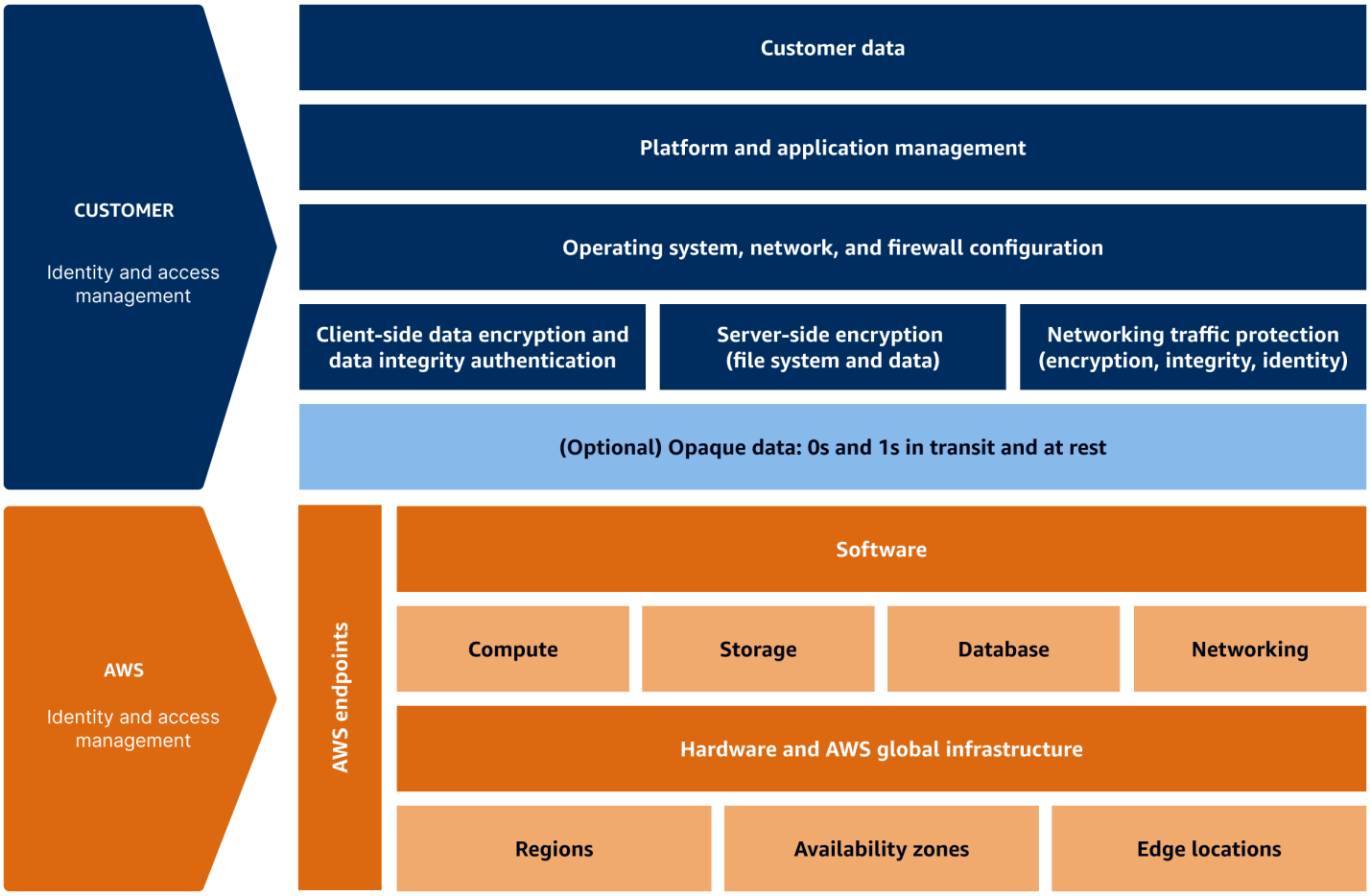
Im Folgenden finden Sie drei verschiedene Servicebeispiele, die Ihnen helfen sollen, zu verstehen, wie sich Ihr Sicherheitsumfang je nachdem, für welche Dienste Sie sich entscheiden, ändert:

- 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

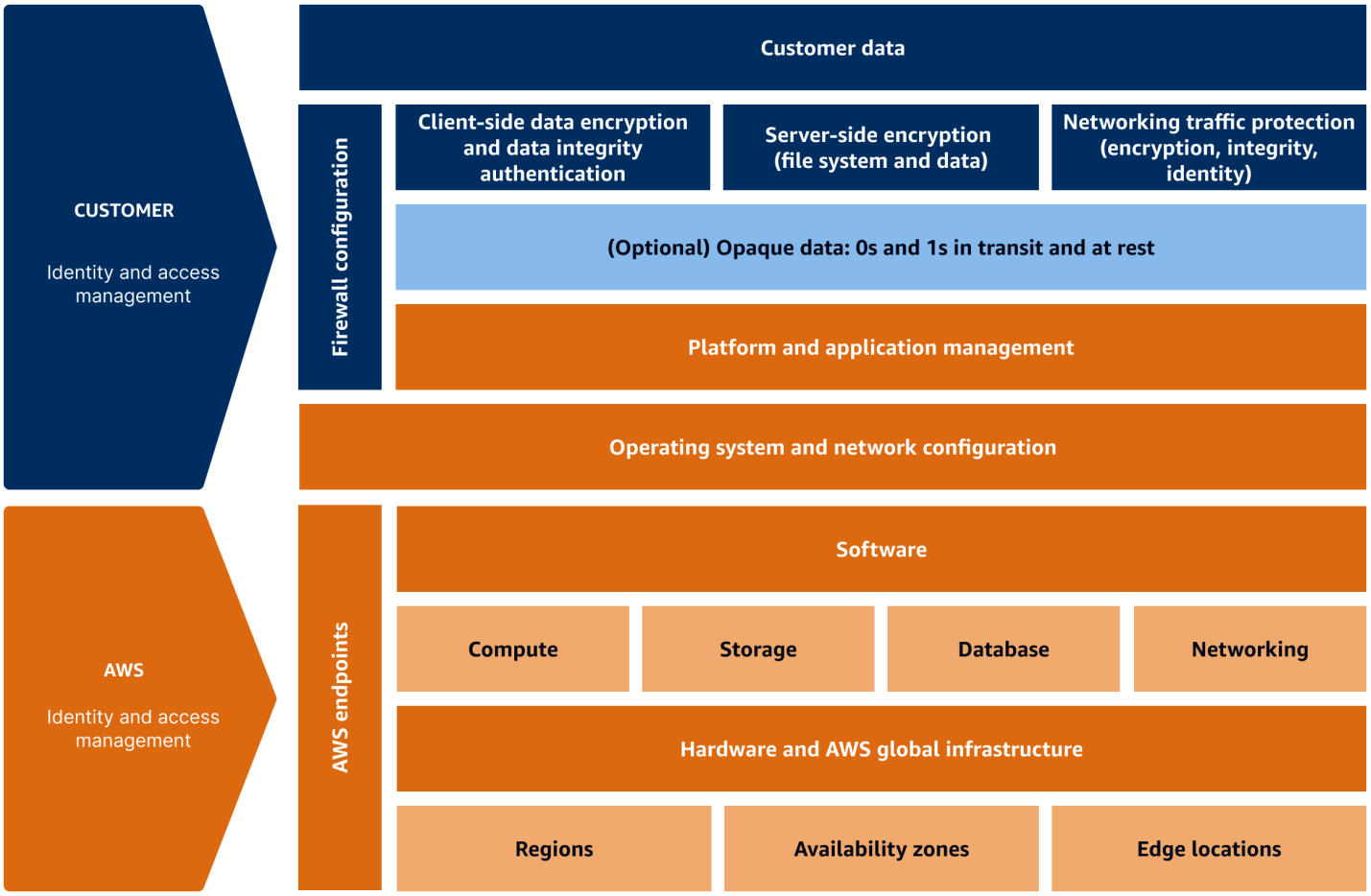
AWS Konzentriert sich bei Infrastrukturdiensten auf die Sicherung der zugrunde liegenden Infrastruktur. Bei Infrastrukturdienstleistungen ist der Umfang für den Kunden größer, da er sich im Vergleich zu den anderen Modellen mit Plattformsicherheit, Betriebssystem-Patching und Anwendungsmanagement befassen muss. Amazon Elastic Compute Cloud (Amazon EC2) ist ein Beispiel für einen gemeinsamen Infrastrukturservice.



Container-Services

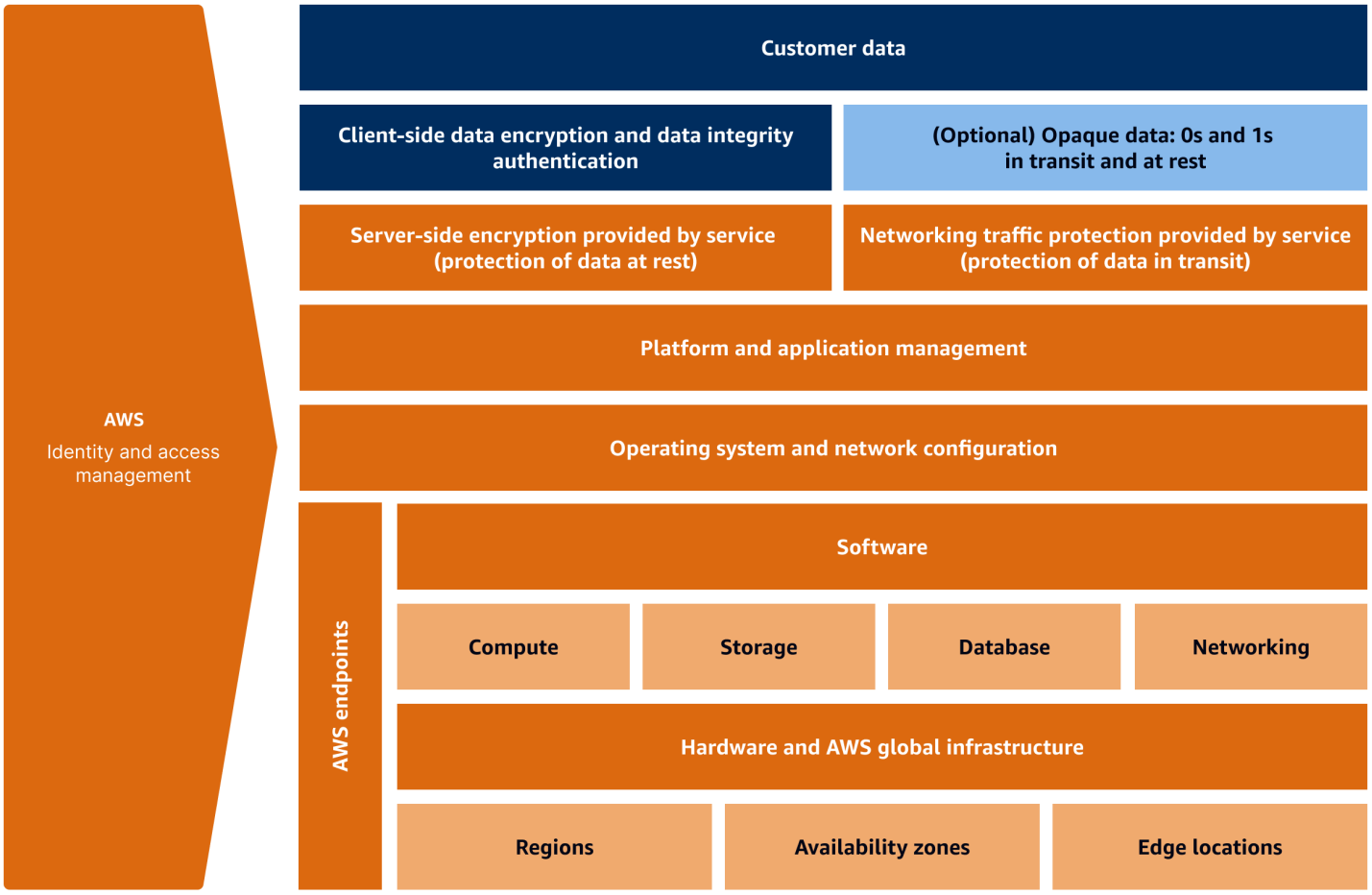
Je abstrahierter und modernisierter die Infrastruktur wird, desto geringer wird der Platzbedarf. Ihr Anwendungsbereich schrumpft, weil sich die Verantwortung für einige Sicherheitselemente auf verlagert. AWS Containerdienste sind ein Beispiel, auf das sich einige der Backend-Verantwortlichkeiten zurückverlagern. 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



Serverless-Services

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:

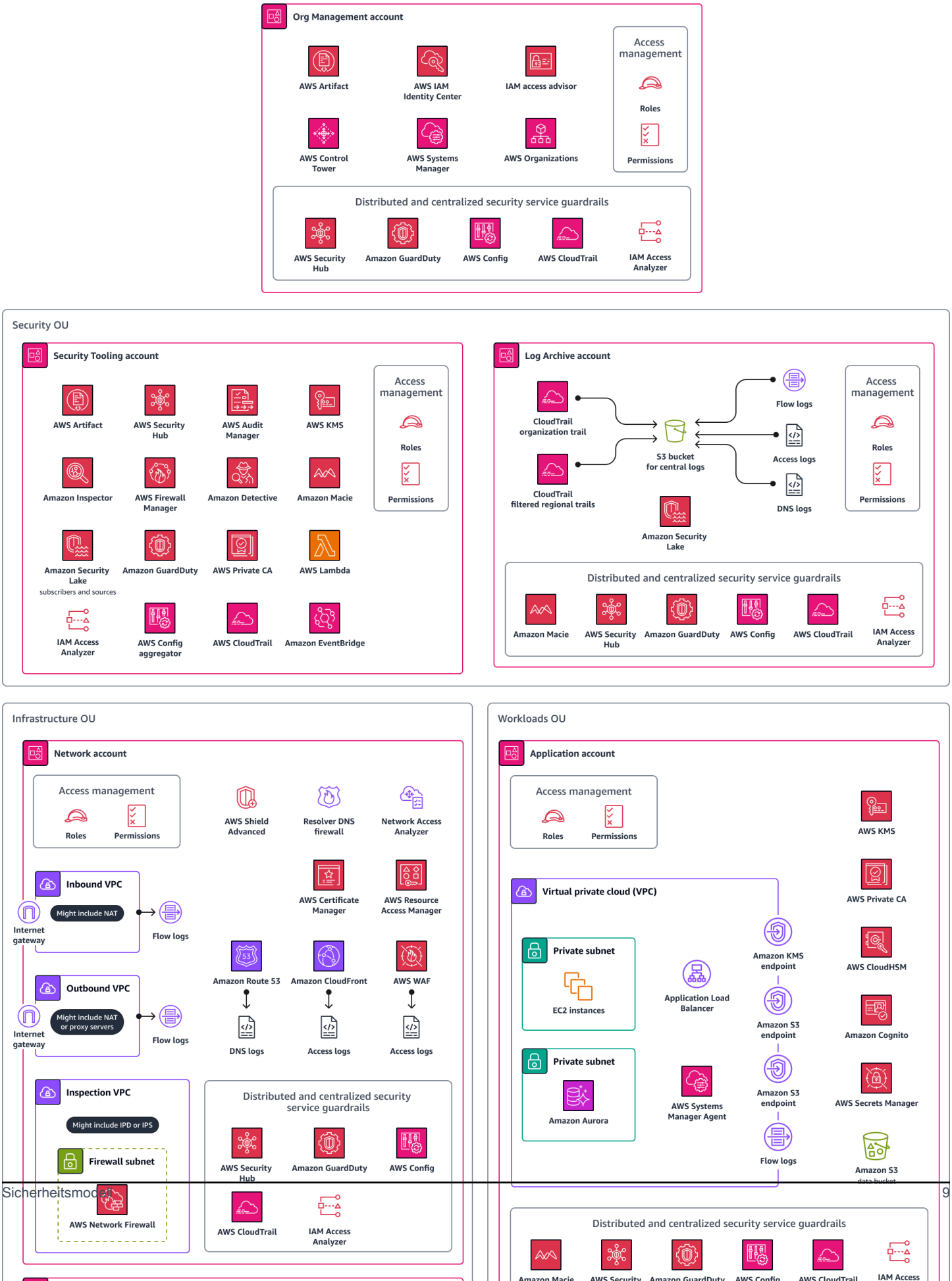
- Architektonisches Modell
- Reifegradmodell
- Modell der Unternehmensführung

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
Access management
Roles
Permissions
AWS Control Tower
AWS Systems Manager
AWS Organizations
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
Access management
Roles
Permissions
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
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
Workloads OU
Application account
Access management
Roles
Permissions
AWS KMS
AWS Private CA
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 CloudHSM
Amazon Cognito
AWS Secrets Manager
Amazon S3
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
- Entspricht dem AWS Cloud Adoption Framework (CAF)AWS
- Passt sich dem AWS Well-Architected Framework an

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 Sicherheitsverantwortliche CISOs, ist aber 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

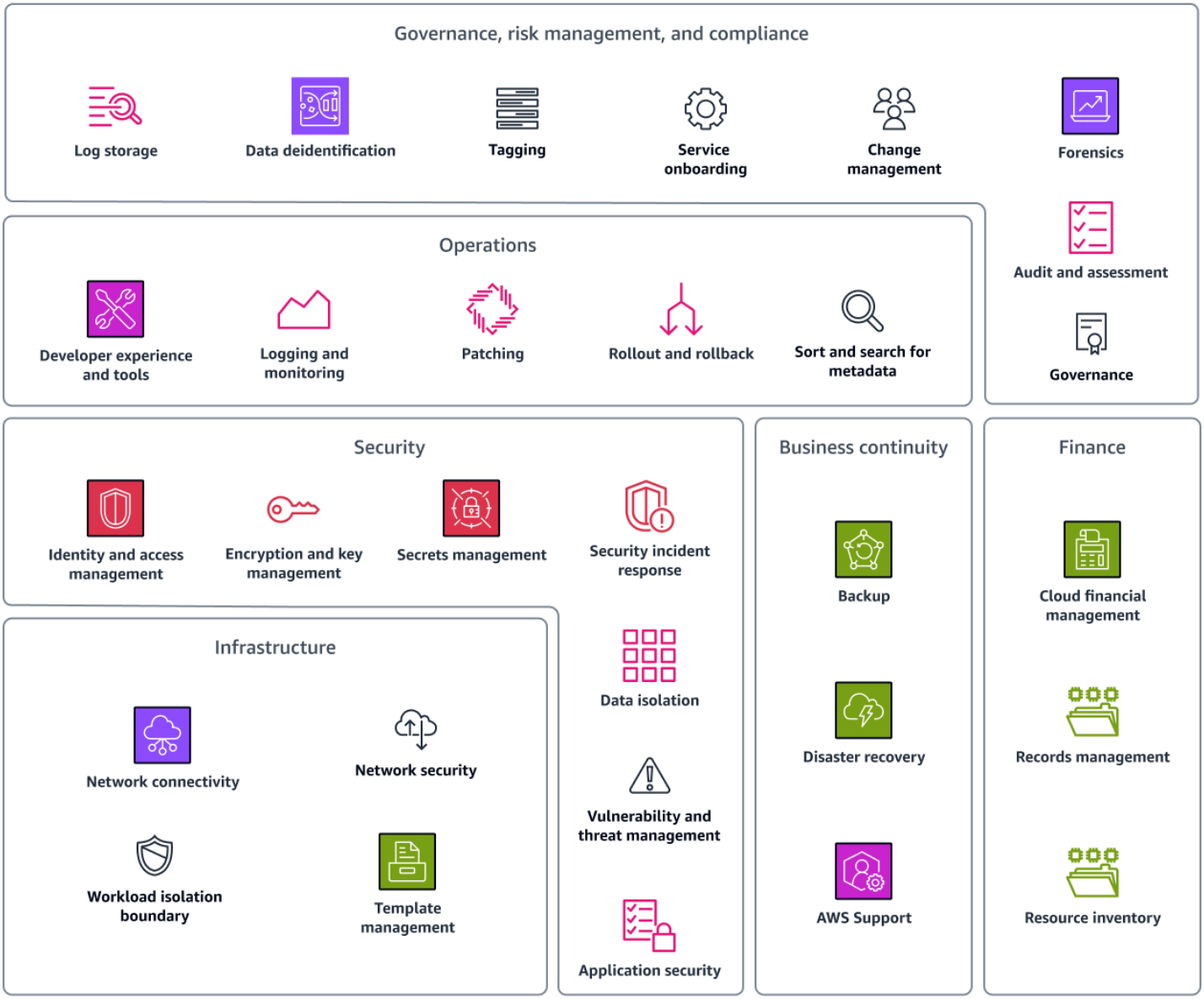
Nachteile des Reifegradmodells:

- 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 von Best Practices 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

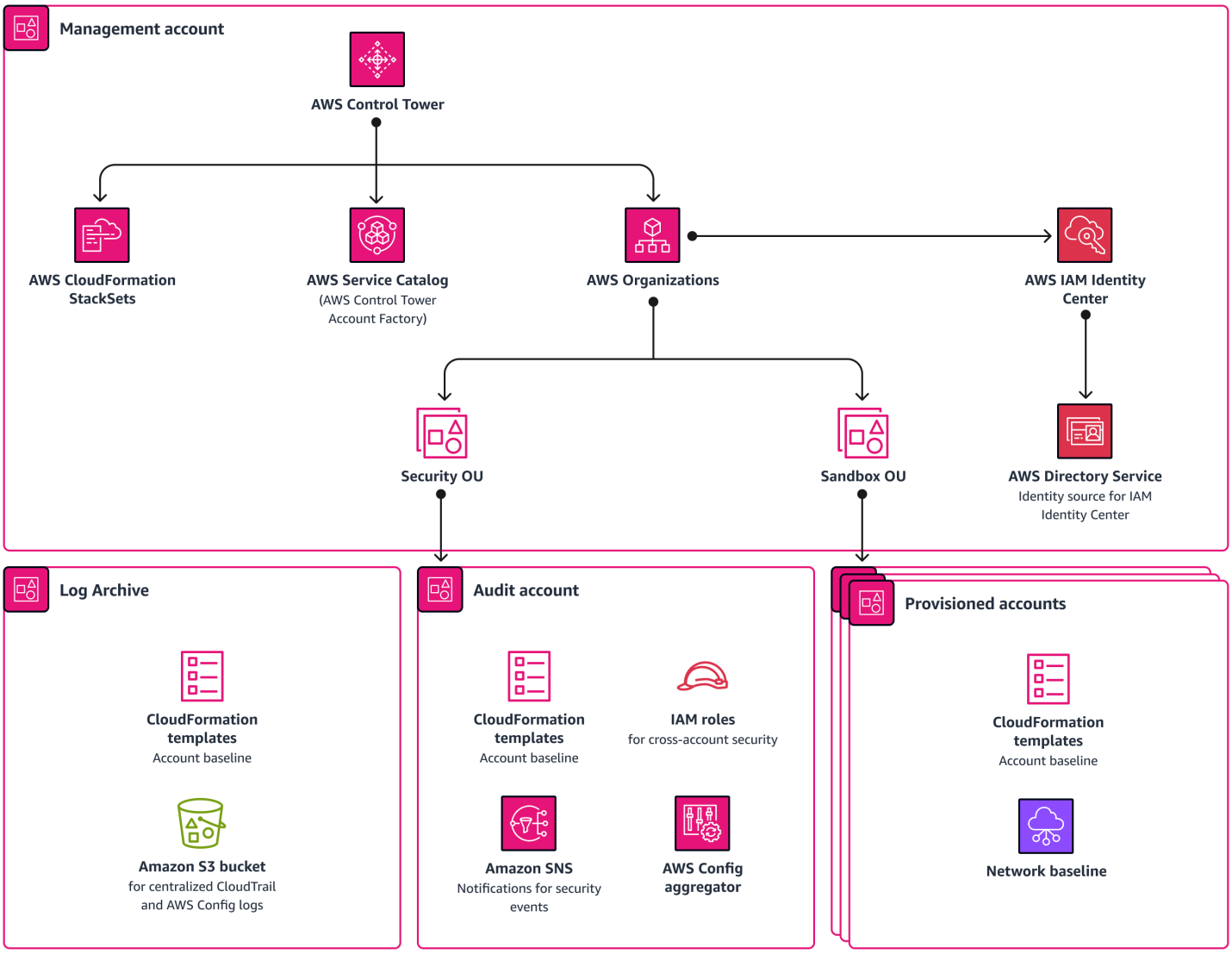
- Bietet eine klare, auf das Geschäft ausgerichtete Sicherheitsausrichtung
- Definiert Erfolgsmessungen anhand der Erreichung von Geschäftsergebnissen

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:

- Verwaltung mehrerer Konten
- Identitäts- und föderiertes Zugriffsmanagement
- Ein zentrales Archiv für Protokolle
- Kontoübergreifender Auditzugriff
- Bereitstellung von Endbenutzerkonten
- 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 beschrieben AWS Security Hub und Prowler, die Sie verwenden können, um eine Bewertung des Cloud-Status in Ihrer Umgebung durchzuführen.

Prowler

Prowlerist ein Open-Source-Befehlszeilentool, mit dem Sie Ihre Konten im Hinblick auf die Einhaltung bewährter Sicherheitsverfahren und anderer AWS Sicherheitsrahmen und -standards bewerten, prüfen und überwachen können. Es überprüft Ihre Konfiguration und identifiziert Sicherheitsprobleme. Sie können Folgendes verwenden … Prowler in Umgebungen mit mehreren Konten, und Drittanbieter können es auch verwenden, um die Sicherheit Ihrer AWS Umgebung zu bewerten.

Im Folgenden sind die Vorteile von aufgeführt Prowler:

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

Prowler Proist auch eine Option für eine kontinuierliche Bewertung. Prowler Pro führt über 250 Prüfungen durch und bietet schnellere Scans sowie Dashboards, mit denen Sie die Scanergebnisse visualisieren können.

AWS Security Hub

AWS Security Hubbietet einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS. Es hilft Ihnen auch dabei, Ihre Umgebung anhand von Industriestandards und Best Practices im Bereich Sicherheit zu überprüfen. Es ist integriert, AWS Control Tower sodass Sie die Security Hub Hub-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 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 beinhaltet 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 konsistenter 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 Incident-Response-Plans 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 Code-Ebene der Infrastruktur bewerten. Amazon Inspector ist ein automatisierter Schwachstellen-Management-Service, der Ihre Ressourcen kontinuierlich auf Sicherheitslücken 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 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:

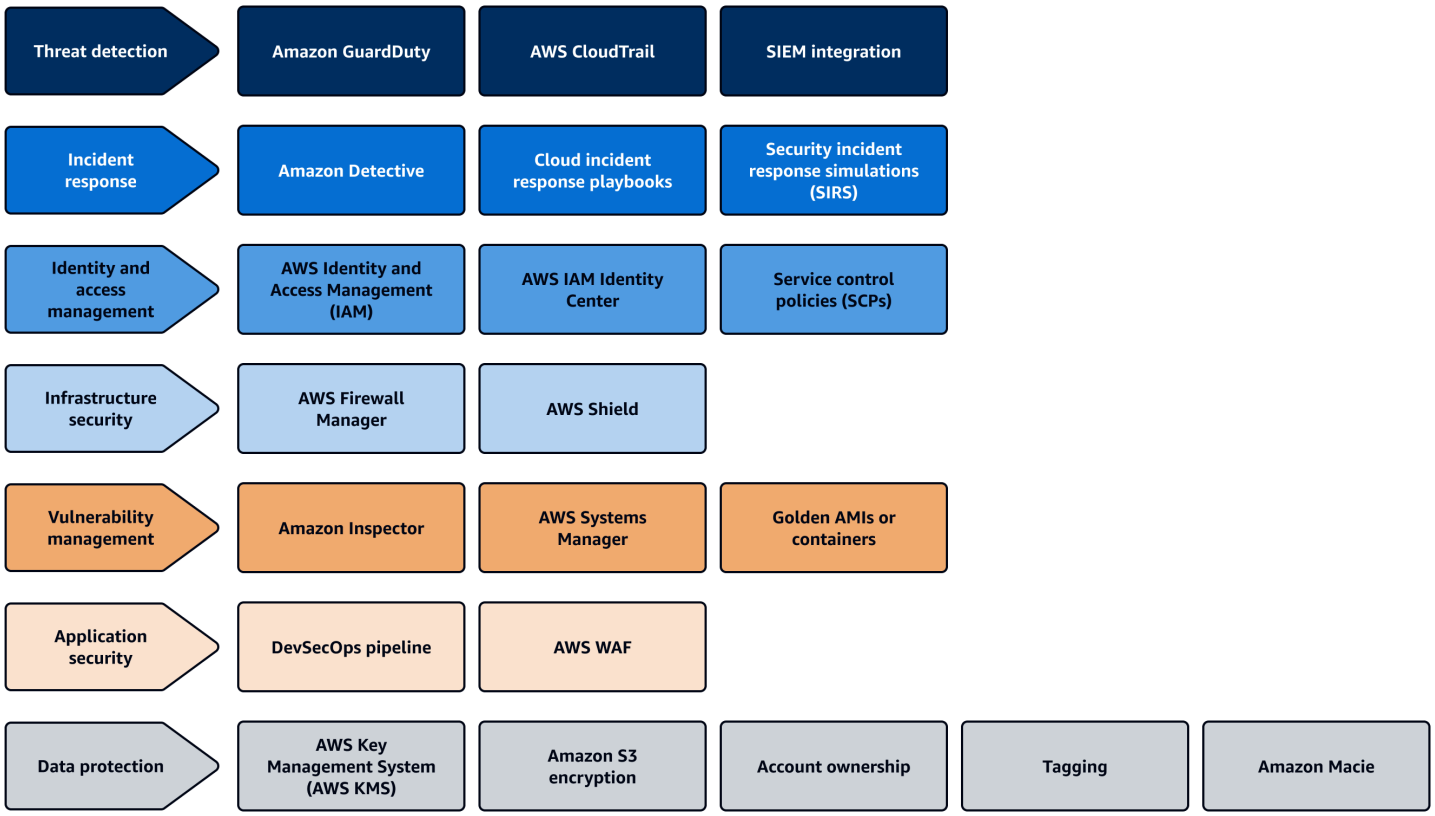
- Prozesse abstimmen und messen
- Tools abstimmen und messen
- Optimieren und messen Sie das Risiko
- Sehen Sie sich Beispiele für Anwendungsfälle in der Reifephase an

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 spezielle 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, bei der häufige und inkrementelle Tests verwendet werden, 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 die Gewährleistung und Steuerung der Sicherheit 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:

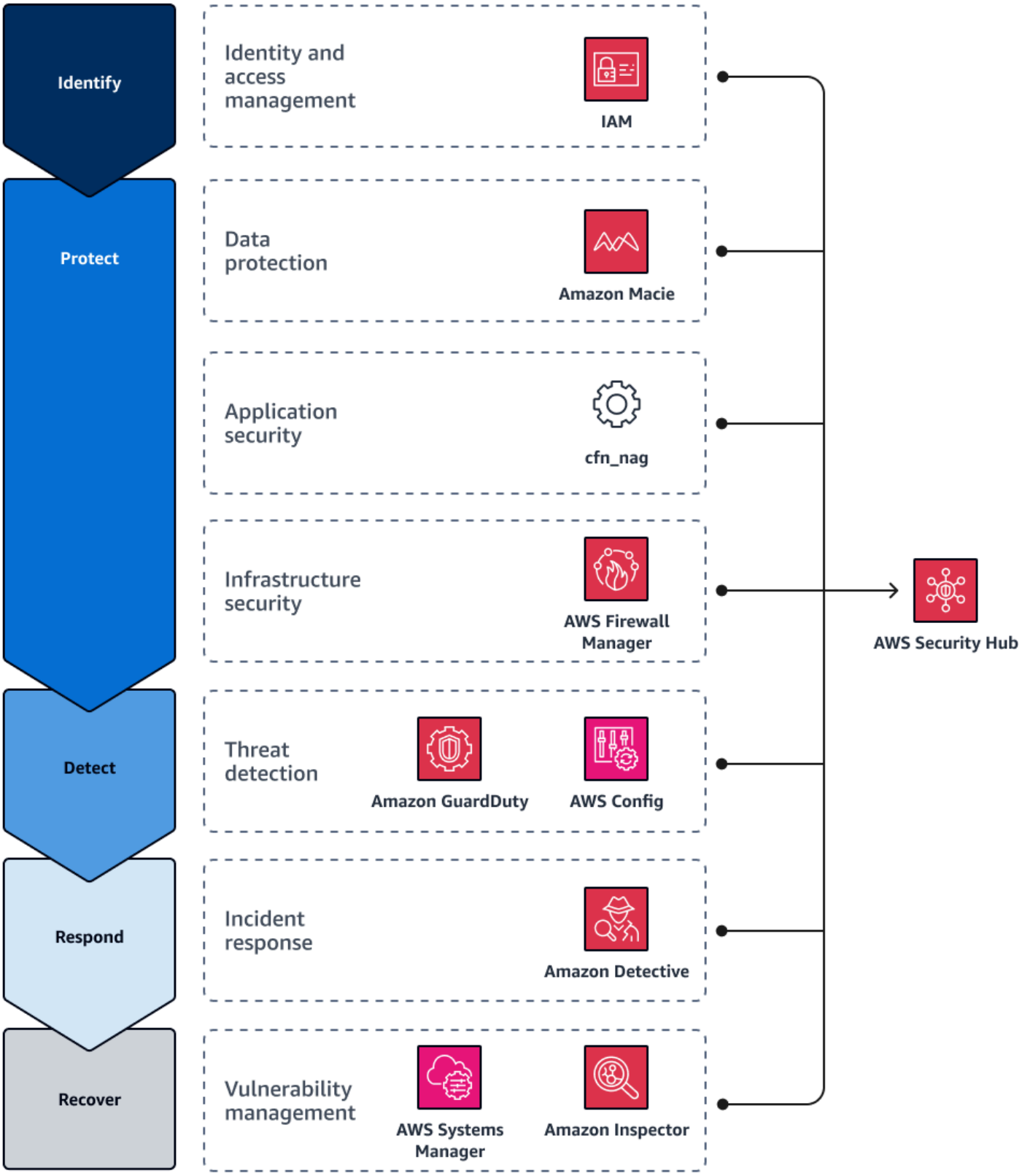
- Spezialisieren Sie sich auf die in AWS CAF definierten Kategorien, wie im vorherigen Bild gezeigt.
- Um dynamischer zu sein, sollten Sie sich auf Innovationen statt auf Betriebsabläufe konzentrieren.
- Gehen Sie schnell in Sprints vor, indem Sie es Mitarbeitern ermöglichen, schnell zu testen, zu scheitern 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 Hubkann Ihnen dabei helfen, dies zu erreichen. Security Hub bietet ein zentralisiertes, einheitliches Dashboard zur Überwachung des Fortschritts 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 gesendet werden. Wenn Sie andere Tools verwenden möchten, können Sie die Security Hub Hub-API AWS Command Line Interface (AWS

CLI) und das AWS Security Finding Format (ASFF) verwenden, um benutzerdefinierte Integrationen zu erstellen. Weitere Informationen zu Security Hub Hub-Integrationen mit anderen Diensten finden Sie unter Produktintegrationen AWS Security Hub in der Security Hub Hub-Dokumentation.



Security Hub 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 Prowler und cfn_nag
- Unterstützt benutzerdefinierte Integrationen mit Tools wie der Security Hub Hub-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 das Sicherheitsrisiko kontinuierlich anpassen und messen. Security Hub bewertet kontinuierlich den Sicherheitsstatus eines Unternehmens und ergreift Maßnahmen zur Behebung identifizierter Probleme. Security Hub zentralisiert und priorisiert Sicherheitserkenntnisse von Across AWS-Konten, Services und unterstützten Drittanbietern. Auf diese Weise können Sie Sicherheitstrends analysieren und Sicherheitsprobleme mit hoher Priorität identifizieren.

Security Hub führt Hunderte von Sicherheitsprüfungen durch und klassifiziert sie anhand des Risikos für Ihre AWS Umgebung. Sie können Ihren Punktestand bei den Sicherheitskontrollen in einem einheitlichen Dashboard in der Security Hub Hub-Konsole einsehen. Weitere Informationen finden Sie unter Ermitteln von Sicherheitsbewertungen in der Security Hub Hub-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 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.

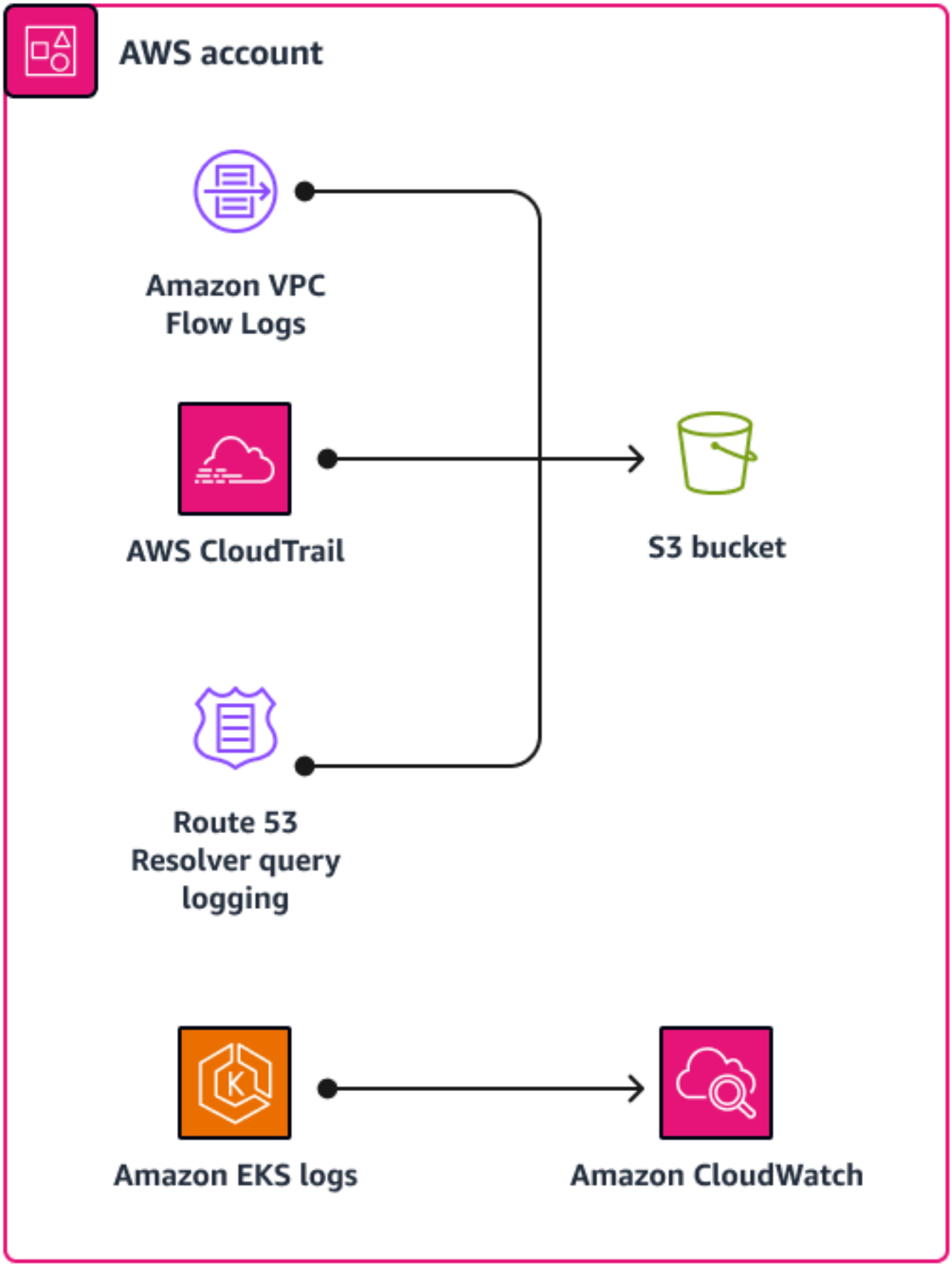
Ausgereift: Beispiel für die Erkennung von Bedrohungen

Geschäftsergebnis von Detective Controls: 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.

Werkzeug: Assisted Log Enabler for AWS (GitHub) ist ein Open-Source-Tool, mit dem Sie die Protokollierung während eines Sicherheitsvorfalls aktivieren können. Es kann Ihnen schnell mehr Einblick in einen Vorfall verschaffen.

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 Enabler sucht nach AWS CloudTrail Trails, DNS-Abfrageprotokollen, VPC-Flow-Protokollen und anderen Protokollen. Wenn sie nicht aktiviert sind, Assisted Log Enabler aktiviert sie. Assisted Log Enabler kann die Protokollierung für alle überprüfen und aktivieren AWS-Regionen.

Sie können auch drosseln Assisted Log Enabler hoch oder runter. 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. Mit dieser Funktion können Sie Folgendes verwenden 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 Assisted 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 drosseln Assisted Log Enabler hoch oder runter, für Ihren Anwendungsfall.

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.

Startphase: Optimierung Ihrer Cloud-Sicherheitsabläufe

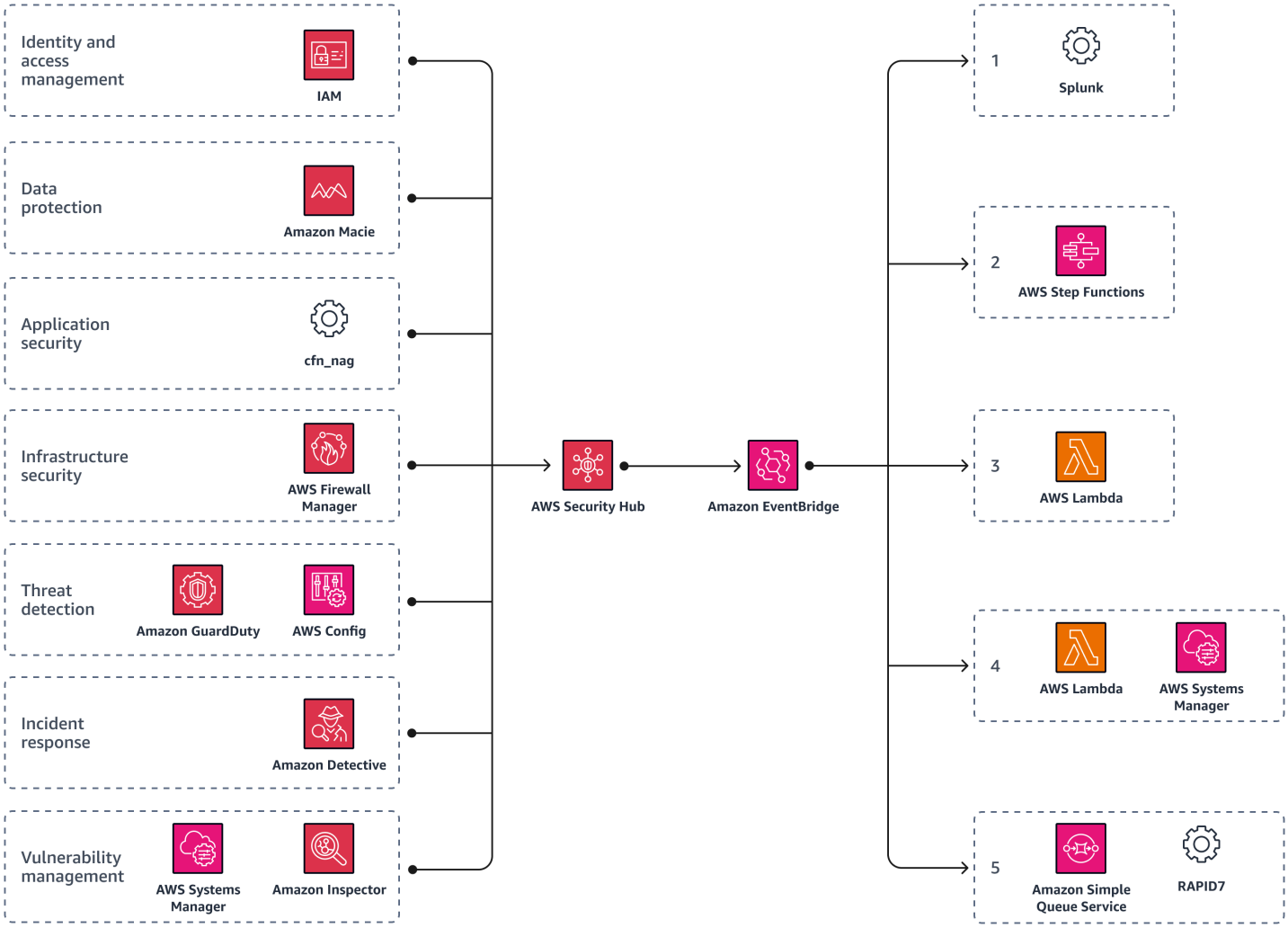
Nachdem Sie einen Basiswert in der Laufphase implementiert haben, geht Ihre Organisation zur Laufphase über. Diese Phase konzentriert sich auf die Demonstration der in der Cloud verfügbaren Cybersicherheitsfunktionen, von denen viele mit lokalen Lösungen nicht oder nur sehr schwer zu implementieren sind. 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 während der Run-Phase verwenden, um Automatisierung und Iteration zu erreichen. Die folgende Abbildung zeigt, wie Security Hub 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 Hub-Dokumentation.



Durch die Verwendung von Security Hub als zentrale Automatisierungszentrale können Sie Aktivitäten auch weiterleiten an Splunk. Splunk kann dann diejenigen erkennen, die anomal sind, und entsprechende Aktionen 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.

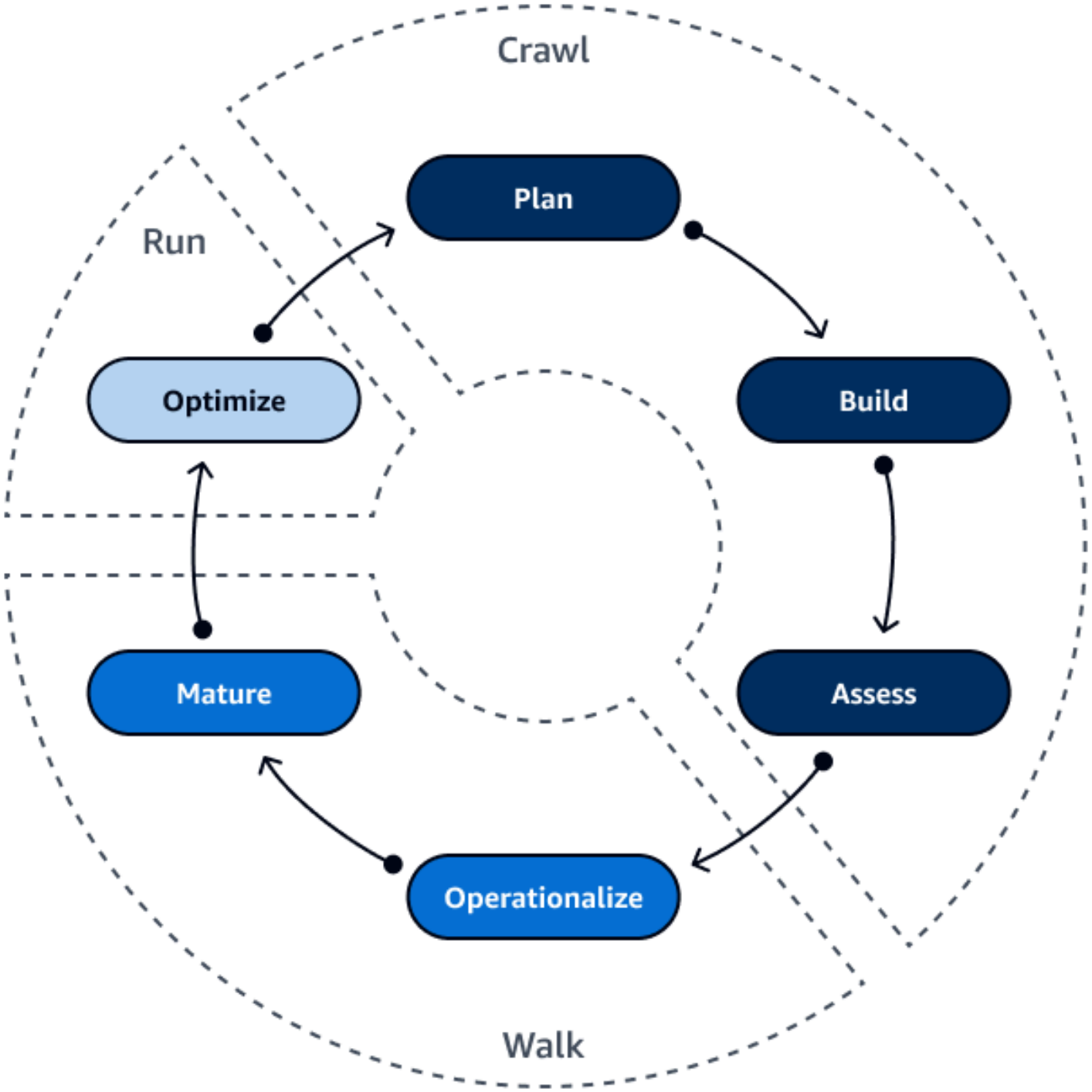
Im Folgenden finden Sie ein Beispiel für wiederholte automatisierte Aktionen, wie im vorherigen Bild dargestellt:

1. Verwenden Sie Splunk 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 stellt, 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 im Sicherheits-Blog unter So automatisieren Sie die Reaktion auf Vorfälle in AWS Cloud den AWS vier EC2 Instanzen.

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.

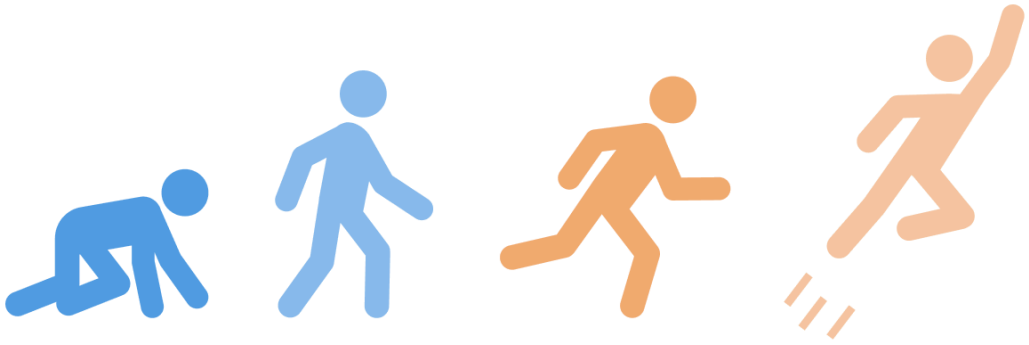


In der Crawl-Phase legen Sie den Grundstein. Sie definieren Ihren Sicherheitsplan, verwenden eine definierte Architektur mit bewährten Sicherheitsmethoden und führen eine kontinuierliche Bewertung der Geschäftsziele Ihres Unternehmens durch.

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

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

AWS Glossar zu präskriptiven Leitlinien

Die folgenden Begriffe werden häufig in Strategien, Leitfäden und Mustern von AWS Prescriptive Guidance verwendet. Um Einträge vorzuschlagen, verwenden Sie bitte den Link Feedback geben am Ende des Glossars.

Zahlen

7 Rs

Sieben gängige Migrationsstrategien für die Verlagerung von Anwendungen in die Cloud. Diese Strategien bauen auf den 5 Rs auf, die Gartner 2011 identifiziert hat, und bestehen aus folgenden Elementen:

- Faktorwechsel/Architekturwechsel – Verschieben Sie eine Anwendung und ändern Sie ihre Architektur, indem Sie alle Vorteile cloudnativer Feature nutzen, um Agilität, Leistung und Skalierbarkeit zu verbessern. Dies beinhaltet in der Regel die Portierung des Betriebssystems und der Datenbank. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank auf die Amazon Aurora PostgreSQL-kompatible Edition.
- Plattformwechsel (Lift and Reshape) – Verschieben Sie eine Anwendung in die Cloud und führen Sie ein gewisses Maß an Optimierung ein, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank zu Amazon Relational Database Service (Amazon RDS) für Oracle in der. AWS Cloud
- Neukauf (Drop and Shop) – Wechseln Sie zu einem anderen Produkt, indem Sie typischerweise von einer herkömmlichen Lizenz zu einem SaaS-Modell wechseln. Beispiel: Migrieren Sie Ihr CRM-System (Customer Relationship Management) zu Salesforce.com.
- Hostwechsel (Lift and Shift) – Verschieben Sie eine Anwendung in die Cloud, ohne Änderungen vorzunehmen, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank zu Oracle auf einer EC2 Instanz in der. AWS Cloud
- Verschieben (Lift and Shift auf Hypervisor-Ebene) – Verlagern Sie die Infrastruktur in die Cloud, ohne neue Hardware kaufen, Anwendungen umschreiben oder Ihre bestehenden Abläufe ändern zu müssen. Sie migrieren Server von einer lokalen Plattform zu einem Cloud-Dienst für dieselbe Plattform. Beispiel: Migrieren Sie eine Microsoft Hyper-V Anwendung zu AWS.
- Beibehaltung (Wiederaufgreifen) – Bewahren Sie Anwendungen in Ihrer Quellumgebung auf. Dazu können Anwendungen gehören, die einen umfangreichen Faktorwechsel erfordern und

die Sie auf einen späteren Zeitpunkt verschieben möchten, sowie ältere Anwendungen, die Sie beibehalten möchten, da es keine geschäftliche Rechtfertigung für ihre Migration gibt.

- Außerbetriebnahme – Dekommissionierung oder Entfernung von Anwendungen, die in Ihrer Quellumgebung nicht mehr benötigt werden.

A

ABAC

Siehe attributbasierte Zugriffskontrolle.

abstrahierte Dienste

Weitere Informationen finden Sie unter Managed Services.

ACID

Siehe Atomarität, Konsistenz, Isolierung und Haltbarkeit.

Aktiv-Aktiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden (mithilfe eines bidirektionalen Replikationstools oder dualer Schreibvorgänge) und beide Datenbanken Transaktionen von miteinander verbundenen Anwendungen während der Migration verarbeiten. Diese Methode unterstützt die Migration in kleinen, kontrollierten Batches, anstatt einen einmaligen Cutover zu erfordern. Es ist flexibler, erfordert aber mehr Arbeit als eine aktiv-passive Migration.

Aktiv-Passiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden, aber nur die Quelldatenbank Transaktionen von verbindenden Anwendungen verarbeitet, während Daten in die Zieldatenbank repliziert werden. Die Zieldatenbank akzeptiert während der Migration keine Transaktionen.

Aggregatfunktion

Eine SQL-Funktion, die mit einer Gruppe von Zeilen arbeitet und einen einzelnen Rückgabewert für die Gruppe berechnet. Beispiele für Aggregatfunktionen sind `SUM` und`MAX`.

AI

Siehe künstliche Intelligenz.

AIOps

Siehe Operationen im Bereich künstliche Intelligenz.

Anonymisierung

Der Prozess des dauerhaften Löschens personenbezogener Daten in einem Datensatz. Anonymisierung kann zum Schutz der Privatsphäre beitragen. Anonymisierte Daten gelten nicht mehr als personenbezogene Daten.

Anti-Muster

Eine häufig verwendete Lösung für ein wiederkehrendes Problem, bei dem die Lösung kontraproduktiv, ineffektiv oder weniger wirksam als eine Alternative ist.

Anwendungssteuerung

Ein Sicherheitsansatz, bei dem nur zugelassene Anwendungen verwendet werden können, um ein System vor Schadsoftware zu schützen.

Anwendungsportfolio

Eine Sammlung detaillierter Informationen zu jeder Anwendung, die von einer Organisation verwendet wird, einschließlich der Kosten für die Erstellung und Wartung der Anwendung und ihres Geschäftswerts. Diese Informationen sind entscheidend für den Prozess der Portfoliofindung und -analyse und hilft bei der Identifizierung und Priorisierung der Anwendungen, die migriert, modernisiert und optimiert werden sollen.

künstliche Intelligenz (KI)

Das Gebiet der Datenverarbeitungswissenschaft, das sich der Nutzung von Computertechnologien zur Ausführung kognitiver Funktionen widmet, die typischerweise mit Menschen in Verbindung gebracht werden, wie Lernen, Problemlösen und Erkennen von Mustern. Weitere Informationen finden Sie unter Was ist künstliche Intelligenz?

Operationen mit künstlicher Intelligenz (AIOps)

Der Prozess des Einsatzes von Techniken des Machine Learning zur Lösung betrieblicher Probleme, zur Reduzierung betrieblicher Zwischenfälle und menschlicher Eingriffe sowie zur Steigerung der Servicequalität. Weitere Informationen zur Verwendung in der AWS Migrationsstrategie finden Sie im Operations Integration Guide. AIOps

Asymmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der ein Schlüsselpaar, einen öffentlichen Schlüssel für die Verschlüsselung und einen privaten Schlüssel für die Entschlüsselung verwendet. Sie können den öffentlichen Schlüssel teilen, da er nicht für die Entschlüsselung verwendet wird. Der Zugriff auf den privaten Schlüssel sollte jedoch stark eingeschränkt sein.

Atomizität, Konsistenz, Isolierung, Haltbarkeit (ACID)

Eine Reihe von Softwareeigenschaften, die die Datenvalidität und betriebliche Zuverlässigkeit einer Datenbank auch bei Fehlern, Stromausfällen oder anderen Problemen gewährleisten.

Attributbasierte Zugriffskontrolle (ABAC)

Die Praxis, detaillierte Berechtigungen auf der Grundlage von Benutzerattributen wie Abteilung, Aufgabenrolle und Teamname zu erstellen. Weitere Informationen finden Sie unter ABAC AWS in der AWS Identity and Access Management (IAM-) Dokumentation.

autoritative Datenquelle

Ein Ort, an dem Sie die primäre Version der Daten speichern, die als die zuverlässigste Informationsquelle angesehen wird. Sie können Daten aus der maßgeblichen Datenquelle an andere Speicherorte kopieren, um die Daten zu verarbeiten oder zu ändern, z. B. zu anonymisieren, zu redigieren oder zu pseudonymisieren.

Availability Zone

Ein bestimmter Standort innerhalb einer AWS-Region , der vor Ausfällen in anderen Availability Zones geschützt ist und kostengünstige Netzwerkkonnektivität mit niedriger Latenz zu anderen Availability Zones in derselben Region bietet.

AWS Framework für die Cloud-Einführung (AWS CAF)

Ein Framework mit Richtlinien und bewährten Verfahren, das Unternehmen bei der Entwicklung eines effizienten und effektiven Plans für die erfolgreiche Umstellung auf die Cloud unterstützt. AWS AWS CAF unterteilt die Leitlinien in sechs Schwerpunktbereiche, die als Perspektiven bezeichnet werden: Unternehmen, Mitarbeiter, Unternehmensführung, Plattform, Sicherheit und Betrieb. Die Perspektiven Geschäft, Mitarbeiter und Unternehmensführung konzentrieren sich auf Geschäftskompetenzen und -prozesse, während sich die Perspektiven Plattform, Sicherheit und Betriebsabläufe auf technische Fähigkeiten und Prozesse konzentrieren. Die Personalperspektive zielt beispielsweise auf Stakeholder ab, die sich mit Personalwesen (HR), Personalfunktionen und Personalmanagement befassen. Aus dieser Perspektive bietet AWS CAF Leitlinien für Personalentwicklung, Schulung und Kommunikation, um das Unternehmen auf eine erfolgreiche

Cloud-Einführung vorzubereiten. Weitere Informationen finden Sie auf der AWS -CAF-Webseite und dem AWS -CAF-Whitepaper.

AWS Workload-Qualifizierungsrahmen (AWS WQF)

Ein Tool, das Workloads bei der Datenbankmigration bewertet, Migrationsstrategien empfiehlt und Arbeitsschätzungen bereitstellt. AWS WQF ist in () enthalten. AWS Schema Conversion Tool AWS SCT Es analysiert Datenbankschemas und Codeobjekte, Anwendungscode, Abhängigkeiten und Leistungsmerkmale und stellt Bewertungsberichte bereit.

B

schlechter Bot

Ein Bot, der Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen soll.

BCP

Siehe Planung der Geschäftskontinuität.

Verhaltensdiagramm

Eine einheitliche, interaktive Ansicht des Ressourcenverhaltens und der Interaktionen im Laufe der Zeit. Sie können ein Verhaltensdiagramm mit Amazon Detective verwenden, um fehlgeschlagene Anmeldeversuche, verdächtige API-Aufrufe und ähnliche Vorgänge zu untersuchen. Weitere Informationen finden Sie unter Daten in einem Verhaltensdiagramm in der Detective-Dokumentation.

Big-Endian-System

Ein System, welches das höchstwertige Byte zuerst speichert. Siehe auch Endianness.

Binäre Klassifikation

Ein Prozess, der ein binäres Ergebnis vorhersagt (eine von zwei möglichen Klassen). Beispielsweise könnte Ihr ML-Modell möglicherweise Probleme wie „Handelt es sich bei dieser E-Mail um Spam oder nicht?“ vorhersagen müssen oder „Ist dieses Produkt ein Buch oder ein Auto?“

Bloom-Filter

Eine probabilistische, speichereffiziente Datenstruktur, mit der getestet wird, ob ein Element Teil einer Menge ist.

Blau/Grün-Bereitstellung

Eine Bereitstellungsstrategie, bei der Sie zwei separate, aber identische Umgebungen erstellen. Sie führen die aktuelle Anwendungsversion in einer Umgebung (blau) und die neue Anwendungsversion in der anderen Umgebung (grün) aus. Mit dieser Strategie können Sie schnell und mit minimalen Auswirkungen ein Rollback durchführen.

Bot

Eine Softwareanwendung, die automatisierte Aufgaben über das Internet ausführt und menschliche Aktivitäten oder Interaktionen simuliert. Manche Bots sind nützlich oder nützlich, wie z. B. Webcrawler, die Informationen im Internet indexieren. Einige andere Bots, sogenannte bösartige Bots, sollen Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen.

Botnetz

Netzwerke von Bots, die mit Malware infiziert sind und unter der Kontrolle einer einzigen Partei stehen, die als Bot-Herder oder Bot-Operator bezeichnet wird. Botnetze sind der bekannteste Mechanismus zur Skalierung von Bots und ihrer Wirkung.

branch

Ein containerisierter Bereich eines Code-Repositorys. Der erste Zweig, der in einem Repository erstellt wurde, ist der Hauptzweig. Sie können einen neuen Zweig aus einem vorhandenen Zweig erstellen und dann Feature entwickeln oder Fehler in dem neuen Zweig beheben. Ein Zweig, den Sie erstellen, um ein Feature zu erstellen, wird allgemein als Feature-Zweig bezeichnet. Wenn das Feature zur Veröffentlichung bereit ist, führen Sie den Feature-Zweig wieder mit dem Hauptzweig zusammen. Weitere Informationen finden Sie unter Über Branches (GitHub Dokumentation).

Zugang durch Glasbruch

Unter außergewöhnlichen Umständen und im Rahmen eines genehmigten Verfahrens ist dies eine schnelle Methode für einen Benutzer, auf einen Bereich zuzugreifen AWS-Konto , für den er in der Regel keine Zugriffsrechte besitzt. Weitere Informationen finden Sie unter dem Indikator Implementation break-glass procedures in den AWS Well-Architected-Leitlinien.

Brownfield-Strategie

Die bestehende Infrastruktur in Ihrer Umgebung. Wenn Sie eine Brownfield-Strategie für eine Systemarchitektur anwenden, richten Sie sich bei der Gestaltung der Architektur nach den Einschränkungen der aktuellen Systeme und Infrastruktur. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Puffer-Cache

Der Speicherbereich, in dem die am häufigsten abgerufenen Daten gespeichert werden.

Geschäftsfähigkeit

Was ein Unternehmen tut, um Wert zu generieren (z. B. Vertrieb, Kundenservice oder Marketing). Microservices-Architekturen und Entwicklungsentscheidungen können von den Geschäftskapazitäten beeinflusst werden. Weitere Informationen finden Sie im Abschnitt Organisiert nach Geschäftskapazitäten des Whitepapers Ausführen von containerisierten Microservices in AWS.

Planung der Geschäftskontinuität (BCP)

Ein Plan, der die potenziellen Auswirkungen eines störenden Ereignisses, wie z. B. einer groß angelegten Migration, auf den Betrieb berücksichtigt und es einem Unternehmen ermöglicht, den Betrieb schnell wieder aufzunehmen.

C

CAF

Weitere Informationen finden Sie unter Framework für die AWS Cloud-Einführung.

Bereitstellung auf Kanaren

Die langsame und schrittweise Veröffentlichung einer Version für Endbenutzer. Wenn Sie sich sicher sind, stellen Sie die neue Version bereit und ersetzen die aktuelle Version vollständig.

CCoE

Weitere Informationen finden Sie im Cloud Center of Excellence.

CDC

Siehe Erfassung von Änderungsdaten.

Erfassung von Datenänderungen (CDC)

Der Prozess der Nachverfolgung von Änderungen an einer Datenquelle, z. B. einer Datenbanktabelle, und der Aufzeichnung von Metadaten zu der Änderung. Sie können CDC für verschiedene Zwecke verwenden, z. B. für die Prüfung oder Replikation von Änderungen in einem Zielsystem, um die Synchronisation aufrechtzuerhalten.

Chaos-Technik

Absichtliches Einführen von Ausfällen oder Störungsereignissen, um die Widerstandsfähigkeit eines Systems zu testen. Sie können AWS Fault Injection Service (AWS FIS) verwenden, um Experimente durchzuführen, die Ihre AWS Workloads stress, und deren Reaktion zu bewerten.

CI/CD

Siehe Continuous Integration und Continuous Delivery.

Klassifizierung

Ein Kategorisierungsprozess, der bei der Erstellung von Vorhersagen hilft. ML-Modelle für Klassifikationsprobleme sagen einen diskreten Wert voraus. Diskrete Werte unterscheiden sich immer voneinander. Beispielsweise muss ein Modell möglicherweise auswerten, ob auf einem Bild ein Auto zu sehen ist oder nicht.

clientseitige Verschlüsselung

Lokale Verschlüsselung von Daten, bevor das Ziel sie AWS-Service empfängt.

Cloud-Exzellenzzentrum (CCoE)

Ein multidisziplinäres Team, das die Cloud-Einführung in der gesamten Organisation vorantreibt, einschließlich der Entwicklung bewährter Cloud-Methoden, der Mobilisierung von Ressourcen, der Festlegung von Migrationszeitplänen und der Begleitung der Organisation durch groß angelegte Transformationen. Weitere Informationen finden Sie in den CCoE-Beiträgen im AWS Cloud Enterprise Strategy Blog.

Cloud Computing

Die Cloud-Technologie, die typischerweise für die Ferndatenspeicherung und das IoT-Gerätemanagement verwendet wird. Cloud Computing ist häufig mit Edge-Computing-Technologie verbunden.

Cloud-Betriebsmodell

In einer IT-Organisation das Betriebsmodell, das zum Aufbau, zur Weiterentwicklung und Optimierung einer oder mehrerer Cloud-Umgebungen verwendet wird. Weitere Informationen finden Sie unter Aufbau Ihres Cloud-Betriebsmodells.

Phasen der Einführung der Cloud

Die vier Phasen, die Unternehmen bei der Migration in der Regel durchlaufen AWS Cloud:

- Projekt – Durchführung einiger Cloud-bezogener Projekte zu Machbarkeitsnachweisen und zu Lernzwecken
- Fundament — Tätigen Sie grundlegende Investitionen, um Ihre Cloud-Einführung zu skalieren (z. B. Einrichtung einer landing zone, Definition eines CCo E, Einrichtung eines Betriebsmodells)
- Migration – Migrieren einzelner Anwendungen
- Neuentwicklung – Optimierung von Produkten und Services und Innovation in der Cloud

Diese Phasen wurden von Stephen Orban im Blogbeitrag The Journey Toward Cloud-First & the Stages of Adoption im AWS Cloud Enterprise Strategy-Blog definiert. Informationen darüber, wie sie mit der AWS Migrationsstrategie zusammenhängen, finden Sie im Leitfaden zur Vorbereitung der Migration.

CMDB

Siehe Datenbank für das Konfigurationsmanagement.

Code-Repository

Ein Ort, an dem Quellcode und andere Komponenten wie Dokumentation, Beispiele und Skripts gespeichert und im Rahmen von Versionskontrollprozessen aktualisiert werden. Zu den gängigen Cloud-Repositorys gehören GitHub oderBitbucket Cloud. Jede Version des Codes wird Zweig genannt. In einer Microservice-Struktur ist jedes Repository einer einzelnen Funktionalität gewidmet. Eine einzelne CI/CD-Pipeline kann mehrere Repositorien verwenden.

Kalter Cache

Ein Puffer-Cache, der leer oder nicht gut gefüllt ist oder veraltete oder irrelevante Daten enthält. Dies beeinträchtigt die Leistung, da die Datenbank-Instance aus dem Hauptspeicher oder der Festplatte lesen muss, was langsamer ist als das Lesen aus dem Puffercache.

Kalte Daten

Daten, auf die selten zugegriffen wird und die in der Regel historisch sind. Bei der Abfrage dieser Art von Daten sind langsame Abfragen in der Regel akzeptabel. Durch die Verlagerung dieser Daten auf leistungsschwächere und kostengünstigere Speicherstufen oder -klassen können Kosten gesenkt werden.

Computer Vision (CV)

Ein Bereich der KI, der maschinelles Lernen nutzt, um Informationen aus visuellen Formaten wie digitalen Bildern und Videos zu analysieren und zu extrahieren. Amazon SageMaker AI bietet beispielsweise Bildverarbeitungsalgorithmen für CV.

Drift in der Konfiguration

Bei einer Arbeitslast eine Änderung der Konfiguration gegenüber dem erwarteten Zustand. Dies kann dazu führen, dass der Workload nicht mehr richtlinienkonform wird, und zwar in der Regel schrittweise und unbeabsichtigt.

Verwaltung der Datenbankkonfiguration (CMDB)

Ein Repository, das Informationen über eine Datenbank und ihre IT-Umgebung speichert und verwaltet, inklusive Hardware- und Softwarekomponenten und deren Konfigurationen. In der Regel verwenden Sie Daten aus einer CMDB in der Phase der Portfolioerkennung und -analyse der Migration.

Konformitätspaket

Eine Sammlung von AWS Config Regeln und Abhilfemaßnahmen, die Sie zusammenstellen können, um Ihre Konformitäts- und Sicherheitsprüfungen individuell anzupassen. Mithilfe einer YAML-Vorlage können Sie ein Conformance Pack als einzelne Entität in einer AWS-Konto AND-Region oder unternehmensweit bereitstellen. Weitere Informationen finden Sie in der Dokumentation unter Conformance Packs. AWS Config

Kontinuierliche Bereitstellung und kontinuierliche Integration (CI/CD)

Der Prozess der Automatisierung der Quell-, Build-, Test-, Staging- und Produktionsphasen des Softwareveröffentlichungsprozesses. CI/CD is commonly described as a pipeline. CI/CDkann Ihnen helfen, Prozesse zu automatisieren, die Produktivität zu steigern, die Codequalität zu verbessern und schneller zu liefern. Weitere Informationen finden Sie unter Vorteile der kontinuierlichen Auslieferung. CD kann auch für kontinuierliche Bereitstellung stehen. Weitere Informationen finden Sie unterKontinuierliche Auslieferung im Vergleich zu kontinuierlicher Bereitstellung.

CV

Siehe Computer Vision.

D

Daten im Ruhezustand

Daten, die in Ihrem Netzwerk stationär sind, z. B. Daten, die sich im Speicher befinden.

Datenklassifizierung

Ein Prozess zur Identifizierung und Kategorisierung der Daten in Ihrem Netzwerk auf der Grundlage ihrer Kritikalität und Sensitivität. Sie ist eine wichtige Komponente jeder Strategie für das Management von Cybersecurity-Risiken, da sie Ihnen hilft, die geeigneten Schutz- und Aufbewahrungskontrollen für die Daten zu bestimmen. Die Datenklassifizierung ist ein Bestandteil der Sicherheitssäule im AWS Well-Architected Framework. Weitere Informationen finden Sie unter Datenklassifizierung.

Datendrift

Eine signifikante Variation zwischen den Produktionsdaten und den Daten, die zum Trainieren eines ML-Modells verwendet wurden, oder eine signifikante Änderung der Eingabedaten im Laufe der Zeit. Datendrift kann die Gesamtqualität, Genauigkeit und Fairness von ML-Modellvorhersagen beeinträchtigen.

Daten während der Übertragung

Daten, die sich aktiv durch Ihr Netzwerk bewegen, z. B. zwischen Netzwerkressourcen.

Datennetz

Ein architektonisches Framework, das verteilte, dezentrale Dateneigentum mit zentraler Verwaltung und Steuerung ermöglicht.

Datenminimierung

Das Prinzip, nur die Daten zu sammeln und zu verarbeiten, die unbedingt erforderlich sind. Durch Datenminimierung im AWS Cloud können Datenschutzrisiken, Kosten und der CO2-Fußabdruck Ihrer Analysen reduziert werden.

Datenperimeter

Eine Reihe präventiver Schutzmaßnahmen in Ihrer AWS Umgebung, die sicherstellen, dass nur vertrauenswürdige Identitäten auf vertrauenswürdige Ressourcen von erwarteten Netzwerken zugreifen. Weitere Informationen finden Sie unter Aufbau eines Datenperimeters auf. AWS

Vorverarbeitung der Daten

Rohdaten in ein Format umzuwandeln, das von Ihrem ML-Modell problemlos verarbeitet werden kann. Die Vorverarbeitung von Daten kann bedeuten, dass bestimmte Spalten oder Zeilen entfernt und fehlende, inkonsistente oder doppelte Werte behoben werden.

Herkunft der Daten

Der Prozess der Nachverfolgung des Ursprungs und der Geschichte von Daten während ihres gesamten Lebenszyklus, z. B. wie die Daten generiert, übertragen und gespeichert wurden.

betroffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

Ein Datenverwaltungssystem, das Business Intelligence wie Analysen unterstützt. Data Warehouses enthalten in der Regel große Mengen historischer Daten und werden in der Regel für Abfragen und Analysen verwendet.

Datenbankdefinitionssprache (DDL)

Anweisungen oder Befehle zum Erstellen oder Ändern der Struktur von Tabellen und Objekten in einer Datenbank.

Datenbankmanipulationssprache (DML)

Anweisungen oder Befehle zum Ändern (Einfügen, Aktualisieren und Löschen) von Informationen in einer Datenbank.

DDL

Siehe Datenbankdefinitionssprache.

Deep-Ensemble

Mehrere Deep-Learning-Modelle zur Vorhersage kombinieren. Sie können Deep-Ensembles verwenden, um eine genauere Vorhersage zu erhalten oder um die Unsicherheit von Vorhersagen abzuschätzen.

Deep Learning

Ein ML-Teilbereich, der mehrere Schichten künstlicher neuronaler Netzwerke verwendet, um die Zuordnung zwischen Eingabedaten und Zielvariablen von Interesse zu ermitteln.

defense-in-depth

Ein Ansatz zur Informationssicherheit, bei dem eine Reihe von Sicherheitsmechanismen und -kontrollen sorgfältig in einem Computernetzwerk verteilt werden, um die Vertraulichkeit, Integrität und Verfügbarkeit des Netzwerks und der darin enthaltenen Daten zu schützen. Wenn Sie diese Strategie anwenden AWS, fügen Sie mehrere Steuerelemente auf verschiedenen Ebenen der AWS Organizations Struktur hinzu, um die Ressourcen zu schützen. Ein defense-in-depth Ansatz könnte beispielsweise Multi-Faktor-Authentifizierung, Netzwerksegmentierung und Verschlüsselung kombinieren.

delegierter Administrator

In AWS Organizations kann ein kompatibler Dienst ein AWS Mitgliedskonto registrieren, um die Konten der Organisation und die Berechtigungen für diesen Dienst zu verwalten. Dieses Konto wird als delegierter Administrator für diesen Service bezeichnet. Weitere Informationen und eine Liste kompatibler Services finden Sie unter Services, die mit AWS Organizations funktionieren in der AWS Organizations -Dokumentation.

Bereitstellung

Der Prozess, bei dem eine Anwendung, neue Feature oder Codekorrekturen in der Zielumgebung verfügbar gemacht werden. Die Bereitstellung umfasst das Implementieren von Änderungen an einer Codebasis und das anschließende Erstellen und Ausführen dieser Codebasis in den Anwendungsumgebungen.

Entwicklungsumgebung

Siehe Umgebung.

Detektivische Kontrolle

Eine Sicherheitskontrolle, die darauf ausgelegt ist, ein Ereignis zu erkennen, zu protokollieren und zu warnen, nachdem ein Ereignis eingetreten ist. Diese Kontrollen stellen eine zweite Verteidigungslinie dar und warnen Sie vor Sicherheitsereignissen, bei denen die vorhandenen präventiven Kontrollen umgangen wurden. Weitere Informationen finden Sie unter Detektivische Kontrolle in Implementierung von Sicherheitskontrollen in AWS.

Abbildung des Wertstroms in der Entwicklung (DVSM)

Ein Prozess zur Identifizierung und Priorisierung von Einschränkungen, die sich negativ auf Geschwindigkeit und Qualität im Lebenszyklus der Softwareentwicklung auswirken. DVSM erweitert den Prozess der Wertstromanalyse, der ursprünglich für Lean-Manufacturing-Praktiken

konzipiert wurde. Es konzentriert sich auf die Schritte und Teams, die erforderlich sind, um durch den Softwareentwicklungsprozess Mehrwert zu schaffen und zu steigern.

digitaler Zwilling

Eine virtuelle Darstellung eines realen Systems, z. B. eines Gebäudes, einer Fabrik, einer Industrieanlage oder einer Produktionslinie. Digitale Zwillinge unterstützen vorausschauende Wartung, Fernüberwachung und Produktionsoptimierung.

Maßtabelle

In einem Sternschema eine kleinere Tabelle, die Datenattribute zu quantitativen Daten in einer Faktentabelle enthält. Bei Attributen von Dimensionstabellen handelt es sich in der Regel um Textfelder oder diskrete Zahlen, die sich wie Text verhalten. Diese Attribute werden häufig zum Einschränken von Abfragen, zum Filtern und zur Kennzeichnung von Ergebnismengen verwendet.

Katastrophe

Ein Ereignis, das verhindert, dass ein Workload oder ein System seine Geschäftsziele an seinem primären Einsatzort erfüllt. Diese Ereignisse können Naturkatastrophen, technische Ausfälle oder das Ergebnis menschlichen Handelns sein, wie z. B. unbeabsichtigte Fehlkonfigurationen oder ein Malware-Angriff.

Disaster Recovery (DR)

Die Strategie und der Prozess, die Sie verwenden, um Ausfallzeiten und Datenverluste aufgrund einer Katastrophe zu minimieren. Weitere Informationen finden Sie unter Disaster Recovery von Workloads unter AWS: Wiederherstellung in der Cloud im AWS Well-Architected Framework.

DML

Siehe Sprache zur Datenbankmanipulation.

Domainorientiertes Design

Ein Ansatz zur Entwicklung eines komplexen Softwaresystems, bei dem seine Komponenten mit sich entwickelnden Domains oder Kerngeschäftszielen verknüpft werden, denen jede Komponente dient. Dieses Konzept wurde von Eric Evans in seinem Buch Domaingesteuertes Design: Bewältigen der Komplexität im Herzen der Software (Boston: Addison-Wesley Professional, 2003) vorgestellt. Informationen darüber, wie Sie domaingesteuertes Design mit dem Strangler-Fig-Muster verwenden können, finden Sie unter Schrittweises Modernisieren älterer Microsoft ASP.NET (ASMX)-Webservices mithilfe von Containern und Amazon API Gateway.

DR

Siehe Disaster Recovery.

Erkennung von Driften

Verfolgung von Abweichungen von einer Basiskonfiguration. Sie können es beispielsweise verwenden, AWS CloudFormation um Abweichungen bei den Systemressourcen zu erkennen, oder Sie können AWS Control Tower damit Änderungen in Ihrer landing zone erkennen, die sich auf die Einhaltung von Governance-Anforderungen auswirken könnten.

DVSM

Siehe Abbildung des Wertstroms in der Entwicklung.

E

EDA

Siehe explorative Datenanalyse.

EDI

Siehe elektronischer Datenaustausch.

Edge-Computing

Die Technologie, die die Rechenleistung für intelligente Geräte an den Rändern eines IoT-Netzwerks erhöht. Im Vergleich zu Cloud Computing kann Edge Computing die Kommunikationslatenz reduzieren und die Reaktionszeit verbessern.

elektronischer Datenaustausch (EDI)

Der automatisierte Austausch von Geschäftsdokumenten zwischen Organisationen. Weitere Informationen finden Sie unter Was ist elektronischer Datenaustausch.

Verschlüsselung

Ein Rechenprozess, der Klartextdaten, die für Menschen lesbar sind, in Chiffretext umwandelt.

Verschlüsselungsschlüssel

Eine kryptografische Zeichenfolge aus zufälligen Bits, die von einem Verschlüsselungsalgorithmus generiert wird. Schlüssel können unterschiedlich lang sein, und jeder Schlüssel ist so konzipiert, dass er unvorhersehbar und einzigartig ist.

Endianismus

Die Reihenfolge, in der Bytes im Computerspeicher gespeichert werden. Big-Endian-Systeme speichern das höchstwertige Byte zuerst. Little-Endian-Systeme speichern das niedrigwertigste Byte zuerst.

Endpunkt

Siehe Service-Endpunkt.

Endpunkt-Services

Ein Service, den Sie in einer Virtual Private Cloud (VPC) hosten können, um ihn mit anderen Benutzern zu teilen. Sie können einen Endpunktdienst mit anderen AWS-Konten oder AWS Identity and Access Management (IAM AWS PrivateLink -) Prinzipalen erstellen und diesen Berechtigungen gewähren. Diese Konten oder Prinzipale können sich privat mit Ihrem Endpunktservice verbinden, indem sie Schnittstellen-VPC-Endpunkte erstellen. Weitere Informationen finden Sie unter Einen Endpunkt-Service erstellen in der Amazon Virtual Private Cloud (Amazon VPC)-Dokumentation.

Unternehmensressourcenplanung (ERP)

Ein System, das wichtige Geschäftsprozesse (wie Buchhaltung, MES und Projektmanagement) für ein Unternehmen automatisiert und verwaltet.

Envelope-Verschlüsselung

Der Prozess der Verschlüsselung eines Verschlüsselungsschlüssels mit einem anderen Verschlüsselungsschlüssel. Weitere Informationen finden Sie unter Envelope-Verschlüsselung in der AWS Key Management Service (AWS KMS) -Dokumentation.

Umgebung

Eine Instance einer laufenden Anwendung. Die folgenden Arten von Umgebungen sind beim Cloud-Computing üblich:

- Entwicklungsumgebung – Eine Instance einer laufenden Anwendung, die nur dem Kernteam zur Verfügung steht, das für die Wartung der Anwendung verantwortlich ist. Entwicklungsumgebungen werden verwendet, um Änderungen zu testen, bevor sie in höhere Umgebungen übertragen werden. Diese Art von Umgebung wird manchmal als Testumgebung bezeichnet.
- Niedrigere Umgebungen – Alle Entwicklungsumgebungen für eine Anwendung, z. B. solche, die für erste Builds und Tests verwendet wurden.

- Produktionsumgebung – Eine Instance einer laufenden Anwendung, auf die Endbenutzer zugreifen können. In einer CI/CD-Pipeline ist die Produktionsumgebung die letzte Bereitstellungsumgebung.
- Höhere Umgebungen – Alle Umgebungen, auf die auch andere Benutzer als das Kernentwicklungsteam zugreifen können. Dies kann eine Produktionsumgebung, Vorproduktionsumgebungen und Umgebungen für Benutzerakzeptanztests umfassen.

Epics

In der agilen Methodik sind dies funktionale Kategorien, die Ihnen helfen, Ihre Arbeit zu organisieren und zu priorisieren. Epics bieten eine allgemeine Beschreibung der Anforderungen und Implementierungsaufgaben. Zu den Sicherheitsthemen AWS von CAF gehören beispielsweise Identitäts- und Zugriffsmanagement, Detektivkontrollen, Infrastruktursicherheit, Datenschutz und Reaktion auf Vorfälle. Weitere Informationen zu Epics in der AWS - Migrationsstrategie finden Sie im Leitfaden zur Programm-Implementierung.

ERP

Siehe Enterprise Resource Planning.

Explorative Datenanalyse (EDA)

Der Prozess der Analyse eines Datensatzes, um seine Hauptmerkmale zu verstehen. Sie sammeln oder aggregieren Daten und führen dann erste Untersuchungen durch, um Muster zu finden, Anomalien zu erkennen und Annahmen zu überprüfen. EDA wird durchgeführt, indem zusammenfassende Statistiken berechnet und Datenvisualisierungen erstellt werden.

F

Faktentabelle

Die zentrale Tabelle in einem Sternschema. Sie speichert quantitative Daten über den Geschäftsbetrieb. In der Regel enthält eine Faktentabelle zwei Arten von Spalten: Spalten, die Kennzahlen enthalten, und Spalten, die einen Fremdschlüssel für eine Dimensionstabelle enthalten.

schnell scheitern

Eine Philosophie, die häufige und inkrementelle Tests verwendet, um den Entwicklungslebenszyklus zu verkürzen. Dies ist ein wichtiger Bestandteil eines agilen Ansatzes.

Grenze zur Fehlerisolierung

Dabei handelt es sich um eine Grenze AWS Cloud, z. B. eine Availability Zone AWS-Region, eine Steuerungsebene oder eine Datenebene, die die Auswirkungen eines Fehlers begrenzt und die Widerstandsfähigkeit von Workloads verbessert. Weitere Informationen finden Sie unter Grenzen zur AWS Fehlerisolierung.

Feature-Zweig

Siehe Zweig.

Features

Die Eingabedaten, die Sie verwenden, um eine Vorhersage zu treffen. In einem Fertigungskontext könnten Feature beispielsweise Bilder sein, die regelmäßig von der Fertigungslinie aus aufgenommen werden.

Bedeutung der Feature

Wie wichtig ein Feature für die Vorhersagen eines Modells ist. Dies wird in der Regel als numerischer Wert ausgedrückt, der mit verschiedenen Techniken wie Shapley Additive Explanations (SHAP) und integrierten Gradienten berechnet werden kann. Weitere Informationen finden Sie unter Interpretierbarkeit von Modellen für maschinelles Lernen mit AWS.

Featuretransformation

Daten für den ML-Prozess optimieren, einschließlich der Anreicherung von Daten mit zusätzlichen Quellen, der Skalierung von Werten oder der Extraktion mehrerer Informationssätze aus einem einzigen Datenfeld. Das ermöglicht dem ML-Modell, von den Daten profitieren. Wenn Sie beispielsweise das Datum „27.05.2021 00:15:37“ in „2021“, „Mai“, „Donnerstag“ und „15“ aufschlüsseln, können Sie dem Lernalgorithmus helfen, nuancierte Muster zu erlernen, die mit verschiedenen Datenkomponenten verknüpft sind.

Eingabeaufforderung mit wenigen Klicks

Bereitstellung einer kleinen Anzahl von Beispielen, die die Aufgabe und das gewünschte Ergebnis veranschaulichen, bevor das LLM aufgefordert wird, eine ähnliche Aufgabe auszuführen. Bei dieser Technik handelt es sich um eine Anwendung des kontextbezogenen Lernens, bei der Modelle anhand von Beispielen (Aufnahmen) lernen, die in Eingabeaufforderungen eingebettet sind. Bei Aufgaben, die spezifische Formatierungs-, Argumentations- oder Fachkenntnisse erfordern, kann die Eingabeaufforderung mit wenigen Handgriffen effektiv sein. Siehe auch Zero-Shot Prompting.

FGAC

Siehe detaillierte Zugriffskontrolle.

Feinkörnige Zugriffskontrolle (FGAC)

Die Verwendung mehrerer Bedingungen, um eine Zugriffsanfrage zuzulassen oder abzulehnen.

Flash-Cut-Migration

Eine Datenbankmigrationsmethode, bei der eine kontinuierliche Datenreplikation durch Erfassung von Änderungsdaten verwendet wird, um Daten in kürzester Zeit zu migrieren, anstatt einen schrittweisen Ansatz zu verwenden. Ziel ist es, Ausfallzeiten auf ein Minimum zu beschränken.

FM

Siehe Fundamentmodell.

Fundamentmodell (FM)

Ein großes neuronales Deep-Learning-Netzwerk, das mit riesigen Datensätzen generalisierter und unbeschrifteter Daten trainiert wurde. FMs sind in der Lage, eine Vielzahl allgemeiner Aufgaben zu erfüllen, z. B. Sprache zu verstehen, Text und Bilder zu generieren und Konversationen in natürlicher Sprache zu führen. Weitere Informationen finden Sie unter Was sind Foundation-Modelle.

G

generative KI

Eine Untergruppe von KI-Modellen, die mit großen Datenmengen trainiert wurden und mit einer einfachen Textaufforderung neue Inhalte und Artefakte wie Bilder, Videos, Text und Audio erstellen können. Weitere Informationen finden Sie unter Was ist Generative KI.

Geoblocking

Siehe geografische Einschränkungen.

Geografische Einschränkungen (Geoblocking)

Bei Amazon eine Option CloudFront, um zu verhindern, dass Benutzer in bestimmten Ländern auf Inhaltsverteilungen zugreifen. Sie können eine Zulassungsliste oder eine Sperrliste verwenden,

um zugelassene und gesperrte Länder anzugeben. Weitere Informationen finden Sie in der Dokumentation unter Beschränkung der geografischen Verteilung Ihrer Inhalte. CloudFront

Gitflow-Workflow

Ein Ansatz, bei dem niedrigere und höhere Umgebungen unterschiedliche Zweige in einem Quellcode-Repository verwenden. Der Gitflow-Workflow gilt als veraltet, und der Trunk-basierte Workflow ist der moderne, bevorzugte Ansatz.

goldenes Bild

Ein Snapshot eines Systems oder einer Software, der als Vorlage für die Bereitstellung neuer Instanzen dieses Systems oder dieser Software verwendet wird. In der Fertigung kann ein Golden Image beispielsweise zur Bereitstellung von Software auf mehreren Geräten verwendet werden und trägt zur Verbesserung der Geschwindigkeit, Skalierbarkeit und Produktivität bei der Geräteherstellung bei.

Greenfield-Strategie

Das Fehlen vorhandener Infrastruktur in einer neuen Umgebung. Bei der Einführung einer Neuausrichtung einer Systemarchitektur können Sie alle neuen Technologien ohne Einschränkung der Kompatibilität mit der vorhandenen Infrastruktur auswählen, auch bekannt als Brownfield. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Integritätsschutz

Eine allgemeine Regel, die dazu beiträgt, Ressourcen, Richtlinien und die Einhaltung von Vorschriften in allen Unternehmenseinheiten zu regeln (OUs). Präventiver Integritätsschutz setzt Richtlinien durch, um die Einhaltung von Standards zu gewährleisten. Sie werden mithilfe von Service-Kontrollrichtlinien und IAM-Berechtigungsgrenzen implementiert. Detektivischer Integritätsschutz erkennt Richtlinienverstöße und Compliance-Probleme und generiert Warnmeldungen zur Abhilfe. Sie werden mithilfe von AWS Config, AWS Security Hub, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector und benutzerdefinierten AWS Lambda Prüfungen implementiert.

H

HEKTAR

Siehe Hochverfügbarkeit.

Heterogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank in eine Zieldatenbank, die eine andere Datenbank-Engine verwendet (z. B. Oracle zu Amazon Aurora). Eine heterogene Migration ist in der Regel Teil einer Neuarchitektur, und die Konvertierung des Schemas kann eine komplexe Aufgabe sein. AWS bietet AWS SCT, welches bei Schemakonvertierungen hilft.

hohe Verfügbarkeit (HA)

Die Fähigkeit eines Workloads, im Falle von Herausforderungen oder Katastrophen kontinuierlich und ohne Eingreifen zu arbeiten. HA-Systeme sind so konzipiert, dass sie automatisch ein Failover durchführen, gleichbleibend hohe Leistung bieten und unterschiedliche Lasten und Ausfälle mit minimalen Leistungseinbußen bewältigen.

historische Modernisierung

Ein Ansatz zur Modernisierung und Aufrüstung von Betriebstechnologiesystemen (OT), um den Bedürfnissen der Fertigungsindustrie besser gerecht zu werden. Ein Historian ist eine Art von Datenbank, die verwendet wird, um Daten aus verschiedenen Quellen in einer Fabrik zu sammeln und zu speichern.

Holdout-Daten

Ein Teil historischer, beschrifteter Daten, der aus einem Datensatz zurückgehalten wird, der zum Trainieren eines Modells für maschinelles Lernen verwendet wird. Sie können Holdout-Daten verwenden, um die Modellleistung zu bewerten, indem Sie die Modellvorhersagen mit den Holdout-Daten vergleichen.

Homogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank zu einer Zieldatenbank, die dieselbe Datenbank-Engine verwendet (z. B. Microsoft SQL Server zu Amazon RDS für SQL Server). Eine homogene Migration ist in der Regel Teil eines Hostwechsels oder eines Plattformwechsels. Sie können native Datenbankserviceprogramme verwenden, um das Schema zu migrieren.

heiße Daten

Daten, auf die häufig zugegriffen wird, z. B. Echtzeitdaten oder aktuelle Translationsdaten. Für diese Daten ist in der Regel eine leistungsstarke Speicherebene oder -klasse erforderlich, um schnelle Abfrageantworten zu ermöglichen.

Hotfix

Eine dringende Lösung für ein kritisches Problem in einer Produktionsumgebung. Aufgrund seiner Dringlichkeit wird ein Hotfix normalerweise außerhalb des typischen DevOps Release-Workflows erstellt.

Hypercare-Phase

Unmittelbar nach dem Cutover, der Zeitraum, in dem ein Migrationsteam die migrierten Anwendungen in der Cloud verwaltet und überwacht, um etwaige Probleme zu beheben. In der Regel dauert dieser Zeitraum 1–4 Tage. Am Ende der Hypercare-Phase überträgt das Migrationsteam in der Regel die Verantwortung für die Anwendungen an das Cloud-Betriebsteam.

I

IaC

Sehen Sie sich Infrastruktur als Code an.

Identitätsbasierte Richtlinie

Eine Richtlinie, die einem oder mehreren IAM-Prinzipalen zugeordnet ist und deren Berechtigungen innerhalb der AWS Cloud Umgebung definiert.

Leerlaufanwendung

Eine Anwendung mit einer durchschnittlichen CPU- und Arbeitsspeicherauslastung zwischen 5 und 20 Prozent über einen Zeitraum von 90 Tagen. In einem Migrationsprojekt ist es üblich, diese Anwendungen außer Betrieb zu nehmen oder sie On-Premises beizubehalten.

IIoT

Siehe Industrielles Internet der Dinge.

unveränderliche Infrastruktur

Ein Modell, das eine neue Infrastruktur für Produktionsworkloads bereitstellt, anstatt die bestehende Infrastruktur zu aktualisieren, zu patchen oder zu modifizieren. Unveränderliche Infrastrukturen sind von Natur aus konsistenter, zuverlässiger und vorhersehbarer als veränderliche Infrastrukturen. Weitere Informationen finden Sie in der Best Practice Deploy using immutable infrastructure im AWS Well-Architected Framework.

Eingehende (ingress) VPC

In einer Architektur AWS mit mehreren Konten ist dies eine VPC, die Netzwerkverbindungen von außerhalb einer Anwendung akzeptiert, überprüft und weiterleitet. Die AWS Security Reference Architecture empfiehlt, Ihr Netzwerkkonto mit eingehendem und ausgehendem Datenverkehr und Inspektion einzurichten, VPCs um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet im weiteren Sinne zu schützen.

Inkrementelle Migration

Eine Cutover-Strategie, bei der Sie Ihre Anwendung in kleinen Teilen migrieren, anstatt eine einziges vollständiges Cutover durchzuführen. Beispielsweise könnten Sie zunächst nur einige Microservices oder Benutzer auf das neue System umstellen. Nachdem Sie sich vergewissert haben, dass alles ordnungsgemäß funktioniert, können Sie weitere Microservices oder Benutzer schrittweise verschieben, bis Sie Ihr Legacy-System außer Betrieb nehmen können. Diese Strategie reduziert die mit großen Migrationen verbundenen Risiken.

Industrie 4.0

Ein Begriff, der 2016 von Klaus Schwab eingeführt wurde und sich auf die Modernisierung von Fertigungsprozessen durch Fortschritte in den Bereichen Konnektivität, Echtzeitdaten, Automatisierung, Analytik und KI/ML bezieht.

Infrastruktur

Alle Ressourcen und Komponenten, die in der Umgebung einer Anwendung enthalten sind.

Infrastructure as Code (IaC)

Der Prozess der Bereitstellung und Verwaltung der Infrastruktur einer Anwendung mithilfe einer Reihe von Konfigurationsdateien. IaC soll Ihnen helfen, das Infrastrukturmanagement zu zentralisieren, Ressourcen zu standardisieren und schnell zu skalieren, sodass neue Umgebungen wiederholbar, zuverlässig und konsistent sind.

industrielles Internet der Dinge (T) IIo

Einsatz von mit dem Internet verbundenen Sensoren und Geräten in Industriesektoren wie Fertigung, Energie, Automobilindustrie, Gesundheitswesen, Biowissenschaften und Landwirtschaft. Weitere Informationen finden Sie unter Aufbau einer digitalen Transformationsstrategie für das industrielle Internet der Dinge (IIoT).

Inspektions-VPC

In einer Architektur AWS mit mehreren Konten eine zentralisierte VPC, die Inspektionen des Netzwerkverkehrs zwischen VPCs (in demselben oder unterschiedlichen AWS-Regionen), dem Internet und lokalen Netzwerken verwaltet. In der AWS Security Reference Architecture wird empfohlen, Ihr Netzwerkkonto mit eingehendem und ausgehendem Datenverkehr sowie Inspektionen einzurichten, VPCs um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet im weiteren Sinne zu schützen.

Internet of Things (IoT)

Das Netzwerk verbundener physischer Objekte mit eingebetteten Sensoren oder Prozessoren, das über das Internet oder über ein lokales Kommunikationsnetzwerk mit anderen Geräten und Systemen kommuniziert. Weitere Informationen finden Sie unter Was ist IoT?

Interpretierbarkeit

Ein Merkmal eines Modells für Machine Learning, das beschreibt, inwieweit ein Mensch verstehen kann, wie die Vorhersagen des Modells von seinen Eingaben abhängen. Weitere Informationen finden Sie unter Interpretierbarkeit des Modells für maschinelles Lernen mit. AWS

IoT

Siehe Internet der Dinge.

IT information library (ITIL, IT-Informationsbibliothek)

Eine Reihe von bewährten Methoden für die Bereitstellung von IT-Services und die Abstimmung dieser Services auf die Geschäftsanforderungen. ITIL bietet die Grundlage für ITSM.

T service management (ITSM, IT-Servicemanagement)

Aktivitäten im Zusammenhang mit der Gestaltung, Implementierung, Verwaltung und Unterstützung von IT-Services für eine Organisation. Informationen zur Integration von Cloud-Vorgängen mit ITSM-Tools finden Sie im Leitfaden zur Betriebsintegration.

BIS

Weitere Informationen finden Sie in der IT-Informationsbibliothek.

ITSM

Siehe IT-Servicemanagement.

L

Labelbasierte Zugangskontrolle (LBAC)

: Eine Implementierung der Mandatory Access Control (MAC), bei der den Benutzern und den Daten selbst jeweils explizit ein Sicherheitslabelwert zugewiesen wird. Die Schnittmenge zwischen der Benutzersicherheitsbeschriftung und der Datensicherheitsbeschriftung bestimmt, welche Zeilen und Spalten für den Benutzer sichtbar sind.

Landing Zone

: Eine landing zone ist eine gut strukturierte AWS Umgebung mit mehreren Konten, die skalierbar und sicher ist. Dies ist ein Ausgangspunkt, von dem aus Ihre Organisationen Workloads und Anwendungen schnell und mit Vertrauen in ihre Sicherheits- und Infrastrukturumgebung starten und bereitstellen können. Weitere Informationen zu Landing Zones finden Sie unter Einrichtung einer sicheren und skalierbaren AWS -Umgebung mit mehreren Konten..

großes Sprachmodell (LLM)

: Ein Deep-Learning-KI-Modell, das anhand einer riesigen Datenmenge vorab trainiert wurde. Ein LLM kann mehrere Aufgaben ausführen, z. B. Fragen beantworten, Dokumente zusammenfassen, Text in andere Sprachen übersetzen und Sätze vervollständigen. Weitere Informationen finden Sie unter Was sind. LLMs

Große Migration

: Eine Migration von 300 oder mehr Servern.

SCHWARZ

: Weitere Informationen finden Sie unter Label-basierte Zugriffskontrolle.

Geringste Berechtigung

: Die bewährte Sicherheitsmethode, bei der nur die für die Durchführung einer Aufgabe erforderlichen Mindestberechtigungen erteilt werden. Weitere Informationen finden Sie unter Geringste Berechtigungen anwenden in der IAM-Dokumentation.

Lift and Shift

: Siehe 7 Rs.

Little-Endian-System

: Ein System, welches das niedrigwertigste Byte zuerst speichert. Siehe auch Endianness.

LLM

Siehe großes Sprachmodell.

Niedrigere Umgebungen

Siehe Umgebung.

M

Machine Learning (ML)

Eine Art künstlicher Intelligenz, die Algorithmen und Techniken zur Mustererkennung und zum Lernen verwendet. ML analysiert aufgezeichnete Daten, wie z. B. Daten aus dem Internet der Dinge (IoT), und lernt daraus, um ein statistisches Modell auf der Grundlage von Mustern zu erstellen. Weitere Informationen finden Sie unter Machine Learning.

Hauptzweig

Siehe Filiale.

Malware

Software, die entwickelt wurde, um die Computersicherheit oder den Datenschutz zu gefährden. Malware kann Computersysteme stören, vertrauliche Informationen durchsickern lassen oder sich unbefugten Zugriff verschaffen. Beispiele für Malware sind Viren, Würmer, Ransomware, Trojaner, Spyware und Keylogger.

verwaltete Dienste

AWS-Services für die die Infrastrukturebene, das Betriebssystem und die Plattformen AWS betrieben werden, und Sie greifen auf die Endgeräte zu, um Daten zu speichern und abzurufen. Amazon Simple Storage Service (Amazon S3) und Amazon DynamoDB sind Beispiele für Managed Services. Diese werden auch als abstrakte Dienste bezeichnet.

Manufacturing Execution System (MES)

Ein Softwaresystem zur Nachverfolgung, Überwachung, Dokumentation und Steuerung von Produktionsprozessen, bei denen Rohstoffe in der Fertigung zu fertigen Produkten umgewandelt werden.

MAP

Siehe Migration Acceleration Program.

Mechanismus

Ein vollständiger Prozess, bei dem Sie ein Tool erstellen, die Akzeptanz des Tools vorantreiben und anschließend die Ergebnisse überprüfen, um Anpassungen vorzunehmen. Ein Mechanismus ist ein Zyklus, der sich im Laufe seiner Tätigkeit selbst verstärkt und verbessert. Weitere Informationen finden Sie unter Aufbau von Mechanismen im AWS Well-Architected Framework.

Mitgliedskonto

Alle AWS-Konten außer dem Verwaltungskonto, die Teil einer Organisation in sind. AWS Organizations Ein Konto kann jeweils nur einer Organisation angehören.

DURCHEINANDER

Siehe Manufacturing Execution System.

Message Queuing-Telemetrietransport (MQTT)

Ein leichtes machine-to-machine (M2M) -Kommunikationsprotokoll, das auf dem Publish/Subscribe-Muster für IoT-Geräte mit beschränkten Ressourcen basiert.

Microservice

Ein kleiner, unabhängiger Dienst, der über genau definierte Kanäle kommuniziert APIs und in der Regel kleinen, eigenständigen Teams gehört. Ein Versicherungssystem kann beispielsweise Microservices beinhalten, die Geschäftsfunktionen wie Vertrieb oder Marketing oder Subdomains wie Einkauf, Schadenersatz oder Analytik zugeordnet sind. Zu den Vorteilen von Microservices gehören Agilität, flexible Skalierung, einfache Bereitstellung, wiederverwendbarer Code und Ausfallsicherheit. Weitere Informationen finden Sie unter Integration von Microservices mithilfe serverloser Dienste. AWS

Microservices-Architekturen

Ein Ansatz zur Erstellung einer Anwendung mit unabhängigen Komponenten, die jeden Anwendungsprozess als Microservice ausführen. Diese Microservices kommunizieren mithilfe von Lightweight über eine klar definierte Schnittstelle. APIs Jeder Microservice in dieser Architektur kann aktualisiert, bereitgestellt und skaliert werden, um den Bedarf an bestimmten Funktionen einer Anwendung zu decken. Weitere Informationen finden Sie unter Implementierung von Microservices auf. AWS

Migration Acceleration Program (MAP)

Ein AWS Programm, das Beratung, Unterstützung, Schulungen und Services bietet, um Unternehmen dabei zu unterstützen, eine solide betriebliche Grundlage für die Umstellung auf

die Cloud zu schaffen und die anfänglichen Kosten von Migrationen auszugleichen. MAP umfasst eine Migrationsmethode für die methodische Durchführung von Legacy-Migrationen sowie eine Reihe von Tools zur Automatisierung und Beschleunigung gängiger Migrationsszenarien.

Migration in großem Maßstab

Der Prozess, bei dem der Großteil des Anwendungsportfolios in Wellen in die Cloud verlagert wird, wobei in jeder Welle mehr Anwendungen schneller migriert werden. In dieser Phase werden die bewährten Verfahren und Erkenntnisse aus den früheren Phasen zur Implementierung einer Migrationsfabrik von Teams, Tools und Prozessen zur Optimierung der Migration von Workloads durch Automatisierung und agile Bereitstellung verwendet. Dies ist die dritte Phase der AWS - Migrationsstrategie.

Migrationsfabrik

Funktionsübergreifende Teams, die die Migration von Workloads durch automatisierte, agile Ansätze optimieren. Zu den Teams in der Migrationsabteilung gehören in der Regel Betriebsabläufe, Geschäftsanalysten und Eigentümer, Migrationsingenieure, Entwickler und DevOps Experten, die in Sprints arbeiten. Zwischen 20 und 50 Prozent eines Unternehmensanwendungsportfolios bestehen aus sich wiederholenden Mustern, die durch einen Fabrik-Ansatz optimiert werden können. Weitere Informationen finden Sie in Diskussion über Migrationsfabriken und den Leitfaden zur Cloud-Migration-Fabrik in diesem Inhaltssatz.

Migrationsmetadaten

Die Informationen über die Anwendung und den Server, die für den Abschluss der Migration benötigt werden. Für jedes Migrationsmuster ist ein anderer Satz von Migrationsmetadaten erforderlich. Beispiele für Migrationsmetadaten sind das Zielsubnetz, die Sicherheitsgruppe und AWS das Konto.

Migrationsmuster

Eine wiederholbare Migrationsaufgabe, in der die Migrationsstrategie, das Migrationsziel und die verwendete Migrationsanwendung oder der verwendete Migrationsservice detailliert beschrieben werden. Beispiel: Rehost-Migration zu Amazon EC2 mit AWS Application Migration Service.

Migration Portfolio Assessment (MPA)

Ein Online-Tool, das Informationen zur Validierung des Geschäftsszenarios für die Migration auf das bereitstellt. AWS Cloud MPA bietet eine detaillierte Portfoliobewertung (richtige Servergröße, Preisgestaltung, Gesamtbetriebskostenanalyse, Migrationskostenanalyse) sowie Migrationsplanung (Anwendungsdatenanalyse und Datenerfassung, Anwendungsgruppierung,

Migrationspriorisierung und Wellenplanung). Das MPA-Tool (Anmeldung erforderlich) steht allen AWS Beratern und APN-Partnerberatern kostenlos zur Verfügung.

Migration Readiness Assessment (MRA)

Der Prozess, bei dem mithilfe des AWS CAF Erkenntnisse über den Cloud-Bereitschaftsstatus eines Unternehmens gewonnen, Stärken und Schwächen identifiziert und ein Aktionsplan zur Schließung festgestellter Lücken erstellt wird. Weitere Informationen finden Sie im Benutzerhandbuch für Migration Readiness. MRA ist die erste Phase der AWS - Migrationsstrategie.

Migrationsstrategie

Der Ansatz, der verwendet wurde, um einen Workload auf den AWS Cloud zu migrieren. Weitere Informationen finden Sie im Eintrag 7 Rs in diesem Glossar und unter Mobilisieren Sie Ihr Unternehmen, um umfangreiche Migrationen zu beschleunigen.

ML

Siehe maschinelles Lernen.

Modernisierung

Umwandlung einer veralteten (veralteten oder monolithischen) Anwendung und ihrer Infrastruktur in ein agiles, elastisches und hochverfügbares System in der Cloud, um Kosten zu senken, die Effizienz zu steigern und Innovationen zu nutzen. Weitere Informationen finden Sie unter Strategie zur Modernisierung von Anwendungen in der AWS Cloud.

Bewertung der Modernisierungsfähigkeit

Eine Bewertung, anhand derer festgestellt werden kann, ob die Anwendungen einer Organisation für die Modernisierung bereit sind, Vorteile, Risiken und Abhängigkeiten identifiziert und ermittelt wird, wie gut die Organisation den zukünftigen Status dieser Anwendungen unterstützen kann. Das Ergebnis der Bewertung ist eine Vorlage der Zielarchitektur, eine Roadmap, in der die Entwicklungsphasen und Meilensteine des Modernisierungsprozesses detailliert beschrieben werden, sowie ein Aktionsplan zur Behebung festgestellter Lücken. Weitere Informationen finden Sie unter Evaluierung der Modernisierungsbereitschaft von Anwendungen in der AWS Cloud.

Monolithische Anwendungen (Monolithen)

Anwendungen, die als ein einziger Service mit eng gekoppelten Prozessen ausgeführt werden. Monolithische Anwendungen haben verschiedene Nachteile. Wenn ein Anwendungs-Feature stark nachgefragt wird, muss die gesamte Architektur skaliert werden. Das Hinzufügen oder

Verbessern der Feature einer monolithischen Anwendung wird ebenfalls komplexer, wenn die Codebasis wächst. Um diese Probleme zu beheben, können Sie eine Microservices-Architektur verwenden. Weitere Informationen finden Sie unter Zerlegen von Monolithen in Microservices.

MPA

Siehe Bewertung des Migrationsportfolios.

MQTT

Siehe Message Queuing-Telemetrietransport.

Mehrklassen-Klassifizierung

Ein Prozess, der dabei hilft, Vorhersagen für mehrere Klassen zu generieren (wobei eines von mehr als zwei Ergebnissen vorhergesagt wird). Ein ML-Modell könnte beispielsweise fragen: „Ist dieses Produkt ein Buch, ein Auto oder ein Telefon?“ oder „Welche Kategorie von Produkten ist für diesen Kunden am interessantesten?“

veränderbare Infrastruktur

Ein Modell, das die bestehende Infrastruktur für Produktionsworkloads aktualisiert und modifiziert. Für eine verbesserte Konsistenz, Zuverlässigkeit und Vorhersagbarkeit empfiehlt das AWS Well-Architected Framework die Verwendung einer unveränderlichen Infrastruktur als bewährte Methode.

O

OAC

Siehe Origin Access Control.

OAI

Siehe Zugriffsidentität von Origin.

COM

Siehe organisatorisches Change-Management.

Offline-Migration

Eine Migrationsmethode, bei der der Quell-Workload während des Migrationsprozesses heruntergefahren wird. Diese Methode ist mit längeren Ausfallzeiten verbunden und wird in der Regel für kleine, unkritische Workloads verwendet.

OI

Siehe Betriebsintegration.

OLA

Siehe Vereinbarung auf operativer Ebene.

Online-Migration

Eine Migrationsmethode, bei der der Quell-Workload auf das Zielsystem kopiert wird, ohne offline genommen zu werden. Anwendungen, die mit dem Workload verbunden sind, können während der Migration weiterhin funktionieren. Diese Methode beinhaltet keine bis minimale Ausfallzeit und wird in der Regel für kritische Produktionsworkloads verwendet.

OPC-UA

Siehe Open Process Communications — Unified Architecture.

Offene Prozesskommunikation — Einheitliche Architektur (OPC-UA)

Ein machine-to-machine (M2M) -Kommunikationsprotokoll für die industrielle Automatisierung. OPC-UA bietet einen Interoperabilitätsstandard mit Datenverschlüsselungs-, Authentifizierungs- und Autorisierungsschemata.

Vereinbarung auf Betriebsebene (OLA)

Eine Vereinbarung, in der klargestellt wird, welche funktionalen IT-Gruppen sich gegenseitig versprechen zu liefern, um ein Service Level Agreement (SLA) zu unterstützen.

Überprüfung der Betriebsbereitschaft (ORR)

Eine Checkliste mit Fragen und zugehörigen bewährten Methoden, die Ihnen helfen, Vorfälle und mögliche Ausfälle zu verstehen, zu bewerten, zu verhindern oder deren Umfang zu reduzieren. Weitere Informationen finden Sie unter Operational Readiness Reviews (ORR) im AWS Well-Architected Framework.

Betriebstechnologie (OT)

Hardware- und Softwaresysteme, die mit der physischen Umgebung zusammenarbeiten, um industrielle Abläufe, Ausrüstung und Infrastruktur zu steuern. In der Fertigung ist die Integration von OT- und Informationstechnologie (IT) -Systemen ein zentraler Schwerpunkt der Industrie 4.0-Transformationen.

Betriebsintegration (OI)

Der Prozess der Modernisierung von Abläufen in der Cloud, der Bereitschaftsplanung, Automatisierung und Integration umfasst. Weitere Informationen finden Sie im Leitfaden zur Betriebsintegration.

Organisationspfad

Ein Pfad, der von erstellt wird und in AWS CloudTrail dem alle Ereignisse für alle AWS-Konten in einer Organisation protokolliert werden. AWS Organizations Diese Spur wird in jedem AWS-Konto , der Teil der Organisation ist, erstellt und verfolgt die Aktivität in jedem Konto. Weitere Informationen finden Sie in der CloudTrail Dokumentation unter Einen Trail für eine Organisation erstellen.

Organisatorisches Veränderungsmanagement (OCM)

Ein Framework für das Management wichtiger, disruptiver Geschäftstransformationen aus Sicht der Mitarbeiter, der Kultur und der Führung. OCM hilft Organisationen dabei, sich auf neue Systeme und Strategien vorzubereiten und auf diese umzustellen, indem es die Akzeptanz von Veränderungen beschleunigt, Übergangsprobleme angeht und kulturelle und organisatorische Veränderungen vorantreibt. In der AWS Migrationsstrategie wird dieses Framework aufgrund der Geschwindigkeit des Wandels, der bei Projekten zur Cloud-Einführung erforderlich ist, als Mitarbeiterbeschleunigung bezeichnet. Weitere Informationen finden Sie im OCM-Handbuch.

Ursprungszugriffskontrolle (OAC)

In CloudFront, eine erweiterte Option zur Zugriffsbeschränkung, um Ihre Amazon Simple Storage Service (Amazon S3) -Inhalte zu sichern. OAC unterstützt alle S3-Buckets insgesamt AWS-Regionen, serverseitige Verschlüsselung mit AWS KMS (SSE-KMS) sowie dynamische `PUT` und `DELETE` Anfragen an den S3-Bucket.

Ursprungszugriffsidentität (OAI)

In CloudFront, eine Option zur Zugriffsbeschränkung, um Ihre Amazon S3 S3-Inhalte zu sichern. Wenn Sie OAI verwenden, CloudFront erstellt es einen Principal, mit dem sich Amazon S3 authentifizieren kann. Authentifizierte Principals können nur über eine bestimmte Distribution auf Inhalte in einem S3-Bucket zugreifen. CloudFront Siehe auch OAC, das eine detailliertere und verbesserte Zugriffskontrolle bietet.

ORR

Weitere Informationen finden Sie unter Überprüfung der Betriebsbereitschaft.

NICHT

Siehe Betriebstechnologie.

Ausgehende (egress) VPC

In einer Architektur AWS mit mehreren Konten eine VPC, die Netzwerkverbindungen verarbeitet, die von einer Anwendung aus initiiert werden. Die AWS Security Reference Architecture empfiehlt die Einrichtung Ihres Netzwerkkontos mit eingehendem und ausgehendem Datenverkehr sowie Inspektion, VPCs um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet im weiteren Sinne zu schützen.

P

Berechtigungsgrenze

Eine IAM-Verwaltungsrichtlinie, die den IAM-Prinzipalen zugeordnet ist, um die maximalen Berechtigungen festzulegen, die der Benutzer oder die Rolle haben kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitys in der IAM-Dokumentation.

persönlich identifizierbare Informationen (PII)

Informationen, die, wenn sie direkt betrachtet oder mit anderen verwandten Daten kombiniert werden, verwendet werden können, um vernünftige Rückschlüsse auf die Identität einer Person zu ziehen. Beispiele für personenbezogene Daten sind Namen, Adressen und Kontaktinformationen.

Personenbezogene Daten

Siehe persönlich identifizierbare Informationen.

Playbook

Eine Reihe vordefinierter Schritte, die die mit Migrationen verbundenen Aufgaben erfassen, z. B. die Bereitstellung zentraler Betriebsfunktionen in der Cloud. Ein Playbook kann die Form von Skripten, automatisierten Runbooks oder einer Zusammenfassung der Prozesse oder Schritte annehmen, die für den Betrieb Ihrer modernisierten Umgebung erforderlich sind.

PLC

Siehe programmierbare Logiksteuerung.

PLM

Siehe Produktlebenszyklusmanagement.

policy

Ein Objekt, das Berechtigungen definieren (siehe identitätsbasierte Richtlinie), Zugriffsbedingungen spezifizieren (siehe ressourcenbasierte Richtlinie) oder die maximalen Berechtigungen für alle Konten in einer Organisation definieren kann AWS Organizations (siehe Dienststeuerungsrichtlinie).

Polyglotte Beharrlichkeit

Unabhängige Auswahl der Datenspeichertechnologie eines Microservices auf der Grundlage von Datenzugriffsmustern und anderen Anforderungen. Wenn Ihre Microservices über dieselbe Datenspeichertechnologie verfügen, kann dies zu Implementierungsproblemen oder zu Leistungseinbußen führen. Microservices lassen sich leichter implementieren und erzielen eine bessere Leistung und Skalierbarkeit, wenn sie den Datenspeicher verwenden, der ihren Anforderungen am besten entspricht. Weitere Informationen finden Sie unter Datenpersistenz in Microservices aktivieren.

Portfoliobewertung

Ein Prozess, bei dem das Anwendungsportfolio ermittelt, analysiert und priorisiert wird, um die Migration zu planen. Weitere Informationen finden Sie in Bewerten der Migrationsbereitschaft.

predicate

Eine Abfragebedingung, die `true` oder zurückgibt`false`, was üblicherweise in einer Klausel vorkommt. `WHERE`

Prädikat Pushdown

Eine Technik zur Optimierung von Datenbankabfragen, bei der die Daten in der Abfrage vor der Übertragung gefiltert werden. Dadurch wird die Datenmenge reduziert, die aus der relationalen Datenbank abgerufen und verarbeitet werden muss, und die Abfrageleistung wird verbessert.

Präventive Kontrolle

Eine Sicherheitskontrolle, die verhindern soll, dass ein Ereignis eintritt. Diese Kontrollen stellen eine erste Verteidigungslinie dar, um unbefugten Zugriff oder unerwünschte Änderungen an Ihrem Netzwerk zu verhindern. Weitere Informationen finden Sie unter Präventive Kontrolle in Implementierung von Sicherheitskontrollen in AWS.

Prinzipal

Eine Entität AWS , die Aktionen ausführen und auf Ressourcen zugreifen kann. Bei dieser Entität handelt es sich in der Regel um einen Root-Benutzer für eine AWS-Konto, eine IAM-Rolle oder einen Benutzer. Weitere Informationen finden Sie unter Prinzipal in Rollenbegriffe und -konzepte in der IAM-Dokumentation.

Datenschutz von Natur aus

Ein systemtechnischer Ansatz, der den Datenschutz während des gesamten Entwicklungsprozesses berücksichtigt.

Privat gehostete Zonen

Ein Container, der Informationen darüber enthält, wie Amazon Route 53 auf DNS-Abfragen für eine Domain und deren Subdomains innerhalb einer oder mehrerer VPCs Domains antworten soll. Weitere Informationen finden Sie unter Arbeiten mit privat gehosteten Zonen in der Route-53-Dokumentation.

proaktive Steuerung

Eine Sicherheitskontrolle, die den Einsatz nicht richtlinienkonformer Ressourcen verhindern soll. Diese Steuerelemente scannen Ressourcen, bevor sie bereitgestellt werden. Wenn die Ressource nicht mit der Steuerung konform ist, wird sie nicht bereitgestellt. Weitere Informationen finden Sie im Referenzhandbuch zu Kontrollen in der AWS Control Tower Dokumentation und unter Proaktive Kontrollen unter Implementierung von Sicherheitskontrollen am AWS.

Produktlebenszyklusmanagement (PLM)

Das Management von Daten und Prozessen für ein Produkt während seines gesamten Lebenszyklus, vom Design, der Entwicklung und Markteinführung über Wachstum und Reife bis hin zur Markteinführung und Markteinführung.

Produktionsumgebung

Siehe Umgebung.

Speicherprogrammierbare Steuerung (SPS)

In der Fertigung ein äußerst zuverlässiger, anpassungsfähiger Computer, der Maschinen überwacht und Fertigungsprozesse automatisiert.

schnelle Verkettung

Verwendung der Ausgabe einer LLM-Eingabeaufforderung als Eingabe für die nächste Aufforderung, um bessere Antworten zu generieren. Diese Technik wird verwendet, um eine komplexe Aufgabe in Unteraufgaben zu unterteilen oder um eine vorläufige Antwort iterativ zu verfeinern oder zu erweitern. Sie trägt dazu bei, die Genauigkeit und Relevanz der Antworten eines Modells zu verbessern und ermöglicht detailliertere, personalisierte Ergebnisse.

Pseudonymisierung

Der Prozess, bei dem persönliche Identifikatoren in einem Datensatz durch Platzhalterwerte ersetzt werden. Pseudonymisierung kann zum Schutz der Privatsphäre beitragen. Pseudonymisierte Daten gelten weiterhin als personenbezogene Daten.

publish/subscribe (pub/sub)

Ein Muster, das asynchrone Kommunikation zwischen Microservices ermöglicht, um die Skalierbarkeit und Reaktionsfähigkeit zu verbessern. In einem auf Microservices basierenden MES kann ein Microservice beispielsweise Ereignismeldungen in einem Kanal veröffentlichen, den andere Microservices abonnieren können. Das System kann neue Microservices hinzufügen, ohne den Veröffentlichungsservice zu ändern.

Q

Abfrageplan

Eine Reihe von Schritten, wie Anweisungen, die für den Zugriff auf die Daten in einem relationalen SQL-Datenbanksystem verwendet werden.

Abfrageplanregression

Wenn ein Datenbankserviceoptimierer einen weniger optimalen Plan wählt als vor einer bestimmten Änderung der Datenbankumgebung. Dies kann durch Änderungen an Statistiken, Beschränkungen, Umgebungseinstellungen, Abfrageparameter-Bindungen und Aktualisierungen der Datenbank-Engine verursacht werden.

R

RACI-Matrix

Siehe verantwortlich, rechenschaftspflichtig, konsultiert, informiert (RACI).

LAPPEN

Siehe Erweiterte Generierung beim Abrufen.

Ransomware

Eine bösartige Software, die entwickelt wurde, um den Zugriff auf ein Computersystem oder Daten zu blockieren, bis eine Zahlung erfolgt ist.

RASCI-Matrix

Siehe verantwortlich, rechenschaftspflichtig, konsultiert, informiert (RACI).

RCAC

Siehe Zugriffskontrolle für Zeilen und Spalten.

Read Replica

Eine Kopie einer Datenbank, die nur für Lesezwecke verwendet wird. Sie können Abfragen an das Lesereplikat weiterleiten, um die Belastung auf Ihrer Primärdatenbank zu reduzieren.

neu strukturieren

Siehe 7 Rs.

Recovery Point Objective (RPO)

Die maximal zulässige Zeitspanne seit dem letzten Datenwiederherstellungspunkt. Damit wird festgelegt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Serviceunterbrechung gilt.

Wiederherstellungszeitziel (RTO)

Die maximal zulässige Verzögerung zwischen der Betriebsunterbrechung und der Wiederherstellung des Dienstes.

Refaktorierung

Siehe 7 Rs.

Region

Eine Sammlung von AWS Ressourcen in einem geografischen Gebiet. Jeder AWS-Region ist isoliert und unabhängig von den anderen, um Fehlertoleranz, Stabilität und Belastbarkeit zu gewährleisten. Weitere Informationen finden Sie unter Geben Sie an, was AWS-Regionen Ihr Konto verwenden kann.

Regression

Eine ML-Technik, die einen numerischen Wert vorhersagt. Zum Beispiel, um das Problem „Zu welchem Preis wird dieses Haus verkauft werden?“ zu lösen Ein ML-Modell könnte ein lineares Regressionsmodell verwenden, um den Verkaufspreis eines Hauses auf der Grundlage bekannter Fakten über das Haus (z. B. die Quadratmeterzahl) vorherzusagen.

rehosten

Siehe 7 Rs.

Veröffentlichung

In einem Bereitstellungsprozess der Akt der Förderung von Änderungen an einer Produktionsumgebung.

umziehen

Siehe 7 Rs.

neue Plattform

Siehe 7 Rs.

Rückkauf

Siehe 7 Rs.

Ausfallsicherheit

Die Fähigkeit einer Anwendung, Störungen zu widerstehen oder sich von ihnen zu erholen. Hochverfügbarkeit und Notfallwiederherstellung sind häufig Überlegungen bei der Planung der Ausfallsicherheit in der. AWS Cloud Weitere Informationen finden Sie unter AWS Cloud Resilienz.

Ressourcenbasierte Richtlinie

Eine mit einer Ressource verknüpfte Richtlinie, z. B. ein Amazon-S3-Bucket, ein Endpunkt oder ein Verschlüsselungsschlüssel. Diese Art von Richtlinie legt fest, welchen Prinzipalen der Zugriff gewährt wird, welche Aktionen unterstützt werden und welche anderen Bedingungen erfüllt sein müssen.

RACI-Matrix (verantwortlich, rechenschaftspflichtig, konsultiert, informiert)

Eine Matrix, die die Rollen und Verantwortlichkeiten aller an Migrationsaktivitäten und Cloud-Operationen beteiligten Parteien definiert. Der Matrixname leitet sich von den in der Matrix definierten Zuständigkeitstypen ab: verantwortlich (R), rechenschaftspflichtig (A), konsultiert (C) und informiert (I). Der Unterstützungstyp (S) ist optional. Wenn Sie Unterstützung einbeziehen, wird die Matrix als RASCI-Matrix bezeichnet, und wenn Sie sie ausschließen, wird sie als RACI-Matrix bezeichnet.

Reaktive Kontrolle

Eine Sicherheitskontrolle, die darauf ausgelegt ist, die Behebung unerwünschter Ereignisse oder Abweichungen von Ihren Sicherheitsstandards voranzutreiben. Weitere Informationen finden Sie unter Reaktive Kontrolle in Implementieren von Sicherheitskontrollen in AWS.

Beibehaltung

Siehe 7 Rs.

zurückziehen

Siehe 7 Rs.

Retrieval Augmented Generation (RAG)

Eine generative KI-Technologie, bei der ein LLM auf eine maßgebliche Datenquelle verweist, die sich außerhalb seiner Trainingsdatenquellen befindet, bevor eine Antwort generiert wird. Ein RAG-Modell könnte beispielsweise eine semantische Suche in der Wissensdatenbank oder in benutzerdefinierten Daten einer Organisation durchführen. Weitere Informationen finden Sie unter Was ist RAG.

Drehung

Der Vorgang, bei dem ein Geheimnis regelmäßig aktualisiert wird, um es einem Angreifer zu erschweren, auf die Anmeldeinformationen zuzugreifen.

Zugriffskontrolle für Zeilen und Spalten (RCAC)

Die Verwendung einfacher, flexibler SQL-Ausdrücke mit definierten Zugriffsregeln. RCAC besteht aus Zeilenberechtigungen und Spaltenmasken.

RPO

Siehe Recovery Point Objective.

RTO

Siehe Ziel der Wiederherstellungszeit.

Runbook

Eine Reihe manueller oder automatisierter Verfahren, die zur Ausführung einer bestimmten Aufgabe erforderlich sind. Diese sind in der Regel darauf ausgelegt, sich wiederholende Operationen oder Verfahren mit hohen Fehlerquoten zu rationalisieren.

S

SAML 2.0

Ein offener Standard, den viele Identitätsanbieter (IdPs) verwenden. Diese Funktion ermöglicht föderiertes Single Sign-On (SSO), sodass sich Benutzer bei den API-Vorgängen anmelden AWS Management Console oder die AWS API-Operationen aufrufen können, ohne dass Sie einen Benutzer in IAM für alle in Ihrer Organisation erstellen müssen. Weitere Informationen zum SAML-2.0.-basierten Verbund finden Sie unter Über den SAML-2.0-basierten Verbund in der IAM-Dokumentation.

SCADA

Siehe Aufsichtskontrolle und Datenerfassung.

SCP

Siehe Richtlinie zur Dienstkontrolle.

Secret

Interne AWS Secrets Manager, vertrauliche oder eingeschränkte Informationen, wie z. B. ein Passwort oder Benutzeranmeldedaten, die Sie in verschlüsselter Form speichern. Es besteht aus dem geheimen Wert und seinen Metadaten. Der geheime Wert kann binär, eine einzelne Zeichenfolge oder mehrere Zeichenketten sein. Weitere Informationen finden Sie unter Was ist in einem Secrets Manager Manager-Geheimnis? in der Secrets Manager Manager-Dokumentation.

Sicherheit durch Design

Ein systemtechnischer Ansatz, der die Sicherheit während des gesamten Entwicklungsprozesses berücksichtigt.

Sicherheitskontrolle

Ein technischer oder administrativer Integritätsschutz, der die Fähigkeit eines Bedrohungsakteurs, eine Schwachstelle auszunutzen, verhindert, erkennt oder einschränkt. Es gibt vier Haupttypen von Sicherheitskontrollen: präventiv, detektiv, reaktionsschnell und proaktiv.

Härtung der Sicherheit

Der Prozess, bei dem die Angriffsfläche reduziert wird, um sie widerstandsfähiger gegen Angriffe zu machen. Dies kann Aktionen wie das Entfernen von Ressourcen, die nicht mehr benötigt werden, die Implementierung der bewährten Sicherheitsmethode der Gewährung geringster Berechtigungen oder die Deaktivierung unnötiger Feature in Konfigurationsdateien umfassen.

System zur Verwaltung von Sicherheitsinformationen und Ereignissen (security information and event management – SIEM)

Tools und Services, die Systeme für das Sicherheitsinformationsmanagement (SIM) und das Management von Sicherheitsereignissen (SEM) kombinieren. Ein SIEM-System sammelt, überwacht und analysiert Daten von Servern, Netzwerken, Geräten und anderen Quellen, um Bedrohungen und Sicherheitsverletzungen zu erkennen und Warnmeldungen zu generieren.

Automatisierung von Sicherheitsreaktionen

Eine vordefinierte und programmierte Aktion, die darauf ausgelegt ist, automatisch auf ein Sicherheitsereignis zu reagieren oder es zu beheben. Diese Automatisierungen dienen als detektive oder reaktionsschnelle Sicherheitskontrollen, die Sie bei der Implementierung bewährter AWS Sicherheitsmethoden unterstützen. Beispiele für automatisierte Antwortaktionen sind das Ändern einer VPC-Sicherheitsgruppe, das Patchen einer EC2 Amazon-Instance oder das Rotieren von Anmeldeinformationen.

Serverseitige Verschlüsselung

Verschlüsselung von Daten am Zielort durch denjenigen AWS-Service , der sie empfängt.

Service-Kontrollrichtlinie (SCP)

Eine Richtlinie, die eine zentrale Steuerung der Berechtigungen für alle Konten in einer Organisation in ermöglicht AWS Organizations. SCPs Definieren Sie Leitplanken oder legen Sie Grenzwerte für Aktionen fest, die ein Administrator an Benutzer oder Rollen delegieren kann. Sie können sie SCPs als Zulassungs- oder Ablehnungslisten verwenden, um festzulegen, welche Dienste oder Aktionen zulässig oder verboten sind. Weitere Informationen finden Sie in der AWS Organizations Dokumentation unter Richtlinien zur Dienststeuerung.

Service-Endpunkt

Die URL des Einstiegspunkts für einen AWS-Service. Sie können den Endpunkt verwenden, um programmgesteuert eine Verbindung zum Zielservice herzustellen. Weitere Informationen finden Sie unter AWS-Service -Endpunkte in der Allgemeine AWS-Referenz.

Service Level Agreement (SLA)

Eine Vereinbarung, in der klargestellt wird, was ein IT-Team seinen Kunden zu bieten verspricht, z. B. in Bezug auf Verfügbarkeit und Leistung der Services.

Service-Level-Indikator (SLI)

Eine Messung eines Leistungsaspekts eines Dienstes, z. B. seiner Fehlerrate, Verfügbarkeit oder Durchsatz.

Service-Level-Ziel (SLO)

Eine Zielkennzahl, die den Zustand eines Dienstes darstellt, gemessen anhand eines Service-Level-Indikators.

Modell der geteilten Verantwortung

Ein Modell, das die Verantwortung beschreibt, mit der Sie gemeinsam AWS für Cloud-Sicherheit und Compliance verantwortlich sind. AWS ist für die Sicherheit der Cloud verantwortlich, während Sie für die Sicherheit in der Cloud verantwortlich sind. Weitere Informationen finden Sie unter Modell der geteilten Verantwortung.

SIEM

Siehe Sicherheitsinformations- und Event-Management-System.

Single Point of Failure (SPOF)

Ein Fehler in einer einzelnen, kritischen Komponente einer Anwendung, der das System stören kann.

SLA

Siehe Service Level Agreement.

SLI

Siehe Service-Level-Indikator.

ALSO

Siehe Service-Level-Ziel.

split-and-seed Modell

Ein Muster für die Skalierung und Beschleunigung von Modernisierungsprojekten. Sobald neue Features und Produktversionen definiert werden, teilt sich das Kernteam auf, um neue Produktteams zu bilden. Dies trägt zur Skalierung der Fähigkeiten und Services Ihrer Organisation bei, verbessert die Produktivität der Entwickler und unterstützt schnelle Innovationen. Weitere Informationen finden Sie unter Schrittweiser Ansatz zur Modernisierung von Anwendungen in der AWS Cloud.

SPOTTEN

Siehe Single Point of Failure.

Sternschema

Eine Datenbank-Organisationsstruktur, die eine große Faktentabelle zum Speichern von Transaktions- oder Messdaten und eine oder mehrere kleinere dimensionale Tabellen zum Speichern von Datenattributen verwendet. Diese Struktur ist für die Verwendung in einem Data Warehouse oder für Business Intelligence-Zwecke konzipiert.

Strangler-Fig-Muster

Ein Ansatz zur Modernisierung monolithischer Systeme, bei dem die Systemfunktionen schrittweise umgeschrieben und ersetzt werden, bis das Legacy-System außer Betrieb genommen werden kann. Dieses Muster verwendet die Analogie einer Feigenrebe, die zu einem etablierten Baum heranwächst und schließlich ihren Wirt überwindet und ersetzt. Das Muster wurde eingeführt von Martin Fowler als Möglichkeit, Risiken beim Umschreiben monolithischer Systeme zu managen. Ein Beispiel für die Anwendung dieses Musters finden Sie unter Schrittweises Modernisieren älterer Microsoft ASP.NET (ASMX)-Webservices mithilfe von Containern und Amazon API Gateway.

Subnetz

Ein Bereich von IP-Adressen in Ihrer VPC. Ein Subnetz muss sich in einer einzigen Availability Zone befinden.

Aufsichtskontrolle und Datenerfassung (SCADA)

In der Fertigung ein System, das Hardware und Software zur Überwachung von Sachanlagen und Produktionsabläufen verwendet.

Symmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der denselben Schlüssel zum Verschlüsseln und Entschlüsseln der Daten verwendet.

synthetisches Testen

Testen eines Systems auf eine Weise, die Benutzerinteraktionen simuliert, um potenzielle Probleme zu erkennen oder die Leistung zu überwachen. Sie können Amazon CloudWatch Synthetics verwenden, um diese Tests zu erstellen.

Systemaufforderung

Eine Technik, mit der einem LLM Kontext, Anweisungen oder Richtlinien zur Verfügung gestellt werden, um sein Verhalten zu steuern. Systemaufforderungen helfen dabei, den Kontext festzulegen und Regeln für Interaktionen mit Benutzern festzulegen.

T

tags

Schlüssel-Wert-Paare, die als Metadaten für die Organisation Ihrer Ressourcen dienen. AWS Mit Tags können Sie Ressourcen verwalten, identifizieren, organisieren, suchen und filtern. Weitere Informationen finden Sie unter Markieren Ihrer AWS -Ressourcen.

Zielvariable

Der Wert, den Sie in überwachtem ML vorhersagen möchten. Dies wird auch als Ergebnisvariable bezeichnet. In einer Fertigungsumgebung könnte die Zielvariable beispielsweise ein Produktfehler sein.

Aufgabenliste

Ein Tool, das verwendet wird, um den Fortschritt anhand eines Runbooks zu verfolgen. Eine Aufgabenliste enthält eine Übersicht über das Runbook und eine Liste mit allgemeinen Aufgaben, die erledigt werden müssen. Für jede allgemeine Aufgabe werden der geschätzte Zeitaufwand, der Eigentümer und der Fortschritt angegeben.

Testumgebungen

Siehe Umgebung.

Training

Daten für Ihr ML-Modell bereitstellen, aus denen es lernen kann. Die Trainingsdaten müssen die richtige Antwort enthalten. Der Lernalgorithmus findet Muster in den Trainingsdaten, die die Attribute der Input-Daten dem Ziel (die Antwort, die Sie voraussagen möchten) zuordnen. Es gibt ein ML-Modell aus, das diese Muster erfasst. Sie können dann das ML-Modell verwenden, um Voraussagen für neue Daten zu erhalten, bei denen Sie das Ziel nicht kennen.

Transit-Gateway

Ein Netzwerk-Transit-Hub, über den Sie Ihre Netzwerke VPCs und Ihre lokalen Netzwerke miteinander verbinden können. Weitere Informationen finden Sie in der Dokumentation unter Was ist ein Transit-Gateway. AWS Transit Gateway

Stammbasierter Workflow

Ein Ansatz, bei dem Entwickler Feature lokal in einem Feature-Zweig erstellen und testen und diese Änderungen dann im Hauptzweig zusammenführen. Der Hauptzweig wird dann sequentiell für die Entwicklungs-, Vorproduktions- und Produktionsumgebungen erstellt.

Vertrauenswürdiger Zugriff

Gewährung von Berechtigungen für einen Dienst, den Sie angeben, um Aufgaben in Ihrer Organisation AWS Organizations und in deren Konten in Ihrem Namen auszuführen. Der vertrauenswürdige Service erstellt in jedem Konto eine mit dem Service verknüpfte Rolle, wenn diese Rolle benötigt wird, um Verwaltungsaufgaben für Sie auszuführen. Weitere Informationen finden Sie in der AWS Organizations Dokumentation unter Verwendung AWS Organizations mit anderen AWS Diensten.

Optimieren

Aspekte Ihres Trainingsprozesses ändern, um die Genauigkeit des ML-Modells zu verbessern. Sie können das ML-Modell z. B. trainieren, indem Sie einen Beschriftungssatz generieren, Beschriftungen hinzufügen und diese Schritte dann mehrmals unter verschiedenen Einstellungen wiederholen, um das Modell zu optimieren.

Zwei-Pizzen-Team

Ein kleines DevOps Team, das Sie mit zwei Pizzen ernähren können. Eine Teamgröße von zwei Pizzen gewährleistet die bestmögliche Gelegenheit zur Zusammenarbeit bei der Softwareentwicklung.

U

Unsicherheit

Ein Konzept, das sich auf ungenaue, unvollständige oder unbekannte Informationen bezieht, die die Zuverlässigkeit von prädiktiven ML-Modellen untergraben können. Es gibt zwei Arten von Unsicherheit: Epistemische Unsicherheit wird durch begrenzte, unvollständige Daten verursacht, wohingegen aleatorische Unsicherheit durch Rauschen und Randomisierung verursacht wird, die in den Daten liegt. Weitere Informationen finden Sie im Leitfaden Quantifizieren der Unsicherheit in Deep-Learning-Systemen.

undifferenzierte Aufgaben

Diese Arbeit wird auch als Schwerstarbeit bezeichnet. Dabei handelt es sich um Arbeiten, die zwar für die Erstellung und den Betrieb einer Anwendung erforderlich sind, aber dem Endbenutzer keinen direkten Mehrwert bieten oder keinen Wettbewerbsvorteil bieten. Beispiele für undifferenzierte Aufgaben sind Beschaffung, Wartung und Kapazitätsplanung.

höhere Umgebungen

Siehe Umgebung.

V

Vacuuming

Ein Vorgang zur Datenbankwartung, bei dem die Datenbank nach inkrementellen Aktualisierungen bereinigt wird, um Speicherplatz zurückzugewinnen und die Leistung zu verbessern.

Versionskontrolle

Prozesse und Tools zur Nachverfolgung von Änderungen, z. B. Änderungen am Quellcode in einem Repository.

VPC-Peering

Eine Verbindung zwischen zwei VPCs , die es Ihnen ermöglicht, den Verkehr mithilfe privater IP-Adressen weiterzuleiten. Weitere Informationen finden Sie unter Was ist VPC-Peering? in der Amazon-VPC-Dokumentation.

Schwachstelle

Ein Software- oder Hardwarefehler, der die Sicherheit des Systems beeinträchtigt.

W

Warmer Cache

Ein Puffer-Cache, der aktuelle, relevante Daten enthält, auf die häufig zugegriffen wird. Die Datenbank-Instance kann aus dem Puffer-Cache lesen, was schneller ist als das Lesen aus dem Hauptspeicher oder von der Festplatte.

warme Daten

Daten, auf die selten zugegriffen wird. Bei der Abfrage dieser Art von Daten sind mäßig langsame Abfragen in der Regel akzeptabel.

Fensterfunktion

Eine SQL-Funktion, die eine Berechnung für eine Gruppe von Zeilen durchführt, die sich in irgendeiner Weise auf den aktuellen Datensatz beziehen. Fensterfunktionen sind nützlich für die Verarbeitung von Aufgaben wie die Berechnung eines gleitenden Durchschnitts oder für den Zugriff auf den Wert von Zeilen auf der Grundlage der relativen Position der aktuellen Zeile.

Workload

Ein Workload ist eine Sammlung von Ressourcen und Code, die einen Unternehmenswert bietet, wie z. B. eine kundenorientierte Anwendung oder ein Backend-Prozess.

Workstream

Funktionsgruppen in einem Migrationsprojekt, die für eine bestimmte Reihe von Aufgaben verantwortlich sind. Jeder Workstream ist unabhängig, unterstützt aber die anderen Workstreams im Projekt. Der Portfolio-Workstream ist beispielsweise für die Priorisierung von Anwendungen, die Wellenplanung und die Erfassung von Migrationsmetadaten verantwortlich. Der Portfolio-Workstream liefert diese Komponenten an den Migrations-Workstream, der dann die Server und Anwendungen migriert.

WURM

Sehen Sie einmal schreiben, viele lesen.

WQF

Siehe AWS Workload-Qualifizierungsrahmen.

einmal schreiben, viele lesen (WORM)

Ein Speichermodell, das Daten ein einziges Mal schreibt und verhindert, dass die Daten gelöscht oder geändert werden. Autorisierte Benutzer können die Daten so oft wie nötig lesen, aber sie können sie nicht ändern. Diese Datenspeicherinfrastruktur gilt als unveränderlich.

Z

Zero-Day-Exploit

Ein Angriff, in der Regel Malware, der eine Zero-Day-Sicherheitslücke ausnutzt.

Zero-Day-Sicherheitslücke

Ein unfehlbarer Fehler oder eine Sicherheitslücke in einem Produktionssystem. Bedrohungsakteure können diese Art von Sicherheitslücke nutzen, um das System anzugreifen. Entwickler werden aufgrund des Angriffs häufig auf die Sicherheitsanfälligkeit aufmerksam.

Zero-Shot-Aufforderung

Bereitstellung von Anweisungen für die Ausführung einer Aufgabe an einen LLM, jedoch ohne Beispiele (Schnappschüsse), die ihm als Orientierungshilfe dienen könnten. Der LLM muss sein vortrainiertes Wissen einsetzen, um die Aufgabe zu bewältigen. Die Effektivität von Zero-Shot Prompting hängt von der Komplexität der Aufgabe und der Qualität der Aufforderung ab. Siehe auch Few-Shot-Prompting.

Zombie-Anwendung

Eine Anwendung, deren durchschnittliche CPU- und Arbeitsspeichernutzung unter 5 Prozent liegt. In einem Migrationsprojekt ist es üblich, diese Anwendungen außer Betrieb zu nehmen.

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.