AWS Sicherheitsreferenzarchitektur (AWS SRA) — Kernarchitektur

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: AWS Sicherheitsreferenzarchitektur (AWS SRA) — Kernarchitektur

Table of Contents

AWS Sicherheitsreferenzarchitektur (AWS SRA) — Kernarchitektur

Sicherheitsteam von Global Services, Amazon Web Services (Mitwirkende)

Dezember 2025 (Geschichte des Dokuments)

Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

Die Amazon Web Services (AWS) Security Reference Architecture (AWS SRA) ist ein ganzheitlicher Satz von Richtlinien für die Bereitstellung aller AWS Sicherheitsdienste in einer Umgebung mit mehreren Konten. Verwenden Sie sie, um AWS Sicherheitsdienste so zu konzipieren, zu implementieren und zu verwalten, dass sie den AWS empfohlenen Verfahren entsprechen. Die Empfehlungen basieren auf einer einseitigen Architektur, die AWS Sicherheitsdienste umfasst. Dabei geht es darum, wie diese zur Erreichung von Sicherheitszielen beitragen, wo sie in Ihrem AWS-Konten Unternehmen am besten eingesetzt und verwaltet werden können und wie sie mit anderen Sicherheitsdiensten interagieren. Diese allgemeinen Architekturrichtlinien ergänzen detaillierte, dienstspezifische Empfehlungen, wie sie beispielsweise auf der Website zur AWS Sicherheitsdokumentation zu finden sind.

Die Architektur und die dazugehörigen Empfehlungen basieren auf unseren gemeinsamen Erfahrungen mit AWS Unternehmenskunden. Bei diesem Dokument handelt es sich um eine Referenz — eine umfassende Anleitung AWS-Services zur Sicherung einer bestimmten Umgebung. Die Lösungsmuster im AWS SRA-Code-Repository wurden für die spezifische Architektur entwickelt, die in dieser Referenz dargestellt wird. Jeder Kunde wird unterschiedliche Anforderungen haben. Daher kann das Design Ihrer AWS Umgebung von den hier aufgeführten Beispielen abweichen. Sie müssen diese Empfehlungen modifizieren und an Ihre individuellen Umgebungs- und Sicherheitsanforderungen anpassen. Im gesamten Dokument schlagen wir gegebenenfalls Optionen für häufig auftretende alternative Szenarien vor.

Die AWS SRA ist eine lebendige Leitlinie und wird regelmäßig auf der Grundlage neuer Service- und Funktionsversionen, Kundenfeedback und der sich ständig ändernden Bedrohungslandschaft aktualisiert. Jedes Update enthält das Revisionsdatum und das zugehörige Änderungsprotokoll.

Obwohl wir uns auf ein einseitiges Diagramm als Grundlage verlassen, geht die Architektur tiefer als ein einzelnes Blockdiagramm und muss auf einer gut strukturierten Grundlage von Grundlagen und Sicherheitsprinzipien aufbauen. Sie können dieses Dokument auf zwei Arten verwenden: als Erläuterung oder als Referenz. Die Themen sind als Geschichte organisiert, sodass Sie sie von Anfang (grundlegende Sicherheitsrichtlinien) bis zum Ende (Diskussion von Codebeispielen, die Sie implementieren können) lesen können. Sie können sich auch im Dokument umsehen, um sich auf die Sicherheitsprinzipien, Dienste, Kontotypen, Anleitungen und Beispiele zu konzentrieren, die für Ihre Bedürfnisse am relevantesten sind.

Dieses Dokument ist in die folgenden Abschnitte und einen Anhang unterteilt:

- Die Bibliothek „Über die AWS SRA“ bietet einen Überblick über die technischen Leitlinien und Codes, die in der AWS SRA-Publikationssammlung enthalten sind.
- Der Wert des AWS SRA beschreibt die Beweggründe für den Aufbau des AWS SRA, beschreibt, wie Sie ihn zur Verbesserung Ihrer Sicherheit einsetzen können, und listet die wichtigsten Erkenntnisse auf.
- Security Foundations überprüft das AWS Cloud Adoption Framework (AWS CAF), das AWS Well-Architected Framework und das AWS Shared Responsibility Model und hebt Elemente hervor, die für die SRA besonders relevant sind. AWS
- AWS Organizations, accounts, and IAM guardrails stellt den AWS Organizations Service vor, erläutert die grundlegenden Sicherheitsfunktionen und Schutzmaßnahmen und gibt einen Überblick über unsere empfohlene Multi-Account-Strategie.
- Bei der AWS Sicherheitsreferenzarchitektur handelt es sich um ein einseitiges Architekturdiagramm, das Funktionen und Sicherheitsdienste und -funktionen zeigt AWS-Konten, die allgemein verfügbar sind.
- KI/ML für Sicherheit beschreibt, wie verschiedene Unternehmen künstliche Intelligenz und maschinelles Lernen (KI/ML) im Hintergrund AWS-Services einsetzen, um Sie beim Erreichen bestimmter Sicherheitsziele zu unterstützen. Sie können diese AWS-Services in Ihr Design einbeziehen, um die Vorteile erweiterter Sicherheitsfunktionen zu nutzen.
- Aufbau Ihrer Sicherheitsarchitektur – Ein schrittweiser Ansatz bietet Anleitungen dazu, wie Sie Ihre eigene Sicherheitsarchitektur in sechs iterativen Phasen aufbauen können, und zwar auf der Grundlage der von der SRA bereitgestellten Referenz. AWS
- AWS Die SRA-Checkliste für bewährte Methoden fasst die im Leitfaden erörterten Empfehlungen in einer Checkliste zusammen, die Sie bei der Erstellung Ihrer Version der Sicherheitsarchitektur befolgen können.

- Die IAM-Ressourcen enthalten eine Zusammenfassung und eine Reihe von Hinweisen für AWS Identity and Access Management (IAM) -Anleitungen, die für Ihre Sicherheitsarchitektur wichtig sind.
- Das Code-Repository für AWS SRA-Beispiele bietet einen Überblick über das zugehörige GitHub Repository, das Entwicklern und Ingenieuren bei der Implementierung einiger der in diesem Dokument vorgestellten Anleitungen und Architekturmuster hilft. Sie können die Beispiele mithilfe von AWS CloudFormation oder Terraform von bereitstellen. HashiCorp Sie unterstützen sowohl Umgebungen als AWS Control Tower auch Umgebungen anderer Art.AWS Control Tower

Der Anhang enthält eine Liste der einzelnen AWS Sicherheits-, Identitäts- und Compliance-Dienste sowie Links zu weiteren Informationen zu den einzelnen Diensten. Der Abschnitt Dokumentenverlauf enthält ein Änderungsprotokoll zur Nachverfolgung der Versionen dieses Dokuments. Sie können auch einen RSS-Feed für Änderungsbenachrichtigungen abonnieren.

Über die AWS SRA-Bibliothek

Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

Dieser Leitfaden ist Teil einer Bibliothek, die Architekturentwürfe und technische Anleitungen für den Entwurf und Aufbau von Sicherheitsarchitekturen enthält. AWS Die Bibliothek besteht aus Implementierungscode (AWS SRA-Codebibliothek), einem Validierungstool (SRA Verify) und zwei sich ergänzenden Kategorien von Leitfäden, die sich mit der Kernarchitektur und den tiefgreifenden Architekturen befassen.

AWS SRA — Kernarchitektur (dieser Leitfaden)

Dieses Handbuch stellt eine Grundlage für die empfohlene AWS Sicherheitsarchitektur dar. Es ist der Ausgangspunkt, der für alle Organisationen gilt, unabhängig von ihrer Branche, ihrem Anwendungstyp oder anderen Überlegungen. Diese Grundlage hilft Ihnen beim Aufbau einer starken und skalierbaren Architektur AWS und hilft Ihnen, eine solide Sicherheitsbasis für AWS mehrere Konten zu schaffen, die sicher skaliert werden kann, wenn Ihr Unternehmen wächst.

AWS SRA — tiefgründige Architekturen

Der AWS SRA — Core Architecture Guide wird durch zusätzliche Veröffentlichungen ergänzt, die Architekturmuster enthalten, die auf spezifische Sicherheitsfunktionen, Anwendungstypen und Compliance- oder regulatorische Anforderungen zugeschnitten sind. Diese Muster erweitern die Kernarchitektur und sollten in Verbindung mit dem AWS SRA — Core Architecture Guide verwendet werden.

Die folgenden Leitfäden enthalten Architekturmuster, die auf bestimmte Sicherheitsfunktionen zugeschnitten sind:

- AWS SRA — Identity Management bietet Anleitungen zur Implementierung einer skalierbaren, robusten und zentralisierten Identitäts- und Zugriffsmanagementlösung auf AWS.
- AWS In SRA — Perimeter Security werden Architekturmuster und AWS-Services die Implementierung von Edge-Sicherheit in einem zentralen Konto oder in einzelnen Konten erörtert.
- AWS SRA — Cyberforensik beschreibt die Konfiguration eines AWS Forensik-Accounts als Ausgangspunkt für die Entwicklung der forensischen Fähigkeiten Ihres Unternehmens und zur Verbesserung der Vorbereitung auf Sicherheitsvorfälle (IR).

Die folgenden Leitfäden enthalten Architekturmuster für bestimmte Anwendungstypen. Möglicherweise möchten Sie sich nach dem Aufbau Ihrer grundlegenden Sicherheitsarchitektur auf diese konzentrieren:

- AWS SRA — KI-Sicherheit bietet Empfehlungen zur Sicherheitsarchitektur für das Entwerfen und Erstellen von Anwendungen, die generative KI-Funktionen mithilfe AWS generativer KI-Services integrieren.
- AWS SRA — IoT bietet Empfehlungen zur Sicherheitsarchitektur für das Design und den Aufbau von IoT-Anwendungen. AWS

Darüber hinaus beschreibt der folgende Leitfaden Architekturmuster, die auf bestimmte Compliance- oder regulatorische Rahmenbedingungen abgestimmt sind:

- AWS Die Privacy Reference Architecture (AWS PRA) bietet eine Sicherheitsarchitektur für Anwendungen, die personenbezogene Daten verarbeiten und umfassende Datenschutzanforderungen wie die Allgemeine Datenschutzverordnung (DSGVO), den California Consumer Privacy Act (CCPA) oder das brasilianische Allgemeine Datenschutzgesetz (LGPD) erfüllen müssen. Die AWS PRA enthält eine Reihe von Richtlinien, die sich speziell auf das Design und die Konfiguration der Datenschutzkontrollen in beziehen. AWS-Services

Wir empfehlen Ihnen, mit dem AWS SRA-Leitfaden zur Kernarchitektur zu beginnen, um die grundlegende Architektur zu verstehen, und dann die ergänzenden Leitfäden zu lesen, um erweiterte Funktionen und Implementierungen zu nutzen. Weitere Informationen zu diesem Inhaltssatz finden Sie unter AWS Sicherheitsreferenzarchitektur.

> **Architekturdiagramme**
>
> Um die Referenzarchitekturdiagramme in der AWS SRA-Bibliothek an Ihre Geschäftsanforderungen anzupassen, können Sie die folgende ZIP-Datei herunterladen und ihren Inhalt extrahieren.
>
> Laden Sie die Quelldatei des Diagramms herunter (PowerPointMicrosoft-Format)

Der Wert der AWS SRA

Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

AWS verfügt über ein umfangreiches (und wachsendes) Angebot an sicherheits- und sicherheitsbezogenen Diensten. Kunden haben sich für die detaillierten Informationen, die in unseren Servicedokumentationen, Blogbeiträgen, Tutorials, Gipfeltreffen und Konferenzen verfügbar sind, sehr geschätzt. Sie sagen uns auch, dass sie das Gesamtbild besser verstehen und sich einen strategischen Überblick über AWS Sicherheitsdienste verschaffen möchten. Wenn wir mit Kunden zusammenarbeiten, um ein tieferes Verständnis für ihre Bedürfnisse zu erlangen, ergeben sich drei Prioritäten:

- Kunden wünschen sich mehr Informationen und empfohlene Muster, wie sie die AWS Sicherheitsdienste ganzheitlich bereitstellen, konfigurieren und betreiben können. Für welche Konten und im Hinblick auf welche Sicherheitsziele sollten die Services bereitgestellt und verwaltet werden? Gibt es ein Sicherheitskonto, für das alle oder die meisten Dienste ausgeführt werden sollen? Wie beeinflusst die Wahl des Standorts (Organisationseinheit oder AWS-Konto) die Sicherheitsziele? Welche Kompromisse (Designüberlegungen) sollten sich Kunden bewusst sein?
- Kunden sind daran interessiert, die vielen Sicherheitsdienste aus unterschiedlichen Perspektiven logisch zu organisieren. AWS Neben der Hauptfunktion der einzelnen Dienste (z. B. Identitätsdienste oder Protokollierungsdienste) helfen diese alternativen Sichtweisen den Kunden bei der Planung, Gestaltung und Implementierung ihrer Sicherheitsarchitektur. Ein Beispiel, das weiter unten in diesem Dokument vorgestellt wird, gruppiert die Dienste anhand der Schutzebenen, die auf die empfohlene Struktur Ihrer AWS Umgebung abgestimmt sind.
- Kunden suchen nach Anleitungen und Beispielen, um Sicherheitsdienste so effektiv wie möglich zu integrieren. Wie sollten sie beispielsweise am besten auf andere Dienste abstimmen und sich AWS Config mit ihnen verbinden, um die Schwerstarbeit bei automatisierten Audit- und Monitoring-Pipelines zu erledigen? Kunden fragen nach Informationen darüber, wie sich die einzelnen AWS Sicherheitsdienste auf andere Sicherheitsdienste verlassen oder diese unterstützen.

In der AWS SRA gehen wir auf jedes dieser Probleme ein. Die erste Priorität in der Liste (wo die Dinge hingehören) ist der Schwerpunkt des Hauptarchitekturdiagramms und der begleitenden Diskussionen in diesem Dokument. Wir bieten eine empfohlene AWS Organizations Architektur

und eine account-by-account Beschreibung, welche Dienste wo eingesetzt werden. Um mit der zweiten Priorität in der Liste zu beginnen (wie man sich die gesamte Palette von Sicherheitsdiensten vorstellen kann), lesen Sie den Abschnitt Sicherheitsdienste in Ihrer gesamten AWS Organisation anwenden. In diesem Abschnitt wird beschrieben, wie Sie Sicherheitsdienste entsprechend der Struktur der Elemente in Ihrer AWS Organisation gruppieren können. Darüber hinaus spiegeln sich dieselben Ideen in der Diskussion über das Anwendungskonto wider, in der hervorgehoben wird, wie Sicherheitsdienste so betrieben werden können, dass sie sich auf bestimmte Ebenen des Kontos konzentrieren: Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Amazon Virtual Private Cloud (Amazon VPC) -Netzwerke und das breitere Konto. Schließlich spiegelt sich die dritte Priorität (Serviceintegration) in der gesamten Anleitung wider — insbesondere in der Erörterung einzelner Dienste in den ausführlichen Leitfäden in der AWS SRA-Bibliothek und des Codes im AWS SRA-Code-Repository.

AWS Wie benutzt man den SRA

Es gibt verschiedene Möglichkeiten, die AWS SRA zu nutzen, je nachdem, an welcher Stelle Sie sich auf Ihrem Weg zur Cloud-Einführung befinden. Im Folgenden finden Sie eine Liste von Möglichkeiten, wie Sie die besten Erkenntnisse aus den AWS SRA-Ressourcen gewinnen können (Architekturdiagramm, schriftliche Anleitungen und Codebeispiele).

- Definieren Sie den Zielstatus für Ihre eigene Sicherheitsarchitektur.

  Ganz gleich, ob Sie Ihre AWS Cloud Reise gerade erst beginnen — Ihre ersten Konten einrichten — oder planen, eine bestehende AWS Umgebung zu verbessern, die AWS SRA ist der richtige Ort, um mit dem Aufbau Ihrer Sicherheitsarchitektur zu beginnen. Beginnen Sie mit einer umfassenden Grundlage für Kontostruktur und Sicherheitsservices und passen Sie diese dann auf der Grundlage Ihres speziellen Technologie-Stacks, Ihrer Fähigkeiten, Sicherheitsziele und Compliance-Anforderungen an. Wenn Sie wissen, dass Sie mehr Workloads erstellen und auf den Markt bringen werden, können Sie Ihre maßgeschneiderte Version der AWS SRA als Grundlage für die Sicherheitsreferenzarchitektur Ihres Unternehmens verwenden. Informationen dazu, wie Sie den in der AWS SRA beschriebenen Zielzustand erreichen können, finden Sie im Abschnitt Aufbau Ihrer Sicherheitsarchitektur — Ein schrittweiser Ansatz.
- Überprüfen (und überarbeiten) Sie die Designs und Funktionen, die Sie bereits implementiert haben.

  Wenn Sie bereits über ein Sicherheitsdesign und eine Implementierung verfügen, lohnt es sich, sich etwas Zeit zu nehmen, um das, was Sie haben, mit dem AWS SRA zu vergleichen. Das

AWS SRA ist umfassend konzipiert und bietet eine diagnostische Grundlage für die Überprüfung Ihrer eigenen Sicherheit. Wenn Ihre Sicherheitsentwürfe mit dem AWS SRA übereinstimmen, können Sie sich darauf verlassen, dass Sie bei der Verwendung bewährte Verfahren befolgen. AWS-Services Wenn Ihre Sicherheitsentwürfe von den Richtlinien der AWS SRA abweichen oder sogar nicht mit ihnen übereinstimmen, ist dies nicht unbedingt ein Zeichen dafür, dass Sie etwas falsch machen. Stattdessen bietet Ihnen diese Beobachtung die Möglichkeit, Ihren Entscheidungsprozess zu überprüfen. Es gibt legitime geschäftliche und technologische Gründe, warum Sie von den Best Practices der AWS SRA abweichen könnten. Möglicherweise erfordern Ihre speziellen Compliance-, behördlichen oder organisatorischen Sicherheitsanforderungen spezifische Servicekonfigurationen. Oder Sie haben möglicherweise eine bevorzugte Funktion für ein Produkt aus der AWS Partner Network oder eine benutzerdefinierte Anwendung, die Sie erstellt und verwaltet haben, anstatt sie zu verwenden AWS-Services. Manchmal stellen Sie bei dieser Überprüfung fest, dass Ihre früheren Entscheidungen auf der Grundlage älterer Technologien, AWS Funktionen oder geschäftlicher Einschränkungen getroffen wurden, die nicht mehr gelten. Dies ist eine gute Gelegenheit, alle Aktualisierungen zu überprüfen, zu priorisieren und sie an der entsprechenden Stelle Ihres technischen Backlogs hinzuzufügen. Was auch immer Sie bei der Bewertung Ihrer Sicherheitsarchitektur im Lichte der AWS SRA entdecken, Sie werden es als wertvoll erachten, diese Analyse zu dokumentieren. Diese historischen Aufzeichnungen von Entscheidungen und ihren Begründungen können dazu beitragen, future Entscheidungen zu fundieren und zu priorisieren.

- Starten Sie die Implementierung Ihrer eigenen Sicherheitsarchitektur.

  Die AWS SRA-Module (Infrastructure as Code, IaC) bieten eine schnelle und zuverlässige Möglichkeit, mit dem Aufbau und der Implementierung Ihrer Sicherheitsarchitektur zu beginnen. Diese Module werden im Abschnitt Code-Repository und im öffentlichen GitHub_Repository ausführlicher beschrieben. Sie ermöglichen es den Technikern nicht nur, auf qualitativ hochwertigen Beispielen für die Muster in den AWS SRA-Leitlinien aufzubauen, sondern enthalten auch empfohlene Sicherheitskontrollen wie IAM-Passwortrichtlinien, den öffentlichen Zugriff von Amazon Simple Storage Service (Amazon S3) für Sperrkonten, die EC2 standardmäßige Amazon Elastic Block Store (Amazon EBS) -Verschlüsselung und die Integration mit, AWS Control Tower sodass die Kontrollen angewendet oder entfernt werden, wenn neue Geräte integriert oder außer Betrieb genommen AWS-Konten werden.
- Erfahren Sie mehr über Sicherheitsdienste und Funktionen. AWS

  Die Anleitungen und Diskussionen in der AWS SRA beinhalten wichtige Funktionen sowie Überlegungen zur Bereitstellung und Verwaltung einzelner sicherheits- und AWS sicherheitsrelevanter Dienste. Ein Merkmal des AWS SRA besteht darin, dass es eine allgemeine

Einführung in die Breite der AWS Sicherheitsdienste und deren Zusammenarbeit in einer Umgebung mit mehreren Konten bietet. Dies ergänzt die eingehende Untersuchung der Funktionen und der Konfiguration der einzelnen Dienste, die in anderen Quellen zu finden sind. Ein Beispiel hierfür ist die Diskussion darüber, wie AWS Security Hub Cloud Security Posture Management (AWS Security Hub CSPM) Sicherheitsergebnisse aus einer Vielzahl von AWS-Services AWS Partner Produkten und sogar aus Ihren eigenen Anwendungen aufnimmt.

- Fördern Sie eine Diskussion über Unternehmensführung und Sicherheitsverantwortung.

  Ein wichtiges Element bei der Gestaltung und Implementierung einer Sicherheitsarchitektur oder -strategie ist es, zu verstehen, wer in Ihrem Unternehmen welche sicherheitsbezogenen Verantwortlichkeiten hat. Beispielsweise hängt die Frage, wo die Sicherheitsergebnisse zusammengefasst und überwacht werden sollen, mit der Frage zusammen, welches Team für diese Aktivität verantwortlich sein wird. Werden alle Ergebnisse unternehmensweit von einem zentralen Team überwacht, das Zugriff auf ein spezielles Security Tooling-Konto benötigt? Oder sind einzelne Anwendungsteams (oder Geschäftsbereiche) für bestimmte Überwachungsaktivitäten verantwortlich und benötigen daher Zugriff auf bestimmte Alarm- und Überwachungstools? Ein weiteres Beispiel: Wenn Ihre Organisation über eine Gruppe verfügt, die alle Verschlüsselungsschlüssel zentral verwaltet, hat dies Einfluss darauf, wer berechtigt ist, Schlüssel AWS Key Management Service (AWS KMS) zu erstellen, und in welchen Konten diese Schlüssel verwaltet werden. Wenn Sie die Merkmale Ihres Unternehmens — die verschiedenen Teams und Zuständigkeiten — kennen, können Sie die SRA besser an Ihre Bedürfnisse anpassen. AWS Umgekehrt wird manchmal die Diskussion über die Sicherheitsarchitektur zum Anstoß, um die bestehenden organisatorischen Verantwortlichkeiten zu erörtern und mögliche Änderungen in Betracht zu ziehen. AWS empfiehlt einen dezentralen Entscheidungsprozess, bei dem die Workload-Teams dafür verantwortlich sind, die Sicherheitskontrollen auf der Grundlage ihrer Workload-Funktionen und -Anforderungen zu definieren. Das Ziel eines zentralisierten Sicherheits- und Governance-Teams besteht darin, ein System aufzubauen, das es den Workload-Verantwortlichen ermöglicht, fundierte Entscheidungen zu treffen, und das es allen Beteiligten ermöglicht, Einblick in die Konfiguration, Ergebnisse und Ereignisse zu erhalten. Die AWS SRA kann als Instrument zur Identifizierung und Information dieser Diskussionen dienen.

Die wichtigsten Umsetzungsrichtlinien der SRA AWS

Hier sind acht wichtige Erkenntnisse aus der AWS SRA, die Sie bei der Entwicklung und Implementierung Ihrer Sicherheit berücksichtigen sollten.

- AWS Organizations und eine angemessene Strategie für mehrere Konten sind notwendige Elemente Ihrer Sicherheitsarchitektur. Die richtige Trennung von Workloads, Teams und Funktionen bildet die Grundlage für die Trennung von Aufgaben und defense-in-depth Strategien. Der Leitfaden behandelt dies in einem späteren Abschnitt weiter.
- Defense-in-depth ist ein wichtiger Entwurfsaspekt bei der Auswahl von Sicherheitskontrollen für Ihr Unternehmen. Es hilft Ihnen, die entsprechenden Sicherheitskontrollen auf verschiedenen Ebenen der AWS Organizations Struktur zu implementieren, wodurch die Auswirkungen eines Problems minimiert werden: Wenn es ein Problem mit einer Ebene gibt, sind Kontrollen vorhanden, die andere wertvolle IT-Ressourcen isolieren. Die AWS SRA zeigt, wie unterschiedliche AWS-Services Funktionen auf den verschiedenen Ebenen des AWS Technologie-Stacks funktionieren und wie die Kombination dieser Services Ihnen dabei hilft, dies zu erreichen. defense-in-depth Dieses defense-in-depth Konzept AWS wird in einem späteren Abschnitt anhand von Entwurfsbeispielen näher erläutert, die unter Anwendungskonto aufgeführt sind.
- Verwenden Sie die Vielzahl von Sicherheitsbausteinen, die sich über mehrere AWS-Services Funktionen erstrecken, um eine robuste und belastbare Cloud-Infrastruktur aufzubauen. Wenn Sie den AWS SRA an Ihre speziellen Bedürfnisse anpassen, sollten Sie nicht nur die Hauptfunktion AWS-Services und die Hauptmerkmale (z. B. Authentifizierung, Verschlüsselung, Überwachung, Berechtigungsrichtlinien) berücksichtigen, sondern auch, wie diese in die Struktur Ihrer Architektur passen. In einem späteren Abschnitt des Handbuchs wird beschrieben, wie einige Dienste in Ihrem gesamten AWS Unternehmen funktionieren. Andere Dienste funktionieren am besten innerhalb eines einzigen Kontos, und einige sind so konzipiert, dass sie einzelnen Auftraggebern die Erlaubnis erteilen oder verweigern. Die Berücksichtigung dieser beiden Perspektiven hilft Ihnen dabei, einen flexibleren, mehrschichtigen Sicherheitsansatz zu entwickeln.
- Wenn möglich (wie in späteren Abschnitten beschrieben), sollten Sie diese Möglichkeit nutzen, AWS-Services die für jedes Konto bereitgestellt werden kann (verteilt statt zentralisiert), und ein einheitliches Set von gemeinsamen Sicherheitsvorkehrungen einrichten, die dazu beitragen können, Ihre Workloads vor Missbrauch zu schützen und die Auswirkungen von Sicherheitsereignissen zu reduzieren. Die AWS SRA verwendet AWS Security Hub CSPM (zentrale Überwachung und Konformitätsprüfungen), Amazon GuardDuty (Bedrohungserkennung und Erkennung von Anomalien), AWS Config (Ressourcenüberwachung und Änderungserkennung), IAM Access Analyzer (Überwachung des Ressourcenzugriffs), AWS CloudTrail (Protokollierung der Service-API-Aktivitäten in Ihrer gesamten Umgebung) und Amazon Macie (Datenklassifizierung) als Basissatz, der AWS-Services in allen eingesetzt werden kann. AWS-Konto
- Nutzen Sie die Funktion zur delegierten Administration von AWS Organizations, wo sie unterstützt wird, wie später im Abschnitt zur delegierten Administration des Handbuchs erklärt wird. Auf

diese Weise können Sie ein AWS Mitgliedskonto als Administrator für unterstützte Dienste registrieren. Die delegierte Verwaltung bietet den verschiedenen Teams in Ihrem Unternehmen die Flexibilität, je nach ihren Zuständigkeiten separate Konten für die Verwaltung der AWS-Services gesamten Umgebung zu verwenden. Darüber hinaus hilft Ihnen die Verwendung eines delegierten Administrators dabei, den Zugriff auf das AWS Organizations Verwaltungskonto einzuschränken und den damit verbundenen Berechtigungsaufwand zu verwalten.

- Implementieren Sie zentralisierte Überwachung, Verwaltung und Steuerung in Ihren AWS Organisationen. Durch AWS-Services die Verwendung dieser Unterstützung für die Aggregation mehrerer Konten (und manchmal mehrerer Regionen) zusammen mit Funktionen für die delegierte Verwaltung ermöglichen Sie Ihren zentralen Sicherheits-, Netzwerk- und Cloud-Engineering-Teams eine umfassende Transparenz und Kontrolle über die entsprechende Sicherheitskonfiguration und Datenerfassung. Darüber hinaus können die Daten an Workload-Teams zurückgegeben werden, sodass diese zu einem früheren Zeitpunkt im Software Development Lifecycle (SDLC) effektive Sicherheitsentscheidungen treffen können.
- Verwenden Sie AWS Control Tower es, um Ihre AWS Umgebung mit mehreren Konten einzurichten und zu verwalten, indem Sie vorgefertigte Sicherheitskontrollen implementieren, um Ihre Sicherheitsreferenzarchitektur zu starten. AWS Control Tower bietet einen Plan für Identitätsmanagement, Verbundzugriff auf Konten, zentrale Protokollierung und definierte Workflows für die Bereitstellung zusätzlicher Konten. Anschließend können Sie die Customizations for AWS Control Tower (cFCT) -Lösung verwenden, um die von verwalteten Konten AWS Control Tower mit zusätzlichen Sicherheitskontrollen, Servicekonfigurationen und Governance zu versehen, wie das SRA-Code-Repository zeigt. AWS Die Account-Factory-Funktion stellt neuen Konten automatisch konfigurierbare Vorlagen zur Verfügung, die auf der genehmigten Kontokonfiguration basieren, um die Konten innerhalb Ihrer Organisation zu standardisieren. AWS Sie können die Verwaltung auch auf eine bestehende Person ausdehnen, AWS-Konto indem Sie sie in eine Organisationseinheit (OU) eintragen, die bereits verwaltet wird. AWS Control Tower
- Die AWS SRA-Codebeispiele zeigen, wie Sie die Implementierung von Mustern innerhalb des AWS SRA-Leitfadens mithilfe von Infrastructure as Code (IaC) automatisieren können. Durch die Kodifizierung der Muster können Sie IaC wie andere Anwendungen in Ihrem Unternehmen behandeln und Tests automatisieren, bevor Sie Code bereitstellen. IaC trägt auch dazu bei, Konsistenz und Wiederholbarkeit sicherzustellen, indem Guardrails in mehreren (z. B. SDLC- oder regionsspezifischen) Umgebungen bereitgestellt werden. Die SRA-Codebeispiele können in einer Umgebung mit mehreren Konten mit oder ohne bereitgestellt werden. AWS Organizations AWS Control Tower Die erforderlichen Lösungen in diesem Repository AWS Control Tower wurden in einer AWS Control Tower Umgebung bereitgestellt und getestet, in der CfCT AWS Control Tower (Customizations for) verwendet AWS CloudFormation wurde. Lösungen, die dies nicht erfordern

AWS Control Tower , wurden in einer AWS Organizations Umgebung getestet, indem AWS CloudFormation Wenn Sie dies nicht tun AWS Control Tower, können Sie die AWS Organizations basierte Bereitstellungslösung verwenden.

Sicherheitsgrundlagen

Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

Die AWS SRA orientiert sich an drei AWS Sicherheitsgrundlagen: dem AWS Cloud Adoption Framework (AWS CAF), AWS Well-Architected und dem Shared Responsibility Model. AWS

AWS Professional Services hat das AWS CAF ins Leben gerufen, um Unternehmen dabei zu unterstützen, einen beschleunigten Weg zur erfolgreichen Cloud-Einführung zu entwickeln und zu beschreiten. Die im Framework enthaltenen Anleitungen und bewährten Verfahren helfen Ihnen dabei, einen umfassenden Ansatz für Cloud Computing in Ihrem gesamten Unternehmen und während Ihres gesamten IT-Lebenszyklus zu entwickeln. Die AWS CAF unterteilt die Leitlinien in sechs Schwerpunktbereiche, die als Perspektiven bezeichnet werden. Jede Perspektive deckt unterschiedliche Zuständigkeiten ab, die funktionsbezogenen Interessengruppen obliegen oder von diesen verwaltet werden. Im Allgemeinen konzentrieren sich die Aspekte Geschäft, Mitarbeiter und Unternehmensführung auf die Geschäftsfähigkeiten, wohingegen sich die Plattform-, Sicherheits- und Betriebsperspektiven auf technische Fähigkeiten konzentrieren.

Die Sicherheitsperspektive der AWS CAF hilft Ihnen dabei, die Auswahl und Implementierung von Kontrollen in Ihrem gesamten Unternehmen zu strukturieren. Die Einhaltung der aktuellen AWS Empfehlungen im Bereich Sicherheit kann Ihnen dabei helfen, Ihre geschäftlichen und regulatorischen Anforderungen zu erfüllen.

AWS Well-Architected unterstützt Cloud-Architekten beim Aufbau einer sicheren, leistungsstarken, belastbaren und effizienten Infrastruktur für ihre Anwendungen und Workloads. Das Framework basiert auf sechs Säulen — betriebliche Exzellenz, Sicherheit, Zuverlässigkeit, Leistungseffizienz, Kostenoptimierung und Nachhaltigkeit — und bietet AWS Kunden und Partnern einen konsistenten Ansatz zur Bewertung von Architekturen und zur Implementierung von Designs, die sich im Laufe der Zeit skalieren lassen. Wir sind der Meinung, dass eine gute Workload-Architektur die Wahrscheinlichkeit für den geschäftlichen Erfolg deutlich erhöht.

In der Sicherheitssäule Well-Architected Framework wird beschrieben, wie Sie Cloud-Technologien nutzen können, um Daten, Systeme und Ressourcen so zu schützen, dass Ihre Sicherheitslage verbessert werden kann. Auf diese Weise können Sie Ihre geschäftlichen und behördlichen Anforderungen erfüllen, indem Sie die aktuellen AWS Empfehlungen befolgen. Es gibt weitere

Schwerpunktbereiche von Well-Architected Framework, die mehr Kontext für bestimmte Bereiche wie Governance, Serverless, KI/ML und Gaming bieten. Diese Objektive werden als AWS Well-Architected-Objektive bezeichnet.

Sicherheit und Compliance liegen in der gemeinsamen Verantwortung des AWS Kunden. Dieses gemeinsame Modell kann Ihnen helfen, Ihre betriebliche Belastung zu verringern, da AWS es die Komponenten vom Host-Betriebssystem und der Virtualisierungsebene bis hin zur physischen Sicherheit der Einrichtungen betreibt, verwaltet und kontrolliert, in denen der Service betrieben wird. Sie übernehmen beispielsweise die Verantwortung und Verwaltung des Gastbetriebssystems (einschließlich Updates und Sicherheitspatches), der Anwendungssoftware, der serverseitigen Datenverschlüsselung, der Routing-Tabellen für den Netzwerkverkehr und der Konfiguration der AWS bereitgestellten Sicherheitsgruppen-Firewall. Bei abstrahierten Services wie Amazon S3 und Amazon DynamoDB werden die Infrastrukturebene, das Betriebssystem und die Plattformen AWS betrieben, und Sie greifen auf die Endpunkte zu, um Daten zu speichern und abzurufen. Sie sind dafür verantwortlich, Ihre Daten (einschließlich Verschlüsselungsoptionen) zu verwalten, Ihre Ressourcen zu klassifizieren und mithilfe von IAM-Tools die entsprechenden Berechtigungen anzuwenden. Dieses gemeinsame Modell wird häufig so beschrieben, dass AWS es für die Sicherheit der Cloud verantwortlich ist (d. h. für den Schutz der Infrastruktur, auf der alle in der Cloud angebotenen Dienste ausgeführt werden AWS Cloud), und dass Sie für die Sicherheit in der Cloud verantwortlich sind (abhängig von den von Ihnen ausgewählten AWS Cloud Diensten).

Im Rahmen der in diesen grundlegenden Dokumenten enthaltenen Leitlinien sind zwei Kategorien von Konzepten für die Gestaltung und das Verständnis der AWS SRA von besonderer Bedeutung: Sicherheitsfunktionen und Prinzipien des Sicherheitsdesigns.

Sicherheitsfähigkeiten

In der Sicherheitsperspektive von AWS CAF werden neun Funktionen beschrieben, mit denen Sie die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Daten und Cloud-Workloads gewährleisten können.

- Sicherheits-Governance zur Entwicklung und Kommunikation von Sicherheitsrollen, Verantwortlichkeiten, Richtlinien, Prozessen und Verfahren in der gesamten AWS Unternehmensumgebung.
- Sicherheitsgarantie zur Überwachung, Bewertung, Verwaltung und Verbesserung der Effektivität Ihrer Sicherheits- und Datenschutzprogramme.
- Identitäts- und Zugriffsmanagement zur Verwaltung von Identitäten und Berechtigungen in großem Umfang.

- Erkennung von Bedrohungen, um potenzielle Sicherheitsfehlkonfigurationen, Bedrohungen oder unerwartetes Verhalten zu verstehen und zu identifizieren.
- Schwachstellenmanagement zur kontinuierlichen Identifizierung, Klassifizierung, Behebung und Minderung von Sicherheitslücken.
- Infrastrukturschutz, um zu überprüfen, ob die Systeme und Dienste in Ihren Workloads geschützt sind.
- Datenschutz zur Wahrung der Transparenz und Kontrolle über Daten und darüber, wie auf sie zugegriffen wird und wie sie in Ihrem Unternehmen verwendet werden.
- Anwendungssicherheit zur Erkennung und Behebung von Sicherheitslücken während des Softwareentwicklungsprozesses.
- Reaktion auf Vorfälle zur Reduzierung potenzieller Schäden durch effektive Reaktion auf Sicherheitsvorfälle.

Prinzipien der Sicherheitsgestaltung

Die Sicherheitssäule des Well-Architected Framework umfasst eine Reihe von sieben Entwurfsprinzipien, die bestimmte Sicherheitsbereiche in praktische Anleitungen umwandeln, die Ihnen helfen können, die Sicherheit Ihrer Workloads zu verbessern. Wo die Sicherheitsfunktionen die gesamte Sicherheitsstrategie prägen, beschreiben diese Well-Architected Framework-Prinzipien, womit Sie beginnen können. Sie werden in diesem AWS SRA sehr bewusst berücksichtigt und bestehen aus folgenden Elementen:

- Implementieren Sie ein starkes Identitätsfundament – Implementieren Sie das Prinzip der geringsten Rechte und setzen Sie die Aufgabentrennung durch, wobei Sie für jede Interaktion mit Ihren AWS Ressourcen die entsprechende Autorisierung erhalten. Zentralisieren Sie die Identitätsverwaltung und vermeiden Sie die Abhängigkeit von langfristigen statischen Anmeldeinformationen.
- Sorgen Sie für Rückverfolgbarkeit – Überwachen Sie Aktionen und Änderungen an Ihrer Umgebung in Echtzeit, generieren Sie Warnmeldungen und prüfen Sie sie. Integrieren Sie die Protokoll- und Metrikerfassung in Systeme, um automatisch zu untersuchen und Maßnahmen zu ergreifen.
- Wenden Sie Sicherheit auf allen Ebenen an – Wenden Sie einen defense-in-depth Ansatz mit mehreren Sicherheitskontrollen an. Wenden Sie mehrere Arten von Kontrollen (z. B. präventive und detektive Kontrollen) auf alle Ebenen an, einschließlich Edge of Network, Virtual Private Cloud

(VPC), Lastenausgleich, Instanz- und Rechendienste, Betriebssystem, Anwendungskonfiguration und Code.

- Automatisieren Sie bewährte Sicherheitsmethoden – Automatisierte, softwarebasierte Sicherheitsmechanismen verbessern Ihre Fähigkeit, sicher, schneller und kostengünstiger zu skalieren. Erstellen Sie sichere Architekturen und implementieren Sie Kontrollen, die als Code in versionskontrollierten Vorlagen definiert und verwaltet werden.
- Schützen Sie Daten bei der Übertragung und Speicherung – Klassifizieren Sie Ihre Daten in Vertraulichkeitsstufen und verwenden Sie gegebenenfalls Mechanismen wie Verschlüsselung, Tokenisierung und Zugriffskontrolle.
- Halten Sie Personen von Daten fern – Verwenden Sie Mechanismen und Tools, um den direkten Zugriff auf Daten oder deren manuelle Verarbeitung zu reduzieren oder zu eliminieren. Sie reduzieren dadurch das Risiko, dass sensible Daten verloren gehen, geändert werden oder anderweitigen Benutzerfehlern unterliegen.
- Bereiten Sie sich auf Sicherheitsereignisse vor – Bereiten Sie sich auf einen Vorfall vor, indem Sie Richtlinien und Prozesse für das Management und die Untersuchung von Vorfällen festlegen, die auf Ihre organisatorischen Anforderungen abgestimmt sind. Simulieren Sie Vorfallreaktionen und nutzen Sie automatisierbare Tools, um die Erkennung, Untersuchung und Wiederherstellung zu beschleunigen.

So verwenden Sie die AWS SRA mit AWS CAF und AWS Well-Architected Framework

AWS CAF, AWS Well-Architected Framework und AWS SRA sind sich ergänzende Frameworks, die zusammenarbeiten, um Ihre Cloud-Migrations- und Modernisierungsbemühungen zu unterstützen.

- Das AWS CAF nutzt AWS Erfahrung und bewährte Verfahren, um Sie dabei zu unterstützen, die Vorteile der Cloud-Einführung mit Ihren gewünschten Geschäftsergebnissen in Einklang zu bringen. Nutzen Sie das AWS CAF, um Transformationsmöglichkeiten zu identifizieren und zu priorisieren, die Cloud-Bereitschaft zu bewerten und zu verbessern und Ihre Transformationsstrategie iterativ weiterzuentwickeln.
- Das AWS Well-Architected Framework bietet AWS Empfehlungen für den Aufbau einer sicheren, leistungsstarken, belastbaren und effizienten Infrastruktur für eine Vielzahl von Anwendungen und Workloads, die Ihren Geschäftsergebnissen entsprechen.

- Die AWS SRA hilft Ihnen zu verstehen, wie Sicherheitsdienste so bereitgestellt und verwaltet werden können, dass sie den Empfehlungen der AWS CAF und des AWS Well-Architected Framework entsprechen.

Aus Sicht der AWS CAF-Sicherheit sollten Sie beispielsweise prüfen, wie Sie die Identitäten Ihrer Mitarbeiter und deren Authentifizierung zentral verwalten können. AWS Auf der Grundlage dieser Informationen entscheiden Sie sich möglicherweise dafür, zu diesem Zweck eine neue oder bestehende Corporate Identity Provider (IdP) -Lösung wie Okta, Active Directory oder Ping Identity zu verwenden. Sie folgen den Anweisungen im AWS Well-Architected Framework und beschließen, Ihren IdP in das zu integrieren, um Ihren Mitarbeitern eine Single-Sign-On-Erfahrung AWS IAM Identity Center zu bieten, mit der ihre Gruppenmitgliedschaften und -berechtigungen synchronisiert werden können. Sie lesen die AWS SRA-Empfehlung, IAM Identity Center im Verwaltungskonto Ihrer AWS Organisation zu aktivieren und es über ein Sicherheitstooling-Konto zu verwalten, das von Ihrem Security Operations Team verwendet wird. Dieses Beispiel zeigt, wie das AWS CAF Ihnen hilft, erste Entscheidungen über Ihren gewünschten Sicherheitsstatus zu treffen, das AWS Well-Architected Framework bietet Anleitungen zur Bewertung der verfügbaren Optionen AWS-Services , um dieses Ziel zu erreichen, und das AWS SRA gibt dann Empfehlungen zur Bereitstellung und Verwaltung der von Ihnen ausgewählten Sicherheitsdienste.

SRA-Bausteine — Konten AWS Organizations und Leitplanken

Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

AWS Sicherheitsdienste, ihre Kontrollen und Interaktionen lassen sich am besten auf der Grundlage einer Strategie für AWS mehrere Konten und Leitplanken für Identitäts- und Zugriffsmanagement einsetzen. Diese Leitplanken ermöglichen Ihnen die Implementierung von geringsten Rechten, Aufgabentrennung und Datenschutz und unterstützen Sie bei Entscheidungen darüber, welche Arten von Kontrollen erforderlich sind, wo die einzelnen Sicherheitsdienste verwaltet werden und wie sie Daten und Berechtigungen in der SRA gemeinsam nutzen dürfen. AWS

Ein AWS-Konto bietet Sicherheit, Zugriffs- und Abrechnungsgrenzen für Ihre AWS Ressourcen und ermöglicht es Ihnen, Ressourcenunabhängigkeit und Isolierung zu erreichen. Die Verwendung mehrerer Konten AWS-Konten spielt eine wichtige Rolle bei der Erfüllung Ihrer Sicherheitsanforderungen. Weitere Informationen finden Sie im Whitepaper Organisieren der AWS Umgebung mithilfe mehrerer Konten im AWS-Konten Abschnitt Vorteile der Nutzung mehrerer Konten. Sie können beispielsweise Ihre Workloads in separaten Konten und Gruppenkonten innerhalb einer Organisationseinheit (OU) auf der Grundlage von Funktionen, Compliance-Anforderungen oder gemeinsamen Kontrollmechanismen organisieren, anstatt die Berichtsstruktur Ihres Unternehmens widerzuspiegeln. Behalten Sie Sicherheit und Infrastruktur im Hinterkopf, damit Ihr Unternehmen bei wachsenden Workloads gemeinsame Leitplanken festlegen kann. Dieser Ansatz bietet robuste Grenzen und Kontrollen zwischen Workloads. Die Trennung auf Kontoebene wird in Kombination mit verwendet AWS Organizations, um Produktionsumgebungen von Entwicklungs- und Testumgebungen zu isolieren oder um eine starke logische Grenze zwischen Workloads zu schaffen, die Daten mit unterschiedlichen Klassifizierungen wie dem Payment Card Industry Data Security Standard (PCI DSS) oder dem Health Insurance Portability and Accountability Act (HIPAA) verarbeiten. Auch wenn Sie Ihre AWS Reise mit einem einzigen Konto beginnen könnten, AWS empfiehlt es sich, mehrere Konten einzurichten, wenn Ihre Workloads an Größe und Komplexität zunehmen.

Mit Berechtigungen können Sie den Zugriff auf AWS Ressourcen festlegen. Berechtigungen werden IAM-Entitäten gewährt, die als Prinzipale (Benutzer, Gruppen und Rollen) bezeichnet werden. Standardmäßig beginnen Prinzipale ohne Berechtigungen. IAM-Prinzipale können AWS erst dann

etwas tun, wenn Sie ihnen Berechtigungen erteilen. Außerdem können Sie Richtlinien einrichten, die für Ihre gesamte AWS Organisation gelten oder so detailliert wie eine individuelle Kombination aus Prinzipal, Aktion, Ressource und Bedingungen sind.

Aus AWS Organizations Sicherheitsgründen verwenden

Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

AWS Organizationshilft Ihnen dabei, Ihre Umgebung zentral zu verwalten und zu steuern, während Sie Ihre AWS Ressourcen erweitern und skalieren. Mithilfe dieser Funktion können Sie programmgesteuert neue Konten erstellen AWS Organizations, Ressourcen zuweisen AWS-Konten, Konten gruppieren, um Ihre Workloads zu organisieren, und Richtlinien für die Verwaltung auf Konten oder Gruppen von Konten anwenden. Eine AWS Organisation konsolidiert Ihre, AWS-Konten sodass Sie sie als eine einzige Einheit verwalten können. Sie hat ein Verwaltungskonto sowie null oder mehr Mitgliedskonten. Die meisten Ihrer Workloads befinden sich in Mitgliedskonten, mit Ausnahme einiger zentral verwalteter Prozesse, die entweder im Verwaltungskonto oder in Konten gespeichert sein müssen, die bestimmten Benutzern als delegierte Administratoren zugewiesen wurden. AWS-Services Sie können Ihrem Sicherheitsteam Tools und Zugriff von einem zentralen Ort aus bereitstellen, um die Sicherheitsanforderungen im Namen einer Organisation zu verwalten. AWS Sie können die Verdoppelung von Ressourcen reduzieren, indem Sie wichtige Ressourcen innerhalb Ihrer AWS Organisation gemeinsam nutzen. Sie können Konten in AWS Organisationseinheiten (OUs) gruppieren, die je nach den Anforderungen und dem Zweck des Workloads unterschiedliche Umgebungen repräsentieren können. AWS Organizations bietet außerdem mehrere Richtlinien, mit denen Sie zusätzliche Sicherheitskontrollen zentral auf alle Mitgliedskonten in Ihren Organisationen anwenden können. Dieser Abschnitt konzentriert sich auf Richtlinien zur Dienststeuerung (SCPs), Ressourcenkontrollrichtlinien (RCPs) und deklarative Richtlinien.

Mit AWS Organizations können Sie Richtlinien für Berechtigungen RCPsauf AWS Organisations SCPs-, OU- oder Kontoebene verwenden und anwenden. SCPs sind Leitplanken, die für Principals innerhalb eines Unternehmenskontos gelten, mit Ausnahme des Verwaltungskontos (was ein Grund dafür ist, Workloads nicht in diesem Konto auszuführen). Wenn Sie einer Organisationseinheit einen SCP zuordnen, wird der SCP vom Kind OUs und den Konten unter dieser Organisationseinheit übernommen. SCPs gewähren keine Berechtigungen. Stattdessen geben sie die maximalen Berechtigungen an, die Ihren Prinzipalen in einer AWS Organisation, Organisationseinheit oder einem Konto zur Verfügung stehen. Sie müssen den Prinzipalen oder Ressourcen in Ihrer

Umgebung dennoch identitäts- oder ressourcenbasierte Richtlinien zuordnen, um ihnen tatsächlich Berechtigungen AWS-Konten zu erteilen. Wenn ein SCP beispielsweise den Zugriff auf Amazon S3 verweigert, hat ein vom SCP betroffener Principal keinen Zugriff auf Amazon S3, selbst wenn ihm der Zugriff durch eine IAM-Richtlinie ausdrücklich gewährt wird. Weitere Informationen darüber, wie IAM-Richtlinien bewertet werden, welche Rolle sie spielen und wie der Zugriff letztlich gewährt oder verweigert wird SCPs, finden Sie unter Bewertungslogik für Richtlinien in der IAM-Dokumentation.

RCPs sind Leitplanken, die für Ressourcen innerhalb der Konten einer Organisation gelten, unabhängig davon, ob die Ressourcen derselben Organisation gehören. SCPsBeeinträchtigen RCPs Sie zum Beispiel nicht die Ressourcen im Verwaltungskonto und gewähren Sie keine Berechtigungen. Wenn Sie ein RCP an eine Organisationseinheit anhängen, wird das RCP vom Kind OUs und den Konten unter der Organisationseinheit übernommen. RCPs bieten eine zentrale Kontrolle über die maximal verfügbaren Berechtigungen für Ressourcen in Ihrer Organisation und unterstützen derzeit eine Teilmenge von. AWS-Services Wir empfehlen Ihnen OUs, bei der Planung SCPs Ihrer Änderungen den IAM-Richtliniensimulator zu verwenden. Sie sollten auch die Daten des Dienstes, auf den zuletzt zugegriffen wurde, in IAM überprüfen und die Dienstnutzung auf API-Ebene protokollieren, um die potenziellen Auswirkungen von SCP-Änderungen zu verstehen.AWS CloudTrail

SCPs und RCPs sind unabhängige Kontrollen. Je nach den Zugriffskontrollen, die Sie durchsetzen möchten RCPs, können Sie wählen, ob Sie nur SCPs oder beide Richtlinientypen aktivieren oder beide Richtlinientypen zusammen verwenden möchten. Wenn Sie beispielsweise verhindern möchten, dass die Prinzipale Ihrer Organisation auf Ressourcen außerhalb Ihrer Organisation zugreifen, setzen Sie diese Kontrolle durch, indem SCPs Sie. Wenn Sie den Zugriff externer Identitäten auf Ihre Ressourcen einschränken oder verhindern möchten, setzen Sie diese Kontrolle durch, indem Sie. RCPs Weitere Informationen und Anwendungsfälle für RCPs und SCPs finden Sie RCPs in der AWS Organizations Dokumentation unter Verwenden von SCPs und.

Sie können AWS Organizations deklarative Richtlinien verwenden, um Ihre gewünschte Konfiguration für eine bestimmte Größe AWS-Service im gesamten Unternehmen zentral zu deklarieren und durchzusetzen. Sie können beispielsweise den öffentlichen Internetzugang zu Amazon VPC-Ressourcen in Ihrer gesamten Organisation blockieren. Im Gegensatz zu Autorisierungsrichtlinien wie SCPs und RCPs werden deklarative Richtlinien auf der Kontrollebene eines AWS Dienstes durchgesetzt. Autorisierungsrichtlinien regeln den Zugriff auf APIs, während deklarative Richtlinien direkt auf Serviceebene angewendet werden, um dauerhafte Absichten durchzusetzen. Diese Richtlinien tragen dazu bei, dass die Basiskonfiguration für einen immer beibehalten AWS-Service wird, auch wenn der Dienst neue Funktionen einführt oder APIs. Die Basiskonfiguration wird auch beibehalten, wenn einer Organisation neue Konten hinzugefügt oder neue Prinzipale und Ressourcen

erstellt werden. Deklarative Richtlinien können auf eine gesamte Organisation oder auf bestimmte OUs Konten angewendet werden.

Jeder AWS-Konto hat einen einzelnen Root-Benutzer, der standardmäßig über vollständige Berechtigungen für alle AWS Ressourcen verfügt. Aus Sicherheitsgründen empfehlen wir, den Root-Benutzer nicht zu verwenden, außer für einige Aufgaben, für die ausdrücklich ein Root-Benutzer erforderlich ist. Wenn Sie mehrere Konten verwalten AWS-Konten AWS Organizations, können Sie die Root-Anmeldung zentral deaktivieren und dann für alle Mitgliedskonten Aktionen mit Root-Rechten ausführen. Nachdem Sie den Root-Zugriff für Mitgliedskonten zentral verwaltet haben, können Sie das Root-Benutzerkennwort, die Zugriffsschlüssel und die Signaturzertifikate löschen und die Multi-Faktor-Authentifizierung (MFA) für Mitgliedskonten deaktivieren. Neue Konten, die im Rahmen des zentral verwalteten Root-Zugriffs erstellt werden, haben standardmäßig keine Root-Benutzeranmeldedaten. Mitgliedskonten können sich nicht mit ihrem Root-Benutzer anmelden oder eine Passwortwiederherstellung für ihren Root-Benutzer durchführen.

AWS Control Towerbietet eine vereinfachte Möglichkeit, mehrere Konten einzurichten und zu verwalten. Es automatisiert die Einrichtung von Konten in Ihrem AWS Unternehmen, automatisiert die Bereitstellung, wendet Kontrollen an (einschließlich präventiver und detektiver Kontrollen) und bietet Ihnen ein Dashboard für mehr Transparenz. Eine zusätzliche IAM-Verwaltungsrichtlinie, eine Berechtigungsgrenze, ist bestimmten IAM-Prinzipalen (Benutzern oder Rollen) zugeordnet und legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einem IAM-Prinzipal gewähren kann.

AWS Organizations hilft Ihnen bei der Konfiguration, die für alle Ihre Konten AWS-Servicesgilt. Sie können beispielsweise die zentrale Protokollierung aller Aktionen konfigurieren, die in Ihrer AWS Organisation ausgeführt werden, indem Sie die Protokollierung durch Mitgliedskonten deaktivieren CloudTrail, und verhindern, dass Mitgliedskonten die Protokollierung deaktivieren. Sie können auch Daten für Regeln, die Sie mithilfe von Use definiert haben, zentral aggregieren AWS Config, sodass Sie Ihre Workloads auf Einhaltung überprüfen und schnell auf Änderungen reagieren können. Sie können CloudFormation Stacks AWS CloudFormation StackSetsfür alle Konten und OUs in Ihrer AWS Organisation zentral verwalten, sodass Sie automatisch ein neues Konto einrichten können, das Ihren Sicherheitsanforderungen entspricht.

Die Standardkonfiguration von AWS Organizations unterstützt die Verwendung von SCPs Sperrlisten. Mithilfe einer Strategie für Ablehnungslisten können Administratoren von Mitgliedskonten alle Dienste und Aktionen delegieren, bis Sie einen SCP erstellen und anhängen, der einen bestimmten Dienst oder eine Reihe von Aktionen verweigert. Ablehnungsbefehle erfordern weniger Wartung als eine Zulassungsliste, da Sie sie nicht aktualisieren müssen, wenn neue Dienste AWS hinzugefügt werden.

Deny-Anweisungen haben normalerweise eine kürzere Zeichenlänge, sodass es einfacher ist, die maximale Größe einzuhalten SCPs. In einer Anweisung, bei der das `Effect` Element den Wert von hat`Deny`, können Sie auch den Zugriff auf bestimmte Ressourcen einschränken oder Bedingungen definieren, unter denen sie gültig SCPs sind. Im Gegensatz dazu gilt eine `Allow` Aussage in einem SCP für alle Ressourcen (`"*"`) und kann nicht durch Bedingungen eingeschränkt werden. Weitere Informationen und Beispiele finden Sie SCPs in der AWS Organizations Dokumentation unter Strategien zur Verwendung.

Designüberlegungen

- Um es SCPs als Zulassungsliste zu verwenden, müssen Sie alternativ das von AWS verwaltete `FullAWSAccess` SCP durch ein SCP ersetzen, das ausdrücklich nur die Services und Aktionen zulässt, die Sie zulassen möchten. Damit eine Berechtigung für ein bestimmtes Konto aktiviert werden kann, muss jeder SCP (vom Root-Konto bis zu jeder Organisationseinheit im direkten Pfad zum Konto und sogar mit dem Konto selbst verknüpft) diese Berechtigung gewähren. Dieses Modell ist restriktiver und eignet sich möglicherweise für stark regulierte und sensible Workloads. Bei diesem Ansatz müssen Sie jeden IAM-Dienst oder jede IAM-Aktion auf dem Pfad von der AWS-Konto zur Organisationseinheit explizit zulassen.
- Idealerweise würden Sie eine Kombination aus Strategien für Ablehnungslisten und Zulassungslisten verwenden. Verwenden Sie die Zulassungsliste, um die Liste der AWS-Services zugelassenen Personen zu definieren, die innerhalb einer AWS Organisation verwendet werden dürfen, und fügen Sie diesen SCP an das Stammverzeichnis Ihrer AWS Organisation an. Wenn Sie für Ihre Entwicklungsumgebung eine andere Gruppe von Diensten zugelassen haben, fügen Sie die entsprechenden Dienste an jede Organisationseinheit SCPs an. Anschließend können Sie mithilfe der Ablehnungsliste Unternehmensleitlinien definieren, indem Sie bestimmte IAM-Aktionen explizit ablehnen.
- RCPs gelten für Ressourcen für eine Teilmenge von. AWS-Services Weitere Informationen finden Sie RCPs in der AWS Organizations Dokumentation unter Liste AWS-Services dieser Unterstützungen. Die Standardkonfiguration von AWS Organizations unterstützt die Verwendung RCPs von Ablehnungslisten. Wenn Sie die Option RCPs in Ihrer Organisation aktivieren, `RCPFullAWSAccess` wird automatisch eine AWS verwaltete Richtlinie mit dem Namen „Stammverzeichnis“ der Organisation, jeder Organisationseinheit und jedem Konto in Ihrer Organisation hinzugefügt. Sie können diese Richtlinie nicht trennen. Dieses Standard-RCP ermöglicht es allen Prinzipalen und Aktionen, auf die zugegriffen wird, die RCP-Bewertung zu durchlaufen. Das heißt, bis Sie mit dem Erstellen und Anhängen

beginnen RCPs, funktionieren alle Ihre vorhandenen IAM-Berechtigungen weiterhin wie bisher. Diese AWS verwaltete Richtlinie gewährt keinen Zugriff. Sie können dann eine neue Liste mit RCPs Ablehnungsaussagen erstellen, um den Zugriff auf Ressourcen in Ihrer Organisation zu blockieren.

Das Verwaltungskonto, der vertrauenswürdige Zugriff und die delegierten Administratoren

Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

Das Verwaltungskonto (auch AWS Organisationsverwaltungskonto oder Organisationsverwaltungskonto genannt) ist einzigartig und unterscheidet sich von allen anderen Konten in AWS Organizations. Es ist das Konto, das die AWS Organisation erstellt. Von diesem Konto aus können Sie Konten AWS-Konten in der AWS Organisation erstellen, andere bestehende Konten zur AWS Organisation einladen (beide Typen werden als Mitgliedskonten betrachtet), Konten aus der AWS Organisation entfernen und IAM-Richtlinien auf das Stammkonto oder Konten innerhalb der AWS Organisation anwenden. OUs

Mit dem Verwaltungskonto werden allgemeine Sicherheitsvorkehrungen durch SCPs, und Dienstbereitstellungen (z. B. CloudTrail) bereitgestellt RCPs, die sich auf alle Mitgliedskonten in der Organisation auswirken. AWS Um die Berechtigungen im Verwaltungskonto weiter einzuschränken, können diese Berechtigungen nach Möglichkeit an ein anderes geeignetes Konto, z. B. ein Sicherheitskonto, delegiert werden.

Das Verwaltungskonto hat die Aufgabe eines Zahlungskontos; von ihm gehen sämtliche Gebühren ab, die auf den Mitgliedskonten anfallen. Sie können das Verwaltungskonto einer AWS Organisation nicht wechseln. Ein AWS-Konto kann jeweils nur Mitglied einer AWS Organisation sein.

Aufgrund der Funktionalität und des Einflussbereichs, den das Verwaltungskonto besitzt, empfehlen wir, den Zugriff auf dieses Konto zu beschränken und Berechtigungen nur Rollen zu gewähren, die diese benötigen. Zwei Funktionen, die Ihnen dabei helfen, sind vertrauenswürdiger Zugriff und delegierter Administrator. Mithilfe des vertrauenswürdigen Zugriffs können Sie einen AWS-Service von Ihnen angegebenen vertrauenswürdigen Dienst aktivieren, der Aufgaben in Ihrer AWS Organisation und deren Konten in Ihrem Namen ausführt. Dies umfasst das Erteilen

von Berechtigungen für den vertrauenswürdigen Service, hat aber keine Auswirkungen auf die Berechtigungen für IAM-Benutzer und -Rollen. Sie können Trusted Access verwenden, um Einstellungen und Konfigurationsdetails festzulegen, die der vertrauenswürdige Dienst in Ihrem Namen in den Konten Ihrer AWS Organisation verwalten soll. Im Abschnitt „Konto für die Unternehmensverwaltung“ der AWS SRA wird beispielsweise erklärt, wie Sie dem CloudTrail Dienst vertrauenswürdigen Zugriff gewähren können, um einen CloudTrail Organisationspfad für alle Konten in Ihrer AWS Organisation zu erstellen.

Einige AWS-Services unterstützen die Funktion für delegierte Administratoren in. AWS OrganizationsMit dieser Funktion können kompatible Dienste ein AWS Mitgliedskonto in der AWS Organisation als Administrator für die Konten der AWS Organisation in diesem Dienst registrieren. Diese Funktion bietet verschiedenen Teams in Ihrem Unternehmen die Flexibilität, je nach ihren Zuständigkeiten separate Konten für die Verwaltung der AWS-Services gesamten Umgebung zu verwenden. Zu den AWS Sicherheitsdiensten in der AWS SRA, die derzeit delegierte Administratoren unterstützen, gehören IAM Identity Center,, Amazon AWS Config AWS Firewall Manager GuardDuty, IAM Access Analyzer, Amazon Macie, AWS Security Hub Cloud Security Posture Management (AWS Security Hub CSPM), Amazon Detective AWS Audit Manager, Amazon Inspector und. AWS Systems Manager Die Verwendung der Funktion für delegierte Administratoren wird in der AWS SRA als bewährte Methode hervorgehoben, und wir delegieren die Verwaltung sicherheitsrelevanter Dienste an das Security Tooling-Konto.

Dedizierte Kontostruktur

> Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

An AWS-Konto bietet Sicherheit, Zugriffs- und Abrechnungsgrenzen für Ihre AWS Ressourcen und ermöglicht es Ihnen, Ressourcenunabhängigkeit und Isolierung zu erreichen. Standardmäßig ist kein Zugriff zwischen Konten zulässig.

Denken Sie bei der Gestaltung Ihrer Organisationseinheit und Kontostruktur zunächst an Sicherheit und Infrastruktur. Wir empfehlen, eine Reihe von Grundlagen OUs für diese spezifischen Funktionen zu erstellen, die in Infrastruktur und Sicherheit OUs unterteilt sind. Diese OU- und Kontoempfehlungen decken einen Teil unserer umfassenderen, umfassenderen Richtlinien für AWS Organizations die Gestaltung der Struktur mehrerer Konten ab. Vollständige Empfehlungen finden Sie

unter Organisieren Ihrer AWS Umgebung mithilfe mehrerer Konten in der AWS Dokumentation und im Blogbeitrag Bewährte Methoden für Organisationseinheiten mit. AWS Organizations

Die AWS SRA verwendet die folgenden Konten, um effektive Sicherheitsoperationen für durchzuführen. AWS Diese speziellen Konten tragen dazu bei, die Aufgabentrennung sicherzustellen, unterschiedliche Verwaltungs- und Zugriffsrichtlinien für verschiedene sensible Anwendungen und Daten zu unterstützen und die Auswirkungen eines Sicherheitsvorfalls zu mildern. In den folgenden Diskussionen konzentrieren wir uns auf Produktions- (Produktions-) Konten und die damit verbundenen Workloads. SDLC-Konten (Software Development Lifecycle) (oft als Entwickler - und Testkonten bezeichnet) sind für die Bereitstellung von Ergebnissen vorgesehen und können unter anderen Sicherheitsrichtlinien betrieben werden als für Produktionskonten.

Account	Organisationseinheit	Rolle im Bereich Sicherheit
Verwaltung	—	Zentrale Steuerung und Verwaltung aller AWS-Regionen Konten. AWS-Konto Derjenige, der die Wurzel der AWS Organisation beherbergt.
Tools für die Sicherheit	Sicherheit	AWS-Konten Spezialisiert auf den Betrieb breit anwendbarer Sicherheitsdienste (wie GuardDuty Security Hub CSPM, Audit Manager, Detective, Amazon Inspector und AWS Config), die Überwachung AWS-Konten und Automatisierung von Sicherheitswarnungen und -reaktionen. (In AWS Control Tower lautet der Standardname für das Konto unter der Security OU Audit account.)
Log-Archiv	Sicherheit	Speziell AWS-Konten für die Aufnahme und Archivierung aller Protokolle und Backups

		für alle AWS-Regionen und AWS-Konten. Dieser sollte als unveränderlicher Speicher konzipiert sein.
Netzwerk	Infrastruktur	Das Gateway zwischen Ihrer Anwendung und dem breiteren Internet. Das Netzwerkk onto isoliert die umfassend eren Netzwerkdienste, die Konfiguration und den Betrieb von den Workloads, der Sicherheit und anderen Infrastrukturen der einzelnen Anwendungen.
Gemeinsam genutzte Services	Infrastruktur	Dieses Konto unterstützt die Dienste, die mehrere Anwendungen und Teams verwenden, um ihre Ergebniss e zu erzielen. Beispiele hierfür sind Identity Center-Verzeichnisdienste (Active Directory), Messaging-Dienste und Metadatendienste.

Anwendung	Workloads	AWS-Konten die die Anwendungen des AWS Unternehmens hosten und die Workloads ausführen. (Diese werden manchmal als Workload-Konten bezeichnet.) Anwendungskonten sollten erstellt werden, um Softwaredienste zu isolieren, anstatt sie Ihren Teams zuzuordnen. Dadurch ist die bereitgestellte Anwendung widerstandsfähiger gegenüber organisatorischen Veränderungen.

AWS Organisation und Kontostruktur der AWS SRA

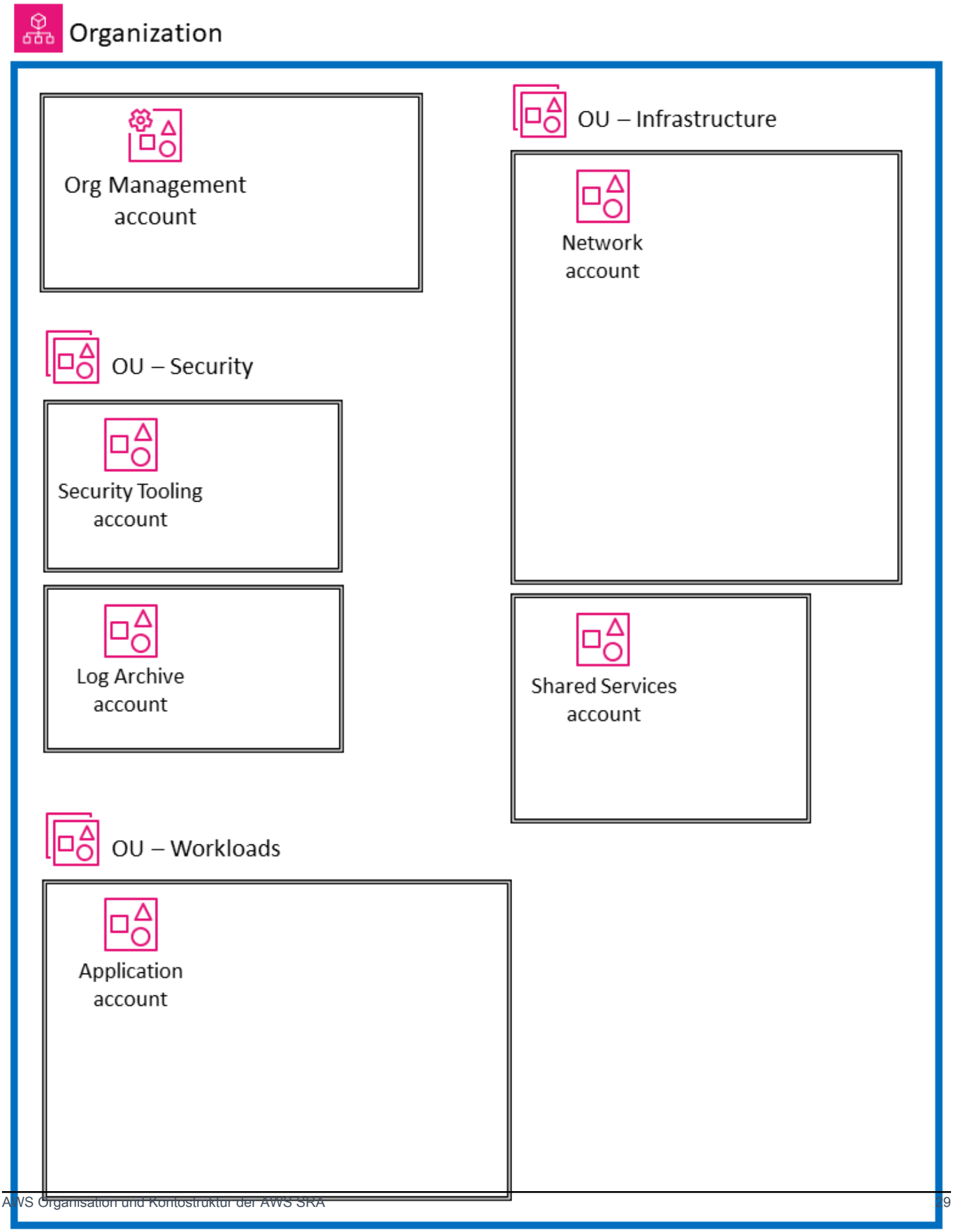
Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

Das folgende Diagramm zeigt die allgemeine Struktur der AWS SRA, ohne dass spezifische Dienste angezeigt werden. Es spiegelt die Struktur der speziellen Konten wider, die im vorherigen Abschnitt erörtert wurde, und wir fügen das Diagramm hier hinzu, um die Diskussion auf die Hauptkomponenten der Architektur zu konzentrieren:

- Alle Konten, die im Diagramm dargestellt werden, sind Teil einer einzigen AWS Organisation.
- In der oberen linken Ecke des Diagramms befindet sich das Org Management-Konto, mit dem die AWS Organisation erstellt wird.
- Unter dem Org Management-Konto befindet sich die Security OU mit zwei spezifischen Konten: eines für Security Tooling und das andere für Log Archive.
- Auf der rechten Seite befindet sich die Infrastruktur-OU mit dem Netzwerkkonto und dem Shared Services-Konto.
- Am unteren Rand des Diagramms befindet sich die Organisationseinheit Workloads, die einem Anwendungskonto zugeordnet ist, in dem sich die Unternehmensanwendung befindet.

Für diese Anleitung gelten alle Konten als Produktionskonten (Produktionskonten), die in einem einzigen System betrieben werden. AWS-Region Die meisten AWS-Services (mit Ausnahme globaler Dienste) sind regional ausgerichtet, was bedeutet, dass die Steuerungs- und Datenebene für den Dienst jeweils unabhängig voneinander existieren. AWS-Region Aus diesem Grund müssen Sie diese Architektur auf alle Bereiche replizieren AWS-Regionen , die Sie verwenden möchten, um sicherzustellen, dass Ihre gesamte Landschaft abgedeckt ist. AWS Wenn Sie in einem bestimmten Bereich keine Workloads haben AWS-Region, sollten Sie die Region mithilfe SCPsoder mithilfe von Protokollierungs- und Überwachungsmechanismen deaktivieren. Sie können Security Hub CSPM verwenden, um Ergebnisse und Sicherheitsbewertungen aus mehreren Aggregationsregionen zu aggregieren AWS-Regionen , um eine zentrale Sichtbarkeit zu gewährleisten.

Wenn Sie ein AWS Unternehmen mit einer großen Anzahl von Konten hosten, ist es von Vorteil, über eine Orchestrierungsebene zu verfügen, die die Kontobereitstellung und Kontoverwaltung erleichtert. AWS Control Tower bietet eine einfache Möglichkeit, eine Umgebung mit AWS mehreren Konten einzurichten und zu verwalten. Die AWS SRA-Codebeispiele im GitHub Repository zeigen, wie Sie die Customizations for AWS Control Tower (cFcT) -Lösung verwenden können, um von SRA empfohlene Strukturen bereitzustellen AWS .


Organization
Org Management account
OU – Infrastructure
Network account
OU – Security
Security Tooling account
Log Archive account
Shared Services account
OU – Workloads
Application account

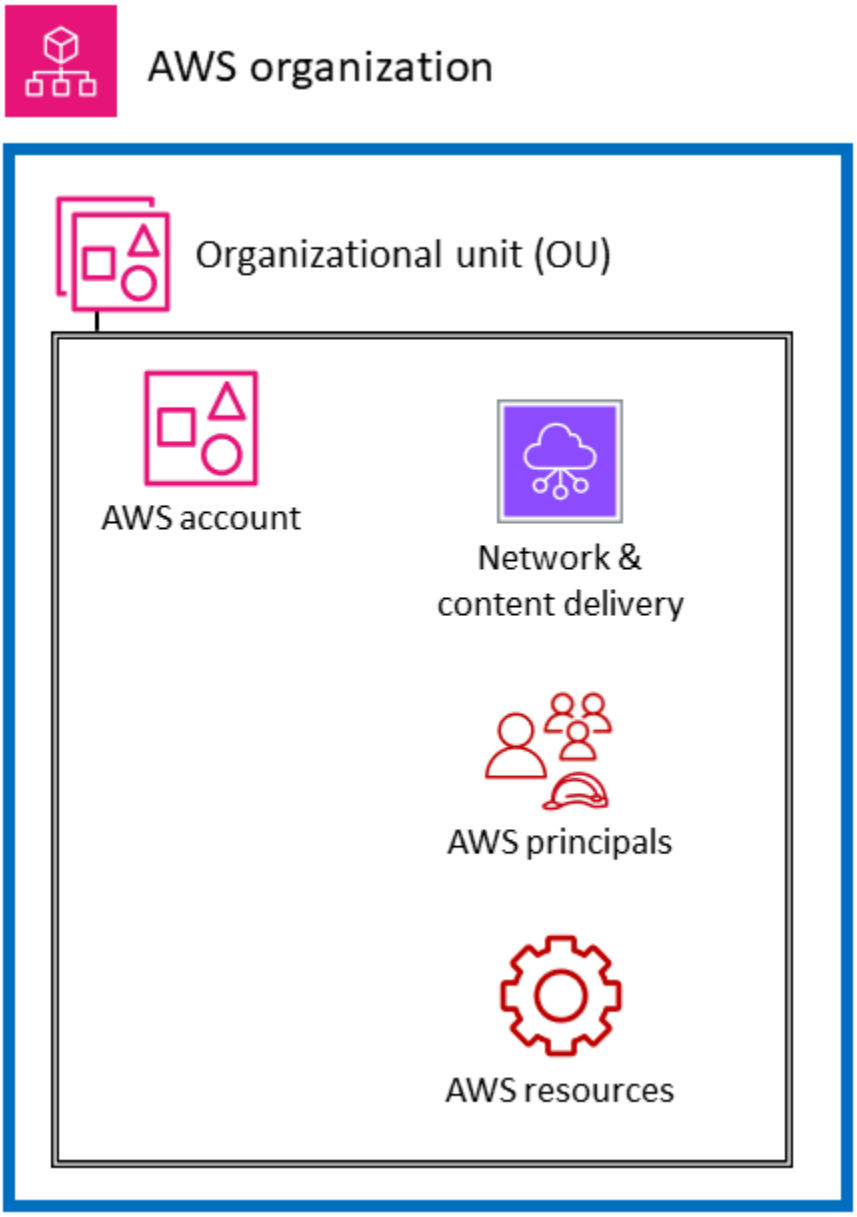
Wenden Sie Sicherheitsdienste in Ihrem gesamten Unternehmen an AWS

Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

Wie in einem früheren Abschnitt beschrieben, suchen Kunden nach einer zusätzlichen Möglichkeit, über das gesamte Spektrum an AWS Sicherheitsdiensten nachzudenken und diese strategisch zu organisieren. Der gängigste organisatorische Ansatz besteht heute darin, Sicherheitsdienste nach Hauptfunktionen zu gruppieren — je nachdem, was die einzelnen Dienste tun. In der Sicherheitsperspektive des AWS CAF sind neun funktionale Funktionen aufgeführt, darunter Identitäts- und Zugriffsmanagement, Infrastrukturschutz, Datenschutz und Bedrohungserkennung. Die Abstimmung AWS-Services mit diesen funktionalen Fähigkeiten ist eine praktische Methode, um Implementierungsentscheidungen in den einzelnen Bereichen zu treffen. Wenn es beispielsweise um Identitäts- und Zugriffsmanagement geht, sind IAM und IAM Identity Center Dienste, die in Betracht gezogen werden sollten. Bei der Gestaltung Ihres Ansatzes zur Bedrohungserkennung GuardDuty könnte dies Ihre erste Überlegung sein.

Als Ergänzung zu dieser funktionalen Sichtweise können Sie Ihre Sicherheit auch aus einer übergreifenden, strukturellen Sicht betrachten. Das heißt, zusätzlich zu der Frage: „Was AWS-Services sollte ich verwenden, um meine Identitäten, meinen logischen Zugriff oder meine Mechanismen zur Bedrohungserkennung zu kontrollieren und zu schützen?“ , Sie können auch fragen: „Welche AWS-Services sollte ich in meinem gesamten AWS Unternehmen anwenden? Welche Verteidigungsebenen sollte ich einrichten, um die Amazon EC2 EC2-Instances im Kern meiner Anwendung zu schützen?“ In dieser Ansicht ordnen AWS-Services Sie Layern in Ihrer AWS Umgebung Funktionen zu. Einige Dienste und Funktionen eignen sich hervorragend für die Implementierung von Kontrollen in Ihrer gesamten AWS Organisation. Das Blockieren des öffentlichen Zugriffs auf Amazon S3 S3-Buckets ist beispielsweise eine spezifische Kontrolle auf dieser Ebene. Dies sollte vorzugsweise in der Stammorganisation erfolgen, anstatt Teil der individuellen Kontoeinrichtung zu sein. Andere Dienste und Funktionen eignen sich am besten zum Schutz einzelner Ressourcen innerhalb eines AWS-Konto. Ein Beispiel für diese Kategorie ist die Implementierung einer untergeordneten Zertifizierungsstelle (CA) innerhalb eines Kontos, für das private TLS-Zertifikate erforderlich sind. Eine weitere ebenso wichtige Gruppierung besteht aus Diensten, die sich auf die virtuelle Netzwerkebene Ihrer AWS Infrastruktur auswirken. Das

folgende Diagramm zeigt sechs Ebenen in einer typischen AWS Umgebung: AWS Organisation, Organisationseinheit (OU), Konto, Netzwerkinfrastruktur, Prinzipale und Ressourcen.



Das Verständnis der Services in diesem strukturellen Kontext, einschließlich der Kontrollen und Schutzmaßnahmen auf jeder Ebene, hilft Ihnen bei der Planung und Implementierung einer defense-in-depth Strategie in Ihrer gesamten AWS Umgebung. Mit dieser Perspektive können Sie Fragen sowohl von oben nach unten beantworten (z. B. „Welche Dienste verwende ich, um Sicherheitskontrollen in meinem gesamten AWS Unternehmen zu implementieren?“) und von unten nach oben (z. B. „Welche Dienste verwalten die Kontrollen auf dieser EC2-Instance?“). In diesem Abschnitt gehen wir die Elemente einer AWS Umgebung durch und identifizieren die zugehörigen

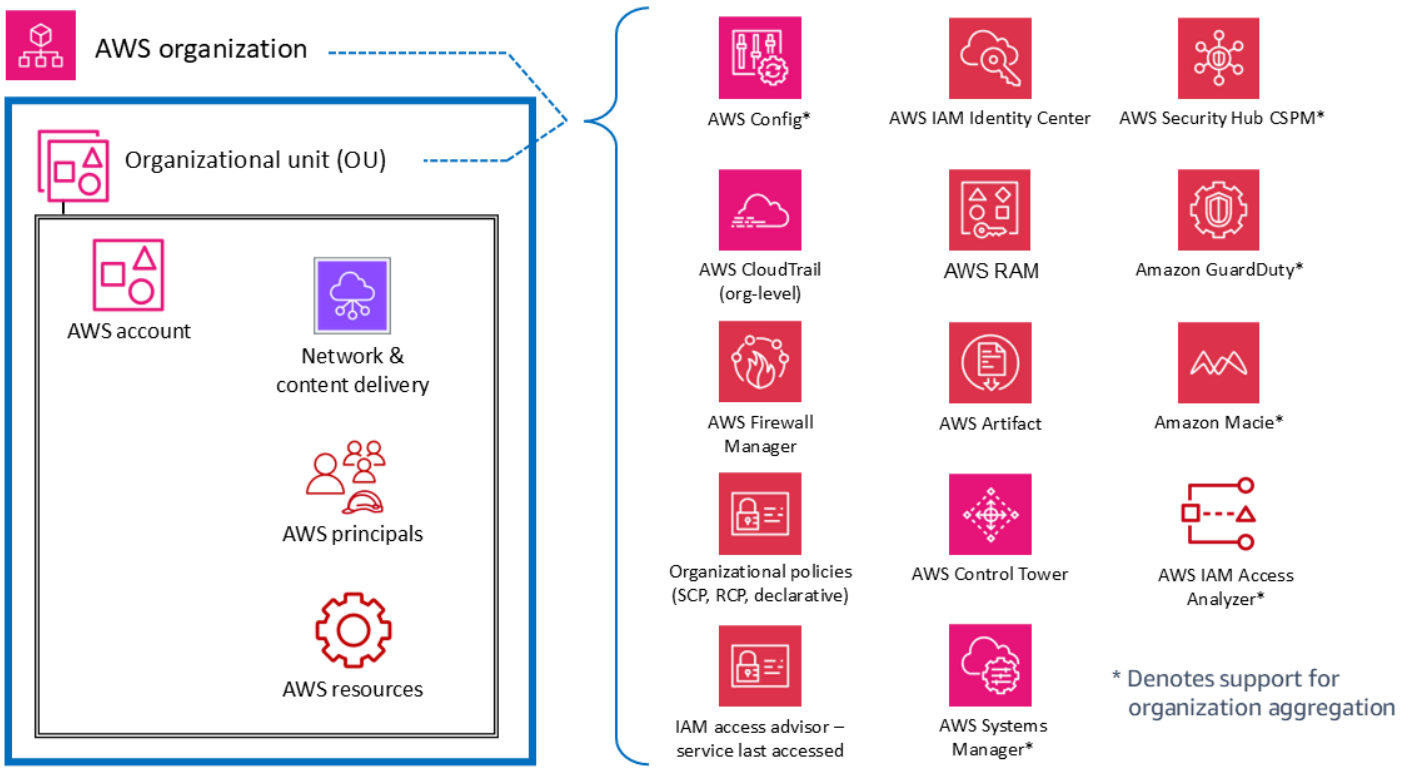
Sicherheitsdienste und -funktionen. Natürlich AWS-Services verfügen einige über umfangreiche Funktionen und unterstützen mehrere Sicherheitsziele. Diese Dienste unterstützen möglicherweise mehrere Elemente Ihrer AWS Umgebung.

Aus Gründen der Übersichtlichkeit beschreiben wir kurz, wie einige der Services den angegebenen Zielen entsprechen. Im nächsten Abschnitt werden die einzelnen Dienste der einzelnen Dienste näher erläutert AWS-Konto.

Unternehmensweit oder mehrere Konten

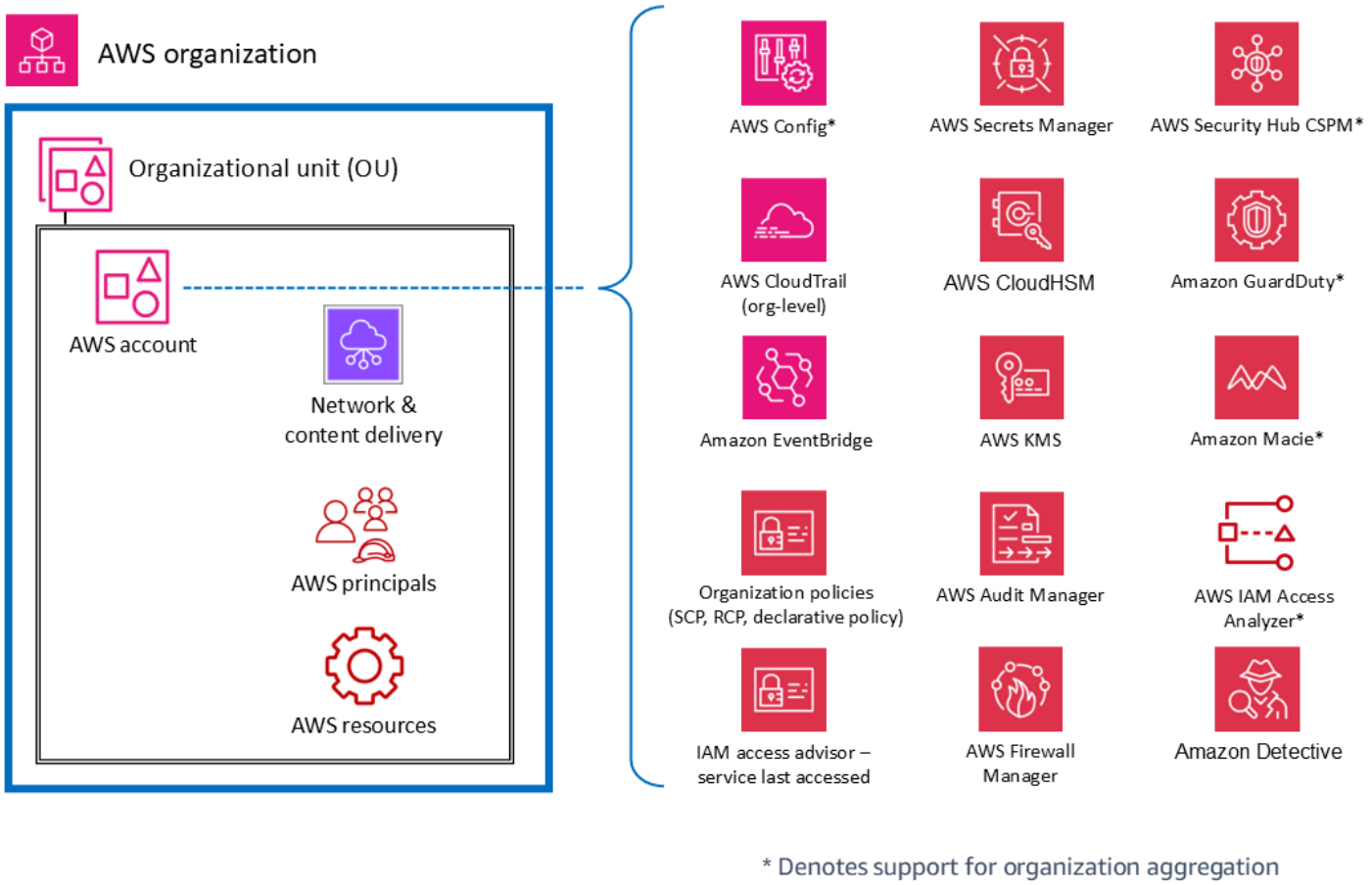
Auf der obersten Ebene gibt es Funktionen, die darauf ausgelegt sind, Führungs- und Kontrollfunktionen oder Leitplanken auf mehrere Konten in einer AWS Organisation (einschließlich der gesamten Organisation oder bestimmter Konten) anzuwenden. AWS-Services OUs Richtlinien zur Servicesteuerung (SCPs) und Richtlinien zur Ressourcenkontrolle (RCPs) sind gute Beispiele für IAM-Funktionen, die präventive, unternehmensweite Schutzmaßnahmen bieten. AWS AWS Organizations bietet außerdem eine deklarative Richtlinie, mit der die Basiskonfiguration zentral definiert und durchgesetzt wird. AWS-Services Ein anderes Beispiel ist CloudTrail die Überwachung anhand eines Organisationspfads, AWS-Konten in dem alle Ereignisse für alle Mitglieder der Organisation protokolliert werden. AWS Dieser umfassende Pfad unterscheidet sich von einzelnen Pfaden, die möglicherweise in jedem Konto erstellt werden. Ein drittes Beispiel ist AWS Firewall Manager, mit dem Sie mehrere Ressourcen für alle Konten in Ihrer AWS Organisation konfigurieren, anwenden und verwalten können: AWS WAF Regeln, AWS WAF klassische Regeln, AWS Shield Advanced Schutzmaßnahmen, Amazon Virtual Private Cloud (Amazon VPC) -Sicherheitsgruppen, AWS Network Firewall Richtlinien und Amazon Route 53 Resolver DNS-Firewall-Richtlinien.

Die im folgenden Diagramm mit einem Sternchen (*) markierten Dienste haben einen doppelten Geltungsbereich: unternehmensweit und kontoorientiert. Diese Dienste überwachen oder kontrollieren grundsätzlich die Sicherheit innerhalb eines einzelnen Kontos. Sie unterstützen jedoch auch die Möglichkeit, die Ergebnisse mehrerer Konten in einem unternehmensweiten Konto zusammenzufassen, um so eine zentrale Transparenz und Verwaltung zu gewährleisten. Gehen Sie aus Gründen der Klarheit davon aus SCPs , dass sie für eine gesamte Organisationseinheit oder AWS-Konto AWS Organisation gelten. Im Gegensatz dazu können Sie GuardDuty sowohl auf Kontoebene (wo individuelle Ergebnisse generiert werden) als auch auf AWS Organisationsebene (mithilfe der Funktion für delegierte Administratoren) konfigurieren und verwalten, sodass die Ergebnisse zusammengefasst angezeigt und verwaltet werden können.



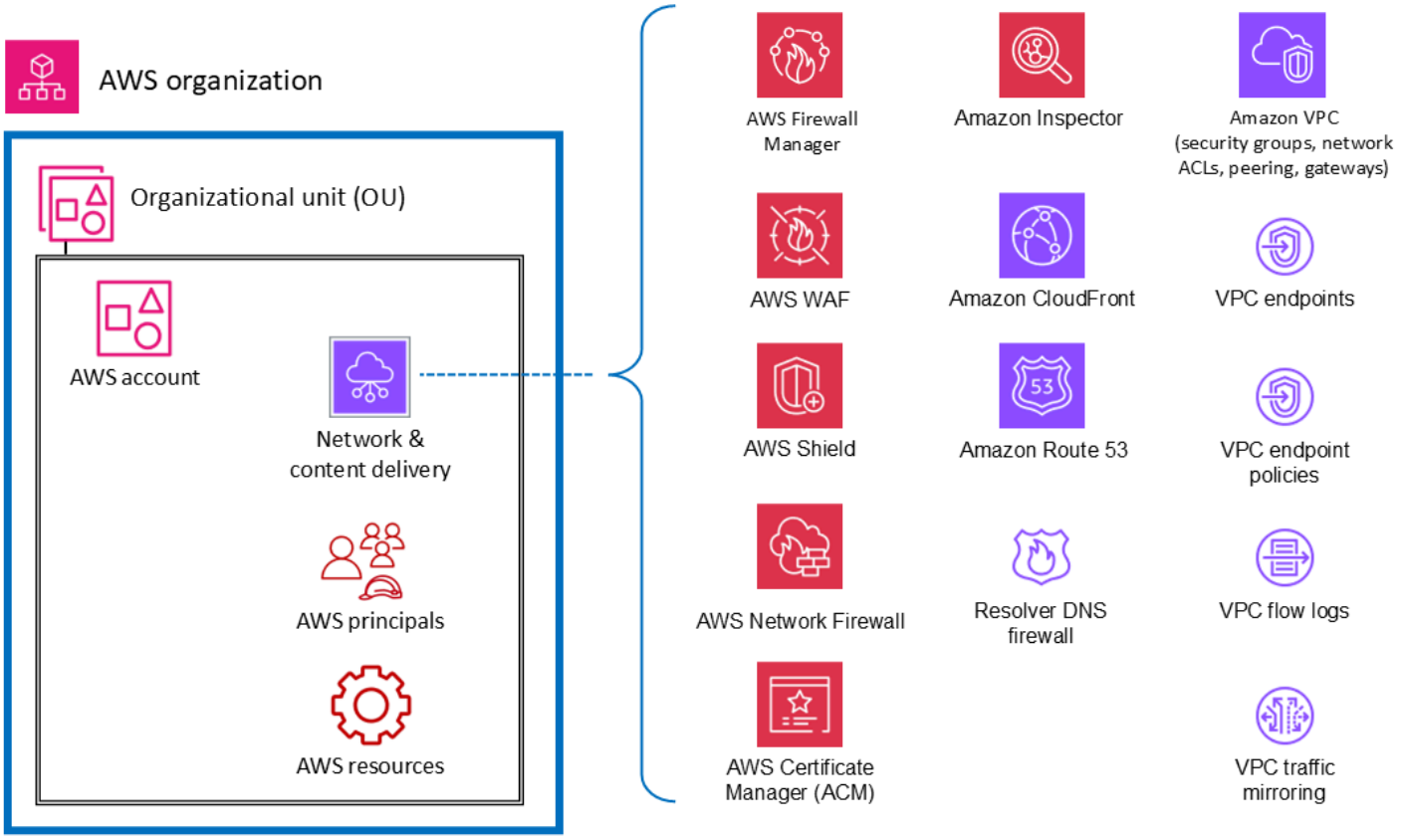
AWS Konten

Darin gibt es Dienste OUs, die helfen, mehrere Arten von Elementen in einem zu schützen AWS-Konto. AWS Secrets Manager Wird beispielsweise häufig von einem bestimmten Konto aus verwaltet und schützt Ressourcen (wie Datenbankanmeldedaten oder Authentifizierungsinformationen), Anwendungen und AWS-Services in diesem Konto. IAM Access Analyzer kann so konfiguriert werden, dass Ergebnisse generiert werden, wenn Principals außerhalb von auf bestimmte Ressourcen zugreifen können. AWS-Konto Wie im vorherigen Abschnitt erwähnt, können viele dieser Dienste auch innerhalb konfiguriert und verwaltet werden AWS Organizations, sodass sie über mehrere Konten hinweg verwaltet werden können. Diese Dienste sind im Diagramm mit einem Sternchen (*) gekennzeichnet. Sie machen es auch einfacher, Ergebnisse aus mehreren Konten zu aggregieren und sie an ein einziges Konto zu übertragen. Dies gibt den einzelnen Anwendungsteams die Flexibilität und Transparenz, um Sicherheitsanforderungen zu verwalten, die für ihre Arbeitslast spezifisch sind, und ermöglicht gleichzeitig zentralen Sicherheitsteams Steuerung und Transparenz. GuardDuty ist ein Beispiel für einen solchen Service. GuardDuty überwacht Ressourcen und Aktivitäten, die mit einem einzelnen Konto verknüpft sind, und GuardDuty Ergebnisse aus mehreren Mitgliedskonten (z. B. allen Konten in einer AWS Organisation) können von einem delegierten Administratorkonto aus gesammelt, angezeigt und verwaltet werden.



Virtuelles Netzwerk, Datenverarbeitung und Bereitstellung von Inhalten

Da der Netzwerkzugriff für die Sicherheit so wichtig ist und die Recheninfrastruktur ein grundlegender Bestandteil vieler AWS Workloads ist, gibt es viele AWS Sicherheitsdienste und -funktionen, die diesen Ressourcen gewidmet sind. Amazon Inspector ist beispielsweise ein Schwachstellen-Management-Service, der Ihre AWS Workloads kontinuierlich auf Schwachstellen überprüft. Diese Scans beinhalten Prüfungen der Netzwerkerreichbarkeit, die darauf hinweisen, dass es in Ihrer Umgebung zulässige Netzwerkpfade zu Amazon EC2 EC2-Instances gibt. Mit Amazon VPC können Sie ein virtuelles Netzwerk definieren, in dem Sie AWS Ressourcen starten können. Dieses virtuelle Netzwerk ähnelt stark einem herkömmlichen Netzwerk und umfasst eine Vielzahl von Funktionen und Vorteilen. VPC-Endpunkte ermöglichen es Ihnen, Ihre VPC privat mit unterstützten AWS-Services und mit den Endpunktdiensten zu verbinden, von denen Sie betrieben werden, AWS PrivateLink ohne dass ein Pfad zum Internet erforderlich ist. Das folgende Diagramm zeigt Sicherheitsdienste, deren Schwerpunkt auf der Netzwerk-, Computer- und Inhaltsbereitstellungsinfrastruktur liegt.



Prinzipien und Ressourcen

AWS Prinzipale und AWS Ressourcen (zusammen mit den IAM-Richtlinien) sind die grundlegenden Elemente der Identitäts- und Zugriffsverwaltung. AWS Ein authentifizierter Principal AWS kann Aktionen ausführen und auf Ressourcen zugreifen. AWS Ein Principal kann als AWS-Konto Root-Benutzer und IAM-Benutzer oder durch Übernahme einer Rolle authentifiziert werden.

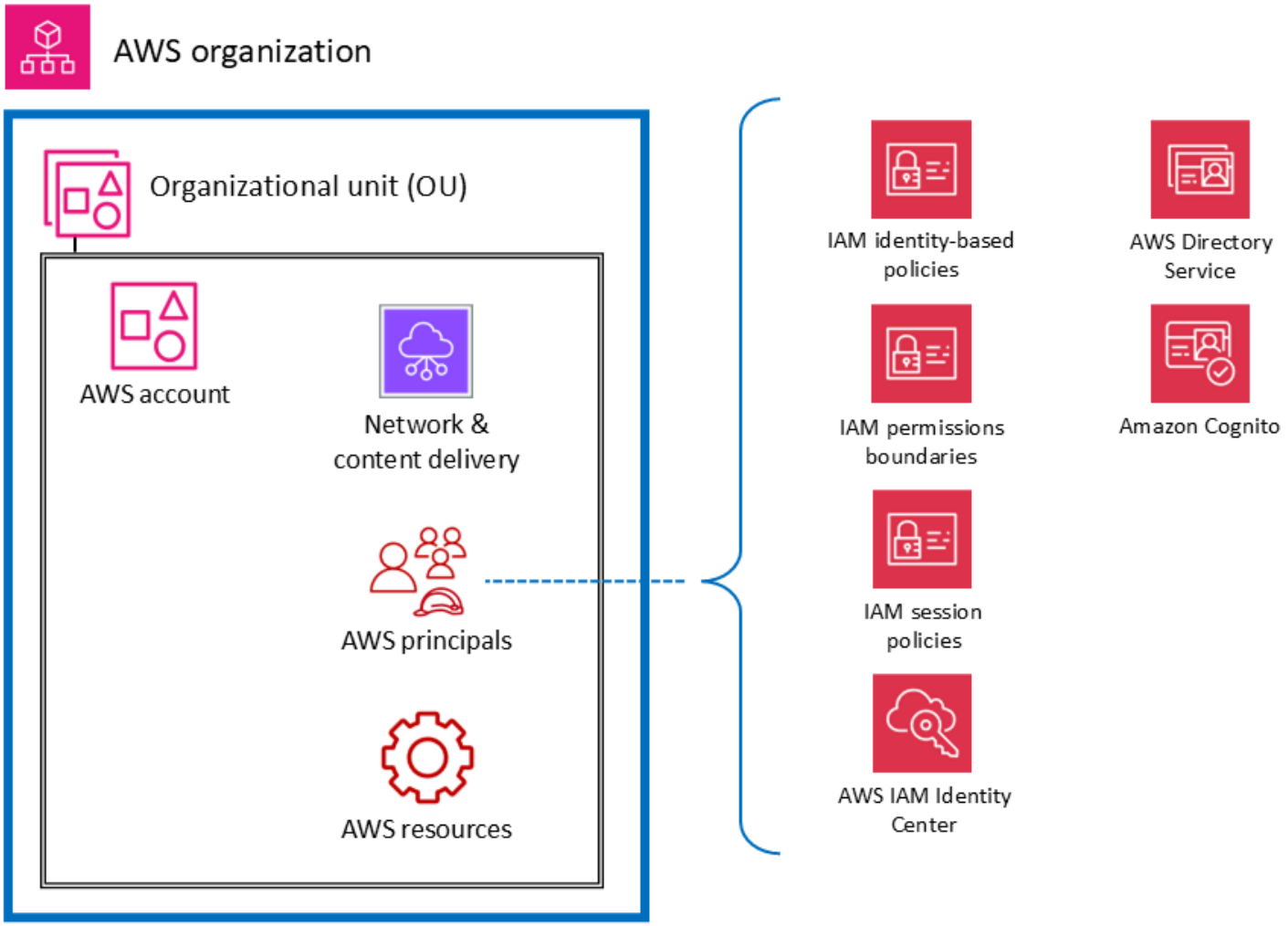
> **Note**
>
> Erstellen Sie keine persistenten API-Schlüssel, die dem AWS Root-Benutzerkonto zugeordnet sind. Der Zugriff auf das Root-Benutzerkonto sollte nur auf die Aufgaben beschränkt werden, für die ein Root-Benutzer erforderlich ist, und dann nur im Rahmen eines strengen Ausnahme- und Genehmigungsverfahrens. Bewährte Methoden zum Schutz des Root-Benutzers Ihres Kontos finden Sie in der IAM-Dokumentation.

Eine AWS Ressource ist ein Objekt, das in einem AWS-Service vorhanden ist und mit dem Sie arbeiten können. Beispiele hierfür sind eine EC2-Instance, ein CloudFormation Stack, ein Amazon

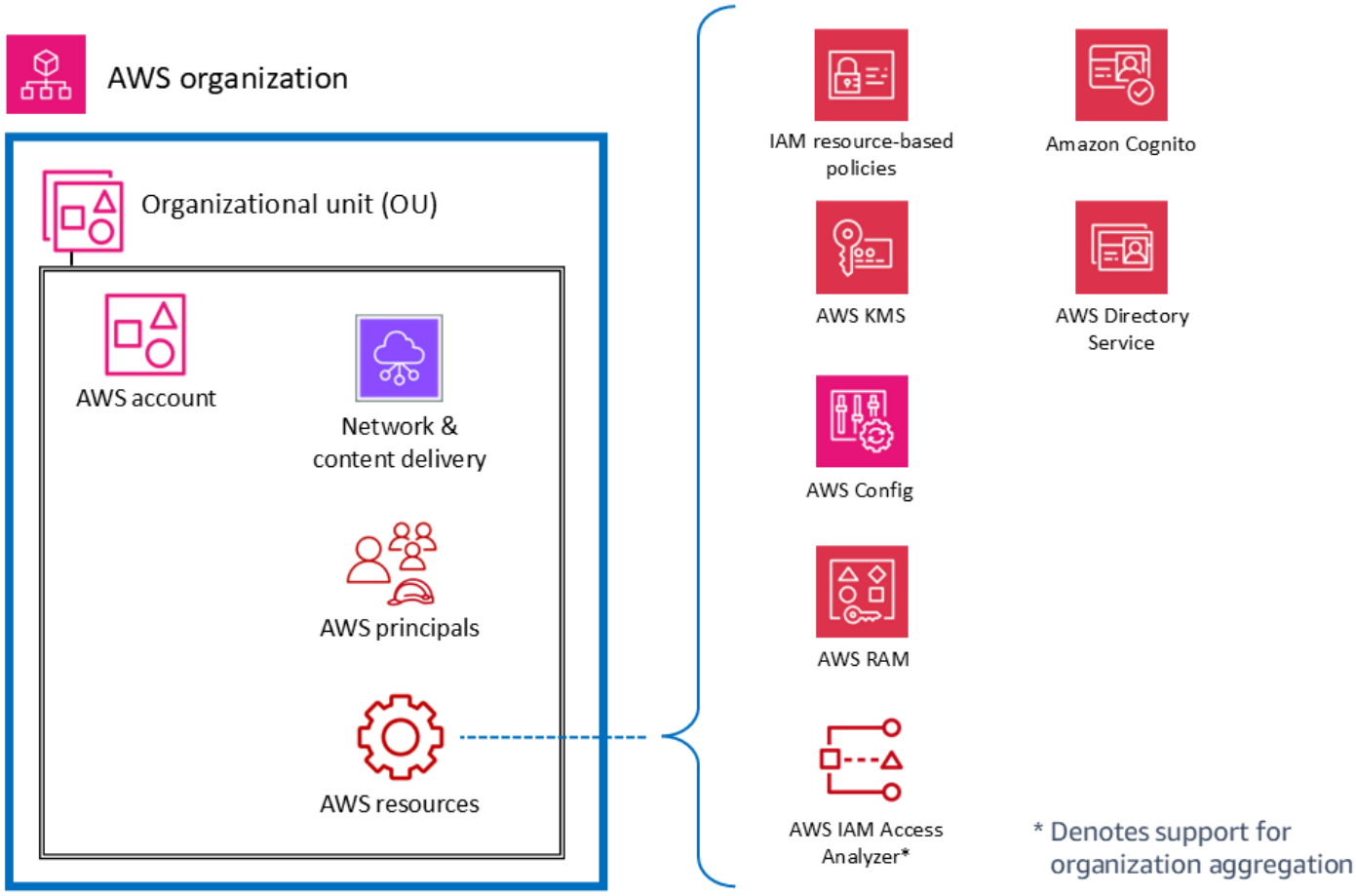
Simple Notification Service (Amazon SNS) -Thema und ein S3-Bucket. IAM-Richtlinien sind Objekte, die Berechtigungen definieren, wenn sie einem IAM-Prinzipal (Benutzer, Gruppe oder Rolle) oder einer IAM-Ressource zugeordnet sind. AWS Identitätsbasierte Richtlinien sind Richtliniendokumente, die Sie einem Prinzipal (Rollen, Benutzer und Benutzergruppen) zuordnen, um zu steuern, welche Aktionen ein Principal auf welchen Ressourcen und unter welchen Bedingungen ausführen kann. Ressourcenbasierte Richtlinien sind Richtliniendokumente, die Sie an eine Ressource wie einen S3-Bucket anhängen. Diese Richtlinien gewähren dem angegebenen Hauptbenutzer die Berechtigung, bestimmte Aktionen an dieser Ressource auszuführen, und definieren die Bedingungen für diese Berechtigung. Ressourcenbasierte Richtlinien sind Inline-Richtlinien. Der Abschnitt mit den IAM-Ressourcen befasst sich eingehender mit den Arten von IAM-Richtlinien und ihrer Verwendung.

Der Einfachheit halber führen wir in dieser Diskussion AWS Sicherheitsdienste und -funktionen für IAM-Prinzipale auf, deren Hauptzweck darin besteht, auf Kontoprinzipalen zu arbeiten oder für diese zu gelten. Wir behalten diese Einfachheit bei und berücksichtigen gleichzeitig die Flexibilität und die weitreichenden Auswirkungen der IAM-Genehmigungsrichtlinien. Eine einzelne Aussage in einer Richtlinie kann Auswirkungen auf mehrere Arten von Entitäten haben. AWS Eine identitätsbasierte IAM-Richtlinie ist zwar einem IAM-Prinzipal zugeordnet und definiert Berechtigungen (Zulassen, Verweigern) für diesen Prinzipal, aber die Richtlinie definiert auch implizit Berechtigungen für die angegebenen Aktionen, Ressourcen und Bedingungen. Auf diese Weise kann eine identitätsbasierte Richtlinie ein entscheidendes Element bei der Definition von Berechtigungen für eine Ressource sein.

Das folgende Diagramm zeigt AWS Sicherheitsdienste und Funktionen für AWS Prinzipale. Identitätsbasierte Richtlinien werden an IAM-Benutzer, -Gruppen oder -Rollen angefügt. Mit diesen Richtlinien können Sie festlegen, welche Aktionen diese Identität durchführen darf (ihre Berechtigungen). Eine IAM-Sitzungsrichtlinie ist eine Inline-Berechtigungsrichtlinie, die Benutzer in der Sitzung weitergeben, wenn sie die Rolle übernehmen. Sie können die Richtlinie selbst verabschieden, oder Sie können Ihren Identity Broker so konfigurieren, dass er die Richtlinie einfügt, wenn sich Ihre Identitäten zusammenschließen. AWS Auf diese Weise können Ihre Administratoren die Anzahl der Rollen reduzieren, die sie erstellen müssen, da mehrere Benutzer dieselbe Rolle übernehmen können, aber über eindeutige Sitzungsberechtigungen verfügen. Der IAM Identity Center-Service ist in den AWS API-Betrieb integriert AWS Organizations und unterstützt Sie bei der Verwaltung des SSO-Zugriffs und der Benutzerberechtigungen AWS-Konten in AWS Organizations allen Bereichen.



Das folgende Diagramm zeigt Dienste und Funktionen für Kontoressourcen. Ressourcenbasierten Richtlinien sind an eine Ressource angefügt. Sie können beispielsweise ressourcenbasierte Richtlinien an S3-Buckets, Amazon Simple Queue Service (Amazon SQS) -Warteschlangen, VPC-Endpunkte und Verschlüsselungsschlüssel anhängen. AWS KMS Sie können ressourcenbasierte Richtlinien verwenden, um festzulegen, wer Zugriff auf die Ressource hat und welche Aktionen sie mit ihr ausführen können. S3-Bucket-Richtlinien, AWS KMS Schlüsselrichtlinien und VPC-Endpunktrichtlinien sind Arten von ressourcenbasierten Richtlinien. IAM Access Analyzer hilft Ihnen dabei, die Ressourcen in Ihrer Organisation und in Ihren Konten, wie S3-Buckets oder IAM-Rollen, zu identifizieren, die mit einer externen Entität gemeinsam genutzt werden. Auf diese Weise können Sie einen unbeabsichtigten Zugriff auf Ihre Ressourcen und Daten identifizieren, der ein Sicherheitsrisiko darstellt. AWS Config ermöglicht es Ihnen, die Konfigurationen der unterstützten AWS Ressourcen in Ihrem AWS-Konten zu beurteilen, zu prüfen und zu bewerten. AWS Config überwacht und zeichnet die AWS Ressourcenkonfigurationen kontinuierlich auf und vergleicht die aufgezeichneten Konfigurationen automatisch mit den gewünschten Konfigurationen.


AWS organization
Organizational unit (OU)
AWS account
Network & content delivery
AWS principals
AWS resources
IAM resource-based policies
Amazon Cognito
AWS KMS
AWS Directory Service
AWS Config
AWS RAM
AWS IAM Access Analyzer*
* Denotes support for organization aggregation

Die AWS Sicherheitsreferenzarchitektur

Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

Das folgende Diagramm veranschaulicht die AWS SRA. Dieses Architekturdiagramm fasst alle AWS sicherheitsrelevanten Dienste zusammen. Es basiert auf einer einfachen, dreistufigen Webarchitektur, die auf eine einzige Seite passt. Bei einem solchen Workload gibt es eine Webebene, über die sich Benutzer mit der Anwendungsebene verbinden und mit ihr interagieren. Diese wiederum kümmert sich um die eigentliche Geschäftslogik der Anwendung: Benutzereingaben entgegennehmen, Berechnungen durchführen und Ausgaben generieren. Die Anwendungsebene speichert und ruft Informationen aus der Datenebene ab. Die Architektur ist bewusst modular aufgebaut und bietet Abstraktion auf hohem Niveau für viele moderne Webanwendungen.

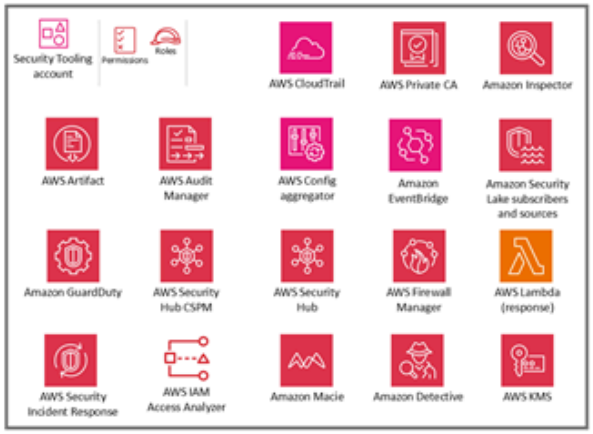
Architekturdiagramme

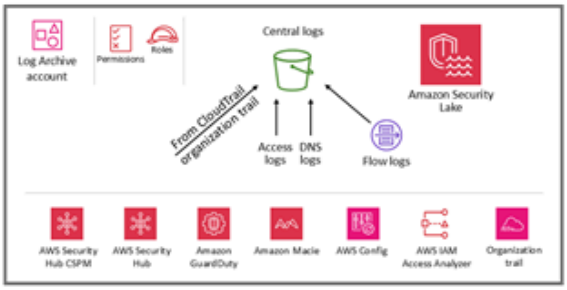
Um die Referenzarchitekturdiagramme in diesem Handbuch an Ihre Geschäftsanforderungen anzupassen, können Sie die folgende ZIP-Datei herunterladen und ihren Inhalt extrahieren.

Laden Sie die Quelldatei des Diagramms herunter (PowerPoint Microsoft-Format)

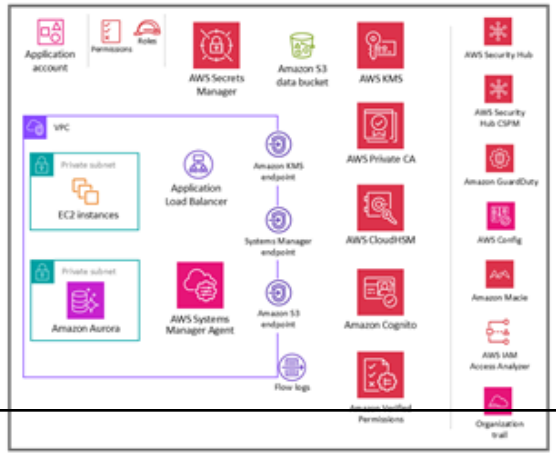
Organization

OU – Security

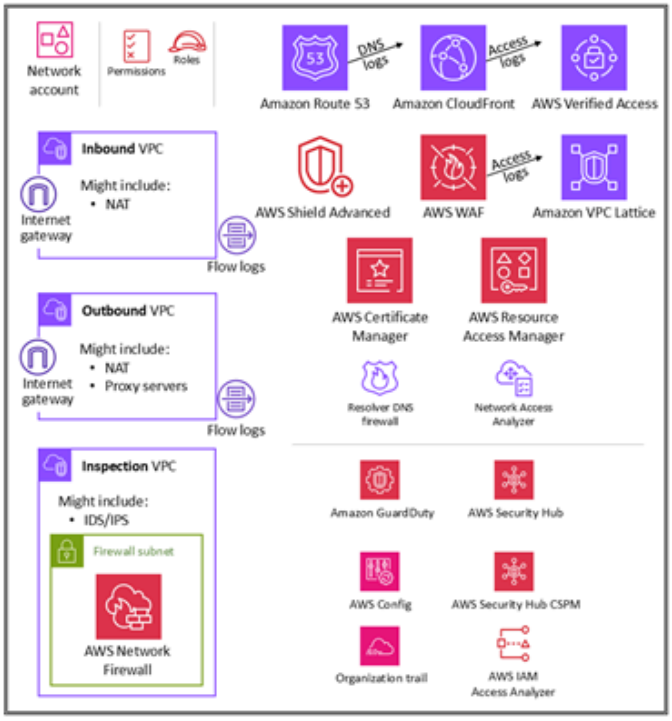


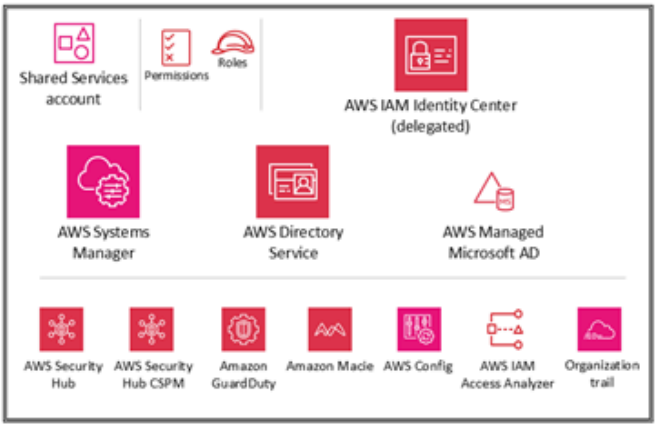


OU – Workloads



OU – Infrastructure





Bei dieser Referenzarchitektur werden die eigentliche Webanwendung und die Datenebene bewusst so einfach wie möglich dargestellt, und zwar durch EC2 Amazon-Instances bzw. eine Amazon Aurora-Datenbank. Die meisten Architekturdiagramme konzentrieren sich auf die Web-, Anwendungs- und Datenebene und befassen sich eingehend damit. Aus Gründen der Lesbarkeit werden in ihnen häufig die Sicherheitskontrollen weggelassen. In diesem Diagramm wird der Schwerpunkt vertauscht, um die Sicherheit zu verdeutlichen, wo immer dies möglich ist, und die Anwendungs- und Datenebene so einfach wie nötig gehalten, um Sicherheitsfunktionen sinnvoll darzustellen.

Die AWS SRA enthält alle AWS sicherheitsrelevanten Dienste, die zum Zeitpunkt der Veröffentlichung verfügbar waren. (Siehe Verlauf der Dokumente.) Aufgrund der jeweiligen Bedrohungslage muss jedoch nicht jeder Workload oder jede Umgebung jeden Sicherheitsservice bereitstellen. Unser Ziel ist es, eine Referenz für eine Reihe von Optionen bereitzustellen, einschließlich einer Beschreibung, wie diese Services architektonisch zusammenpassen, sodass Ihr Unternehmen je nach Risiko Entscheidungen treffen kann, die für Ihre Infrastruktur, Arbeitslast und Sicherheitsanforderungen am besten geeignet sind.

In den folgenden Abschnitten werden die einzelnen Organisationseinheiten und Konten beschrieben, um ihre Ziele und die damit verbundenen individuellen AWS Sicherheitsservices zu verstehen. Für jedes Element (in der Regel ein AWS-Service) enthält dieses Dokument die folgenden Informationen:

- Kurzer Überblick über das Element und seinen Sicherheitszweck in der AWS SRA. Genauere Beschreibungen und technische Informationen zu den einzelnen Diensten finden Sie im Anhang.
- Empfohlene Platzierung, um den Service am effektivsten zu aktivieren und zu verwalten. Dies wird in den einzelnen Architekturdiagrammen für jedes Konto und jede Organisationseinheit erfasst.
- Links zu Konfiguration, Verwaltung und Datenaustausch mit anderen Sicherheitsdiensten. Wie stützt sich dieser Dienst auf andere Sicherheitsdienste oder unterstützt diese?
- Überlegungen zum Design. Zunächst werden in dem Dokument optionale Funktionen oder Konfigurationen hervorgehoben, die wichtige Auswirkungen auf die Sicherheit haben. Zweitens werden diese Optionen in Fällen beschrieben, in denen die Erfahrung unserer Teams häufig Variationen unserer Empfehlungen beinhaltet, die in der Regel auf alternative Anforderungen oder Einschränkungen zurückzuführen sind.

OUs und Konten

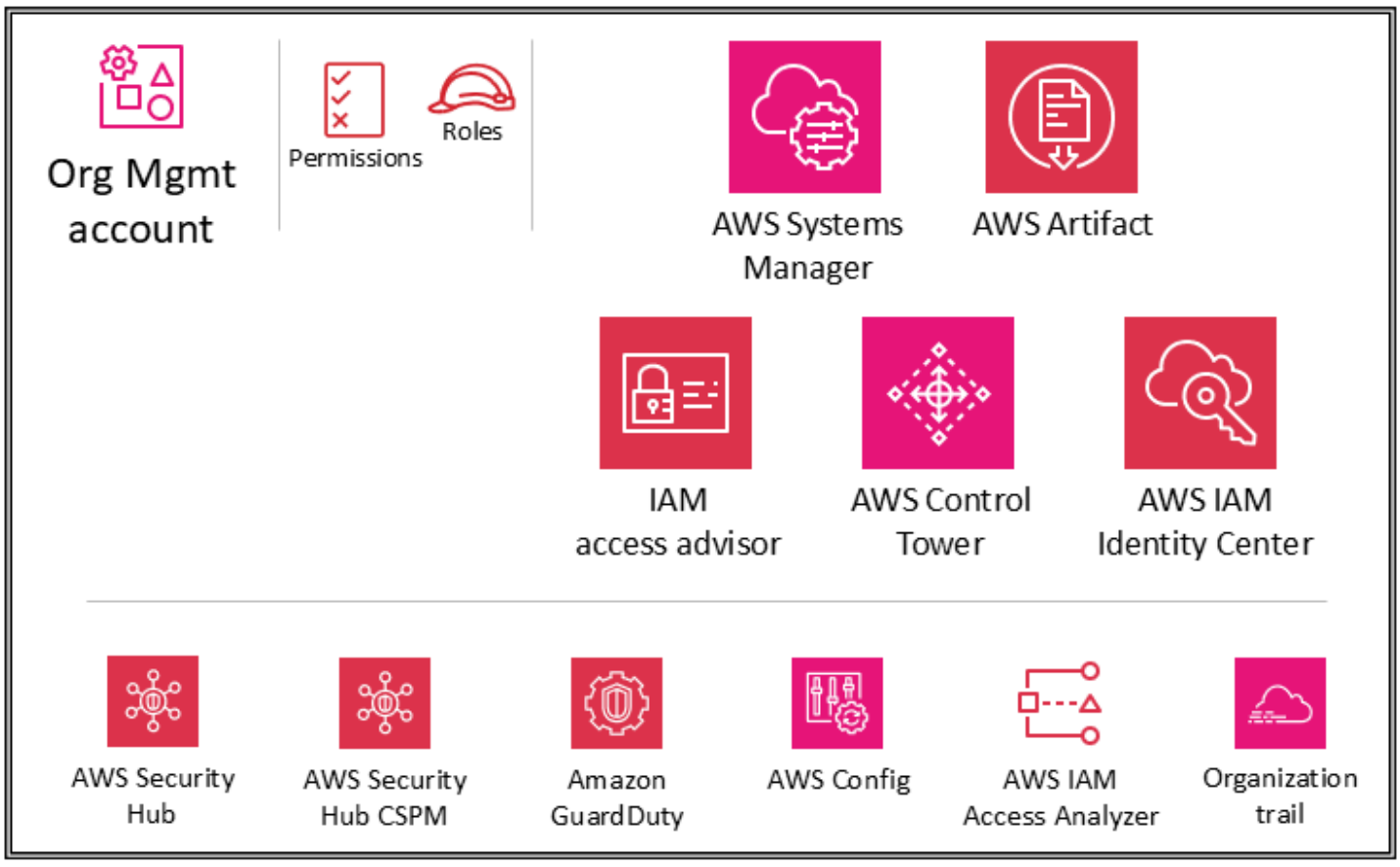
- Konto „Org Management“
- Security OU — Security Tooling-Konto

- Security OU — Konto protokollieren
- Infrastruktur-OE – Netzwerkkonto
- Infrastructure OU — Shared Services-Konto
- Workloads OU — Anwendungskonto

Konto „Org Management“

Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

Das folgende Diagramm zeigt die AWS Sicherheitsdienste, die im Org Management-Konto konfiguriert sind.



In den Abschnitten Aus AWS Organizations Sicherheitsgründen verwenden und Das Verwaltungskonto, vertrauenswürdiger Zugriff und delegierte Administratoren weiter oben in diesem Handbuch wurden der Zweck und die Sicherheitsziele des Org Management-Kontos

ausführlich erörtert. Folgen Sie den bewährten Sicherheitsmethoden für Ihr Org Management-Konto. Dazu gehören die Verwendung einer E-Mail-Adresse, die von Ihrem Unternehmen verwaltet wird, die Pflege der korrekten administrativen und sicherheitstechnischen Kontaktinformationen (z. B. das Anhängen einer Telefonnummer an das Konto für den Fall, dass der Kontoinhaber kontaktiert AWS werden muss), die Aktivierung der Multi-Faktor-Authentifizierung (MFA) für alle Benutzer und die regelmäßige Überprüfung, wer Zugriff auf das Org Management-Konto hat. Dienste, die im Organisationsverwaltungskonto bereitgestellt werden, sollten mit geeigneten Rollen, Vertrauensrichtlinien und anderen Berechtigungen konfiguriert werden, sodass die Administratoren dieser Dienste (die im Organisationsverwaltungskonto darauf zugreifen müssen) nicht auch unangemessen auf andere Dienste zugreifen können.

Service-Kontrollrichtlinien

Mit AWS Organizationskönnen Sie Richtlinien für mehrere AWS-Konten zentral verwalten. Sie können beispielsweise Richtlinien zur Servicesteuerung (SCPs) auf mehrere AWS-Konten Mitglieder einer Organisation anwenden. SCPs ermöglichen es Ihnen, zu definieren, was AWS-Service APIs von IAM-Prinzipalen (wie IAM-Benutzern und Rollen) in den Mitgliedern Ihrer Organisation ausgeführt werden kann und welche nicht. AWS-Konten SCPs werden über das Organisationsverwaltungskonto erstellt und angewendet, AWS-Konto das Sie bei der Erstellung Ihrer Organisation verwendet haben. Weitere Informationen dazu finden Sie weiter oben SCPs in dieser Referenz im Abschnitt „AWS Organizations Aus Sicherheitsgründen verwenden“.

Wenn Sie Ihr AWS Unternehmen AWS Control Tower zur Verwaltung verwenden, wird es eine Reihe von SCPs präventiven Schutzmaßnahmen einrichten (die als verpflichtend, dringend empfohlen oder optional eingestuft werden). Diese Leitplanken unterstützen Sie bei der Verwaltung Ihrer Ressourcen, indem sie unternehmensweite Sicherheitskontrollen durchsetzen. Diese verwenden SCPs automatisch ein aws-control-tower Tag mit dem Wert. managed-by-control-tower

> **Designüberlegung**
>
> SCPs betreffen nur Mitgliedskonten in der AWS Organisation. Sie werden zwar vom Organisationsverwaltungskonto aus angewendet, haben jedoch keine Auswirkungen auf Benutzer oder Rollen in diesem Konto. Weitere Informationen zur Funktionsweise der SCP-Bewertungslogik und Beispiele für empfohlene Strukturen finden Sie im AWS Blogbeitrag How to use service control policies in AWS Organizations.

Richtlinien zur Ressourcenkontrolle

Richtlinien zur Ressourcenkontrolle (RCPs) bieten eine zentrale Kontrolle über die maximal verfügbaren Berechtigungen für Ressourcen in Ihrer Organisation. Ein RCP definiert eine Leitplanke für Berechtigungen oder begrenzt die Aktionen, die Identitäten mit Ressourcen in Ihrer Organisation durchführen können. Sie können RCPs damit einschränken, wer auf Ihre Ressourcen zugreifen kann, und Anforderungen an den Zugriff auf Ihre Ressourcen für Mitglieder Ihrer Organisation durchsetzen. AWS-Konten Sie können sie RCPs direkt an einzelne Konten oder an das Stammverzeichnis der Organisation anhängen. OUs Eine ausführliche Erläuterung der RCPs Funktionsweise finden Sie in der AWS Organizations Dokumentation unter RCP-Bewertung. Weitere Informationen dazu finden Sie weiter oben RCPs in dieser Referenz im Abschnitt Verwendung aus AWS Organizations Sicherheitsgründen.

Wenn Sie Ihr AWS Unternehmen AWS Control Tower zur Verwaltung verwenden, wird es eine Reihe von RCPs präventiven Schutzmaßnahmen einrichten (die als verpflichtend, dringend empfohlen oder optional eingestuft werden). Diese Leitplanken unterstützen Sie bei der Verwaltung Ihrer Ressourcen, indem sie unternehmensweite Sicherheitskontrollen durchsetzen. Diese verwenden SCPs automatisch ein `aws-control-tower` Tag mit dem Wert. `managed-by-control-tower`

Designüberlegungen

- RCPs wirken sich nur auf Ressourcen in Mitgliedskonten der Organisation aus. Sie haben keine Auswirkungen auf Ressourcen im Verwaltungskonto. Dies bedeutet auch, dass sie für Mitgliedskonten RCPs gelten, die als delegierte Administratoren benannt wurden.
- RCPs gelten für Ressourcen für eine Teilmenge von. AWS-Services Weitere Informationen finden Sie RCPs in der AWS Organizations Dokumentation unter Liste AWS-Services dieser Unterstützungen. Sie können die AWS Lambda Funktionen AWS-Config-Regelnund verwenden, um die Durchsetzung von Sicherheitskontrollen für Ressourcen zu überwachen und zu automatisieren, die derzeit nicht von unterstützt werden RCPs.

Deklarative Richtlinien

Eine deklarative Richtlinie ist eine Art von AWS Organizations Verwaltungsrichtlinie, mit deren Hilfe Sie Ihre gewünschte Konfiguration für eine bestimmte AWS-Service Größe in einem Unternehmen zentral deklarieren und durchsetzen können. Deklarative Richtlinien unterstützen derzeit Amazon EC2 -, Amazon VPC - und Amazon EBS-Dienste. Zu den verfügbaren Serviceattributen gehören

die Durchsetzung von Instance Metadata Service Version 2 (IMDSv2), die Möglichkeit der Fehlerbehebung über die serielle EC2-Konsole, das Zulassen von Amazon Machine Image (AMI) -Einstellungen und das Blockieren des öffentlichen Zugriffs für Amazon EBS-Snapshots, Amazon AMIs EC2- und Amazon VPC-Ressourcen. Die neuesten unterstützten Dienste und Attribute finden Sie in der Dokumentation unter Declarative Policies. AWS Organizations

Sie können die Basiskonfiguration für eine erzwingen, AWS-Service indem Sie einige Auswahlen auf den AWS Control Tower Konsolen AWS Organizations und treffen oder einige AWS Command Line Interface (AWS CLI) und AWS SDK-Befehle verwenden. Deklarative Richtlinien werden in der Steuerungsebene des Dienstes durchgesetzt, was bedeutet, dass die Basiskonfiguration für einen immer beibehalten AWS-Service wird, auch wenn der Dienst neue Funktionen einführt oder APIs wenn neue Konten zu einer Organisation hinzugefügt werden oder wenn neue Principals und Ressourcen erstellt werden. Deklarative Richtlinien können auf eine gesamte Organisation oder auf bestimmte Konten angewendet werden. OUs Bei der effektiven Richtlinie handelt es sich um eine Reihe von Regeln, die vom Stamm der Organisation übernommen werden, OUs sowie die Richtlinien, die direkt mit dem Konto verknüpft sind. Wenn eine deklarative Richtlinie getrennt wird, wird das Attribut status auf den Zustand zurückgesetzt, in dem die deklarative Richtlinie hinzugefügt wurde.

Sie können deklarative Richtlinien verwenden, um benutzerdefinierte Fehlermeldungen zu erstellen. Wenn beispielsweise ein API-Vorgang aufgrund einer deklarativen Richtlinie fehlschlägt, können Sie die Fehlermeldung festlegen oder eine benutzerdefinierte URL angeben, z. B. einen Link zu einem internen Wiki oder einen Link zu einer Meldung, die den Fehler beschreibt. Auf diese Weise erhalten Benutzer mehr Informationen, sodass sie das Problem selbst beheben können. Sie können den Prozess der Erstellung deklarativer Richtlinien, der Aktualisierung deklarativer Richtlinien und des Löschens deklarativer Richtlinien auch mithilfe von überprüfen. AWS CloudTrail

Deklarative Richtlinien bieten Kontostatusberichte, mit denen Sie den aktuellen Status aller Attribute überprüfen können, die von deklarativen Richtlinien für die betreffenden Konten unterstützt werden. Sie können auswählen, welche Konten in den Berichtsbereich aufgenommen werden OUs sollen, oder Sie können eine gesamte Organisation auswählen, indem Sie das Stammkonto auswählen. Dieser Bericht hilft Ihnen bei der Bewertung der Einsatzbereitschaft, indem er eine Aufschlüsselung nach AWS-Region und gibt an, ob der aktuelle Status eines Attributs kontenübergreifend einheitlich (anhand des `numberOfMatchedAccounts` Werts) oder kontenübergreifend inkonsistent (anhand des `numberOfUnmatchedAccounts` Werts) ist.

> **Designüberlegung**
>
> Wenn Sie ein Dienstattribut mithilfe einer deklarativen Richtlinie konfigurieren, kann sich die Richtlinie auf mehrere auswirken. APIs Alle nicht konformen Aktionen schlagen fehl. Kontoadministratoren können den Wert des Dienstattributs nicht auf individueller Kontoebene ändern.

Zentralisierter Root-Zugriff

Alle Mitgliedskonten AWS Organizations haben ihren eigenen Root-Benutzer, d. h. eine Identität, die vollständigen Zugriff auf alle AWS-Services Ressourcen in diesem Mitgliedskonto hat. IAM bietet eine zentrale Root-Zugriffsverwaltung zur Verwaltung des Root-Zugriffs für alle Mitgliedskonten. Dies verhindert die Nutzung von Root-Benutzern durch Mitglieder und ermöglicht eine Wiederherstellung in großem Umfang. Die zentrale Root-Zugriffsfunktion verfügt über zwei grundlegende Funktionen: Verwaltung von Root-Anmeldeinformationen und Root-Sitzungen.

- Die Funktion zur Verwaltung von Root-Anmeldeinformationen ermöglicht eine zentrale Verwaltung und trägt dazu bei, Root-Benutzer für alle Verwaltungskonten zu schützen. Diese Funktion umfasst die Entfernung langfristiger Root-Anmeldeinformationen, die Verhinderung der Wiederherstellung von Root-Anmeldeinformationen durch Mitgliedskonten und die Bereitstellung neuer Mitgliedskonten ohne standardmäßige Root-Anmeldeinformationen. Es bietet auch eine einfache Möglichkeit, die Einhaltung der Vorschriften nachzuweisen. Wenn die Root-Benutzerverwaltung zentralisiert ist, können Sie Root-Benutzerkennwörter, Zugriffsschlüssel und Signaturzertifikate entfernen und die Multi-Faktor-Authentifizierung (MFA) für alle Mitgliedskonten deaktivieren.
- Mit der Funktion für Root-Sitzungen können Sie privilegierte Root-Benutzeraktionen ausführen, indem Sie kurzfristige Anmeldeinformationen für Mitgliedskonten aus dem Organisationsverwaltungskonto oder aus delegierten Administratorkonten verwenden. Mit dieser Funktion können Sie kurzfristigen Root-Zugriff ermöglichen, der auf bestimmte Aktionen beschränkt ist und dabei dem Prinzip der geringsten Rechte entspricht.

Für die zentrale Verwaltung von Root-Anmeldeinformationen müssen Sie die Funktionen zur Verwaltung von Root-Anmeldeinformationen und Rootsitzungen auf Organisationsebene über das Organisationsverwaltungskonto oder über ein delegiertes Administratorkonto aktivieren. Gemäß den bewährten AWS SRA-Praktiken delegieren wir diese Funktion an das Security Tooling-Konto. Informationen zur Konfiguration und Verwendung des zentralen Root-Benutzerzugriffs finden

Sie im AWS Sicherheits-Blogbeitrag Zentrale Verwaltung des Root-Zugriffs für Kunden mit. AWS Organizations

IAM Identity Center

AWS IAM Identity Centerist ein Identitätsverbunddienst, mit dem Sie den SSO-Zugriff auf all Ihre Workloads AWS-Konten, Principals und Cloud-Workloads zentral verwalten können. IAM Identity Center unterstützt Sie auch bei der Verwaltung des Zugriffs und der Berechtigungen für häufig verwendete SaaS-Anwendungen (Software as a Service) von Drittanbietern. Identitätsanbieter können mithilfe von SAML 2.0 in IAM Identity Center integriert werden. Die just-in-time Massenverwaltung und Bereitstellung können mithilfe des Systems for Cross-Domain Identity Management (SCIM) erfolgen. IAM Identity Center kann auch als Identitätsanbieter mithilfe von in lokale oder AWS verwaltete Microsoft Active Directory (AD) -Domänen integriert werden. AWS Directory Service IAM Identity Center umfasst ein Benutzerportal, in dem Ihre Endbenutzer die ihnen zugewiesenen AWS-Konten IAM Identity Center, Rollen, Cloud-Anwendungen und benutzerdefinierten Anwendungen an einem Ort finden und darauf zugreifen können.

IAM Identity Center ist standardmäßig nativ in das Org Management-Konto integriert AWS Organizations und wird dort ausgeführt. Um jedoch die geringsten Rechte auszuüben und den Zugriff auf das Verwaltungskonto streng zu kontrollieren, kann die Verwaltung von IAM Identity Center an ein bestimmtes Mitgliedskonto delegiert werden. In der AWS SRA ist das Shared Services-Konto das delegierte Administratorkonto für IAM Identity Center. Bevor Sie die delegierte Administration für IAM Identity Center aktivieren, sollten Sie sich mit diesen Überlegungen vertraut machen. Weitere Informationen zur Delegierung finden Sie im Abschnitt Shared Services-Konto. Auch nachdem Sie die Delegierung aktiviert haben, muss IAM Identity Center weiterhin im Org Management-Konto ausgeführt werden, um bestimmte Aufgaben im Zusammenhang mit IAM Identity Center auszuführen. Dazu gehört auch die Verwaltung von Berechtigungssätzen, die im Org Management-Konto bereitgestellt werden.

In der IAM Identity Center-Konsole werden Konten nach ihrer kapselnden Organisationseinheit angezeigt. Auf diese Weise können Sie Ihre Berechtigungen schnell ermitteln AWS-Konten, allgemeine Berechtigungssätze anwenden und den Zugriff von einem zentralen Ort aus verwalten.

IAM Identity Center umfasst einen Identitätsspeicher, in dem bestimmte Benutzerinformationen gespeichert werden müssen. IAM Identity Center muss jedoch nicht die maßgebliche Quelle für Personalinformationen sein. In Fällen, in denen Ihr Unternehmen bereits über eine zuverlässige Quelle verfügt, unterstützt IAM Identity Center die folgenden Arten von Identitätsanbietern (). IdPs

- IAM Identity Center-Identitätsspeicher — Wählen Sie diese Option, wenn die folgenden beiden Optionen nicht verfügbar sind. Im Identitätsspeicher werden Benutzer erstellt, Gruppenzuweisungen vorgenommen und Berechtigungen zugewiesen. Auch wenn sich Ihre autoritative Quelle außerhalb von IAM Identity Center befindet, wird eine Kopie der Hauptattribute im Identitätsspeicher gespeichert.
- Microsoft Active Directory (AD) — Wählen Sie diese Option, wenn Sie weiterhin Benutzer entweder in Ihrem Verzeichnis in AWS Directory Service for Microsoft Active Directory oder in Ihrem selbstverwalteten Verzeichnis in Active Directory verwalten möchten.
- Externer Identitätsanbieter — Wählen Sie diese Option, wenn Sie Benutzer lieber in einem externen, SAML-basierten Drittanbieter-IdP verwalten möchten.

Sie können sich auf einen bestehenden IdP verlassen, der bereits in Ihrem Unternehmen vorhanden ist. Dies erleichtert die Verwaltung des Zugriffs über mehrere Anwendungen und Dienste hinweg, da Sie den Zugriff von einem einzigen Standort aus erstellen, verwalten und widerrufen. Wenn beispielsweise jemand Ihr Team verlässt, können Sie ihm den Zugriff auf alle Anwendungen und Dienste (einschließlich AWS-Konten) von einem Standort aus entziehen. Dadurch müssen Sie nicht mehr mehrere Anmeldeinformationen angeben und haben die Möglichkeit, sich in Ihre Personalprozesse (HR) zu integrieren.

> **Designüberlegung**
>
> Verwenden Sie einen externen IdP, wenn diese Option für Ihr Unternehmen verfügbar ist. Wenn Ihr IdP System for Cross-Domain Identity Management (SCIM) unterstützt, nutzen Sie die SCIM-Funktion in IAM Identity Center, um die Bereitstellung von Benutzern, Gruppen und Berechtigungen (Synchronisation) zu automatisieren. Auf diese Weise kann der AWS Zugriff für neue Mitarbeiter, Mitarbeiter, die in ein anderes Team wechseln, und Mitarbeiter, die das Unternehmen verlassen, mit Ihrem Unternehmensablauf synchronisiert werden. Sie können jederzeit nur ein Verzeichnis oder einen SAML 2.0-Identitätsanbieter mit IAM Identity Center verbinden. Sie können jedoch zu einem anderen Identitätsanbieter wechseln.

IAM-Zugriffsberater

Der IAM Access Advisor bietet Rückverfolgbarkeitsdaten in Form von Informationen zum zuletzt aufgerufenen Dienst für Sie und. AWS-Konten OUs Verwenden Sie diese detektive Kontrolle, um zu einer Strategie mit den geringsten Rechten beizutragen. Für IAM-Prinzipale können Sie zwei Arten

von Informationen anzeigen, auf die zuletzt zugegriffen wurde: zulässige AWS-Service Informationen und Informationen zu zulässigen Aktionen. Die Informationen enthalten das Datum und die Uhrzeit des Zugriffsversuchs.

Mit dem IAM-Zugriff innerhalb des Org Management-Kontos können Sie die Daten zum letzten Zugriff auf den Dienst für das Organisationsverwaltungskonto, die Organisationseinheit, das Mitgliedskonto oder die IAM-Richtlinie in Ihrer Organisation einsehen. AWS Diese Informationen sind in der IAM-Konsole innerhalb des Verwaltungskontos verfügbar und können auch programmgesteuert abgerufen werden, indem Sie den IAM Access Advisor APIs in oder einen programmatischen Client verwenden. AWS CLI Die Informationen geben an, welche Auftraggeber in einer Organisation oder einem Konto zuletzt versucht haben, auf den Service zuzugreifen, und wann dies geschah. Die Informationen, auf die zuletzt zugegriffen wurde, geben Aufschluss über die tatsächliche Nutzung der Dienste (siehe Beispielszenarien), sodass Sie die IAM-Berechtigungen auf die Dienste beschränken können, die tatsächlich genutzt werden.

AWS Systems Manager

Quick Setup und Explorer — Funktionen, die sowohl den Support AWS Organizations als auch den Betrieb über das Org Management-Konto ermöglichen. AWS Systems Manager

Quick Setup ist eine Automatisierungsfunktion von Systems Manager. Es ermöglicht dem Org Management-Konto, auf einfache Weise Konfigurationen zu definieren, damit Systems Manager in Ihrem Namen für alle Konten in Ihrem AWS Unternehmen tätig wird. Sie können Quick Setup für Ihr gesamtes AWS Unternehmen aktivieren oder eine bestimmte Option auswählen OUs. Quick Setup kann den AWS Systems Manager Agenten (SSM Agent) so planen, dass er alle zwei Wochen Updates für Ihre EC2-Instances ausführt, und kann einen täglichen Scan dieser Instances einrichten, um fehlende Patches zu identifizieren.

Explorer ist ein anpassbares Operations-Dashboard, das Informationen über Ihre Ressourcen enthält. AWS Der Explorer zeigt eine aggregierte Ansicht der Betriebsdaten für Ihre AWS Konten und Across AWS-Regionen an. Dazu gehören Daten über Ihre EC2-Instances und Details zur Patch-Compliance. Nachdem Sie das integrierte Setup (zu dem auch Systems Manager gehört OpsCenter) abgeschlossen haben AWS Organizations, können Sie Daten im Explorer nach Organisationseinheit oder für eine gesamte AWS Organisation aggregieren. Systems Manager aggregiert die Daten im AWS Org Management-Konto, bevor sie im Explorer angezeigt werden.

Im Abschnitt Workloads OU weiter unten in diesem Handbuch wird die Verwendung des SSM-Agenten auf den EC2-Instances im Anwendungskonto beschrieben.

AWS Control Tower

AWS Control Towerbietet eine einfache Möglichkeit, eine sichere AWS Umgebung mit mehreren Konten einzurichten und zu verwalten, die als landing zone bezeichnet wird. AWS Control Tower erstellt Ihre landing zone mithilfe AWS Organizations von Best Practices und bietet fortlaufende Kontoverwaltung und -steuerung sowie Implementierung. Sie können AWS Control Tower damit in wenigen Schritten neue Konten einrichten und gleichzeitig sicherstellen, dass die Konten Ihren Unternehmensrichtlinien entsprechen. Sie können sogar bestehende Konten zu einer neuen AWS Control Tower Umgebung hinzufügen.

AWS Control Tower verfügt über einen breiten und flexiblen Funktionsumfang. Ein wesentliches Merkmal ist die Fähigkeit, die Funktionen mehrerer anderer Systeme AWS-Services, darunter, und IAM Identity Center AWS Organizations AWS Service Catalog, zu orchestrieren, um eine landing zone aufzubauen. Beispielsweise werden standardmäßig zur Festlegung einer Basislinie Richtlinien AWS CloudFormation zur AWS Organizations Dienststeuerung (SCPs) AWS Control Tower verwendet, um Konfigurationsänderungen zu verhindern, und AWS-Config-Regeln Regeln zur kontinuierlichen Erkennung von Nichtkonformitäten. AWS Control Tower verwendet Blueprints, die Ihnen helfen, Ihre AWS Umgebung mit mehreren Konten schnell an den Entwurfsprinzipien von AWS Well Architected Security Foundation auszurichten. Zu den Governance-Funktionen gehören AWS Control Tower Schutzmaßnahmen, die verhindern, dass Ressourcen eingesetzt werden, die nicht den ausgewählten Richtlinien entsprechen.

Sie können mit der Implementierung von AWS SRA-Leitlinien beginnen. AWS Control Tower Richtet beispielsweise eine AWS Control Tower AWS Organisation mit der empfohlenen Multi-Account-Architektur ein. Es bietet Vorlagen für Identitätsmanagement, Verbundzugriff auf Konten, Zentralisierung der Protokollierung, Einrichtung kontenübergreifender Sicherheitsaudits, Definition eines Workflows für die Bereitstellung neuer Konten und Implementierung von Kontenbasislinien mit Netzwerkkonfigurationen.

In der AWS SRA gehört AWS Control Tower es zum Organisationsverwaltungskonto, weil es dieses Konto AWS Control Tower verwendet, um automatisch eine AWS Organisation einzurichten, und dieses Konto als Verwaltungskonto festlegt. Dieses Konto wird für die Abrechnung in Ihrer gesamten Organisation verwendet. AWS Es wird auch für die Account Factory Factory-Bereitstellung von Konten sowie für die Verwaltung und Verwaltung OUs von Leitplanken verwendet. Wenn Sie AWS Control Tower in einer bestehenden AWS Organisation starten, können Sie das bestehende Verwaltungskonto verwenden. AWS Control Tower verwendet dieses Konto als designiertes Verwaltungskonto.

Designüberlegung

Wenn Sie zusätzliche Basiseinstellungen für Kontrollen und Konfigurationen für Ihre Konten vornehmen möchten, können Sie Anpassungen für AWS Control Tower (cFcT) verwenden. Mit CfCT können Sie Ihre AWS Control Tower landing zone mithilfe einer CloudFormation Vorlage anpassen und SCPs. Sie können die benutzerdefinierte Vorlage und die Richtlinien für einzelne Konten und OUs innerhalb Ihrer Organisation bereitstellen. CfCT lässt sich in AWS Control Tower Lebenszyklusereignisse integrieren, um sicherzustellen, dass der Ressourceneinsatz mit Ihrer landing zone synchron bleibt.

AWS Artifact

AWS Artifactbietet On-Demand-Zugriff auf AWS Sicherheits- und Compliance-Berichte und ausgewählte Online-Vereinbarungen. Zu den verfügbaren Berichten AWS Artifact gehören SOC-Berichte (System and Organization Controls), PCI-Berichte (Payment Card Industry) und Zertifizierungen von Akkreditierungsstellen aus verschiedenen Regionen und Compliance-Branchen, die die Implementierung und Betriebseffizienz von Sicherheitskontrollen belegen. AWS AWS Artifact hilft Ihnen bei der Durchführung Ihrer Sorgfaltspflicht und bietet mehr Transparenz in unserer Sicherheitskontrollumgebung. AWS Außerdem können Sie damit die Sicherheit und AWS Einhaltung der Vorschriften kontinuierlich überwachen und sofort auf neue Berichte zugreifen.

AWS Artifact Mit Vereinbarungen können Sie AWS Vereinbarungen wie den Business Associate Addendum (BAA) für ein einzelnes Konto und für die Konten, die Teil Ihrer Organisation sind, überprüfen, akzeptieren und deren Status verfolgen. AWS Organizations

Sie können die AWS Prüfartefakte Ihren Prüfern oder Aufsichtsbehörden als Nachweis für Sicherheitskontrollen zur Verfügung stellen. AWS Sie können auch die in einigen AWS Prüfartefakten enthaltenen Hinweise zur Verantwortung nutzen, um Ihre Cloud-Architektur zu entwerfen. Anhand dieser Leitlinien können Sie festlegen, welche zusätzlichen Sicherheitskontrollen Sie einrichten können, um die spezifischen Anwendungsfälle Ihres Systems zu unterstützen.

AWS Artifact wird im Org Management-Konto gehostet und bietet einen zentralen Ort, an dem Sie Vereinbarungen überprüfen, akzeptieren und verwalten können AWS. Das liegt daran, dass Vereinbarungen, die auf dem Verwaltungskonto akzeptiert werden, auf die Mitgliedskonten übertragen werden.

Designüberlegung

Benutzer innerhalb des Organisationsverwaltungskontos sollten darauf beschränkt werden, nur die Vereinbarungsfunktion von AWS Artifact und sonst nichts zu verwenden. Die Implementierung der Aufgabentrennung AWS Artifact erfolgt auch im Security Tooling-Konto, wo Sie Zugriffsberechtigungen an Ihre Compliance-Beteiligten und externen Prüfer delegieren können, um auf Prüfartefakte zuzugreifen. Sie können diese Trennung implementieren, indem Sie detaillierte IAM-Berechtigungsrichtlinien definieren. Beispiele finden Sie in der Dokumentation unter Beispiele für IAM-Richtlinien. AWS

Leitplanken für verteilte und zentralisierte Sicherheitsdienste

Im AWS SRA,, AWS Security Hub, Amazon AWS Security Hub CSPM GuardDuty, IAM Access Analyzer AWS Config, AWS CloudTrail Organization Trails und oft Amazon Macie werden mit entsprechenden delegierten Guardrails für alle Konten bereitgestellt und bieten außerdem eine zentrale Überwachung, Verwaltung und Steuerung in Ihrer gesamten Organisation. AWS Sie finden diese Gruppe von Diensten in allen Kontotypen, die in der SRA vertreten sind. AWS Diese sollten Teil der Dienste sein AWS-Services , die im Rahmen des Onboarding- und Baselining-Prozesses Ihres Kontos bereitgestellt werden müssen. Das GitHub Code-Repository bietet eine Beispielimplementierung AWS sicherheitsorientierter Dienste für alle Ihre Konten, einschließlich des Org Management-Kontos. AWS

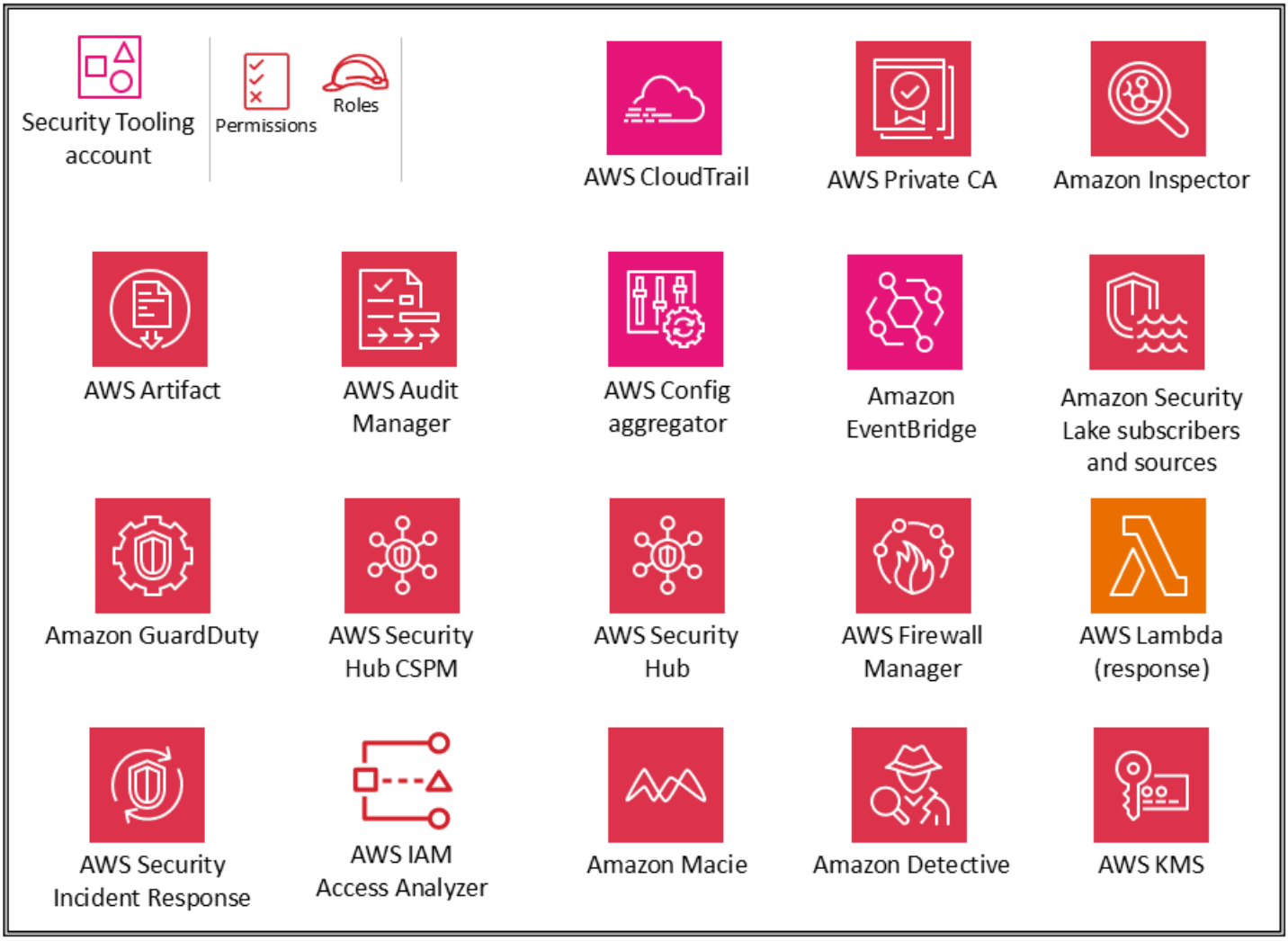
Zusätzlich zu diesen Services umfasst AWS SRA zwei sicherheitsorientierte Services, Amazon Detective und AWS Audit Manager, die die Integration und delegierte Administratorfunktionen in unterstützen. AWS Organizations Diese sind jedoch nicht Teil der empfohlenen Services für das Account-Baselining. Wir haben festgestellt, dass diese Dienste in den folgenden Szenarien am besten verwendet werden:

- Sie verfügen über ein engagiertes Team oder eine Gruppe von Ressourcen, die diese Funktionen der digitalen Forensik und IT-Audits ausführen. Detective wird am besten von Sicherheitsanalystenteams eingesetzt, und Audit Manager ist hilfreich für Ihre internen Audit- oder Compliance-Teams.
- Sie möchten sich zu Beginn Ihres Projekts auf ein Kernpaket von Tools wie AWS Config Amazon GuardDuty und AWS Security Hub CSPM konzentrieren und dann darauf aufbauen, indem Sie Dienste nutzen, die zusätzliche Funktionen bieten. AWS Security Hub

Security OU — Security Tooling-Konto

Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

Das folgende Diagramm zeigt die AWS Sicherheitsdienste, die im Security Tooling-Konto konfiguriert sind.



Das Security Tooling-Konto ist für den Betrieb von Sicherheitsdiensten, die Überwachung AWS-Konten und Automatisierung von Sicherheitswarnungen und deren Reaktion vorgesehen. Zu den Sicherheitszielen gehören die folgenden:

- Richten Sie ein spezielles Konto mit kontrolliertem Zugriff ein, um den Zugriff auf die Sicherheitsleitplanken, die Überwachung und die Reaktion darauf zu verwalten.
- Sorgen Sie für die entsprechende zentrale Sicherheitsinfrastruktur, um die Daten der Sicherheitsoperationen zu überwachen und die Rückverfolgbarkeit zu gewährleisten. Erkennung, Untersuchung und Reaktion sind wichtige Bestandteile des Sicherheitslebenszyklus und können zur Unterstützung eines Qualitätsprozesses, zur Erfüllung gesetzlicher Verpflichtungen oder zur Einhaltung gesetzlicher Vorschriften sowie zur Identifizierung und Abwehr von Bedrohungen eingesetzt werden.
- Unterstützen Sie die defense-in-depth Unternehmensstrategie weiter, indem Sie eine weitere Kontrollebene für die entsprechende Sicherheitskonfiguration und -vorgänge wie Verschlüsselungsschlüssel und Sicherheitsgruppeneinstellungen beibehalten. Dies ist ein Konto, in dem Sicherheitsbeauftragte arbeiten. Typisch sind Rollen mit Lese-/Auditfunktion zur Anzeige AWS unternehmensweiter Informationen, wohingegen write/modify Rollen in ihrer Anzahl begrenzt, streng kontrolliert, überwacht und protokolliert werden.

Designüberlegungen

- AWS Control Tower benennt das Konto unter der Sicherheits-OU standardmäßig das Auditkonto. Sie können das Konto während der AWS Control Tower Einrichtung umbenennen.
- Es kann angemessen sein, mehr als ein Security Tooling-Konto zu haben. Beispielsweise werden die Überwachung und Reaktion auf Sicherheitsereignisse häufig einem speziellen Team zugewiesen. Die Netzwerksicherheit kann ein eigenes Konto und eigene Rollen in Zusammenarbeit mit der Cloud-Infrastruktur oder dem Netzwerkteam erfordern. Bei solchen Aufteilungen wird weiterhin das Ziel verfolgt, zentralisierte Sicherheitsenklaven voneinander zu trennen, wobei die Trennung von Pflichten, geringsten Rechten und die mögliche Einfachheit der Teamzuweisungen weiter betont werden. Wenn Sie diese Option verwenden AWS Control Tower, wird die Erstellung zusätzlicher Funktionen im AWS-Konten Rahmen der Sicherheits-Organisationseinheit eingeschränkt.

Delegierter Administrator für Sicherheitsdienste

Das Security Tooling-Konto dient als Administratorkonto für Sicherheitsdienste, die in einer gesamten administrator/member Struktur verwaltet werden. AWS-Konten Wie bereits erwähnt, erfolgt dies

über die AWS Organizations delegierte Administratorfunktion. Zu den Services in der AWS SRA, die derzeit delegierte Administratoren unterstützen, gehören die zentrale IAM-Verwaltung des Root-Zugriffs,, AWS Config, Amazon AWS Firewall Manager GuardDuty, IAM Access Analyzer, Amazon Macie,,, Amazon Detective AWS Security Hub, AWS Security Hub CSPM, Amazon Inspector AWS Audit Manager, und. AWS CloudTrail AWS Systems Manager Ihr Sicherheitsteam verwaltet die Sicherheitsfunktionen dieser Dienste und überwacht alle sicherheitsspezifischen Ereignisse oder Ergebnisse.

AWS IAM Identity Center unterstützt die delegierte Verwaltung eines Mitgliedskontos. AWS SRA verwendet das Shared Services-Konto als delegiertes Administratorkonto für IAM Identity Center, wie später im Abschnitt IAM Identity Center des Shared Services-Kontos erklärt wird.

Zentralisierter Root-Zugriff

Das Security Tooling-Konto ist das delegierte Administratorkonto für die zentrale Verwaltung der Root-Zugriffsfunktionen durch IAM. Diese Funktion muss auf Organisationsebene aktiviert werden, indem die Verwaltung von Anmeldeinformationen und privilegierte Root-Aktionen in Mitgliedskonten aktiviert werden. Delegierten Administratoren müssen explizit `sts:AssumeRoot` Berechtigungen erteilt werden, um privilegierte Root-Aktionen im Namen von Mitgliedskonten ausführen zu können. Diese Berechtigung ist erst verfügbar, nachdem die privilegierte Root-Aktion in einem Mitgliedskonto im Organisationsverwaltungs- oder delegierten Administratorkonto aktiviert wurde. Mit dieser Berechtigung können Benutzer privilegierte Root-Benutzeraufgaben für Mitgliedskonten zentral vom Security Tooling-Konto aus ausführen. Nachdem Sie eine privilegierte Sitzung gestartet haben, können Sie eine falsch konfigurierte S3-Bucket-Richtlinie löschen, eine falsch konfigurierte SQS-Warteschlangenrichtlinie löschen, die Root-Benutzeranmeldedaten für ein Mitgliedskonto löschen und die Root-Benutzeranmeldeinformationen für ein Mitgliedskonto erneut aktivieren. Sie können diese Aktionen von der Konsole aus ausführen, indem Sie AWS Command Line Interface ()AWS CLI oder über. APIs

AWS CloudTrail

AWS CloudTrailist ein Service, der die Verwaltung, Einhaltung und Prüfung von Aktivitäten in Ihrem Unternehmen unterstützt AWS-Konto. Mit CloudTrail können Sie Kontoaktivitäten im Zusammenhang mit Aktionen in Ihrer gesamten AWS Infrastruktur protokollieren, kontinuierlich überwachen und speichern. CloudTrail ist in integriert AWS Organizations, und diese Integration kann verwendet werden, um einen einzigen Trail zu erstellen, der alle Ereignisse für alle Konten in der AWS Organisation protokolliert. Ein solcher Trail wird als Organisations-Trail bezeichnet. Sie können einen Organisationspfad nur über das Verwaltungskonto für die Organisation oder über ein delegiertes

Administratorkonto erstellen und verwalten. Wenn Sie einen Organisationspfad erstellen, wird in jedem Pfad, der zu Ihrer AWS Organisation gehört AWS-Konto , ein Pfad mit dem von Ihnen angegebenen Namen erstellt. Der Trail protokolliert Aktivitäten für alle Konten, einschließlich des Verwaltungskontos, in der AWS Organisation und speichert die Protokolle in einem einzigen S3-Bucket. Aufgrund der Sensibilität dieses S3-Buckets sollten Sie ihn sichern, indem Sie die bewährten Methoden befolgen, die weiter unten in diesem Handbuch im Abschnitt Amazon S3 als zentraler Protokollspeicher beschrieben werden. Alle Accounts in der AWS Organisation können den Organisations-Trail in ihrer Trail-Liste sehen. Mitglieder AWS-Konten haben jedoch nur Lesezugriff auf diesen Trail. Wenn Sie in der CloudTrail Konsole einen Organisations-Trail erstellen, handelt es sich bei dem Trail standardmäßig um einen Trail mit mehreren Regionen. Weitere bewährte Sicherheitsmethoden finden Sie in der CloudTrailDokumentation.

In der AWS SRA ist das Security Tooling-Konto das delegierte Administratorkonto für die Verwaltung. CloudTrail Der entsprechende S3-Bucket zum Speichern der Organization Trail Logs wird im Log Archive-Konto erstellt. Dies dient dazu, die Verwaltung und Nutzung von CloudTrail Protokollberechtigungen voneinander zu trennen. Informationen zum Erstellen oder Aktualisieren eines S3-Buckets zum Speichern von Protokolldateien für einen Organization Trail finden Sie in der CloudTrail Dokumentation. Aus Sicherheitsgründen empfiehlt es sich, den `aws:SourceArn` Bedingungsschlüssel des Organisationstrails zur Ressourcenrichtlinie des S3-Buckets (und aller anderen Ressourcen wie KMS-Schlüssel oder SNS-Themen) hinzuzufügen. Dadurch wird sichergestellt, dass der S3-Bucket nur Daten akzeptiert, die mit dem jeweiligen Trail verknüpft sind. Der Trail ist mit einer Protokolldateivalidierung zur Überprüfung der Integrität der Protokolldatei konfiguriert. Die Protokoll- und Digest-Dateien werden mithilfe von SSE-KMS verschlüsselt. Der Organization Trail ist auch in eine Protokollgruppe in CloudWatch Logs integriert, um Ereignisse zur langfristigen Aufbewahrung zu senden.

> **Note**
>
> Sie können Organisationspfade sowohl über Verwaltungs- als auch über delegierte Administratorkonten erstellen und verwalten. Es hat sich jedoch bewährt, den Zugriff auf das Verwaltungskonto zu beschränken und die delegierte Administratorfunktion zu verwenden, sofern sie verfügbar ist.

Designüberlegungen

- CloudTrail protokolliert standardmäßig keine Datenereignisse, da es sich dabei häufig um umfangreiche Aktivitäten handelt. Sie sollten jedoch Datenereignisse für bestimmte kritische AWS Ressourcen wie S3-Buckets, Lambda-Funktionen, Protokollereignisse von außen, AWS die an den CloudTrail Lake gesendet werden, und SNS-Themen erfassen. Konfigurieren Sie dazu Ihren Organisationspfad so, dass er Datenereignisse aus bestimmten Ressourcen einbezieht, indem Sie die Daten ARNs der einzelnen Ressourcen angeben.
- Wenn ein Mitgliedskonto Zugriff auf CloudTrail Protokolldateien für sein eigenes Konto benötigt, können Sie die CloudTrail Protokolldateien der Organisation selektiv vom zentralen S3-Bucket aus teilen. Wenn Mitgliedskonten jedoch lokale CloudWatch Amazon-Protokollgruppen für die CloudTrail Protokolle ihres Kontos benötigen oder die Protokollverwaltung und Datenereignisse (schreibgeschützt, schreibgeschützt, Verwaltungsereignisse, Datenereignisse) anders als der Organisations-Trail konfigurieren möchten, können sie einen lokalen Trail mit den entsprechenden Kontrollen erstellen. Für lokale kontospezifische Protokolle fallen zusätzliche Kosten an.

AWS Security Hub CSPM

AWS Security Hub Cloud Security Posture Management (AWS Security Hub CSPM), früher bekannt als AWS Security Hub, bietet Ihnen einen umfassenden Überblick über Ihren Sicherheitsstatus AWS und hilft Ihnen dabei, Ihre Umgebung anhand von Branchenstandards und bewährten Methoden zu überprüfen. Security Hub CSPM sammelt Sicherheitsdaten aus allen AWS integrierten Diensten, unterstützten Produkten von Drittanbietern und anderen benutzerdefinierten Sicherheitsprodukten, die Sie möglicherweise verwenden. Er hilft Ihnen dabei, Ihre Sicherheitstrends laufend zu überwachen und zu analysieren und Sicherheitsprobleme mit höchster Priorität zu identifizieren. Zusätzlich zu den aufgenommenen Quellen generiert Security Hub CSPM seine eigenen Ergebnisse, die durch Sicherheitskontrollen repräsentiert werden, die einem oder mehreren Sicherheitsstandards entsprechen. Zu diesen Standards gehören AWS Foundational Security Best Practices (FSBP), Benchmark v1.20 und v1.4.0 der Center for Internet Security (CIS) AWS Foundations, SP 800-53 Rev. 5 des National Institute of Standards and Technology (NIST), Payment Card Industry Data Security Standard (PCI DSS) und servicemanaged Standards. Eine Liste der aktuellen Sicherheitsstandards und Einzelheiten zu bestimmten Sicherheitskontrollen finden Sie in der Standardreferenz für Security Hub CSPM in der Security Hub CSPM-Dokumentation.

Security Hub CSPM lässt sich in all Ihre bestehenden und future Konten in Ihrem AWS Unternehmen integrieren, AWS Organizations um die Verwaltung des Sicherheitsstatus zu vereinfachen. Sie können die zentrale CSPM-Konfigurationsfunktion von Security Hub aus dem delegierten Administratorkonto (in diesem Fall Security Tooling) verwenden, um anzugeben, wie der Security Hub CSPM-Dienst, die Sicherheitsstandards und die Sicherheitskontrollen in Ihren Unternehmenskonten und Organisationseinheiten () regionsübergreifend konfiguriert werden. OUs Sie können diese Einstellungen in wenigen Schritten von einer Hauptregion aus konfigurieren, die als Heimatregion bezeichnet wird. Wenn Sie die zentrale Konfiguration nicht verwenden, müssen Sie Security Hub CSPM für jedes Konto und jede Region separat konfigurieren. Der delegierte Administrator kann Konten OUs als selbstverwaltete Konten festlegen, bei denen das Mitglied die Einstellungen in jeder Region separat konfigurieren kann, oder als zentral verwaltete Konten, bei denen der delegierte Administrator das Mitgliedskonto oder die Organisationseinheit regionsübergreifend konfigurieren kann. Sie können alle Konten OUs in Ihrer Organisation als zentral verwaltete Konten, alle selbstverwaltete Konten oder als eine Kombination aus beidem festlegen. Dies vereinfacht die Durchsetzung einer konsistenten Konfiguration und bietet gleichzeitig die Flexibilität, sie für jede Organisationseinheit und jedes Konto zu ändern.

Das delegierte Security Hub-CSPM-Administratorkonto kann auch Ergebnisse, Einblicke und Kontrolldetails aller Mitgliedskonten einsehen. Sie können zusätzlich eine Aggregationsregion innerhalb des delegierten Administratorkontos festlegen, um Ihre Ergebnisse für Ihre Konten und Ihre verknüpften Regionen zu zentralisieren. Ihre Ergebnisse werden kontinuierlich und bidirektional zwischen der Aggregator-Region und allen anderen Regionen synchronisiert.

Security Hub CSPM unterstützt Integrationen mit mehreren. AWS-Services Amazon GuardDuty AWS Config, Amazon Macie, IAM Access Analyzer, Amazon Inspector AWS Firewall Manager, Amazon Route 53 Resolver DNS Firewall und AWS Systems Manager Patch Manager können die Ergebnisse an Security Hub CSPM weiterleiten. Security Hub CSPM verarbeitet Ergebnisse mithilfe eines Standardformats, dem AWS Security Finding Format (ASFF). Security Hub CSPM korreliert die Ergebnisse der integrierten Produkte, um die wichtigsten zu priorisieren. Sie können die Metadaten der Security Hub CSPM-Ergebnisse anreichern, um die Sicherheitsergebnisse besser zu kontextualisieren, zu priorisieren und Maßnahmen zu ergreifen. Diese Erweiterung fügt jedem Ergebnis, das in Security Hub CSPM aufgenommen wird, Ressourcen-Tags, ein neues AWS Anwendungs-Tag und Informationen zu Kontonamen hinzu. Auf diese Weise können Sie die Ergebnisse für Automatisierungsregeln verfeinern, Ergebnisse und Erkenntnisse suchen oder filtern und den Sicherheitsstatus der einzelnen Anwendungen beurteilen. Darüber hinaus können Sie Automatisierungsregeln verwenden, um die Ergebnisse automatisch zu aktualisieren. Wenn Security Hub CSPM Ergebnisse aufnimmt, kann es eine Vielzahl von Regelaktionen anwenden, z. B. die

Unterdrückung von Ergebnissen, die Änderung ihres Schweregrads und das Hinzufügen von Notizen zu Ergebnissen. Diese Regelaktionen werden wirksam, wenn die Ergebnisse Ihren angegebenen Kriterien entsprechen, z. B. der Ressource oder dem Konto, mit IDs der das Ergebnis verknüpft ist, oder dem Titel. Sie können Automatisierungsregeln verwenden, um ausgewählte Suchfelder im ASFF zu aktualisieren. Die Regeln gelten sowohl für neue als auch für aktualisierte Ergebnisse.

Während der Untersuchung eines Sicherheitsereignisses können Sie von Security Hub CSPM zu Amazon Detective wechseln, um einen GuardDuty Befund zu untersuchen. Security Hub CSPM empfiehlt, die delegierten Administratorkonten für Dienste wie Detective (sofern vorhanden) aufeinander abzustimmen, um eine reibungslosere Integration zu gewährleisten. Wenn Sie beispielsweise keine Administratorkonten zwischen Detective und Security Hub CSPM abgleichen, funktioniert das Navigieren von den Ergebnissen zu Detective nicht. Eine umfassende Liste finden Sie unter Überblick über AWS-Service Integrationen mit Security Hub CSPM in der Security Hub CSPM-Dokumentation.

Sie können Security Hub CSPM mit der Network Access Analyzer-Funktion von Amazon VPC verwenden, um die Einhaltung Ihrer AWS Netzwerkkonfiguration kontinuierlich zu überwachen. Auf diese Weise können Sie unerwünschten Netzwerkzugriff blockieren und verhindern, dass Ihre kritischen Ressourcen von außen zugänglich sind. Weitere Architektur- und Implementierungsdetails finden Sie im AWS Blogbeitrag Kontinuierliche Überprüfung der Netzwerk-Compliance mit Amazon VPC Network Access Analyzer und AWS Security Hub CSPM.

Zusätzlich zu seinen Überwachungsfunktionen unterstützt Security Hub CSPM die Integration mit Amazon, EventBridge um die Behebung bestimmter Fehler zu automatisieren. Sie können benutzerdefinierte Aktionen definieren, die ausgeführt werden, wenn ein Ergebnis eingeht. Sie können beispielsweise benutzerdefinierte Aktionen konfigurieren, damit Ergebnisse an ein Ticketing-System oder ein automatisiertes Behebungssystem gesendet werden. Weitere Diskussionen und Beispiele finden Sie in den AWS Blogbeiträgen Automated response and remediation with AWS Security Hub CSPM und How to deploy the AWS solution for Security Hub CSPM automated response and remediation.

Security Hub CSPM verwendet Service-Linked AWS-Config-Regeln , um die meisten seiner Sicherheitsprüfungen für Kontrollen durchzuführen. Um diese Kontrollen zu unterstützen, AWS Config muss sie für alle Konten — einschließlich des Administratorkontos (oder delegierten Administratorkontos) und der Mitgliedskonten — in allen Konten aktiviert sein, in AWS-Region denen Security Hub CSPM aktiviert ist.

Designüberlegungen

- Wenn ein Compliance-Standard wie PCI-DSS bereits in Security Hub CSPM vorhanden ist, ist der vollständig verwaltete Security Hub CSPM-Dienst der einfachste Weg, ihn zu operationalisieren. Wenn Sie jedoch Ihren eigenen Compliance- oder Sicherheitsstandard zusammenstellen möchten, der Sicherheits-, Betriebs- oder Kostenoptimierungsprüfungen beinhalten kann, bieten Konformitätspakete einen vereinfachten Anpassungsprozess. AWS Config (Weitere Informationen zu Konformitätspaketen AWS Config und Konformitätspaketen finden Sie im AWS ConfigAbschnitt.)
- Zu den häufigsten Anwendungsfällen für Security Hub CSPM gehören:
  - Als Dashboard, das Anwendungsbesitzern Einblick in den Sicherheits- und Compliance-Status ihrer Ressourcen bietet AWS
  - Als zentrale Ansicht der Sicherheitsergebnisse, die von Sicherheitsabteilungen, Incident-Respondern und Bedrohungsjägern genutzt werden, um AWS Sicherheits- und Compliance-Ergebnisse in allen Regionen zu analysieren und entsprechende Maßnahmen zu ergreifen AWS-Konten
  - Um Sicherheits- und Compliance-Erkenntnisse aus verschiedenen Regionen zu aggregieren AWS-Konten und an ein zentrales SIEM (Security Information and Event Management) oder ein anderes Sicherheitsorchestrierungssystem weiterzuleiten

  Weitere Anleitungen zu diesen Anwendungsfällen, einschließlich ihrer Einrichtung, finden Sie im Blogbeitrag Drei wiederkehrende Security Hub CSPM-Nutzungsmuster und deren Implementierung.

Beispiel für eine Implementierung

Die AWS SRA-Codebibliothek bietet eine Beispielimplementierung von Security Hub CSPM. Es umfasst die automatische Aktivierung des Dienstes, die delegierte Verwaltung an ein Mitgliedskonto (Security Tooling) und die Konfiguration zur Aktivierung von Security Hub CSPM für alle bestehenden und future Konten in der Organisation. AWS

AWS Security Hub

AWS Security Hubist eine einheitliche Cloud-Sicherheitslösung, die Ihre kritischen Sicherheitsbedrohungen priorisiert und Ihnen hilft, in großem Umfang darauf zu reagieren. Security Hub erkennt Sicherheitsprobleme nahezu in Echtzeit, indem es Sicherheitssignale aus verschiedenen Quellen wie Posture Management (AWS Security Hub CSPM), Schwachstellenmanagement (Amazon Inspector), vertrauliche Daten (Amazon Macie) und Bedrohungserkennung (Amazon) automatisch korreliert und anreichert. GuardDuty Auf diese Weise können Sicherheitsteams aktive Risiken in ihren Cloud-Umgebungen durch automatisierte Analysen und kontextuelle Einblicke priorisieren. Security Hub bietet eine visuelle Darstellung des potenziellen Angriffspfads, den Angreifer ausnutzen können, um Zugriff auf Ressourcen zu erhalten, die mit einer Sicherheitslücke verknüpft sind. Dadurch werden komplexe Sicherheitssignale in umsetzbare Erkenntnisse umgewandelt, sodass Sie schnell fundierte Entscheidungen zu Ihrer Sicherheit treffen können.

Security Hub wurde strategisch neu gestaltet, um die Aktivierung der zugehörigen Sicherheitsdienst-Bausteine zu vereinfachen, um ein Sicherheitsergebnis zu erzielen. Indem Sie die Sicherheitsergebnisse in einer Bedrohungsmatrix über verschiedene Sicherheitssignale hinweg nahezu in Echtzeit korrelieren, können Sie die kritischsten Risiken zuerst priorisieren. Die Ergebnisse werden korreliert, um Risiken im Zusammenhang mit Ressourcen zu erkennen. AWS Sicherheitslücken stellen umfassendere Schwächen bei Sicherheitskontrollen, Fehlkonfigurationen oder anderen Bereichen dar, die durch aktive Bedrohungen ausgenutzt werden könnten. Bei einer Sicherheitslücke kann es sich beispielsweise um eine EC2-Instance handeln, die über das Internet erreichbar ist und Software-Sicherheitslücken aufweist, die mit hoher Wahrscheinlichkeit ausgenutzt werden können.

Security Hub und Security Hub CSPM sind ergänzende Dienste. Security Hub CSPM bietet einen umfassenden Überblick über Ihren Sicherheitsstatus und hilft Ihnen dabei, Ihre Cloud-Umgebung anhand von Industriestandards und Best Practices zu bewerten. Security Hub bietet ein einheitliches Erlebnis, mit dem Sie kritische Sicherheitsprobleme priorisieren und darauf reagieren können. Die CSPM-Ergebnisse von Security Hub werden automatisch an Security Hub weitergeleitet, wo sie mit Ergebnissen anderer Sicherheitsdienste wie Amazon Inspector korreliert werden, um Risiken zu generieren. Auf diese Weise können Sie die kritischsten Risiken in Ihrer Umgebung identifizieren.

Security Hub bietet auch eine Zusammenfassung der Ressourcen in Ihrer AWS Umgebung nach Typ und den zugehörigen Ergebnissen. Ressourcen werden nach Risiken und Angriffssequenzen priorisiert. Wenn Sie einen Ressourcentyp auswählen, können Sie alle Ressourcen überprüfen, die diesem Ressourcentyp zugeordnet sind.

Für ein optimales Erlebnis empfehlen wir, Security Hub und Security Hub CSPM sowie die folgenden anderen Sicherheitsdienste zu aktivieren: Amazon GuardDuty, Amazon Inspector und Amazon Macie. Anhand der Ergebnisse der Security Hub Hub-Abdeckung können Sie sich einen Überblick darüber verschaffen, ob diese Dienste und Funktionen für alle Mitgliedskonten Ihres Unternehmens einheitlich aktiviert sind.

In der AWS SRA fungiert das Security Tooling-Konto als delegierter Administrator für Security Hub, Security Hub CSPM und andere Sicherheitsdienste. AWS Im Security Tooling-Konto können Sie alle Ressourcen einsehen, die mit Mitgliedskonten verknüpft sind. Sie können auch alle Ressourcen in Ihrem Zuhause AWS-Region von Linked AWS-Regionen aus einsehen.

Hinweis zur Implementierung

Die Aktivierung von Security Hub erfordert drei Schritte, einschließlich Verfahren, bei denen berücksichtigt wird, ob Sie Security Hub CSPM zuvor aktiviert haben. Security Hub ist nativ integriert AWS Organizations, was den Konfigurations- und Implementierungsprozess vereinfacht und alle Ergebnisse an einem einzigen Ort zentralisiert und aggregiert. Verwenden Sie gemäß den AWS SRA-Best Practices das Security Tooling-Konto als delegiertes Administratorkonto für die Verwaltung und Konfiguration von Security Hub. Verwenden Sie die Security Hub Hub-Konfigurationseinstellungen, um alle Regionen OUs, und Konten automatisch zu aktivieren, einschließlich future Regionen und Konten. Sie sollten auch eine regionsübergreifende Aggregation einrichten, um Ergebnisse, Ressourcen und Trends aus mehreren Regionen AWS-Regionen in einer einzigen Heimatregion zusammenzufassen. Während der Konfiguration können Sie auch alle nativen Integrationen wie Jira Cloud oder aktivieren. ServiceNow

Designüberlegungen

- Die Ergebnisse von Security Hub werden im Open Cybersecurity Schema Framework (OCSF) formatiert. Security Hub generiert Ergebnisse in OCSF und empfängt Ergebnisse in OCSF von Security Hub CSPM und anderen. AWS-Services Diese OCSF-Ergebnisse können EventBridge zur Automatisierung über Amazon gesendet oder in einem zentralen Protokollaggregationskonto gespeichert werden, um die Analyse und Aufbewahrung von Sicherheitsprotokollen durchzuführen.

- Das AWS Org Management-Konto kann sich nicht selbst als delegierter Administrator in Security Hub bezeichnen. Dies entspricht der bewährten AWS SRA-Methode, das Security Tooling-Konto als delegierten Administrator festzulegen. Beachten Sie auch:
  - Das designierte Administratorkonto für Security Hub CSPM wird automatisch zum designierten Administrator für Security Hub.
  - Durch das Entfernen der delegierten Administration über Security Hub wird auch die delegierte Administration für Security Hub CSPM entfernt. Wenn Sie die delegierte Verwaltung über Security Hub CSPM entfernen, wird sie auch für Security Hub entfernt.
- Security Hub umfasst Funktionen, die Ergebnisse auf der Grundlage Ihrer Spezifikationen automatisch ändern und darauf reagieren. Security Hub unterstützt die folgenden Arten von Automatisierungen:
  - Automatisierungsregeln, die Ergebnisse automatisch aktualisieren, Ergebnisse unterdrücken und Ergebnisse auf der Grundlage definierter Kriterien nahezu in Echtzeit an Ticketing-Tools senden.
  - Automatisierte Reaktion und Problembehebung, bei der benutzerdefinierte EventBridge Regeln erstellt werden, die automatische Maßnahmen definieren, die auf der Grundlage bestimmter Ergebnisse und Erkenntnisse ergriffen werden sollen.
- Security Hub kann Amazon Inspector mithilfe von Richtlinien für alle Mitgliedskonten und Regionen konfigurieren GuardDuty und Security Hub CSPM während der Bereitstellung konfigurieren. Richtlinien generieren AWS Organizations Richtlinien für Konten und Regionen. Bereitstellungen sind einmalige Aktionen, die eine Sicherheitsfunktion für ausgewählte Konten und Regionen ermöglichen. Bereitstellungen gelten nicht für neu aktivierte Konten. Als Alternative können Sie Funktionen für neue Mitgliedskonten in Security Hub GuardDuty CSPM automatisch aktivieren.

Amazon GuardDuty

Amazon GuardDuty ist ein Service zur Bedrohungserkennung, der kontinuierlich nach böswilligen Aktivitäten und unberechtigtem Verhalten sucht, um Sie AWS-Konten und Ihre Workloads zu schützen. Sie müssen immer die entsprechenden Protokolle für Überwachungs- und Prüfungszwecke erfassen und speichern, GuardDuty beziehen jedoch unabhängige Datenströme direkt aus AWS CloudTrail Amazon VPC-Flussprotokollen und AWS DNS-Protokollen. Sie müssen weder die Amazon S3 S3-Bucket-Richtlinien verwalten noch die Art und Weise ändern, wie Sie Ihre Logs sammeln und speichern. GuardDutyBerechtigungen werden als dienstbezogene Rollen verwaltet, die Sie

jederzeit widerrufen können, indem Sie sie deaktivieren GuardDuty. Auf diese Weise kann der Dienst ohne komplexe Konfiguration einfach aktiviert werden, und das Risiko, dass eine Änderung der IAM-Berechtigungen oder der S3-Bucket-Richtlinie den Betrieb des Dienstes beeinträchtigt, wird vermieden.

Neben der Bereitstellung grundlegender Datenquellen GuardDuty bietet es optionale Funktionen zur Identifizierung von Sicherheitslücken. Dazu gehören EKS-Schutz, RDS-Schutz, S3-Schutz, Malware-Schutz und Lambda-Schutz. Für neue Melder sind diese optionalen Funktionen standardmäßig aktiviert, mit Ausnahme von EKS-Schutz, der manuell aktiviert werden muss.

- Mit GuardDuty S3 Protection werden zusätzlich zu den standardmäßigen CloudTrail Verwaltungsereignissen auch Amazon S3 S3-Datenereignisse GuardDuty überwacht. CloudTrail Die Überwachung von Datenereignissen ermöglicht GuardDuty die Überwachung von API-Vorgängen auf Objektebene im Hinblick auf potenzielle Sicherheitsrisiken für Daten in Ihren S3-Buckets.
- GuardDuty Malware Protection erkennt das Vorhandensein von Malware auf Amazon EC2 EC2-Instances oder Container-Workloads, indem es agentenlose Scans auf verbundenen Amazon Elastic Block Store (Amazon EBS) -Volumes initiiert. GuardDuty erkennt auch potenzielle Malware in S3-Buckets, indem neu hochgeladene Objekte oder neue Versionen vorhandener Objekte gescannt werden.
- GuardDuty RDS Protection wurde entwickelt, um Zugriffsaktivitäten auf Amazon Aurora-Datenbanken zu profilieren und zu überwachen, ohne die Datenbankleistung zu beeinträchtigen.
- GuardDuty EKS Protection umfasst EKS Audit Log Monitoring und EKS Runtime Monitoring. GuardDuty Überwacht mit EKS Audit Log Monitoring Kubernetes-Auditprotokolle von Amazon EKS-Clustern und analysiert sie auf potenziell bösartige und verdächtige Aktivitäten. EKS Runtime Monitoring verwendet den GuardDuty Security Agent (ein Amazon EKS-Add-on), um die Laufzeit einzelner Amazon EKS-Workloads transparent zu machen. Der GuardDuty Security Agent hilft dabei, bestimmte Container in Ihren Amazon EKS-Clustern zu identifizieren, die möglicherweise gefährdet sind. Es kann auch Versuche erkennen, Rechte von einem einzelnen Container auf den zugrunde liegenden Amazon EC2 EC2-Host oder auf die breitere AWS Umgebung auszuweiten.

GuardDuty bietet auch eine Funktion namens Extended Threat Detection, die automatisch mehrstufige Angriffe erkennt, die sich über Datenquellen, mehrere Ressourcentypen und einen Zeitraum innerhalb eines AWS Zeitraums erstrecken. AWS-Konto GuardDutykorreliert diese Ereignisse, die als Signale bezeichnet werden, um Szenarien zu identifizieren, die sich als potenzielle Bedrohungen für Ihre AWS Umgebung darstellen, und generiert dann eine Ermittlung

der Angriffssequenz. Dies deckt Bedrohungsszenarien ab, bei denen es um Sicherheitslücken im Zusammenhang mit dem Missbrauch von AWS Zugangsdaten geht, und um Versuche, Daten in Ihrem AWS-Konten System zu kompromittieren. GuardDuty betrachtet alle Arten der Erkennung von Angriffssequenzen als kritisch. Diese Funktion ist standardmäßig aktiviert und es fallen keine zusätzlichen Kosten an.

In der AWS SRA GuardDuty ist sie für alle Konten aktiviert AWS Organizations, und alle Ergebnisse können von den entsprechenden Sicherheitsteams im GuardDuty delegierten Administratorkonto (in diesem Fall dem Security Tooling-Konto) eingesehen und bearbeitet werden. GuardDuty aktive Ergebnisse werden in einen zentralen S3-Bucket im Log Archive-Konto exportiert, sodass Sie die Ergebnisse über 90 Tage hinaus aufbewahren können. Die Ergebnisse werden aus dem delegierten Administratorkonto exportiert und enthalten auch alle Ergebnisse der zugehörigen Mitgliedskonten in derselben Region. Die Ergebnisse im S3-Bucket werden mit einem vom AWS KMS Kunden verwalteten Schlüssel verschlüsselt. Die S3-Bucket-Richtlinie und die KMS-Schlüsselrichtlinie sind so konfiguriert, dass nur GuardDuty die Ressourcen verwendet werden können.

Wenn AWS Security Hub CSPM aktiviert, werden die GuardDuty Ergebnisse automatisch an Security Hub CSPM und Security Hub weitergeleitet. Wenn Amazon Detective aktiviert ist, werden die GuardDuty Ergebnisse in den Detective-Protokollaufnahmeprozess aufgenommen. GuardDuty und Detective unterstützen serviceübergreifende Benutzerworkflows, bei denen GuardDuty Links von der Konsole bereitgestellt werden, die Sie von einem ausgewählten Ergebnis zu einer Detective-Seite weiterleiten, die kuratierte Visualisierungen zur Untersuchung dieses Ergebnisses enthält. Sie können beispielsweise auch Amazon integrieren GuardDuty , um bewährte Verfahren EventBridge zu automatisieren GuardDuty, z. B. die Automatisierung von Antworten auf neue GuardDuty Erkenntnisse.

> **Beispiel für eine Implementierung**
>
> Die AWS SRA-Codebibliothek bietet eine Beispielimplementierung von GuardDuty. Es umfasst die verschlüsselte S3-Bucket-Konfiguration, delegierte Verwaltung und GuardDuty Aktivierung für alle bestehenden und future Konten in der Organisation. AWS

AWS Config

AWS Configist ein Service, mit dem Sie die Konfigurationen der unterstützten AWS Ressourcen in Ihrem System bewerten, prüfen und auswerten können. AWS-Konten AWS Config überwacht und zeichnet die AWS Ressourcenkonfigurationen kontinuierlich auf und vergleicht die aufgezeichneten

Konfigurationen automatisch mit den gewünschten Konfigurationen. Sie können auch andere Services integrieren, um die Schwerstarbeit AWS Config bei automatisierten Audit- und Monitoring-Pipelines zu erledigen. AWS Config Sie können beispielsweise in einzelne Geheimnisse auf Änderungen achten. AWS Secrets Manager

Sie können die Konfigurationseinstellungen Ihrer AWS Ressourcen auswerten, indem Sie AWS-Config-Regeln. AWS Config stellt eine Bibliothek mit anpassbaren, vordefinierten Regeln bereit, die als verwaltete Regeln bezeichnet werden. Sie können aber auch Ihre eigenen benutzerdefinierten Regeln schreiben. Sie können AWS-Config-Regeln im proaktiven Modus (bevor Ressourcen bereitgestellt wurden) oder im Detektivmodus (nachdem Ressourcen bereitgestellt wurden) arbeiten. Ressourcen können bei Konfigurationsänderungen und/oder regelmäßig nach einem Zeitplan ausgewertet werden.

Ein Conformance Pack ist eine Sammlung von AWS Config Regeln und Behebungsmaßnahmen, die als einzelne Einheit in einem Konto und einer Region oder unternehmensweit in einem Unternehmen eingesetzt werden können. AWS Organizations Conformance Packs werden erstellt, indem eine YAML-Vorlage erstellt wird, die die Liste der AWS Config verwalteten oder benutzerdefinierten Regeln und Abhilfemaßnahmen enthält. Verwenden Sie eine der Beispielvorlagen für Conformance AWS Packs, um mit der Evaluierung Ihrer Umgebung zu beginnen.

AWS Config lässt sich integrieren AWS Security Hub CSPM , um die Ergebnisse AWS Config verwalteter und benutzerdefinierter Regelauswertungen als Ergebnisse an Security Hub CSPM zu senden.

AWS-Config-Regeln kann in Verbindung mit verwendet werden, um Ressourcen, die nicht AWS Systems Manager den Vorschriften entsprechen, wirksam zu beheben. Sie verwenden den Systems Manager Explorer, um den Compliance-Status der AWS Config Regeln in Ihrem AWS-Konten Across zu ermitteln, AWS-Regionen und verwenden dann Systems Manager Automation-Dokumente (Runbooks), um Ihre nicht konformen AWS Config Regeln zu beheben. Einzelheiten zur Implementierung finden Sie im Blogbeitrag Korrigieren Sie nicht konforme AWS Config Regeln mit Automation-Runbooks. AWS Systems Manager

Der AWS Config Aggregator sammelt Konfigurations- und Compliance-Daten für mehrere Konten, Regionen und Organisationen in. AWS Organizations Das Aggregator-Dashboard zeigt die Konfigurationsdaten der aggregierten Ressourcen an. Inventar- und Compliance-Dashboards bieten wichtige und aktuelle Informationen über Ihre AWS Ressourcenkonfigurationen und den Compliance-Status innerhalb AWS-Konten, innerhalb oder innerhalb einer Organisation. AWS-Regionen AWS Sie ermöglichen es Ihnen, Ihren AWS Ressourcenbestand zu visualisieren und zu bewerten, ohne

AWS Config erweiterte Abfragen schreiben zu müssen. Sie erhalten wichtige Erkenntnisse wie eine Zusammenfassung der Compliance nach Ressourcen, die zehn Konten mit den meisten nicht konformen Ressourcen, einen Vergleich der ausgeführten und gestoppten EC2-Instances nach Typ und EBS-Volumes nach Volume-Typ und -Größe.

Wenn Sie Ihr AWS Unternehmen verwalten, wird es eine Reihe von AWS Config Regeln als detektivische Leitplanken einsetzen (kategorisiert als verpflichtend, dringend empfohlen oder optional). AWS Control Tower Diese Leitplanken helfen Ihnen dabei, Ihre Ressourcen zu verwalten und die Einhaltung der Vorschriften für alle Konten in Ihrer Organisation zu überwachen. AWS Diese AWS Config Regeln verwenden automatisch ein `aws-control-tower` Tag mit dem Wert. `managed-by-control-tower`

AWS Config muss für jedes Mitgliedskonto in der AWS Organisation aktiviert sein und AWS-Region das die Ressourcen enthält, die Sie schützen möchten. Sie können AWS Config Regeln für alle Konten in Ihrer AWS Organisation zentral verwalten (z. B. erstellen, aktualisieren und löschen). Über das AWS Config delegierte Administratorkonto können Sie ein gemeinsames AWS Config Regelwerk für alle Konten bereitstellen und Konten angeben, für die keine AWS Config Regeln erstellt werden sollen. Das AWS Config delegierte Administratorkonto kann auch Ressourcenkonfigurations- und Compliance-Daten aus allen Mitgliedskonten zusammenfassen, sodass eine zentrale Ansicht bereitgestellt wird. Verwenden Sie das Konto „ APIs Vom delegierten Administrator“, um die Verwaltung durchzusetzen, indem Sie sicherstellen, dass die zugrunde liegenden AWS Config Regeln nicht von den Mitgliedskonten in Ihrer AWS Organisation geändert werden können. AWS Config ist nativ integriert, um Ergebnisse an zu senden AWS Security Hub CSPM, sofern Security Hub CSPM aktiviert ist und mindestens eine AWS Config verwaltete oder benutzerdefinierte Regel vorhanden ist.

In der AWS SRA ist das AWS Config delegierte Administratorkonto das Security Tooling-Konto. Der AWS Config Bereitstellungskanal ist so konfiguriert, dass er Snapshots der Ressourcenkonfiguration in einem zentralen S3-Bucket im Log Archive-Konto bereitstellt. Da das Log Archive-Konto der zentrale Protokoll-Repository-Speicher ist, wird es zum Speichern der Ressourcenkonfiguration verwendet.

Designüberlegungen

- AWS Config streamt Benachrichtigungen über Konfiguration und Konformitätsänderungen an Amazon EventBridge. Das bedeutet, dass Sie die systemeigenen Filterfunktionen verwenden können EventBridge , um AWS Config Ereignisse zu filtern, sodass Sie bestimmte Arten von Benachrichtigungen an bestimmte Ziele weiterleiten können. Sie

können beispielsweise Compliance-Benachrichtigungen für bestimmte Regeln oder Ressourcentypen an bestimmte E-Mail-Adressen senden oder Benachrichtigungen über Konfigurationsänderungen an ein externes IT Service Management- (ITSM) - oder Configuration Management Database (CMDB) -Tool weiterleiten. Weitere Informationen finden Sie im Blogbeitrag AWS Config Best Practices.

- Zusätzlich zur AWS Config proaktiven Regelauswertung können Sie ein policy-as-code Evaluierungstool verwenden AWS CloudFormation Guard, das proaktiv die Einhaltung der Ressourcenkonfigurationen überprüft. Die AWS CloudFormation Guard Befehlszeilenschnittstelle (CLI) bietet Ihnen eine deklarative, domänenspezifische Sprache (DSL), mit der Sie Richtlinien als Code ausdrücken können. Darüber hinaus können Sie AWS CLI Befehle verwenden, um strukturierte Daten im JSON- oder YAML-Format wie CloudFormation Änderungssätze, JSON-basierte Terraform-Konfigurationsdateien oder Kubernetes-Konfigurationen zu validieren. Sie können die Evaluierungen lokal ausführen, indem Sie die AWS CloudFormation Guard CLI als Teil Ihres Authoring-Prozesses verwenden, oder sie innerhalb Ihrer Bereitstellungspipeline ausführen. Wenn Sie über AWS Cloud Development Kit (AWS CDK)Anwendungen verfügen, können Sie cdk-nag für die proaktive Überprüfung von Best Practices verwenden.

Beispiel für eine Implementierung

Die AWS SRA-Codebibliothek bietet eine Beispielimplementierung, mit der AWS Config Konformitätspakete für alle AWS-Konten und Regionen innerhalb einer Organisation bereitgestellt werden. AWS Das AWS Config Aggregator-Modul hilft Ihnen bei der Konfiguration eines AWS Config Aggregators, indem es die Verwaltung an ein Mitgliedskonto (Security Tooling) innerhalb des Org Management-Kontos delegiert und dann AWS Config Aggregator innerhalb des delegierten Administratorkontos für alle vorhandenen und future Konten in der Organisation konfiguriert. AWS Sie können das AWS Config Control Tower Management Account-Modul verwenden, um es AWS Config innerhalb des Org Management-Kontos zu aktivieren — es ist nicht aktiviert von. AWS Control Tower

Amazon Security Lake

Amazon Security Lake ist ein vollständig verwalteter Sicherheits-Data-Lake-Service. Sie können Security Lake verwenden, um Sicherheitsdaten aus AWS Umgebungen, SaaS-Anbietern (Software as a Service), vor Ort und Quellen von Drittanbietern automatisch zu zentralisieren. Security Lake

hilft Ihnen beim Aufbau einer normalisierten Datenquelle, die die Verwendung von Analysetools für Sicherheitsdaten vereinfacht, sodass Sie sich einen umfassenderen Überblick über Ihre Sicherheitslage im gesamten Unternehmen verschaffen können. Der Data Lake wird von Amazon Simple Storage Service (Amazon S3) -Buckets unterstützt, und Sie behalten das Eigentum an Ihren Daten. Security Lake sammelt automatisch Protokolle für AWS-Services Amazon VPC, Amazon Route 53, Amazon S3 AWS Lambda, Amazon EKS-Auditprotokolle, AWS Security Hub CSPM Ergebnisse und AWS WAF Protokolle. AWS CloudTrail

AWS SRA empfiehlt, dass Sie das Log Archive-Konto als delegiertes Administratorkonto für Security Lake verwenden. Weitere Informationen zur Einrichtung des delegierten Administratorkontos finden Sie unter Amazon Security Lake im Abschnitt Security OU – Konto protokollieren. Sicherheitsteams, die auf Security Lake-Daten zugreifen möchten oder die Möglichkeit benötigen, mithilfe benutzerdefinierter ETL-Funktionen (Extrahieren, Transformieren und Laden) nicht systemeigene Protokolle in die Security Lake-Buckets zu schreiben, sollten innerhalb des Security Tooling-Kontos arbeiten.

Security Lake kann Protokolle von verschiedenen Cloud-Anbietern, Protokolle von Drittanbieterlösungen oder andere benutzerdefinierte Protokolle sammeln. Wir empfehlen, dass Sie das Security Tooling-Konto verwenden, um die ETL-Funktionen auszuführen, um die Protokolle in das Open Cybersecurity Schema Framework (OCSF) -Format zu konvertieren und eine Datei im Apache Parquet-Format auszugeben. Security Lake erstellt die kontoübergreifende Rolle mit den entsprechenden Berechtigungen für das Security Tooling-Konto und die benutzerdefinierte Quelle, die von Lambda-Funktionen oder AWS Glue Crawlern unterstützt wird, um Daten in die S3-Buckets für Security Lake zu schreiben.

Der Security Lake-Administrator sollte Sicherheitsteams konfigurieren, die das Security Tooling-Konto verwenden und Zugriff auf die Protokolle benötigen, die Security Lake als Abonnenten sammelt. Security Lake unterstützt zwei Arten des Abonnentenzugriffs:

- Datenzugriff — Abonnenten können direkt auf die Amazon S3 S3-Objekte für Security Lake zugreifen. Security Lake verwaltet die Infrastruktur und die Berechtigungen. Wenn Sie das Security Tooling-Konto als Security Lake-Datenzugriffs-Abonnent konfigurieren, wird das Konto über Amazon Simple Queue Service (Amazon SQS) über neue Objekte in den Security Lake-Buckets benachrichtigt, und Security Lake erstellt die Berechtigungen für den Zugriff auf diese neuen Objekte.
- Zugriff abfragen — Abonnenten können mithilfe von Diensten wie Amazon Athena Quelldaten aus AWS Lake Formation Tabellen in Ihrem S3-Bucket abfragen. Der kontenübergreifende Zugriff wird mithilfe von Lake Formation automatisch für den Abfragezugriff eingerichtet. Wenn

Sie das Security Tooling-Konto als Abonnent für den Security Lake-Abfragezugriff konfigurieren, erhält das Konto nur Lesezugriff auf die Protokolle im Security Lake-Konto. Wenn Sie diesen Abonnententyp verwenden, werden Athena und die AWS Glue Tabellen über AWS Resource Access Manager (AWS RAM) vom Security Lake Log Archive-Konto mit dem Security Tooling-Konto gemeinsam genutzt. Um diese Funktion zu aktivieren, müssen Sie die Einstellungen für den kontoübergreifenden Datenaustausch auf Version 3 aktualisieren.

Weitere Informationen zum Erstellen von Abonnenten finden Sie unter Abonnentenverwaltung in der Security Lake-Dokumentation.

Bewährte Methoden für die Erfassung benutzerdefinierter Quellen finden Sie in der Security Lake-Dokumentation unter Sammeln von Daten aus benutzerdefinierten Quellen.

Sie können Amazon Quick Sight, Amazon OpenSearch Service und Amazon verwenden, SageMaker um Analysen für die Sicherheitsdaten einzurichten, die Sie in Security Lake speichern.

> **Designüberlegung**
>
> Wenn ein Anwendungsteam Abfragezugriff auf Security Lake-Daten benötigt, um eine Geschäftsanforderung zu erfüllen, sollte der Security Lake-Administrator dieses Anwendungskonto als Abonnent konfigurieren.

Amazon Macie

Amazon Macie ist ein vollständig verwalteter Service für Datensicherheit und Datenschutz, der maschinelles Lernen und Musterabgleich verwendet, um Ihre sensiblen Daten zu erkennen und zu schützen. AWS Sie müssen die Art und Klassifizierung der Daten, die Ihr Workload verarbeitet, identifizieren, um sicherzustellen, dass angemessene Kontrollen durchgesetzt werden. Sie können Macie auf zwei Arten verwenden, um die Erkennung vertraulicher Daten und die Berichterstattung zu automatisieren: durch die automatische Erkennung sensibler Daten und durch die Erstellung und Ausführung von Aufträgen zur Erkennung sensibler Daten. Mit der automatisierten Erkennung sensibler Daten bewertet Macie täglich Ihr S3-Bucket-Inventar und verwendet Stichprobenverfahren, um repräsentative S3-Objekte aus Ihren Buckets zu identifizieren und auszuwählen. Macie ruft dann die ausgewählten Objekte ab, analysiert sie und untersucht sie auf sensible Daten. Aufgaben zur Erkennung sensibler Daten ermöglichen tiefere und gezieltere Analysen. Mit dieser Option definieren Sie den Umfang und die Tiefe der Analyse, einschließlich der zu analysierenden S3-Buckets, der

Stichprobentiefe und benutzerdefinierter Kriterien, die sich aus den Eigenschaften von S3-Objekten ergeben. Wenn Macie ein potenzielles Problem mit der Sicherheit oder dem Datenschutz eines Buckets feststellt, erstellt es eine Richtlinienfeststellung für Sie. Die automatische Datenerkennung ist standardmäßig für alle neuen Macie-Kunden aktiviert, und bestehende Macie-Kunden können sie mit einem Klick aktivieren.

Macie ist bis jetzt in allen Konten aktiviert. AWS Organizations Principals, die über die entsprechenden Berechtigungen für das delegierte Administratorkonto (in diesem Fall das Security Tooling-Konto) verfügen, können Macie in jedem Konto aktivieren oder sperren, Aufträge zur Erkennung sensibler Daten für Buckets erstellen, die Mitgliedskonten gehören, und alle Richtlinienergebnisse für alle Mitgliedskonten einsehen. Ergebnisse sensibler Daten können nur von dem Konto eingesehen werden, das den Job mit sensiblen Ergebnissen erstellt hat. Weitere Informationen finden Sie in der Macie-Dokumentation unter Verwaltung mehrerer Macie-Konten als Organisation.

Die Ergebnisse von Macie werden AWS Security Hub CSPM zur Überprüfung und Analyse weitergeleitet. Macie arbeitet auch mit Amazon zusammen EventBridge , um automatisierte Reaktionen auf Ergebnisse wie Warnmeldungen, Feeds in SIEM-Systeme (Security Information and Event Management) und automatisierte Problembehebungen zu ermöglichen.

Designüberlegungen

- Wenn S3-Objekte mit einem Schlüssel AWS Key Management Service (AWS KMS) verschlüsselt sind, den Sie verwalten, können Sie diesem KMS-Schlüssel die mit dem Macie-Dienst verknüpfte Rolle als Schlüsselbenutzer hinzufügen, damit Macie die Daten scannen kann.
- Macie ist für das Scannen von Objekten in Amazon S3 optimiert. Somit kann jeder von MacIE unterstützte Objekttyp, der (dauerhaft oder vorübergehend) in Amazon S3 platziert werden kann, nach sensiblen Daten durchsucht werden. Das bedeutet, dass Daten aus anderen Quellen — zum Beispiel regelmäßige Snapshot-Exporte von Amazon Relational Database Service (Amazon RDS) - oder Amazon Aurora Aurora-Datenbanken, exportierte Amazon DynamoDB-Tabellen oder extrahierte Textdateien aus systemeigenen Anwendungen oder Drittanbieteranwendungen — nach Amazon S3 verschoben und von Macie ausgewertet werden können.

Beispiel für eine Implementierung

Die AWS SRA-Codebibliothek bietet eine Beispielimplementierung von Amazon Macie. Dazu gehört das Delegieren der Verwaltung an ein Mitgliedskonto und die Konfiguration von Macie innerhalb des delegierten Administratorkontos für alle bestehenden und future Konten in der Organisation. AWS Macie ist außerdem so konfiguriert, dass die Ergebnisse an einen zentralen S3-Bucket gesendet werden, der mit einem vom Kunden verwalteten Schlüssel verschlüsselt ist. AWS KMS

IAM Access Analyzer

Wenn Sie Ihre AWS Cloud Einführung beschleunigen und weiterhin innovativ sein möchten, ist es wichtig, eine strenge Kontrolle über den detaillierten Zugriff (Berechtigungen) zu behalten, die Zunahme von Zugriffen einzudämmen und sicherzustellen, dass Berechtigungen effektiv genutzt werden. Übermäßiger und ungenutzter Zugriff stellt Sicherheitsprobleme dar und erschwert es Unternehmen, das Prinzip der geringsten Rechte durchzusetzen. Dieses Prinzip ist ein wichtiger Pfeiler der Sicherheitsarchitektur, bei dem die IAM-Berechtigungen kontinuierlich angepasst werden müssen, um ein Gleichgewicht zwischen Sicherheitsanforderungen und Betriebs- und Anwendungsentwicklungsanforderungen herzustellen. An diesen Bemühungen sind mehrere Interessengruppen beteiligt, darunter zentrale Sicherheits- und Cloud Center of Excellence (CCoE) - Teams sowie dezentrale Entwicklungsteams.

AWS Identity and Access Management Access Analyzer bietet Tools, mit denen Sie effizient detaillierte Berechtigungen festlegen, beabsichtigte Berechtigungen überprüfen und Berechtigungen verfeinern können, indem ungenutzter Zugriff entfernt wird, sodass Sie die Sicherheitsstandards Ihres Unternehmens erfüllen können. Mithilfe von Dashboards und erhalten Sie Einblick in den externen und internen Zugriff auf AWS Ressourcen und die Ergebnisse ungenutzter Zugriffe. AWS Security Hub CSPM Darüber hinaus unterstützt es Amazon EventBridge für ereignisbasierte benutzerdefinierte Benachrichtigungs- und Behebungsworkflows.

Die Funktion „Ergebnisse der externen Zugriffsanalyse“ von IAM Access Analyzer hilft Ihnen dabei, die Ressourcen in Ihrer AWS Organisation und in Ihren Konten zu identifizieren, die mit einer externen Entität gemeinsam genutzt werden, z. B. Amazon S3 S3-Buckets oder IAM-Rollen. Die AWS Organisation oder das Konto, das Sie auswählen, wird als Vertrauenszone bezeichnet. Der Analyzer analysiert anhand automatisierter Argumentation alle unterstützten Ressourcen innerhalb der Vertrauenszone und generiert Ergebnisse für Prinzipale, die von außerhalb der Vertrauenszone auf die Ressourcen zugreifen können. Diese Ergebnisse helfen Ihnen dabei,

Ressourcen zu identifizieren, die mit einer externen Entität gemeinsam genutzt werden, und geben Ihnen vor der Bereitstellung von Ressourcenberechtigungen einen Überblick darüber, wie sich Ihre Richtlinie auf den öffentlichen und kontoübergreifenden Zugriff auf Ihre Ressource auswirkt. Dies ist ohne zusätzliche Kosten verfügbar.

In ähnlicher Weise hilft Ihnen die Suchfunktion für den internen Zugriff von IAM Access Analyzer dabei, die Ressourcen in Ihrer AWS Organisation und die Konten zu identifizieren, die innerhalb Ihrer Organisation oder Ihres Kontos mit Prinzipalen gemeinsam genutzt werden. Diese Analyse unterstützt das Prinzip der geringsten Rechte, indem sichergestellt wird, dass nur die dafür vorgesehenen Prinzipale innerhalb Ihrer Organisation auf Ihre angegebenen Ressourcen zugreifen können. Diese Funktion ist kostenpflichtig und erfordert eine explizite Konfiguration der zu überprüfenden Ressourcen. Verwenden Sie diese Funktion mit Bedacht, um bestimmte sensible Ressourcen zu überwachen, die von Haus aus gesperrt werden müssen, auch intern.

Die Ergebnisse von IAM Access Analyzer helfen Ihnen auch dabei, ungenutzten Zugriff zu identifizieren, der in Ihren AWS Organisationen und Konten gewährt wurde, darunter:

- Ungenutzte IAM-Rollen — Rollen, für die innerhalb des angegebenen Nutzungsfensters keine Zugriffsaktivität besteht.
- Ungenutzte IAM-Benutzer, Anmeldeinformationen und Zugriffsschlüssel — Anmeldeinformationen, die IAM-Benutzern gehören und für den Zugriff auf AWS-Services Ressourcen verwendet werden.
- Ungenutzte IAM-Richtlinien und -Berechtigungen — Berechtigungen auf Service- und Aktionsebene, die von einer Rolle innerhalb eines bestimmten Nutzungsfensters nicht verwendet wurden. IAM Access Analyzer verwendet identitätsbasierte Richtlinien, die Rollen zugeordnet sind, um zu bestimmen, auf welche Dienste und Aktionen diese Rollen zugreifen können. Der Analyzer bietet eine Übersicht über ungenutzte Berechtigungen für alle Berechtigungen auf Dienstebene.

Sie können die mit IAM Access Analyzer generierten Ergebnisse verwenden, um einen Überblick über jeden unbeabsichtigten oder ungenutzten Zugriff auf der Grundlage der Richtlinien und Sicherheitsstandards Ihres Unternehmens zu erhalten und diesen zu korrigieren. Nach der Behebung werden diese Ergebnisse bei der nächsten Ausführung des Analyzers als behoben markiert. Wenn das Ergebnis beabsichtigt ist, können Sie es in IAM Access Analyzer als archiviert markieren und anderen Ergebnissen, die ein größeres Sicherheitsrisiko darstellen, Priorität einräumen. Darüber hinaus können Sie Archivierungsregeln einrichten, um bestimmte Ergebnisse automatisch zu archivieren. Sie können beispielsweise eine Archivregel erstellen, um alle Ergebnisse für einen bestimmten Amazon-S3-Bucket, auf den Sie regelmäßig Zugriff gewähren, automatisch zu archivieren.

Als Builder können Sie IAM Access Analyzer verwenden, um zu Beginn Ihres Entwicklungs- und Bereitstellungsprozesses (CI/CD) automatisierte IAM-Richtlinienprüfungen durchzuführen, um die Sicherheitsstandards Ihres Unternehmens einzuhalten. Sie können benutzerdefinierte Richtlinienprüfungen und Richtlinienüberprüfungen in IAM Access Analyzer integrieren, AWS CloudFormation um Richtlinienprüfungen als Teil der Pipelines Ihres Entwicklungsteams zu automatisieren. CI/CD Dies umfasst:

- Überprüfung der IAM-Richtlinien — IAM Access Analyzer validiert Ihre Richtlinien anhand der Grammatik und der Best Practices der IAM-Richtlinien. AWS Sie können sich die Ergebnisse der Überprüfungen der Richtlinienvalidierung ansehen, darunter Sicherheitswarnungen, Fehler, allgemeine Warnungen und Vorschläge für Ihre Richtlinie. Derzeit sind über 100 Überprüfungen zur Richtlinienvalidierung verfügbar, die mithilfe von AWS Command Line Interface (AWS CLI) und automatisiert werden können APIs.
- Benutzerdefinierte IAM-Richtlinienprüfungen — Mit den benutzerdefinierten Richtlinienprüfungen von IAM Access Analyzer werden Ihre Richtlinien anhand Ihrer angegebenen Sicherheitsstandards überprüft. Benutzerdefinierte Richtlinienprüfungen verwenden automatisierte Argumentation, um ein höheres Maß an Sicherheit bei der Einhaltung Ihrer Unternehmenssicherheitsstandards zu bieten. Zu den Arten von benutzerdefinierten Richtlinienprüfungen gehören:
  - Mit einer Referenzrichtlinie vergleichen: Wenn Sie eine Richtlinie bearbeiten, können Sie sie mit einer Referenzrichtlinie vergleichen, z. B. mit einer vorhandenen Version der Richtlinie, um zu überprüfen, ob das Update neuen Zugriff gewährt. Die CheckNoNewAccessAPI vergleicht zwei Richtlinien (eine aktualisierte Richtlinie und eine Referenzrichtlinie), um festzustellen, ob die aktualisierte Richtlinie einen neuen Zugriff gegenüber der Referenzrichtlinie einführt, und gibt die Antwort „Bestanden“ oder „Nicht bestanden“ zurück.
  - Vergleich mit einer Liste von IAM-Aktionen: Mithilfe der CheckAccessNotGrantedAPI können Sie sicherstellen, dass eine Richtlinie keinen Zugriff auf eine Liste kritischer Aktionen gewährt, die in Ihrem Sicherheitsstandard definiert sind. Diese API überprüft anhand einer Richtlinie und einer Liste von bis zu 100 IAM-Aktionen, ob die Richtlinie mindestens eine der Aktionen zulässt, und gibt die Antwort „Bestanden“ oder „Nicht bestanden“ zurück.

Sicherheitsteams und andere Autoren von IAM-Richtlinien können IAM Access Analyzer verwenden, um Richtlinien zu erstellen, die den Grammatik- und Sicherheitsstandards der IAM-Richtlinien entsprechen. Das manuelle Verfassen von Richtlinien in der richtigen Größe kann fehleranfällig und zeitaufwändig sein. Die Richtliniengenerierungsfunktion von IAM Access Analyzer unterstützt Sie bei der Erstellung von IAM-Richtlinien, die auf der Zugriffsaktivität eines Prinzipals basieren. IAM Access Analyzer überprüft die AWS CloudTrail Protokolle auf unterstützte Dienste und generiert

eine Richtlinienvorlage, die die Berechtigungen enthält, die vom Principal im angegebenen Zeitraum verwendet wurden. Sie können diese Vorlage dann verwenden, um eine Richtlinie mit detaillierten Berechtigungen zu erstellen, die nur die erforderlichen Berechtigungen gewährt.

- Für Ihr Konto muss ein CloudTrail Trail aktiviert sein, um eine Richtlinie auf der Grundlage der Zugriffsaktivität zu generieren.
- IAM Access Analyzer identifiziert keine Aktivitäten auf Aktionsebene für Datenereignisse, wie z. B. Amazon S3 S3-Datenereignisse, in generierten Richtlinien.
- Die `iam:PassRole` Aktion wird nicht von generierten Richtlinien verfolgt CloudTrail und ist auch nicht in diesen enthalten.

IAM Access Analyzer wird im Security Tooling-Konto über die delegierte Administratorfunktion unter bereitgestellt. AWS Organizations Der delegierte Administrator ist berechtigt, Analyzer zu erstellen und zu verwalten, wobei die AWS Organisation die Vertrauenszone darstellt.

Designüberlegung

Um kontobezogene Ergebnisse zu erhalten (wobei das Konto als vertrauenswürdige Grenze dient), erstellen Sie für jedes Mitgliedskonto einen kontobezogenen Analysator. Dies kann im Rahmen der Konto-Pipeline erfolgen. Kontobezogene Erkenntnisse fließen auf Ebene der Mitgliedskonten in Security Hub CSPM ein. Von dort aus werden sie zum delegierten Security Hub-CSPM-Administratorkonto (Security Tooling) weitergeleitet.

Implementierungsbeispiele

- Die AWS SRA-Codebibliothek bietet eine Beispielimplementierung von IAM Access Analyzer. Es zeigt, wie ein Analyzer auf Organisationsebene innerhalb eines delegierten Administratorkontos und ein Analyzer auf Kontoebene in jedem Konto konfiguriert werden.
- Informationen dazu, wie Sie benutzerdefinierte Richtlinienprüfungen in Builder-Workflows integrieren können, finden Sie im AWS Blogbeitrag Introducing IAM Access Analyzer Custom Policy Checks.

AWS Firewall Manager

AWS Firewall Managerträgt zum Schutz Ihres Netzwerks bei, indem es Ihre Verwaltungs- und Wartungsaufgaben für AWS WAF AWS Shield Advanced,, Amazon VPC-Sicherheitsgruppen und die Amazon Route 53 Resolver DNS-Firewall für mehrere Konten und Ressourcen vereinfacht. AWS Network Firewall Mit Firewall Manager richten Sie Ihre AWS WAF Firewallregeln, Shield Advanced-Schutzmaßnahmen, Amazon VPC-Sicherheitsgruppen, Netzwerk-Firewall-Firewalls und DNS-Firewall-Regelgruppenzuordnungen nur einmal ein. Danach wendet der Service die Regeln und Schutzmaßnahmen automatisch auf Ihre Konten und Ressourcen an, selbst wenn Sie diese erst später hinzufügen.

Firewall Manager ist besonders nützlich, wenn Sie Ihr gesamtes AWS Unternehmen schützen möchten und nicht nur eine kleine Anzahl bestimmter Konten und Ressourcen, oder wenn Sie häufig neue Ressourcen hinzufügen, die Sie schützen möchten. Firewall Manager verwendet Sicherheitsrichtlinien, damit Sie eine Reihe von Konfigurationen definieren können, einschließlich relevanter Regeln, Schutzmaßnahmen und Aktionen, die bereitgestellt werden müssen, sowie der Konten und Ressourcen (gekennzeichnet durch Tags), die ein- oder ausgeschlossen werden sollen. Sie können detaillierte und flexible Konfigurationen erstellen und gleichzeitig die Kontrolle auf eine große Anzahl von Konten ausdehnen und. VPCs Diese Richtlinien setzen die von Ihnen konfigurierten Regeln automatisch und konsistent durch, auch wenn neue Konten und Ressourcen erstellt werden. Firewall Manager ist in allen Konten aktiviert AWS Organizations, und Konfiguration und Verwaltung werden von den entsprechenden Sicherheitsteams im delegierten Administratorkonto von Firewall Manager (in diesem Fall dem Security Tooling-Konto) durchgeführt.

Sie müssen sie AWS Config für jede Ressource aktivieren AWS-Region , die die Ressourcen enthält, die Sie schützen möchten. Wenn Sie die Aktivierung nicht AWS Config für alle Ressourcen durchführen möchten, müssen Sie sie für Ressourcen aktivieren, die dem Typ der von Ihnen verwendeten Firewall Manager Manager-Richtlinien zugeordnet sind. Wenn Sie AWS Security Hub CSPM sowohl als auch Firewall Manager verwenden, sendet Firewall Manager Ihre Ergebnisse automatisch an Security Hub CSPM. Firewall Manager erstellt Ergebnisse für Ressourcen, die nicht richtlinientreu sind, und für erkannte Angriffe und sendet die Ergebnisse an Security Hub CSPM. Wenn Sie eine Firewall Manager Manager-Richtlinie für einrichten AWS WAF, können Sie die Protokollierung auf Web-Zugriffskontrolllisten (Web ACLs) für alle in den Geltungsbereich fallenden Konten zentral aktivieren und die Protokolle unter einem einzigen Konto zentralisieren.

Mit Firewall Manager können Sie einen oder mehrere Administratoren haben, die die Firewall-Ressourcen Ihres Unternehmens verwalten können. Wenn Sie mehrere Administratoren zuweisen, können Sie restriktive Bedingungen für den administrativen Geltungsbereich festlegen, um die

Ressourcen (Konten, Regionen OUs, Richtlinientypen) zu definieren, die jeder Administrator verwalten kann. Dies gibt Ihnen die Flexibilität, innerhalb Ihrer Organisation unterschiedliche Administratorrollen zu haben, und hilft Ihnen, das Prinzip des geringsten Zugriffs beizubehalten. Die AWS SRA verwendet einen Administrator, der den gesamten administrativen Bereich an das Security Tooling-Konto delegiert hat.

> **Designüberlegung**
>
> Kundenbetreuer einzelner Mitgliedskonten in der AWS Organisation können zusätzliche Kontrollen (wie AWS WAF Regeln und Amazon VPC-Sicherheitsgruppen) in den verwalteten Diensten von Firewall Manager entsprechend ihren jeweiligen Anforderungen konfigurieren.

> **Beispiel für eine Implementierung**
>
> Die AWS SRA-Codebibliothek bietet eine Beispielimplementierung von Firewall Manager. Sie demonstriert die delegierte Administration (Security Tooling), stellt eine maximal zulässige Sicherheitsgruppe bereit, konfiguriert eine Sicherheitsgruppenrichtlinie und konfiguriert mehrere Richtlinien. AWS WAF

Amazon EventBridge

Amazon EventBridge ist ein serverloser Event-Bus-Service, der es einfach macht, Ihre Anwendungen mit Daten aus einer Vielzahl von Quellen zu verbinden. Er wird häufig in der Sicherheitsautomatisierung eingesetzt. Sie können Routing-Regeln einrichten, um zu bestimmen, wohin Ihre Daten gesendet werden sollen, um Anwendungsarchitekturen zu erstellen, die in Echtzeit auf all Ihre Datenquellen reagieren. Sie können einen benutzerdefinierten Event-Bus erstellen, um Ereignisse von Ihren benutzerdefinierten Anwendungen zu empfangen, und zusätzlich den Standard-Event-Bus in jedem Konto verwenden. Sie können im Security Tooling-Konto einen Event-Bus erstellen, der sicherheitsspezifische Ereignisse von anderen Konten in der Organisation empfangen kann. AWS Indem Sie beispielsweise Amazon GuardDuty und AWS Security Hub CSPM with verknüpfen AWS-Config-Regeln, erstellen Sie eine flexible EventBridge, automatisierte Pipeline für die Weiterleitung von Sicherheitsdaten, das Auslösen von Warnmeldungen und die Verwaltung von Maßnahmen zur Problemlösung.

Designüberlegungen

- EventBridge ist in der Lage, Ereignisse an eine Reihe verschiedener Ziele weiterzuleiten. Ein wertvolles Muster für die Automatisierung von Sicherheitsmaßnahmen besteht darin, bestimmte Ereignisse mit einzelnen AWS Lambda Respondern zu verknüpfen, die dann die entsprechenden Maßnahmen ergreifen. Unter bestimmten Umständen möchten Sie beispielsweise eine öffentliche EventBridge S3-Bucket-Suche an einen Lambda-Responder weiterleiten, der die Bucket-Richtlinie korrigiert und die öffentlichen Berechtigungen entfernt. Diese Responder können in Ihre Ermittlungs-Playbooks und Runbooks integriert werden, um die Reaktionsaktivitäten zu koordinieren.
- Eine bewährte Methode für ein erfolgreiches Sicherheitsteam besteht darin, den Fluss von Sicherheitsereignissen und Ergebnissen in ein Benachrichtigungs- und Workflowsystem wie ein Ticketsystem, ein System oder ein anderes bug/issue SIEM-System (Security Information and Event Management) zu integrieren. Dadurch entfällt der Arbeitsablauf von E-Mails und statischen Berichten und Sie können Ereignisse oder Ergebnisse leichter weiterleiten, eskalieren und verwalten. Die integrierten flexiblen Routing-Funktionen EventBridge sind ein leistungsstarker Wegbereiter für diese Integration.

Amazon Detective

Amazon Detective unterstützt Ihre Strategie zur reaktionsschnellen Sicherheitskontrolle, indem es Ihren Sicherheitsanalysten die Analyse, Untersuchung und schnelle Identifizierung der Grundursache von Sicherheitsergebnissen oder verdächtigen Aktivitäten erleichtert. Detective extrahiert automatisch zeitbasierte Ereignisse wie Anmeldeversuche, API-Aufrufe und Netzwerkverkehr aus AWS CloudTrail Protokollen und Amazon VPC-Flow-Protokollen. Detective verarbeitet diese Ereignisse mithilfe unabhängiger Protokollstreams und Amazon CloudTrail VPC-Flow-Logs. Mit Detective können Sie auf historische Ereignisdaten von bis zu einem Jahr zugreifen. Detective verwendet maschinelles Lernen und Visualisierung, um eine einheitliche, interaktive Ansicht des Verhaltens Ihrer Ressourcen und der Interaktionen zwischen ihnen im Laufe der Zeit zu erstellen — dies wird als Verhaltensdiagramm bezeichnet. Sie können das Verhaltensdiagramm untersuchen, um unterschiedliche Aktionen wie fehlgeschlagene Anmeldeversuche oder verdächtige API-Aufrufe zu untersuchen.

Detective ist in Amazon Security Lake integriert, sodass Sicherheitsanalysten in Security Lake gespeicherte Protokolle abfragen und abrufen können. Sie können diese Integration verwenden, um zusätzliche Informationen aus CloudTrail Protokollen und Amazon VPC-Flow-Protokollen

abzurufen, die in Security Lake gespeichert sind, während Sie Sicherheitsuntersuchungen in Detective durchführen.

Detective erfasst auch Ergebnisse, die von Amazon erkannt wurden GuardDuty, einschließlich Bedrohungen, die von GuardDuty Runtime Monitoring erkannt wurden. Wenn ein Konto Detective aktiviert, wird es zum Administratorkonto für das Verhaltensdiagramm. Bevor Sie versuchen, Detective zu aktivieren, stellen Sie sicher, dass Ihr Konto GuardDuty seit mindestens 48 Stunden registriert ist. Wenn Sie diese Anforderung nicht erfüllen, können Sie sie nicht aktivieren DetectiveDetective.

Zu den weiteren optionalen Datenquellen für Detective gehören Amazon EKS-Auditprotokolle und AWS Security Hub CSPM. Die Amazon EKS-Audit-Log-Datenquelle erweitert die bereitgestellten Informationen zu den folgenden Entitätstypen: Amazon EKS-Cluster, Kubernetes-Pods, Container-Images und Kubernetes-Themen. Die Security Hub-Datenquelle ist Teil von AWS Security Findings, wo sie die Ergebnisse produktübergreifend in Security Hub korreliert und in Detective aufnimmt.

Detective gruppiert automatisch mehrere Ergebnisse, die sich auf ein einzelnes Sicherheitskompromittierungsereignis beziehen, in Suchgruppen. Bedrohungsakteure führen in der Regel eine Abfolge von Aktionen durch, die zu mehreren Sicherheitsergebnissen führen, die über Zeit und Ressourcen verteilt sind. Daher sollte das Finden von Gruppen der Ausgangspunkt für Untersuchungen sein, an denen mehrere Entitäten und Ergebnisse beteiligt sind. Detective bietet auch Zusammenfassungen von Suchgruppen mithilfe generativer KI, die Fundgruppen automatisch analysiert und Erkenntnisse in natürlicher Sprache bereitstellt, um Ihnen zu helfen, Sicherheitsuntersuchungen zu beschleunigen.

Detective integriert sich in AWS Organizations. Das Org Management-Konto delegiert ein Mitgliedskonto als Detective-Administratorkonto. In der AWS SRA ist dies das Security Tooling-Konto. Das Detective-Administratorkonto bietet die Möglichkeit, alle aktuellen Mitgliedskonten in der Organisation automatisch als Detective-Mitgliedskonten zu aktivieren und auch neue Mitgliedskonten hinzuzufügen, sobald sie der AWS Organisation hinzugefügt werden. Detective-Administratorkonten haben auch die Möglichkeit, Mitgliedskonten, die derzeit nicht in der AWS Organisation, sondern in derselben Region ansässig sind, einzuladen, ihre Daten zum Verhaltensdiagramm des primären Kontos beizutragen. Wenn ein Mitgliedskonto die Einladung annimmt und aktiviert ist, beginnt Detective, die Daten des Mitgliedskontos aufzunehmen und in dieses Verhaltensdiagramm zu extrahieren.

Designüberlegung

Sie können von den AWS Security Hub CSPM Konsolen GuardDuty und aus zu Detective Finding Profiles navigieren. Diese Links können dazu beitragen, den Ermittlungsprozess zu rationalisieren. Ihr Konto muss das Administratorkonto sowohl für Detective als auch für den Dienst sein, von dem Sie wechseln (GuardDutyoder Security Hub CSPM). Wenn die primären Konten für die Dienste identisch sind, funktionieren die Integrationslinks problemlos.

AWS Audit Manager

AWS Audit Managerhilft Ihnen dabei, Ihre AWS Nutzung kontinuierlich zu überprüfen, um die Verwaltung von Audits und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen. Es ermöglicht Ihnen, von der manuellen Erfassung, Prüfung und Verwaltung von Nachweisen zu einer Lösung überzugehen, die die Beweiserhebung automatisiert, eine einfache Möglichkeit bietet, die Quelle von Prüfungsnachweisen nachzuverfolgen, die Zusammenarbeit im Team ermöglicht und die Sicherheit und Integrität von Nachweisen gewährleistet. Wenn es Zeit für ein Audit ist, hilft Audit Manager Ihnen, Beteiligtenüberprüfungen bei Ihren Kontrollen zu verwalten.

Mit Audit Manager können Sie anhand vorgefertigter Frameworks wie dem Center for Internet Security (CIS) Benchmark, dem CIS AWS Foundations Benchmark, System and Organization Controls 2 (SOC 2) und dem Payment Card Industry Data Security Standard (PCI DSS) prüfen. Es bietet Ihnen auch die Möglichkeit, Ihre eigenen Frameworks mit Standard- oder benutzerdefinierten Kontrollen zu erstellen, die auf Ihren spezifischen Anforderungen für interne Audits basieren.

Audit Manager sammelt vier Arten von Nachweisen. Drei Arten von Nachweisen werden automatisiert: Nachweise zur Konformitätsprüfung von AWS Config und AWS Security Hub CSPM, Nachweise für Verwaltungsereignisse von AWS CloudTrail und und Konfigurationsnachweise aus AWS service-to-service API-Aufrufen. Für Nachweise, die nicht automatisiert werden können, können Sie mit Audit Manager manuelle Nachweise hochladen.

Standardmäßig werden Ihre Daten in Audit Manager mithilfe AWS verwalteter Schlüssel verschlüsselt. Die AWS SRA verwendet einen vom Kunden verwalteten Schlüssel für die Verschlüsselung, um eine bessere Kontrolle über den logischen Zugriff zu ermöglichen. Sie sollten auch einen S3-Bucket in dem Bereich konfigurieren, in AWS-Region dem Audit Manager den Bewertungsbericht veröffentlicht. Diese Buckets sollten mit einem vom Kunden verwalteten Schlüssel verschlüsselt werden und über eine Bucket-Richtlinie verfügen, die so konfiguriert ist, dass nur Audit Manager Berichte veröffentlichen kann.

> **Note**
>
> Audit Manager hilft bei der Erfassung von Nachweisen, die für die Überprüfung der Einhaltung bestimmter Compliance-Standards und -Vorschriften relevant sind. Es bewertet jedoch nicht Ihre Einhaltung. Daher enthalten die mit Audit Manager gesammelten Nachweise möglicherweise keine Details zu Ihren betrieblichen Prozessen, die für Audits erforderlich sind. Audit Manager ist kein Ersatz für Rechtsberater oder Compliance-Experten. Wir empfehlen Ihnen, die Dienste eines externen Gutachters in Anspruch zu nehmen, der für die Compliance-Rahmenbedingungen, anhand derer Sie bewertet wurden, zertifiziert ist.

Audit Manager Manager-Bewertungen können sich auf mehrere Konten in Ihren AWS Organisationen beziehen. Audit Manager sammelt und konsolidiert Nachweise in einem delegierten Administratorkonto in. AWS Organizations Diese Prüfungsfunktion wird hauptsächlich von Compliance- und internen Auditteams verwendet und erfordert lediglich Lesezugriff auf Ihre. AWS-Konten

> **Designüberlegungen**
>
> - Audit Manager ergänzt andere AWS Sicherheitsdienste wie AWS Security Hub CSPM AWS Security Hub, und und AWS Config hilft bei der Implementierung eines Risikomanagement-Frameworks. Audit Manager bietet unabhängige Funktionen zur Risikoabsicherung, während Security Hub CSPM Sie bei der Überwachung Ihrer Risiken unterstützt und AWS Config Konformitätspakete beim Risikomanagement helfen. Prüfer, die mit dem vom Institute of Internal Auditors (IIA) entwickelten Drei-Lines-Modell vertraut sind, sollten beachten, dass diese Kombination Ihnen AWS-Services hilft, die drei Verteidigungslinien abzudecken. Weitere Informationen finden Sie in der zweiteiligen Blogserie auf dem Blog AWS Cloud Operations & Migrations.
> - Damit Audit Manager Security Hub CSPM-Beweise sammeln kann, muss das delegierte Administratorkonto für beide Dienste identisch sein. AWS-Konto Aus diesem Grund ist das Security Tooling-Konto in der AWS SRA der delegierte Administrator für Audit Manager.

AWS Artifact

AWS Artifactwird innerhalb des Security Tooling-Kontos gehostet, um die Funktionen zur Verwaltung von Compliance-Artefakten vom Org Management-Konto zu trennen. AWS Diese Aufgabentrennung

ist wichtig, da wir empfehlen, das AWS Org Management-Konto nicht für Bereitstellungen zu verwenden, es sei denn, dies ist unbedingt erforderlich. Geben Sie stattdessen Bereitstellungen an Mitgliedskonten weiter. Da die Verwaltung von Auditartefakten von einem Mitgliedskonto aus erfolgen kann und die Funktion eng mit dem Sicherheits- und Compliance-Team abgestimmt ist, wird das Security Tooling-Konto als Administratorkonto für eingerichtet. AWS Artifact Sie können AWS Artifact Berichte verwenden, um AWS Sicherheits- und Compliance-Dokumente wie AWS ISO-Zertifizierungen, Payment Card Industry (PCI) und System and Organization Controls (SOC) - Berichte herunterzuladen.

AWS Artifact unterstützt die Funktion zur delegierten Verwaltung nicht. Stattdessen können Sie diese Funktion auf nur IAM-Rollen im Security Tooling-Konto beschränken, die Ihren Audit- und Compliance-Teams gehören, sodass diese diese Berichte herunterladen, überprüfen und bei Bedarf externen Prüfern zur Verfügung stellen können. Darüber hinaus können Sie bestimmte IAM-Rollen mithilfe von IAM-Richtlinien so einschränken, dass sie nur auf bestimmte AWS Artifact Berichte zugreifen können. Beispiele für IAM-Richtlinien finden Sie in der Dokumentation.AWS Artifact

> **Designüberlegung**
>
> Wenn Sie sich AWS-Konto für ein eigenes Audit- und Compliance-Team entscheiden, können Sie ein Sicherheitsauditkonto einrichten, das vom Security Tooling-Konto getrennt ist. AWS Artifact AWS Artifact Berichte belegen, dass ein Unternehmen einen dokumentierten Prozess befolgt oder eine bestimmte Anforderung erfüllt. Prüfartefakte werden während des gesamten Lebenszyklus der Systementwicklung gesammelt und archiviert und können als Nachweis für interne oder externe Audits und Bewertungen verwendet werden.

AWS KMS

AWS Key Management Service(AWS KMS) hilft Ihnen dabei, kryptografische Schlüssel zu erstellen und zu verwalten und deren Verwendung in einer Vielzahl von AWS-Services und in Ihren Anwendungen zu kontrollieren. AWS KMS ist ein sicherer und robuster Dienst, der Hardware-Sicherheitsmodule zum Schutz kryptografischer Schlüssel verwendet. Er folgt branchenüblichen Lebenszyklusprozessen für Schlüsselmaterial, wie z. B. Speicherung, Rotation und Zugriffskontrolle von Schlüsseln. AWS KMS kann zum Schutz Ihrer Daten mit Verschlüsselungs- und Signaturschlüsseln beitragen und kann über das Encryption SDK sowohl für die serverseitige als auch für die AWS clientseitige Verschlüsselung verwendet werden. Aus Gründen des Schutzes und der Flexibilität werden drei Arten von Schlüsseln AWS KMS unterstützt: vom Kunden verwaltete Schlüssel, AWS verwaltete Schlüssel und AWS eigene Schlüssel. Kundenverwaltete Schlüssel sind

AWS KMS Schlüssel in Ihrem AWS-Konto System, die Sie selbst erstellen, besitzen und verwalten. AWS Verwaltete AWS KMS Schlüssel sind Schlüssel in Ihrem Konto, die in Ihrem Namen von einem integrierten System erstellt AWS-Service , verwaltet und verwendet werden AWS KMS. AWS Eigene Schlüssel sind eine Sammlung von AWS KMS Schlüsseln, die ein Benutzer AWS-Service besitzt und verwaltet, sodass sie in mehreren Schlüsseln verwendet AWS-Konten werden können. Weitere Informationen zur Verwendung von AWS KMS Schlüsseln finden Sie in der AWS KMS Dokumentation und in den AWS KMS kryptografischen Details.

Eine Bereitstellungsoption besteht darin, die Verantwortung für die AWS KMS Schlüsselverwaltung auf ein einziges Konto zu zentralisieren und gleichzeitig die Fähigkeit, Schlüssel im Anwendungskonto zu verwenden, an Anwendungsressourcen zu delegieren, indem eine Kombination aus Schlüssel- und IAM-Richtlinien verwendet wird. Dieser Ansatz ist sicher und einfach zu verwalten, kann jedoch aufgrund von AWS KMS Drosselungslimits und Kontodienstbeschränkungen und der Überflutung des Sicherheitsteams mit operativen Schlüsselverwaltungsaufgaben auf Hürden stoßen. Eine weitere Bereitstellungsoption ist ein dezentrales Modell, bei dem Sie die Nutzung mehrerer Konten zulassen AWS KMS und es den Verantwortlichen für die Infrastruktur und die Workloads in einem bestimmten Konto ermöglichen, ihre eigenen Schlüssel zu verwalten. Dieses Modell bietet Ihren Workload-Teams mehr Kontrolle, Flexibilität und Agilität bei der Verwendung von Verschlüsselungsschlüsseln. Es trägt auch dazu bei, API-Beschränkungen zu vermeiden, den Umfang der Auswirkungen auf AWS-Konto nur eine zu beschränken und die Berichterstattung, Prüfung und andere Aufgaben im Zusammenhang mit der Einhaltung von Vorschriften zu vereinfachen. In einem dezentralen Modell ist es wichtig, Leitplanken zu implementieren und durchzusetzen, sodass die dezentralen Schlüssel auf die gleiche Weise verwaltet werden und die Verwendung von AWS KMS Schlüsseln gemäß den etablierten bewährten Verfahren und Richtlinien geprüft wird. Weitere Informationen finden Sie im Whitepaper AWS Key Management Service Best Practices. AWS SRA empfiehlt ein verteiltes Schlüsselverwaltungsmodell, bei dem sich die AWS KMS Schlüssel lokal innerhalb des Kontos befinden, in dem sie verwendet werden. Wir empfehlen, dass Sie nicht einen einzigen Schlüssel in einem Konto für alle kryptografischen Funktionen verwenden. Schlüssel können auf der Grundlage von Funktions- und Datenschutzanforderungen und zur Durchsetzung des Prinzips der geringsten Rechte erstellt werden. In einigen Fällen würden Verschlüsselungsberechtigungen von Entschlüsselungsberechtigungen getrennt gehalten, und Administratoren würden zwar Lebenszyklusfunktionen verwalten, wären aber nicht in der Lage, Daten mit den von ihnen verwalteten Schlüsseln zu ver- oder entschlüsseln.

AWS KMS Wird im Security Tooling-Konto verwendet, um die Verschlüsselung zentraler Sicherheitsdienste zu verwalten, z. B. des von der AWS CloudTrail Organisation verwalteten Organization Trails. AWS

AWS Private CA

AWS Private Certificate Authority(AWS Private CA) ist ein verwalteter privater CA-Dienst, mit dem Sie den Lebenszyklus Ihrer privaten Endentitäts-TLS-Zertifikate für EC2-Instances, Container, IoT-Geräte und lokale Ressourcen sicher verwalten können. Er ermöglicht verschlüsselte TLS-Kommunikation mit laufenden Anwendungen. Damit AWS Private CA können Sie Ihre eigene CA-Hierarchie (eine Stammzertifizierungsstelle über untergeordnete CAs Zertifikate bis hin zu Endzertifikaten) erstellen und damit Zertifikate ausstellen, um interne Benutzer, Computer, Anwendungen, Dienste, Server und andere Geräte zu authentifizieren und Computercode zu signieren. Von einer privaten Zertifizierungsstelle ausgestellte Zertifikate werden nur innerhalb Ihrer AWS Organisation als vertrauenswürdig eingestuft, nicht im Internet.

Ein Public Key Infrastructure (PKI) oder ein Sicherheitsteam kann für die Verwaltung der gesamten PKI-Infrastruktur verantwortlich sein. Dies beinhaltet die Verwaltung und Erstellung der privaten CA. Es muss jedoch eine Bestimmung geben, die es Workload-Teams ermöglicht, ihre Zertifikatsanforderungen selbst zu erfüllen. Die AWS SRA stellt eine zentralisierte CA-Hierarchie dar, in der die Stammzertifizierungsstelle innerhalb des Security Tooling-Kontos gehostet wird. Auf diese Weise können Sicherheitsteams strenge Sicherheitskontrollen durchsetzen, da die Stammzertifizierungsstelle die Grundlage der gesamten PKI bildet. Die Erstellung von privaten Zertifikaten aus der privaten Zertifizierungsstelle wird jedoch an Anwendungsentwicklungsteams delegiert, indem die CA mithilfe von AWS Resource Access Manager ()AWS RAM an ein Anwendungskonto weitergegeben wird. AWS RAM verwaltet die für die kontoübergreifende gemeinsame Nutzung erforderlichen Berechtigungen. Dadurch entfällt die Notwendigkeit einer privaten Zertifizierungsstelle für jedes Konto und die Bereitstellung ist kostengünstiger. Weitere Informationen zum Arbeitsablauf und zur Implementierung finden Sie im Blogbeitrag How AWS RAM to Share Your AWS Private CA Cros-Account.

> **Note**
>
> AWS Certificate Manager (ACM) unterstützt Sie auch bei der Bereitstellung, Verwaltung und Bereitstellung von öffentlichen TLS-Zertifikaten zur Verwendung mit. AWS-Services Um diese Funktionalität zu unterstützen, muss sich ACM in der Datei befinden AWS-Konto , die das öffentliche Zertifikat verwenden würde. Dies wird später in diesem Handbuch im Abschnitt Anwendungskonto erörtert.

Designüberlegungen

- Mit AWS Private CA können Sie eine Hierarchie von Zertifizierungsstellen mit bis zu fünf Ebenen erstellen. Sie können auch mehrere Hierarchien erstellen, jede mit einem eigenen Stamm. Die AWS Private CA Hierarchie sollte dem PKI-Design Ihrer Organisation entsprechen. Beachten Sie jedoch, dass mit einer Erhöhung der CA-Hierarchie die Anzahl der Zertifikate im Zertifizierungspfad zunimmt, was wiederum die Validierungszeit eines Endzertifikats verlängert. Eine klar definierte Zertifizierungsstellenhierarchie bietet Vorteile wie eine detaillierte Sicherheitskontrolle, die für jede Zertifizierungsstelle geeignet ist, die Delegierung untergeordneter Zertifizierungsstellen an eine andere Anwendung, was zur Aufteilung der Verwaltungsaufgaben führt, die Verwendung von CA mit begrenztem widerrufbarem Vertrauen, die Möglichkeit, unterschiedliche Gültigkeitszeiträume zu definieren, und die Möglichkeit, Pfadbeschränkungen durchzusetzen. Im Idealfall befinden sich Ihr Stammverzeichnis und Ihr untergeordnetes System getrennt. CAs AWS-Konten Weitere Informationen zur Planung einer CA-Hierarchie mithilfe von Hilfe AWS Private CA finden Sie in der AWS Private CA Dokumentation und im Blogbeitrag So sichern Sie eine unternehmensweite AWS Private CA Hierarchie für die Automobil- und Fertigungsindustrie.
- AWS Private CA kann in Ihre bestehende CA-Hierarchie integriert werden, sodass Sie die Automatisierungs- und systemeigenen AWS Integrationsfunktionen von ACM in Verbindung mit der bestehenden Vertrauensbasis, die Sie heute verwenden, nutzen können. Sie können eine untergeordnete Zertifizierungsstelle erstellen, die von einer übergeordneten Zertifizierungsstelle vor Ort AWS Private CA unterstützt wird. Weitere Informationen zur Implementierung finden Sie in der Dokumentation unter Installation eines untergeordneten Zertifizierungsstellenzertifikats, das von einer externen übergeordneten Zertifizierungsstelle signiert wurde. AWS Private CA

Amazon Inspector

Amazon Inspector ist ein automatisierter Schwachstellen-Management-Service, der automatisch Amazon EC2 EC2-Instances, Container-Images in Amazon Elastic Container Registry (Amazon ECR), AWS Lambda Funktionen und Code-Repositorys in Ihren Quellcode-Managern auf bekannte Softwareschwachstellen und unbeabsichtigte Netzwerkgefährdungen erkennt und scannt.

Amazon Inspector bewertet Ihre Umgebung während des gesamten Lebenszyklus Ihrer Ressourcen kontinuierlich, indem Ressourcen automatisch gescannt werden, wenn Sie Änderungen daran vornehmen. Zu den Ereignissen, die ein erneutes Scannen einer Ressource auslösen, gehören

die Installation eines neuen Pakets auf einer EC2-Instance, die Installation eines Patches und die Veröffentlichung eines neuen CVE-Berichts (Common Vulnerabilities and Exposures), der sich auf die Ressource auswirkt. Amazon Inspector unterstützt Benchmark-Bewertungen des Center of Internet Security (CIS) für Betriebssysteme in EC2-Instances.

Amazon Inspector lässt sich in Entwicklertools wie Jenkins und TeamCity zur Bewertung von Container-Images integrieren. Sie können Ihre Container-Images innerhalb Ihrer Continuous Integration und Continuous Delivery (CI/CD) tools, and push security to an earlier point in the software development lifecycle. Assessment findings are available in the CI/CDDashboard) auf Softwareschwachstellen untersuchen, sodass Sie automatisierte Aktionen als Reaktion auf kritische Sicherheitsprobleme wie blockierte Builds oder Image-Pushes an Container-Registries durchführen können. Wenn Sie über ein aktives Plug-in verfügen AWS-Konto, können Sie das Amazon Inspector-Plugin von Ihrem CI/CD Tool-Marktplatz aus installieren und Ihrer Build-Pipeline einen Amazon Inspector-Scan hinzufügen, ohne den Amazon Inspector-Service aktivieren zu müssen. Diese Funktion funktioniert mit CI/CD Tools, die überall gehostet werden — vor Ort AWS, vor Ort oder in Hybrid-Clouds —, sodass Sie in all Ihren Entwicklungspipelines konsistent eine einzige Lösung verwenden können. Wenn Amazon Inspector aktiviert ist, erkennt er automatisch all Ihre EC2-Instances, Container-Images in Amazon ECR und CI/CD Tools sowie Lambda-Funktionen in großem Umfang und überwacht sie kontinuierlich auf bekannte Sicherheitslücken.

Mit den Ergebnissen zur Netzwerkerreichbarkeit von Amazon Inspector wird die Erreichbarkeit Ihrer EC2-Instances zu oder von VPC-Edges wie Internet-Gateways, VPC-Peering-Verbindungen oder virtuellen privaten Netzwerken () über ein virtuelles Gateway bewertet. VPNs Diese Regeln helfen dabei, die Überwachung Ihrer AWS Netzwerke zu automatisieren und zu ermitteln, wo der Netzwerkzugriff auf Ihre EC2-Instances aufgrund schlecht verwalteter Sicherheitsgruppen, Zugriffskontrolllisten (), Internet-Gateways usw. falsch konfiguriert sein könnte. ACLs Weitere Informationen finden Sie in der Amazon Inspector Inspector-Dokumentation.

Wenn Amazon Inspector Sicherheitslücken oder offene Netzwerkpfade identifiziert, wird ein Ergebnis generiert, das Sie untersuchen können. Das Ergebnis umfasst umfassende Informationen über die Sicherheitsanfälligkeit, einschließlich einer Risikobewertung, der betroffenen Ressource und Empfehlungen zur Behebung. Die Risikobewertung ist speziell auf Ihre Umgebung zugeschnitten und wird berechnet, indem up-to-date CVE-Informationen mit zeitlichen und umweltbedingten Faktoren wie Netzwerkzugänglichkeit und Ausnutzbarkeit korreliert werden, um ein kontextbezogenes Ergebnis zu erhalten.

Amazon Inspector Code Security scannt den Quellcode von Erstanbieteranwendungen, Abhängigkeiten von Drittanbieteranwendungen und Infrastructure as Code (IaC) auf

Sicherheitslücken. Nachdem Sie Code Security aktiviert haben, können Sie eine Scan-Konfiguration erstellen und auf Ihr Code-Repository anwenden, um die Häufigkeit, den Scantyp und die zu scannenden Repositorys festzulegen. Code Security unterstützt statische Anwendungssicherheitstests (SAST), Software Composition Analysis (SCA) und IaC-Scans. Um die Häufigkeit zu konfigurieren, können Sie Scans bei Bedarf, bei Codeänderungen oder in regelmäßigen Abständen definieren. Beim Codescan werden Codefragmente erfasst, um erkannte Sicherheitslücken hervorzuheben. Die Codefragmente werden mit KMS-Schlüsseln verschlüsselt gespeichert. Der delegierte Administrator einer Organisation kann keine Codefragmente einsehen, die zu Mitgliedskonten gehören. Nachdem Sie Ihre Quellcode-Manager (SCMs) in Code Security integriert haben, werden alle Code-Repositorys in der Amazon Inspector Inspector-Konsole als Projekte aufgeführt. Code Security überwacht nur den Standardzweig jedes Repositorys. Amazon Inspector optimiert die Behebung von Sicherheitsproblemen, indem es spezifische Empfehlungen zur Behebung von Codefehlern direkt dort bereitstellt, wo Entwickler arbeiten. Die bidirektionale Integration mit Ihrem SCM schlägt automatisch Korrekturen als Kommentare in Pull-Anfragen (PRs) und Merge-Anfragen (MRs) für kritische und wichtige Ergebnisse vor und warnt Entwickler vor den wichtigsten Sicherheitslücken, die behoben werden müssen, ohne ihren Arbeitsablauf zu unterbrechen.

Um nach Sicherheitslücken zu suchen, müssen EC2-Instances mithilfe eines AWS Systems Manager Agenten (SSMAgent) verwaltet werden. AWS Systems Manager Für die Netzwerkerreichbarkeit von EC2-Instances oder das Scannen von Container-Images nach Sicherheitslücken in Amazon ECR- oder Lambda-Funktionen sind keine Agenten erforderlich.

Amazon Inspector ist in die delegierte Verwaltung integriert AWS Organizations und unterstützt diese. In der AWS SRA wird das Security Tooling-Konto zum delegierten Administratorkonto für Amazon Inspector. Das delegierte Administratorkonto von Amazon Inspector kann Ergebnisdaten und bestimmte Einstellungen für Mitglieder der AWS Organisation verwalten. Dazu gehören die Anzeige der Details der aggregierten Ergebnisse für alle Mitgliedskonten, die Aktivierung oder Deaktivierung von Scans für Mitgliedskonten und die Überprüfung gescannter Ressourcen innerhalb der Organisation. AWS

Designüberlegungen

- Amazon Inspector integriert sich automatisch mit AWS Security Hub CSPM Security Hub, wenn beide Dienste aktiviert sind. Sie können diese Integration verwenden, um alle Ergebnisse von Amazon Inspector an Security Hub CSPM zu senden, das diese Ergebnisse dann in die Analyse Ihres Sicherheitsstatus einbezieht.

- Amazon Inspector exportiert automatisch Ereignisse für Ergebnisse, Änderungen der Ressourcenabdeckung und erste Scans einzelner Ressourcen nach Amazon EventBridge und optional in einen Amazon Simple Storage Service (Amazon S3) -Bucket. Um aktive Ergebnisse in einen S3-Bucket zu exportieren, benötigen Sie einen AWS KMS Schlüssel, mit dem Amazon Inspector Ergebnisse verschlüsseln kann, und einen S3-Bucket mit Berechtigungen, die es Amazon Inspector ermöglichen, Objekte hochzuladen. EventBridgeDie Integration ermöglicht es Ihnen, Ergebnisse im Rahmen Ihrer bestehenden Sicherheits- und Compliance-Workflows nahezu in Echtzeit zu überwachen und zu verarbeiten. EventBridge Ereignisse werden zusätzlich zu dem Mitgliedskonto, von dem sie stammen, auf dem delegierten Administratorkonto von Amazon Inspector veröffentlicht.
- Amazon Inspector Code Security-Integrationen mit GitHub SaaS, GitHub Enterprise Cloud und GitHub Enterprise Server erfordern einen öffentlichen Internetzugang.

Beispiel für eine Implementierung

Die AWS SRA-Codebibliothek bietet eine Beispielimplementierung von Amazon Inspector. Es demonstriert die delegierte Administration (Security Tooling) und konfiguriert Amazon Inspector für alle bestehenden und future Konten in der Organisation. AWS

AWS Security Incident Response

AWS Security Incident Responseist ein Service, der Ihnen hilft, sich auf Sicherheitsvorfälle in Ihrer Umgebung vorzubereiten und darauf zu reagieren. AWS Er analysiert die Ergebnisse, eskaliert Sicherheitsereignisse und verwaltet Fälle, die Ihre sofortige Aufmerksamkeit erfordern. Darüber hinaus erhalten Sie Zugriff auf das AWS Customer Incident Response Team (CIRT), das die betroffenen Ressourcen untersucht. AWS Security Incident Response bietet außerdem automatisierte Reaktions- und Problembehebungsfunktionen mithilfe von AWS Systems Manager Dokumenten (SSM-Dokumenten), die Sicherheitsteams dabei unterstützen, effizienter auf Sicherheitsvorfälle zu reagieren und diese zu beheben. AWS Security Incident Response lässt sich in Amazon GuardDuty integrieren AWS Security Hub CSPM, um Sicherheitserkenntnisse zu erhalten und automatisierte Antworten zu orchestrieren.

In der AWS SRA AWS Security Incident Response wird es im Security Tooling-Konto als delegiertes Administratorkonto bereitgestellt. Das Security Tooling-Konto wird ausgewählt, weil es dem Zweck des Kontos entspricht, Sicherheitsdienste zu betreiben und Sicherheitswarnungen und -reaktionen

zu automatisieren. Das Security Tooling-Konto fungiert auch als delegiertes Administratorkonto für Security Hub CSPM und trägt so zur GuardDuty Vereinfachung des Workflow-Managements AWS Security Incident Response bei. AWS Security Incident Response ist so konfiguriert, dass es funktioniert AWS Organizations, sodass Sie die Reaktionen auf Vorfälle in allen Konten Ihres Unternehmens vom Security Tooling-Konto aus verwalten können.

AWS Security Incident Response hilft Ihnen bei der Implementierung der folgenden Phasen des Incident-Response-Lebenszyklus:

- Vorbereitung: Erstellung und Pflege von Reaktionsplänen und SSM-Dokumenten für Eindämmungsmaßnahmen.
- Erkennung und Analyse: Analysieren Sie automatisch Sicherheitsergebnisse und bestimmen Sie den Schweregrad des Vorfalls.
- Erkennung und Analyse: Eröffnen Sie einen vom Service unterstützten Fall und wenden Sie sich an das AWS CIRT, um weitere Unterstützung zu erhalten. CIRT ist eine Gruppe von Personen, die bei aktiven Sicherheitsereignissen Unterstützung bieten.
- Eindämmung und Beseitigung: Führen Sie automatisierte Eindämmungsmaßnahmen mithilfe von SSM-Dokumenten durch.
- Aktivitäten nach dem Vorfall: Dokumentieren Sie die Einzelheiten des Vorfalls und führen Sie Analysen nach dem Vorfall durch.

Sie können es auch verwenden, um selbst AWS Security Incident Response verwaltete Fälle zu erstellen. AWS Security Incident Response kann eine ausgehende Benachrichtigung oder einen Fall erstellen, wenn Sie sich eines Problems bewusst sein oder entsprechend handeln müssen, das sich auf Ihr Konto oder Ihre Ressourcen auswirken könnte. Diese Funktion ist nur verfügbar, wenn Sie die Workflows proaktive Reaktion und Alert-Triaging als Teil Ihres Abonnements aktivieren.

Designüberlegungen

- Überprüfen und testen Sie bei der Implementierung AWS Security Incident Response die automatisierten Reaktionsaktionen sorgfältig, bevor Sie sie in der Produktion aktivieren. Automatisierung kann die Reaktion auf Vorfälle beschleunigen, falsch konfigurierte automatisierte Aktionen können sich jedoch auf legitime Workloads auswirken.
- Erwägen Sie die Verwendung von SSM-Dokumenten AWS Security Incident Response zur Implementierung unternehmensspezifischer Eindämmungsverfahren bei gleichzeitiger Beibehaltung der im Service integrierten Best Practices für häufig auftretende Vorfälle.

- Wenn Sie die Verwendung AWS Security Incident Response in einer VPC planen, stellen Sie sicher, dass Sie die entsprechenden VPC-Endpunkte für Systems Manager und andere integrierte Dienste konfiguriert haben, um Containment-Aktionen in privaten Subnetzen zu ermöglichen.

Bereitstellung gemeinsamer Sicherheitsdienste in allen AWS-Konten

Im Abschnitt Anwenden von Sicherheitsdiensten im gesamten AWS Unternehmen weiter oben in dieser Referenz wurden Sicherheitsdienste hervorgehoben, die eine schützen AWS-Konto, und es wurde darauf hingewiesen, dass viele dieser Dienste auch innerhalb dieser Datenbank konfiguriert und verwaltet werden können AWS Organizations. Einige dieser Dienste sollten für alle Konten bereitgestellt werden, und Sie werden sie in der AWS SRA sehen. Dies ermöglicht einheitliche Leitplanken und ermöglicht eine zentrale Überwachung, Verwaltung und Steuerung in Ihrem gesamten Unternehmen. AWS

Security Hub CSPM,, GuardDuty AWS Config, IAM Access Analyzer und CloudTrail Organization Trails werden in allen Konten angezeigt. Die ersten drei unterstützen die Funktion für delegierte Administratoren, die bereits im Abschnitt Verwaltungskonto, vertrauenswürdiger Zugriff und delegierte Administratoren beschrieben wurde. CloudTrail verwendet derzeit einen anderen Aggregationsmechanismus.

Das AWS GitHub SRA-Code-Repository bietet eine Beispielimplementierung für die Aktivierung von Security Hub CSPM,, GuardDuty AWS Config AWS Firewall Manager, und CloudTrail Organization Trails für all Ihre Konten, einschließlich des AWS Org Management-Kontos.

Designüberlegungen

- Bestimmte Kontokonfigurationen erfordern möglicherweise zusätzliche Sicherheitsdienste. Beispielsweise sollten Konten, die S3-Buckets verwalten (die Konten Application und Log Archive), auch Amazon Macie enthalten und die Aktivierung der CloudTrail S3-Datenereignisprotokollierung in diesen gängigen Sicherheitsdiensten in Betracht ziehen. (Macie unterstützt die delegierte Verwaltung mit zentraler Konfiguration und Überwachung.) Ein anderes Beispiel ist Amazon Inspector, das nur für Konten gilt, die entweder EC2-Instances oder Amazon ECR-Images hosten.
- Zusätzlich zu den zuvor in diesem Abschnitt beschriebenen Diensten umfasst die AWS SRA zwei sicherheitsorientierte Dienste, Amazon Detective und AWS Audit Manager, die

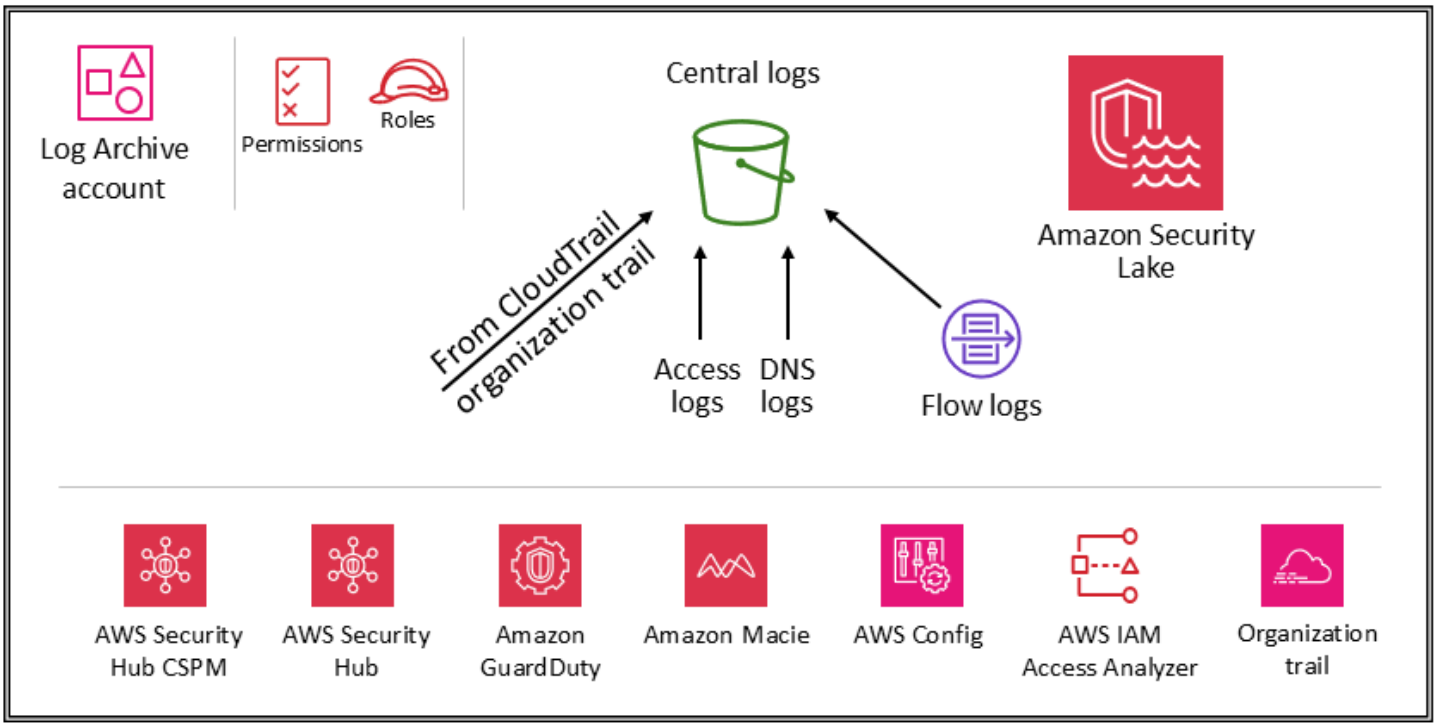
die AWS Organizations Integration und die delegierte Administratorfunktion unterstützen. Diese Dienste sind jedoch nicht Teil der empfohlenen Dienste für das Konto-Baselining, da wir festgestellt haben, dass diese Dienste in den folgenden Szenarien am besten verwendet werden:

- Sie haben ein engagiertes Team oder eine Gruppe von Ressourcen, die diese Funktionen ausführen. Detective wird am besten von Sicherheitsanalystenteams eingesetzt, und Audit Manager ist hilfreich für Ihre internen Audit- oder Compliance-Teams.
- Sie möchten sich zu Beginn Ihres Projekts auf ein Kernpaket von Tools wie GuardDuty Security Hub CSPM konzentrieren und dann darauf aufbauen, indem Sie Dienste nutzen, die zusätzliche Funktionen bieten.

Security OU — Konto protokollieren

Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

Das folgende Diagramm zeigt die AWS Sicherheitsdienste, die im Log Archive-Konto konfiguriert sind.



Das Log Archive-Konto dient der Erfassung und Archivierung aller sicherheitsrelevanten Protokolle und Backups. Mit zentralisierten Protokollen können Sie Amazon S3 S3-Objektzugriffe, unbefugte Aktivitäten anhand von Identitäten, Änderungen der IAM-Richtlinien und andere kritische Aktivitäten, die mit sensiblen Ressourcen ausgeführt werden, überwachen, prüfen und Warnmeldungen dazu geben. Die Sicherheitsziele sind einfach: Es sollte sich um unveränderlichen Speicher handeln, auf den nur über kontrollierte, automatisierte und überwachte Mechanismen zugegriffen werden kann und der auf Beständigkeit ausgelegt sein (z. B. durch die Verwendung geeigneter Replikations- und Archivierungsprozesse). Es können tiefgreifende Kontrollen implementiert werden, um die Integrität und Verfügbarkeit der Protokolle und des Protokollverwaltungsprozesses zu schützen. Zusätzlich zu präventiven Kontrollen, wie der Zuweisung von Rollen mit den geringsten Rechten für den Zugriff und der Verschlüsselung von Protokollen mit einem kontrollierten AWS KMS Schlüssel, können Sie auch detektive Kontrollen einsetzen, AWS Config um diese Sammlung von Berechtigungen im Falle unerwarteter Änderungen zu überwachen (und Warnmeldungen und Korrekturen vorzunehmen).

Designüberlegung

Die von Ihren Infrastruktur-, Betriebs- und Workload-Teams verwendeten Betriebsprotokolldaten überschneiden sich häufig mit den Protokolldaten, die von Sicherheits-, Audit- und Compliance-Teams verwendet werden. Wir empfehlen Ihnen, Ihre Betriebsprotokolldaten im Log Archive-Konto zu konsolidieren. Je nach Ihren spezifischen Sicherheits- und Governance-Anforderungen müssen Sie möglicherweise die in diesem

Konto gespeicherten Betriebsprotokolldaten filtern. Möglicherweise müssen Sie auch angeben, wer Zugriff auf die Betriebsprotokolldaten im Log Archive-Konto hat.

Arten von Protokollen

Zu den primären Protokollen, die in der AWS SRA angezeigt werden, gehören AWS CloudTrail (Organization Trail), Amazon VPC-Flow-Logs, Zugriffsprotokolle von Amazon CloudFront und AWS WAF und DNS-Logs von Amazon Route 53. Diese Protokolle bieten eine Prüfung der Aktionen, die von einem Benutzer, einer Rolle oder einer Netzwerkeinheit ergriffen (oder versucht) wurden (z. B. anhand einer IP-Adresse identifiziert). AWS-Service Andere Protokolltypen (z. B. Anwendungsprotokolle oder Datenbankprotokolle) können ebenfalls erfasst und archiviert werden. Weitere Informationen zu Protokollquellen und bewährten Methoden für die Protokollierung finden Sie in der Sicherheitsdokumentation der einzelnen Dienste.

Amazon S3 als zentraler Protokollspeicher

Viele AWS-Services Protokollinformationen in Amazon S3 — entweder standardmäßig oder ausschließlich. AWS CloudTrail, Amazon VPC Flow Logs, Elastic Load Balancing GuardDuty, Amazon AWS Config, und AWS WAF sind einige Beispiele für Dienste, die Informationen in Amazon S3 protokollieren. Das bedeutet, dass die Protokollintegrität durch S3-Objektintegrität, die Protokollvertraulichkeit durch S3-Objektzugriffskontrollen und die Protokollverfügbarkeit durch S3 Object Lock, S3-Objektversionen und S3-Lebenszyklusregeln erreicht wird. Durch die Protokollierung von Informationen in einem dedizierten und zentralen S3-Bucket, der sich in einem speziellen Konto befindet, können Sie diese Protokolle in nur wenigen Buckets verwalten und strenge Sicherheitskontrollen, Zugriffskontrollen und Aufgabentrennung durchsetzen.

In der AWS SRA stammen die in Amazon S3 gespeicherten Primärprotokolle CloudTrail, daher wird in diesem Abschnitt beschrieben, wie Sie diese Objekte schützen können. Diese Anleitung gilt auch für alle anderen S3-Objekte, die entweder von Ihren eigenen Anwendungen oder von anderen AWS-Services erstellt wurden. Wenden Sie diese Muster immer dann an, wenn Sie Daten in Amazon S3 haben, die eine hohe Integrität, strenge Zugriffskontrolle und automatische Aufbewahrung oder Zerstörung erfordern.

Alle neuen Objekte (einschließlich CloudTrail Protokolle), die in S3-Buckets hochgeladen werden, werden standardmäßig mithilfe der serverseitigen Amazon-Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln (SSE-S3) verschlüsselt. Dies trägt zum Schutz der gespeicherten Daten bei, die Zugriffskontrolle wird jedoch ausschließlich durch IAM-

Richtlinien gesteuert. Um eine zusätzliche verwaltete Sicherheitsebene bereitzustellen, können Sie serverseitige Verschlüsselung mit AWS KMS Schlüsseln verwenden, die Sie verwalten (SSE-KMS) für alle Sicherheits-S3-Buckets. Dadurch wird eine zweite Ebene der Zugriffskontrolle hinzugefügt. Um Protokolldateien lesen zu können, muss ein Benutzer sowohl über Amazon S3 S3-Leseberechtigungen für das S3-Objekt als auch über eine zugewiesene IAM-Richtlinie oder -Rolle verfügen, die ihm Berechtigungen zum Entschlüsseln gemäß der zugehörigen Schlüsselrichtlinie gewährt.

Zwei Optionen helfen Ihnen, die Integrität von CloudTrail Protokollobjekten, die in Amazon S3 gespeichert sind, zu schützen oder zu überprüfen. CloudTrail bietet eine Überprüfung der Integrität von Protokolldateien, um festzustellen, ob eine Protokolldatei nach CloudTrail der Übermittlung geändert oder gelöscht wurde. Die andere Option ist S3 Object Lock.

Sie können nicht nur den S3-Bucket selbst schützen, sondern auch das Prinzip der geringsten Rechte für die Protokollierungsdienste (z. B. CloudTrail) und das Log Archive-Konto einhalten. Beispielsweise `AWSCloudTrail_FullAccess` können Benutzer mit Berechtigungen, die durch die AWS verwaltete IAM-Richtlinie gewährt wurden, die sensibelsten und wichtigsten Überwachungsfunktionen in ihrem System deaktivieren oder neu konfigurieren. AWS-Konten Beschränken Sie die Anwendung dieser IAM-Richtlinie auf so wenige Personen wie möglich.

Verwenden Sie detektive Kontrollen, wie sie von AWS Config IAM Access Analyzer bereitgestellt werden, um dieses umfassendere Kollektiv präventiver Kontrollen im Hinblick auf unerwartete Änderungen zu überwachen (und zu warnen und zu korrigieren).

Eine eingehendere Diskussion der bewährten Sicherheitsmethoden für S3-Buckets finden Sie in der Amazon S3-Dokumentation, in Online-Tech-Talks und im Blogbeitrag Die 10 besten Sicherheitsmethoden für die Sicherung von Daten in Amazon S3.

> **Beispiel für eine Implementierung**
>
> Die AWS SRA-Codebibliothek bietet eine Beispielimplementierung für den öffentlichen Zugriff Amazon S3 S3-Blockkonten. Dieses Modul blockiert den öffentlichen Zugriff auf Amazon S3 für alle bestehenden und future Konten in der AWS Organisation.

Amazon Security Lake

AWS SRA empfiehlt, dass Sie das Log Archive-Konto als delegiertes Administratorkonto für Amazon Security Lake verwenden. Wenn Sie dies tun, sammelt Security Lake unterstützte Protokolle in speziellen S3-Buckets im selben Konto wie andere von der SRA empfohlene Sicherheitsprotokolle.

Um die Verfügbarkeit der Protokolle und den Protokollverwaltungsprozess zu schützen, sollte auf die S3-Buckets für Security Lake nur vom Security Lake-Dienst oder von IAM-Rollen zugegriffen werden, die von Security Lake für Quellen oder Abonnenten verwaltet werden. Verwenden Sie nicht nur präventive Kontrollen, wie die Zuweisung von Rollen mit den geringsten Rechten für den Zugriff und die Verschlüsselung von Protokollen mit einem kontrollierten AWS KMS Schlüssel, sondern auch detektivische Kontrollen, AWS Config um diese Sammlung von Berechtigungen für unerwartete Änderungen zu überwachen (und zu warnen und zu korrigieren).

Der Security Lake-Administrator kann die Protokollerfassung in Ihrer gesamten Organisation aktivieren. AWS Diese Protokolle werden in regionalen S3-Buckets im Log Archive-Konto gespeichert. Um die Protokolle zu zentralisieren und die Speicherung und Analyse zu vereinfachen, kann der Security Lake-Administrator außerdem eine oder mehrere Rollup-Regionen auswählen, in denen Protokolle aus allen regionalen S3-Buckets konsolidiert und gespeichert werden. Protokolle aus den unterstützten Dateien AWS-Services werden automatisch in ein standardisiertes Open-Source-Schema namens Open Cybersecurity Schema Framework (OCSF) konvertiert und im Apache Parquet-Format in Security Lake S3-Buckets gespeichert. Mit der OCSF-Unterstützung normalisiert und konsolidiert Security Lake auf effiziente Weise Sicherheitsdaten aus und anderen Unternehmenssicherheitsquellen, um ein einheitliches AWS und zuverlässiges Repository für sicherheitsrelevante Informationen zu schaffen.

Security Lake kann Protokolle sammeln, die mit AWS CloudTrail Verwaltungsereignissen und CloudTrail Datenereignissen für Amazon S3 und verknüpft sind AWS Lambda. Um CloudTrail Verwaltungsereignisse in Security Lake zu erfassen, benötigen Sie mindestens einen CloudTrail regionsübergreifenden Organisations-Trail, der CloudTrail Verwaltungsereignisse mit Lese- und Schreibzugriff sammelt. Die Protokollierung muss für den Trail aktiviert sein. Ein Trail mit mehreren Regionen überträgt Protokolldateien aus mehreren Regionen in einen einzigen S3-Bucket für eine einzelne AWS-Konto. Wenn sich die Regionen in verschiedenen Ländern befinden, sollten Sie die Anforderungen für den Datenexport berücksichtigen, um festzustellen, ob Trails für mehrere Regionen aktiviert werden können.

AWS Security Hub CSPM ist eine unterstützte native Datenquelle in Security Lake, und Sie sollten Security Hub CSPM-Ergebnisse zu Security Lake hinzufügen. Security Hub CSPM generiert

Erkenntnisse aus vielen verschiedenen Integrationen AWS-Services und Integrationen von Drittanbietern. Diese Ergebnisse helfen Ihnen dabei, sich einen Überblick über Ihre Compliance-Situation zu verschaffen und festzustellen, ob Sie die Sicherheitsempfehlungen und -lösungen befolgen. AWS AWS Partner

Um Transparenz und umsetzbare Erkenntnisse aus Protokollen und Ereignissen zu gewinnen, können Sie die Daten mithilfe von Tools wie Amazon Athena, Amazon OpenSearch Service, Amazon Quick und Lösungen von Drittanbietern abfragen. Benutzer, die Zugriff auf die Security Lake-Protokolldaten benötigen, sollten nicht direkt auf das Log Archive-Konto zugreifen. Sie sollten nur über das Security Tooling-Konto auf Daten zugreifen. Oder sie können andere AWS-Konten oder lokale Standorte verwenden, die Analysetools wie OpenSearch Service, Quick oder Tools von Drittanbietern wie SIEM-Tools (Security Information and Event Management) bereitstellen. Um Zugriff auf die Daten zu gewähren, sollte der Administrator Security Lake-Abonnenten im Log Archive-Konto konfigurieren und das Konto, das Zugriff auf die Daten benötigt, als Abfragezugriffs-Abonnent konfigurieren. Weitere Informationen finden Sie unter Amazon Security Lake im Abschnitt Security OU – Security Tooling-Konto dieses Handbuchs.

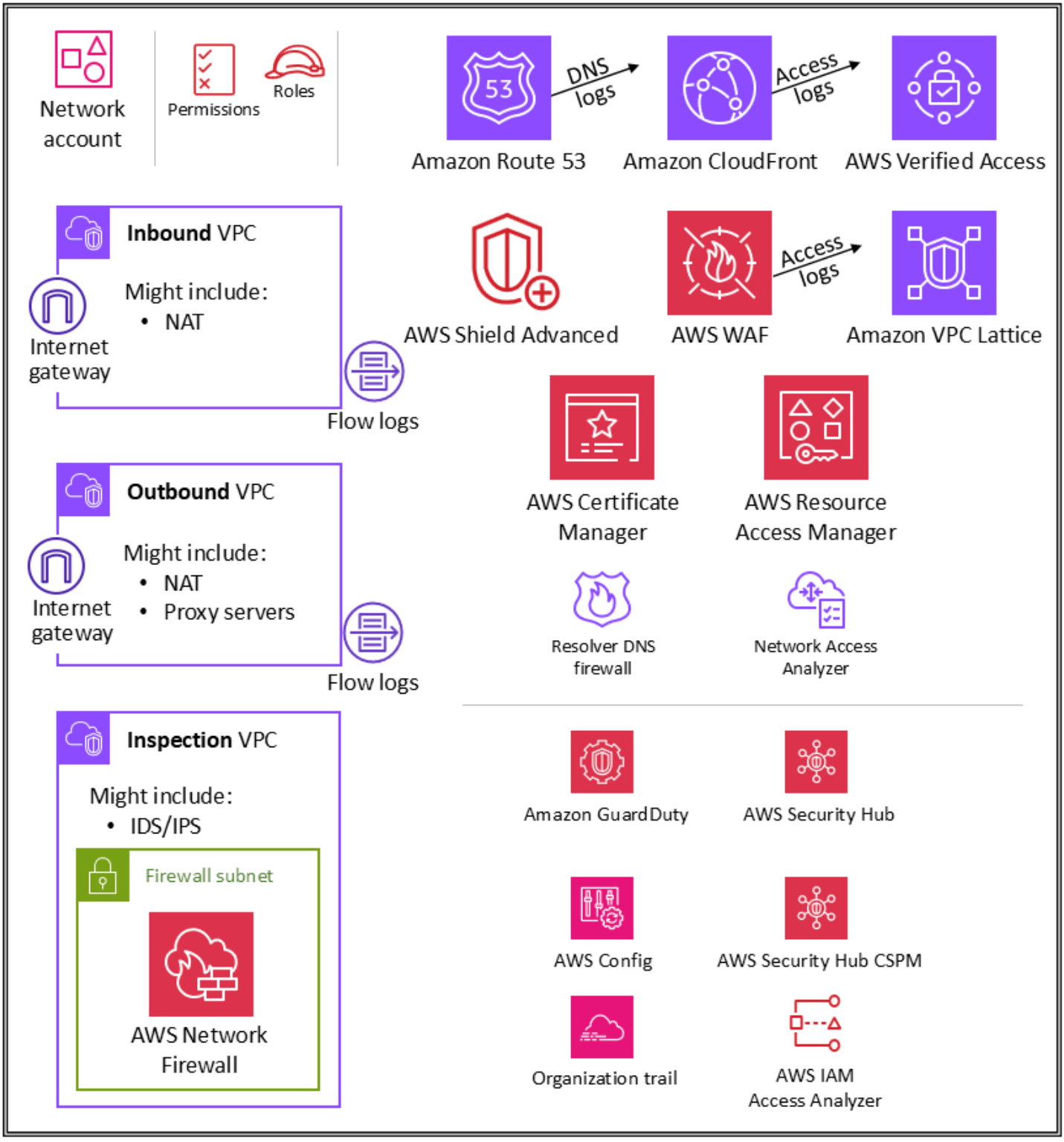
Security Lake bietet eine AWS verwaltete Richtlinie, mit der Sie den Administratorzugriff auf den Service verwalten können. Weitere Informationen finden Sie im Security Lake-Benutzerhandbuch. Als bewährte Methode empfehlen wir, die Konfiguration von Security Lake über Entwicklungspipelines einzuschränken und Konfigurationsänderungen über die AWS Konsolen oder die AWS Command Line Interface (AWS CLI) zu verhindern. Darüber hinaus sollten Sie strenge IAM-Richtlinien und Dienststeuerungsrichtlinien (SCPs) einrichten, um nur die für die Verwaltung von Security Lake erforderlichen Berechtigungen bereitzustellen. Sie können Benachrichtigungen so konfigurieren, dass jeder direkte Zugriff auf diese S3-Buckets erkannt wird.

> **Designüberlegung**
>
> Wenn Sie CloudTrail Verwaltungsereignisse in Security Lake aktivieren, führen diese zu Security Lake-Gebühren. Für die Erfassung von CloudTrail Verwaltungsereignissen in Security Lake ist ein CloudTrail regionsübergreifender Organisationspfad erforderlich, in dem CloudTrail Verwaltungsereignisse mit Lese- und Schreibzugriff erfasst werden. Dieser erste Trail steht Ihnen kostenlos zur Verfügung. CloudTrail Managementereignisse machen in der Regel nur einen kleinen Prozentsatz (etwa 5%) der gesamten CloudTrail Ereignisse aus. Dies gilt für Kunden, die ein Log Archive-Konto verwenden AWS Control Tower oder über zentralisierte CloudTrail Protokolle verfügen.

Infrastruktur-OE – Netzwerkkonto

Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

Das folgende Diagramm zeigt die AWS Sicherheitsdienste, die im Netzwerkkonto konfiguriert sind.



Das Netzwerkkonto verwaltet das Gateway zwischen Ihrer Anwendung und dem weiteren Internet. Es ist wichtig, diese bidirektionale Schnittstelle zu schützen. Das Netzwerkkonto isoliert die Netzwerkservices, die Konfiguration und den Betrieb von den Workloads, der Sicherheit

und anderen Infrastrukturen der einzelnen Anwendungen. Diese Regelung schränkt nicht nur Konnektivität, Berechtigungen und Datenfluss ein, sondern unterstützt auch die Aufgabentrennung und die geringsten Berechtigungen für die Teams, die mit diesen Konten arbeiten müssen. Durch die Aufteilung des Netzwerkflusses in separate eingehende und ausgehende virtuelle private Clouds (VPCs) können Sie sensible Infrastrukturen und vertraulichen Datenverkehr vor unerwünschtem Zugriff schützen. Das eingehende Netzwerk gilt allgemein als risikoreicher und verdient eine angemessene Weiterleitung, Überwachung und mögliche Problembehebung. Diese Infrastrukturkonten erben die Zugriffsberechtigungen des Organisationsverwaltungskontos und der Infrastruktur-OE. Teams für Netzwerk und Sicherheits verwalten den Großteil der Infrastruktur in diesem Konto.

Netzwerkarchitektur

Obwohl Netzwerkdesign und -spezifikationen den Rahmen dieses Dokuments sprengen würden, empfehlen wir die folgenden drei Optionen für die Netzwerkkonnektivität zwischen den verschiedenen Konten: VPC-Peering, und AWS PrivateLink. AWS Transit Gateway Wichtige Überlegungen bei der Auswahl dieser Optionen sind Betriebsnormen, Budgets und spezifische Bandbreitenanforderungen.

- VPC-Peering – Die einfachste Methode, zwei miteinander zu verbinden, VPCs ist die Verwendung von VPC-Peering. Eine Verbindung ermöglicht eine vollständige bidirektionale Konnektivität zwischen den. VPCs VPCs die sich in separaten Konten befinden und auch gemeinsam genutzt werden AWS-Regionen können. Im großen Maßstab, wenn Sie Dutzende bis Hunderte haben VPCs, führt die Verbindung dieser Verbindungen mit Peering zu einem Geflecht von Hunderten bis Tausenden von Peering-Verbindungen, was schwierig zu verwalten und zu skalieren sein kann. VPC-Peering eignet sich am besten, wenn Ressourcen in einer VPC mit Ressourcen in einer anderen VPC kommunizieren müssen, die Umgebung beider kontrolliert und gesichert VPCs wird und die Anzahl der VPCs zu verbindenden Ressourcen weniger als 10 beträgt (um die individuelle Verwaltung jeder Verbindung zu ermöglichen).
- AWS PrivateLink– PrivateLink bietet private Konnektivität zwischen Diensten und VPCs Anwendungen. Sie können Ihre eigene Anwendung in Ihrer VPC erstellen und sie als PrivateLink -gestützten Dienst (als Endpunktdienst bezeichnet) konfigurieren. Andere AWS Principals können je nach Art des Dienstes eine Verbindung von ihrer VPC zu Ihrem Endpunktdienst herstellen, indem sie einen Schnittstellen-VPC-Endpunkt oder einen Gateway Load Balancer-Endpunkt verwenden. Bei der Verwendung PrivateLink wird der Dienstdatenverkehr nicht über ein öffentlich routbares Netzwerk geleitet. Verwenden Sie diese Option, PrivateLink wenn Sie über ein Client-Server-Setup verfügen, in dem Sie einem oder mehreren Verbrauchern VPCs unidirektionalen Zugriff auf einen bestimmten Dienst oder eine Gruppe von Instanzen in der Service Provider-VPC gewähren

möchten. Dies ist auch eine gute Option, wenn sich die IP-Adressen der Clients und Server der beiden VPCs überschneiden, da elastische Netzwerkschnittstellen innerhalb der Client-VPC PrivateLink verwendet werden, sodass keine IP-Konflikte mit dem Dienstanbieter auftreten.

- AWS Transit Gateway– Transit Gateway bietet ein hub-and-spoke Design für Verbindungen VPCs und lokale Netzwerke als vollständig verwalteten Dienst, ohne dass Sie virtuelle Geräte bereitstellen müssen. AWS verwaltet Hochverfügbarkeit und Skalierbarkeit. Ein Transit-Gateway ist eine regionale Ressource und kann Tausende von VPCs innerhalb derselben verbinden AWS-Region. Sie können Ihre hybride Konnektivität (VPN und AWS Direct Connect Verbindungen) mit einem einzigen Transit-Gateway verbinden und so die gesamte Routing-Konfiguration Ihres AWS Unternehmens an einem Ort konsolidieren und kontrollieren. Ein Transit-Gateway löst die Komplexität, die mit der Erstellung und Verwaltung mehrerer VPC-Peering-Verbindungen in großem Maßstab verbunden ist. Dies ist die Standardeinstellung für die meisten Netzwerkarchitekturen, aber aufgrund spezifischer Anforderungen in Bezug auf Kosten, Bandbreite und Latenz ist VPC-Peering möglicherweise besser für Ihre Anforderungen geeignet.

Eingehende (Erfassungs)-VPC

Die eingehende VPC soll Netzwerkverbindungen akzeptieren, überprüfen und weiterleiten, die von außerhalb der Anwendung initiiert wurden. Abhängig von den Besonderheiten der Anwendung können Sie mit einer gewissen Network Address Translation (NAT) in dieser VPC rechnen. Flow-Protokolle von dieser VPC werden erfasst und im Protokollarchiv-Konto gespeichert.

Ausgehende (Ausgabe)-VPC

Die ausgehende VPC ist für die Verarbeitung von Netzwerkverbindungen vorgesehen, die von der Anwendung aus initiiert werden. Abhängig von den Besonderheiten der Anwendung können Sie erwarten, dass Traffic NAT, AWS-Service spezifische VPC-Endpunkte und das Hosten externer API-Endpunkte in dieser VPC angezeigt werden. Flow-Protokolle von dieser VPC werden erfasst und im Protokollarchiv-Konto gespeichert.

Überprüfungs-VPC

Eine spezielle Inspektions-VPC bietet einen vereinfachten und zentralen Ansatz für die Verwaltung von Inspektionen zwischen VPCs (in demselben oder in verschiedenen AWS-Regionen), dem Internet und lokalen Netzwerken. Stellen Sie für die AWS SRA sicher, dass der gesamte Datenverkehr zwischen den Daten die Inspektions-VPC VPCs durchläuft, und vermeiden Sie es, die Inspektions-VPC für andere Workloads zu verwenden.

AWS Network Firewall

AWS Network Firewallist ein hochverfügbarer, verwalteter Netzwerk-Firewall-Service für Ihre VPC. Damit können Sie mühelos Stateful-Inspection, Intrusion Prevention und Detection sowie Webfilterung implementieren und verwalten, um Ihre virtuellen Netzwerke zu schützen. AWS Sie können die Network Firewall verwenden, um TLS-Sitzungen zu entschlüsseln und den eingehenden und ausgehenden Verkehr zu überprüfen. Weitere Informationen zur Konfiguration der Network Firewall finden Sie im Blogbeitrag AWS Network Firewall — Neuer verwalteter Firewall-Service in VPC.

Sie verwenden in Ihrer VPC eine Firewall pro Availability Zone. Für jede Availability Zone wählen Sie ein Subnetz aus, das den Firewall-Endpunkt hostet, der Ihren Datenverkehr filtert. Der Firewall-Endpunkt in einer Availability Zone kann alle Subnetze innerhalb der Zone schützen, mit Ausnahme des Subnetzes, in dem er sich befindet. Je nach Anwendungsfall und Bereitstellungsmodell kann das Firewall-Subnetz entweder öffentlich oder privat sein. Die Firewall ist für den eingehenden oder ausgehenden Datenverkehr vollständig transparent und führt keine Network Address Translation (NAT) durch. Sie behält die Quell- und Zieladresse bei. In dieser Referenzarchitektur werden die Firewall-Endpunkte in einer Überprüfungs-VPC gehostet. Der gesamte Datenverkehr von der eingehenden VPC und zur ausgehenden VPC wird zur Überprüfung durch dieses Firewall-Subnetz geleitet.

Die Network Firewall macht Firewall-Aktivitäten anhand von CloudWatch Amazon-Metriken in Echtzeit sichtbar und bietet eine bessere Sichtbarkeit des Netzwerkverkehrs, indem Protokolle an Amazon Simple Storage Service (Amazon S3) und Amazon Data Firehose gesendet werden. CloudWatch Die Network Firewall ist mit Ihrem bestehenden Sicherheitsansatz kompatibel, einschließlich Technologien von AWS Partnern. Sie können auch bestehende Suricata-Regelsätze importieren, die möglicherweise intern geschrieben oder extern von Drittanbietern oder Open-Source-Plattformen bezogen wurden.

In der AWS SRA wird die Network Firewall innerhalb des Netzwerkkontos verwendet, da die auf die Netzwerksteuerung ausgerichtete Funktionalität des Dienstes der Absicht des Kontos entspricht.

Designüberlegungen

- AWS Firewall Manager unterstützt Network Firewall, sodass Sie Netzwerk-Firewall-Regeln zentral in Ihrem Unternehmen konfigurieren und bereitstellen können. (Einzelheiten finden Sie in der AWS Dokumentation unter Verwenden von AWS Network Firewall Richtlinien in Firewall Manager.) Wenn Sie Firewall Manager konfigurieren, erstellt er automatisch

eine Firewall mit Regelsätzen in den Konten VPCs , die Sie angeben. Außerdem wird für jede Availability Zone, die öffentliche Subnetze enthält, ein Endpunkt in einem dedizierten Subnetz bereitgestellt. Gleichzeitig werden alle Änderungen am zentral konfigurierten Regelsatz automatisch nachgelagert auf den bereitgestellten Firewalls von Network Firewall aktualisiert.

- Mit Network Firewall sind mehrere Bereitstellungsmodelle verfügbar. Welchen Ansatz Sie wählen, hängt von Ihrem Anwendungsfall und Ihren Anforderungen ab. Beispiele sind unter anderem:
  - Ein verteiltes Bereitstellungsmodell, bei dem die Network Firewall einzeln bereitgestellt wird VPCs.
  - Ein zentralisiertes Bereitstellungsmodell, bei dem Network Firewall in einer zentralen VPC für Ost-West-(VPC-zu-VPC) oder Nord-Süd-Datenverkehr (ausgehender und eingehender Internetzugriff, On-Premises) bereitgestellt wird.
  - Ein kombiniertes Bereitstellungsmodell, bei dem Network Firewall in einer zentralen VPC für den Ost-West- und einen Teil des Nord-Süd-Datenverkehrs bereitgestellt wird.
- Es ist eine bewährte Methode, das Network-Firewall-Subnetz nicht für die Bereitstellung sonstiger Services zu verwenden. Dies liegt daran, dass Network Firewall den Datenverkehr von Quellen oder Zielen innerhalb des Firewall-Subnetzes nicht überprüfen kann.

Network Access Analyzer

Network Access Analyzer ist ein Feature von Amazon VPC, das unbeabsichtigten Zugriff auf Ihre Ressourcen identifiziert. Sie können Network Access Analyzer verwenden, um die Netzwerksegmentierung zu validieren, Ressourcen zu identifizieren, auf die über das Internet oder nur über vertrauenswürdige IP-Adressbereiche zugegriffen werden kann, und um zu überprüfen, ob Sie über angemessene Netzwerkkontrollen für alle Netzwerkpfade verfügen.

Network Access Analyzer verwendet automatische Argumentationsalgorithmen, um die Netzwerkpfade zu analysieren, die ein Paket zwischen Ressourcen in einem AWS Netzwerk zurücklegen kann, und liefert Ergebnisse für Pfade, die Ihrem definierten Netzwerkzugriffsbereich entsprechen. Network Access Analyzer führt eine statische Analyse einer Netzwerkkonfiguration durch, was bedeutet, dass im Rahmen dieser Analyse keine Pakete im Netzwerk übertragen werden.

Die Regeln von Amazon Inspector Network Reachability bieten ein verwandtes Feature. Die durch diese Regeln generierten Ergebnisse werden im Anwendungskonto verwendet. Sowohl Network

Access Analyzer als auch Network Reachability verwenden die neueste Technologie aus der Initiative AWS Provable Security und wenden diese Technologie mit unterschiedlichen Schwerpunkten an. Das Network Reachability-Paket konzentriert sich speziell auf EC2 Instanzen und deren Internetzugriff.

Das Netzwerkkonto definiert die kritische Netzwerkinfrastruktur, die den Verkehr in und aus Ihrer AWS Umgebung steuert. Dieser Datenverkehr muss genau überwacht werden. In der AWS SRA wird Network Access Analyzer innerhalb des Netzwerkkontos verwendet, um unbeabsichtigte Netzwerkzugriffe zu identifizieren, Ressourcen zu identifizieren, auf die über Internet-Gateways zugegriffen werden kann, und um zu überprüfen, ob geeignete Netzwerksteuerungen wie Netzwerkfirewalls und NAT-Gateways auf allen Netzwerkpfaden zwischen Ressourcen und Internet-Gateways vorhanden sind.

> **Designüberlegung**
>
> Network Access Analyzer ist eine Funktion von Amazon VPC und kann in jedem AWS-Konto verwendet werden, der über eine VPC verfügt. Netzwerkadministratoren können eng abgegrenzte, kontenübergreifende IAM-Rollen einrichten, um zu überprüfen, ob die genehmigten Netzwerkpfade innerhalb der einzelnen Rollen durchgesetzt werden. AWS-Konto

AWS RAM

AWS Resource Access Manager(AWS RAM) hilft Ihnen dabei, die AWS Ressourcen, die Sie in einem System erstellen, sicher mit anderen zu teilen. AWS-Konto AWS-KontenAWS RAM bietet einen zentralen Ort, um die gemeinsame Nutzung von Ressourcen zu verwalten und diese Benutzererfahrung für alle Konten zu standardisieren. Dies macht es einfacher, Ressourcen zu verwalten und gleichzeitig die Vorteile der administrativen und abrechnungstechnischen Isolierung zu nutzen und den Umfang der Vorteile einer Strategie mit mehreren Konten zur Eindämmung der Auswirkungen zu reduzieren. Wenn Ihr Konto von verwaltet wird AWS Organizations, AWS RAM können Sie Ressourcen für alle Konten in der Organisation oder nur für Konten innerhalb einer oder mehrerer bestimmter Organisationseinheiten (OUs) gemeinsam nutzen. Sie können Inhalte auch mit bestimmten AWS-Konten Konten teilen, unabhängig davon, ob das Konto Teil einer Organisation ist. Sie können einige unterstützte Ressourcentypen auch für bestimmte IAM-Rollen und -Benutzer freigeben.

AWS RAM ermöglicht es Ihnen, Ressourcen gemeinsam zu nutzen, die keine ressourcenbasierten IAM-Richtlinien unterstützen, z. B. VPC-Subnetze und Route 53-Regeln. Außerdem können die Besitzer einer Ressource mit sehen AWS RAM, welche Principals Zugriff auf einzelne Ressourcen haben, die sie gemeinsam genutzt haben. IAM-Prinzipale können die Liste der Ressourcen, die für sie freigegeben wurden, direkt abrufen. Dies ist bei Ressourcen, die durch IAM-Ressourcenrichtlinien gemeinsam genutzt werden, nicht möglich. AWS RAM Wird verwendet, um Ressourcen außerhalb Ihrer AWS Organisation gemeinsam zu nutzen, wird ein Einladungsprozess eingeleitet. Der Empfänger muss die Einladung annehmen, bevor der Zugriff auf die Ressourcen gewährt wird. Dies bietet zusätzliche Kontrollen und Abwägungen.

AWS RAM wird vom Ressourcenbesitzer in dem Konto aufgerufen und verwaltet, in dem die gemeinsam genutzte Ressource bereitgestellt wird. Ein in der AWS SRA AWS RAM dargestellter häufiger Anwendungsfall besteht darin, dass Netzwerkadministratoren VPC-Subnetze und Transit-Gateways mit der gesamten Organisation gemeinsam nutzen. AWS Dies ermöglicht die Entkopplung von Netzwerkverwaltungsfunktionen AWS-Konto und trägt zur Aufgabentrennung bei. Weitere Informationen zu VPC Sharing finden Sie im AWS Blogbeitrag VPC Sharing: A new approach to multiple accounts and VPC management and the AWS network infrastructure whitepaper.

> **Designüberlegung**
>
> Obwohl AWS RAM ein Dienst nur innerhalb des Netzwerkkontos in der AWS SRA bereitgestellt wird, wird er normalerweise in mehr als einem Konto bereitgestellt. Sie können beispielsweise Ihr Data Lake-Management auf ein einziges Data Lake-Konto zentralisieren und dann die AWS Lake Formation Datenkatalogressourcen (Datenbanken und Tabellen) mit anderen Konten in Ihrer AWS Organisation gemeinsam nutzen. Weitere Informationen finden Sie in der AWS Lake Formation Dokumentation und im AWS Blogbeitrag Sichere gemeinsame AWS-Konten Nutzung AWS Lake Formation Ihrer Daten. Darüber hinaus können Sicherheitsadministratoren beim Aufbau einer AWS Private Certificate Authority Hierarchie bewährte Methoden anwenden. AWS RAM CAs kann mit externen Dritten geteilt werden, die Zertifikate ausstellen können, ohne Zugriff auf die CA-Hierarchie zu haben. Auf diese Weise können Quellorganisationen den Zugriff Dritter einschränken und entziehen.

AWS Verified Access

AWS Verified Accessbietet sicheren Zugriff auf Unternehmensanwendungen und Ressourcen ohne VPN. Es verbessert die Sicherheitslage und hilft bei der Anwendung von Zero-Trust-Zugriff, indem jede Zugriffsanfrage in Echtzeit anhand vordefinierter Anforderungen bewertet wird. Sie können für

jede Anwendung eine eigene Zugriffsrichtlinie mit Bedingungen definieren, die auf Identitätsdaten und Gerätestatus basieren. Verified Access bietet sicheren Zugriff auf HTTP (S) -Anwendungen, z. B. browserbasierte Anwendungen und Nicht-HTTP (S) -Anwendungen über TCP-, SSH- und RDP-Protokolle für Anwendungen wie Git-Repositorys, Datenbanken und Instanzgruppen. EC2 Auf diese kann über ein Befehlszeilenterminal oder über eine Desktop-Anwendung zugegriffen werden. Verified Access vereinfacht auch Sicherheitsabläufe, indem es Administratoren hilft, Zugriffsrichtlinien effizient festzulegen und zu überwachen. Dadurch bleibt mehr Zeit, um Richtlinien zu aktualisieren, auf Sicherheits- und Verbindungsvorfälle zu reagieren und die Einhaltung von Compliance-Standards zu überprüfen. Verified Access unterstützt auch die Integration mit AWS WAF , sodass Sie häufig auftretende Bedrohungen wie SQL-Injection und Cross-Site Scripting (XSS) herausfiltern können. Verified Access ist nahtlos integriert AWS IAM Identity Center, sodass sich Benutzer bei SAML-basierten Identitätsanbietern von Drittanbietern authentifizieren können (). IdPs Wenn Sie bereits über eine benutzerdefinierte IdP-Lösung verfügen, die mit OpenID Connect (OIDC) kompatibel ist, kann Verified Access Benutzer auch authentifizieren, indem eine direkte Verbindung mit Ihrem IdP hergestellt wird. Verified Access protokolliert jeden Zugriffsversuch, sodass Sie schnell auf Sicherheitsvorfälle und Prüfanfragen reagieren können. Verified Access unterstützt die Übermittlung dieser Protokolle an Amazon Simple Storage Service (Amazon S3), Amazon CloudWatch Logs und Amazon Data Firehose.

Verified Access unterstützt zwei gängige Muster von Unternehmensanwendungen: interne Anwendungen und Internetanwendungen. Verified Access lässt sich mithilfe von Application Load Balancers oder elastischen Netzwerkschnittstellen in Anwendungen integrieren. Wenn Sie einen Application Load Balancer verwenden, benötigt Verified Access einen internen Load Balancer. Da Verified Access auf AWS WAF Instanzebene unterstützt, kann eine bestehende Anwendung, die in einen Application Load Balancer AWS WAF integriert ist, Richtlinien vom Load Balancer auf die Verified Access-Instanz verschieben. Eine Unternehmensanwendung wird als Verified-Access-Endpunkt dargestellt. Jeder Endpunkt ist einer Verified-Access-Gruppe zugeordnet und erbt die Zugriffsrichtlinie für die Gruppe. Eine Verified-Access-Gruppe besteht aus einer Sammlung von Verified-Access-Endpunkten und einer Verified-Access-Richtlinie auf Gruppenebene. Gruppen vereinfachen die Richtlinienverwaltung und ermöglichen es IT-Administratoren, grundlegende Kriterien festzulegen. Anwendungsbesitzer können je nach Sensibilität der Anwendung weitere detaillierte Richtlinien definieren.

In der AWS SRA wird Verified Access innerhalb des Netzwerkkontos gehostet. Das zentrale IT-Team richtet zentral verwaltete Konfigurationen ein. Sie können beispielsweise Vertrauensanbieter wie Identitätsanbieter (z. B. Okta) und Anbieter von Gerätevertrauensstellungen (z. B. Jamf) miteinander verbinden, Gruppen erstellen und die Richtlinien auf Gruppenebene festlegen. Diese Konfigurationen

können dann mithilfe AWS RAM von für Dutzende, Hunderte oder Tausende von Workload-Konten gemeinsam genutzt werden. Auf diese Weise können Anwendungsteams die zugrunde liegenden Endgeräte verwalten, die ihre Anwendungen verwalten, ohne dass andere Teams zusätzliche Kosten verursachen müssen. AWS RAM bietet eine skalierbare Möglichkeit, Verified Access für Unternehmensanwendungen zu nutzen, die auf unterschiedlichen Workload-Konten gehostet werden.

> **Designüberlegung**
>
> Sie können Endpunkte für Anwendungen mit ähnlichen Sicherheitsanforderungen gruppieren, um die Richtlinienverwaltung zu vereinfachen, und die Gruppe dann mit Anwendungskonten teilen. Alle Anwendungen in der Gruppe verwenden dieselbe Gruppenrichtlinie. Wenn für eine Anwendung in der Gruppe aufgrund eines besonderen Anwendungsfalls eine bestimmte Richtlinie erforderlich ist, können Sie für diese Anwendung eine Richtlinie auf Anwendungsebene anwenden.

Amazon VPC Lattice

Amazon VPC Lattice ist ein Anwendungsnetzwerkservice, der die Kommunikation verbindet, überwacht und sichert service-to-service. Ein Service, der oft als Microservice bezeichnet wird, ist eine unabhängig einsetzbare Softwareeinheit, die eine bestimmte Aufgabe erfüllt. VPC Lattice verwaltet automatisch die Netzwerkkonnektivität und das Routing auf Anwendungsebene zwischen Diensten VPCs und AWS-Konten ohne dass Sie die zugrunde liegende Netzwerkkonnektivität, Frontend-Load Balancer oder Sidecar-Proxys verwalten müssen. Es bietet einen vollständig verwalteten Proxy auf Anwendungsebene, der Routing auf Anwendungsebene auf der Grundlage von Anforderungsmerkmalen wie Pfaden und Headern ermöglicht. VPC Lattice ist in die VPC-Infrastruktur integriert und bietet daher einen konsistenten Ansatz für eine Vielzahl von Rechenarten wie Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS) und. AWS Lambda VPC Lattice unterstützt auch gewichtetes Routing für Bereitstellungen blue/green und Bereitstellungen im kanarischen Stil. Sie können VPC Lattice verwenden, um ein Servicenetzwerk mit einer logischen Grenze zu erstellen, das die Diensterkennung und Konnektivität automatisch implementiert. VPC Lattice lässt sich zur service-to-service Authentifizierung und Autorisierung mithilfe von Authentifizierungsrichtlinien in IAM integrieren.

VPC Lattice lässt sich integrieren AWS RAM , um die gemeinsame Nutzung von Diensten und Servicenetzwerken zu ermöglichen. AWS SRA stellt eine verteilte Architektur dar, in der Entwickler oder Dienstbesitzer VPC-Lattice-Dienste in ihrem Anwendungskonto erstellen. Servicebesitzer

definieren die Listener, Routing-Regeln und Zielgruppen zusammen mit Authentifizierungsrichtlinien. Anschließend geben sie die Services für andere Konten frei und ordnen die Services VPC-Lattice-Servicenetzwerken zu. Diese Netzwerke werden von Netzwerkadministratoren im Netzwerkkonto erstellt und mit dem Anwendungskonto gemeinsam genutzt. Netzwerkadministratoren konfigurieren die Authentifizierungsrichtlinien und die Überwachung von Services auf Netzwerkebene. Administratoren ordnen VPCs VPC-Lattice-Dienste einem oder mehreren Dienstnetzwerken zu. Eine ausführliche Anleitung zu dieser verteilten Architektur finden Sie im AWS Blogbeitrag Aufbau sicherer Multi-Account-Multi-VPC-Konnektivität für Ihre Anwendungen mit Amazon VPC Lattice

Designüberlegungen

- Je nach dem Betriebsmodell Ihres Unternehmens oder der Sichtbarkeit des Servicenetzwerks können Netzwerkadministratoren ihre Servicenetzwerke gemeinsam nutzen und den Service-Besitzern die Kontrolle geben, ihre Dienste und diesen Servicenetzwerken zuzuordnen. VPCs Oder Servicebesitzer können ihre Services gemeinsam nutzen, und Netzwerkadministratoren können die Services Servicenetzwerken zuordnen.
- Ein Client kann nur Anfragen an Services senden, die einem Servicenetzwerk zugeordnet sind, wenn sich der Client in einer VPC befindet, die demselben Servicenetzwerk zugeordnet ist. Client-Datenverkehr, der eine VPC-Peering-Verbindung oder ein Transit-Gateway durchquert, wird verweigert.

Edge-Sicherheit

Edge-Sicherheit umfasst im Allgemeinen drei Arten von Schutzmaßnahmen: sichere Inhaltsbereitstellung, Schutz auf Netzwerk- und Anwendungsebene sowie Abwehr von verteilten Denial-of-Service-Angriffen (DDoS). Inhalte wie Daten, Videos und Anwendungen APIs müssen schnell und sicher bereitgestellt werden, wobei die empfohlene Version von TLS zur Verschlüsselung der Kommunikation zwischen Endpunkten verwendet wird. Für den Inhalt sollten außerdem Zugriffsbeschränkungen durch signierte URLs, signierte Cookies und Token-Authentifizierung gelten. Die Sicherheit auf Anwendungsebene sollte darauf ausgelegt sein, den Bot-Verkehr zu kontrollieren, gängige Angriffsmuster wie SQL-Injection oder Cross-Site Scripting (XSS) zu blockieren und Sichbarkeit des Web-Datenverkehrs gewährleisten. Am Netzwerkrand bietet DDo S-Mitigation eine wichtige Schutzschicht, die die kontinuierliche Verfügbarkeit geschäftskritischer Geschäftsabläufe und Dienste gewährleistet. Anwendungen und Anwendungen APIs sollten vor SYN-Floods, UDP-

Floods oder anderen Reflection-Angriffen geschützt sein und über eine integrierte Abwehr verfügen, um grundlegende Angriffe auf Netzwerkebene zu stoppen.

AWS bietet verschiedene Dienste zur Bereitstellung einer sicheren Umgebung, von der Core-Cloud bis zum Rand des Netzwerks. AWS Amazon CloudFront, AWS Certificate Manager (ACM), AWS Shield AWS WAF, und Amazon Route 53 arbeiten zusammen, um einen flexiblen, mehrschichtigen Sicherheitsperimeter zu schaffen. Mit CloudFront können Inhalte oder Anwendungen über HTTPS bereitgestellt werden APIs, indem TLSv1 .3 zur Verschlüsselung und Sicherung der Kommunikation zwischen Viewer-Clients und verwendet wird. CloudFront Sie können ACM verwenden, um ein benutzerdefiniertes SSL-Zertifikat zu erstellen und es kostenlos in einer CloudFront Distribution bereitzustellen. ACM kümmert sich automatisch um die Erneuerung des Zertifikats. Shield ist ein verwalteter DDo S-Schutzdienst, der zum Schutz von Anwendungen beiträgt, die auf ausgeführt AWS werden. Er bietet dynamische Erkennung und automatische Inline-Abwehrmaßnahmen, die Ausfallzeiten und Latenz von Anwendungen minimieren. AWS WAF ermöglicht die Erstellung von Regeln zum Filtern von Web-Traffic auf der Grundlage bestimmter Bedingungen (IP-Adressen, HTTP-Header und -Hauptteil oder benutzerdefiniert URIs), häufigen Webangriffen und allgegenwärtigen Bots. Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service. Route 53 verbindet Benutzeranfragen mit Internetanwendungen, die vor Ort AWS oder vor Ort ausgeführt werden. Die AWS SRA verwendet eine zentralisierte Architektur für Netzwerkeingänge, die innerhalb des Netzwerkkontos gehostet wird AWS Transit Gateway, sodass die Edge-Sicherheitsinfrastruktur ebenfalls in diesem Konto zentralisiert ist.

Amazon CloudFront

Amazon CloudFront ist ein sicheres Content Delivery Network (CDN), das inhärenten Schutz vor gängigen Versuchen auf Netzwerkebene und Transport DDo S bietet. Sie können Ihre Inhalte oder Anwendungen mithilfe von TLS-Zertifikaten bereitstellen, und erweiterte TLS-Funktionen werden automatisch aktiviert. APIs Sie können AWS Certificate Manager (ACM) verwenden, um ein benutzerdefiniertes TLS-Zertifikat zu erstellen und die HTTPS-Kommunikation zwischen Zuschauern und zu erzwingen CloudFront, wie weiter unten im Abschnitt ACM beschrieben. Sie können außerdem verlangen, dass für die Kommunikation zwischen CloudFront und Ihrem benutzerdefinierten Ursprung eine end-to-end Verschlüsselung bei der Übertragung implementiert wird. Für dieses Szenario müssen Sie ein TLS-Zertifikat auf Ihrem Ursprungsserver installieren. Wenn es sich bei Ihrem Ursprung um einen Elastic Load Balancer handelt, können Sie ein Zertifikat verwenden, das von ACM generiert wurde, oder ein Zertifikat, das von einer externen Zertifizierungsstelle (CA) validiert und in ACM importiert wurde. Wenn S3-Bucket-Website-Endpunkte als Ursprung für dienen CloudFront, können Sie die Verwendung von HTTPS mit Ihrem Ursprung nicht konfigurieren CloudFront , da Amazon S3 HTTPS für Website-Endpunkte nicht unterstützt. (Sie

können jedoch weiterhin HTTPS zwischen Zuschauern und CloudFront verlangen.) Daher sollten Sie ein Zertifikat verwenden, das von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde.

CloudFront bietet mehrere Optionen, um den Zugriff auf Ihre Inhalte zu sichern und einzuschränken. Beispielsweise kann es den Zugriff auf Ihren Amazon S3 S3-Ursprung einschränken, indem es signierte URLs und signierte Cookies verwendet. Weitere Informationen finden Sie in der CloudFront Dokumentation unter Sicheren Zugriff konfigurieren und den Zugriff auf Inhalte einschränken.

Die AWS SRA veranschaulicht zentralisierte CloudFront Verteilungen im Netzwerkkonto, da sie dem zentralisierten Netzwerkmuster entsprechen, das mithilfe von AWS Transit Gateway Durch die Bereitstellung und Verwaltung von CloudFront Verteilungen im Netzwerkkonto profitieren Sie von den Vorteilen zentraler Steuerungen. Sie können alle CloudFront Distributionen an einem zentralen Ort verwalten, was es einfacher macht, den Zugriff zu kontrollieren, Einstellungen zu konfigurieren und die Nutzung über alle Konten hinweg zu überwachen. Darüber hinaus können Sie die ACM-Zertifikate, DNS-Einträge und die CloudFront Protokollierung von einem zentralen Konto aus verwalten.

Das CloudFront Sicherheits-Dashboard bietet AWS WAF Transparenz und Kontrolle direkt in Ihrer CloudFront Distribution. Sie erhalten Einblick in die wichtigsten Sicherheitstrends Ihrer Anwendung, den erlaubten und blockierten Datenverkehr sowie die Bot-Aktivitäten. Sie können Ermittlungstools wie visuelle Protokollanalysen und integrierte Blockierungskontrollen verwenden, um Datenverkehrsmuster zu isolieren und den Datenverkehr zu blockieren, ohne Protokolle abzufragen oder Sicherheitsregeln zu schreiben.

Designüberlegungen

- Alternativ können Sie die Anwendung auch CloudFront als Teil der Anwendung im Anwendungskonto bereitstellen. In diesem Szenario trifft das Anwendungsteam beispielsweise Entscheidungen darüber, wie die CloudFront Distributionen bereitgestellt werden, legt die geeigneten Cache-Richtlinien fest und übernimmt die Verantwortung für die Verwaltung, Prüfung und Überwachung der CloudFront Distributionen. Durch die Verteilung der CloudFront Distributionen auf mehrere Konten können Sie von zusätzlichen Servicekontingenten profitieren. Ein weiterer Vorteil CloudFront ist, dass Sie die inhärente und automatisierte Origin Access Identity (OAI) und Origin Access Control (OAC) -Konfiguration verwenden können, um den Zugriff auf Amazon S3 S3-Ursprünge einzuschränken.
- Wenn Sie Webinhalte über ein CDN bereitstellen, müssen Sie verhindern CloudFront, dass Zuschauer das CDN umgehen und direkt auf Ihre ursprünglichen Inhalte zugreifen.

Um diese Beschränkung für den Zugriff auf die Herkunft AWS WAF zu erreichen, können Sie benutzerdefinierte Header verwenden CloudFront und hinzufügen und die Header überprüfen, bevor Sie Anfragen an Ihren benutzerdefinierten Ursprung weiterleiten. Eine ausführliche Erläuterung dieser Lösung finden Sie im AWS Sicherheits-Blogbeitrag How to enhance Amazon CloudFront Origin Security with AWS WAF and AWS Secrets Manager. Eine alternative Methode besteht darin, nur die CloudFront Präfixliste in der Sicherheitsgruppe einzuschränken, die dem Application Load Balancer zugeordnet ist. Dadurch wird sichergestellt, dass nur eine CloudFront Distribution auf den Load Balancer zugreifen kann.

AWS WAF

AWS WAFist eine Firewall für Webanwendungen, die dazu beiträgt, Ihre Webanwendungen vor Web-Exploits wie häufigen Sicherheitslücken und Bots zu schützen, die die Anwendungsverfügbarkeit beeinträchtigen, die Sicherheit gefährden oder übermäßig viele Ressourcen verbrauchen könnten. Es kann in eine CloudFront Amazon-Distribution, eine Amazon API Gateway-REST-API, einen Application Load Balancer, eine AWS AppSync GraphQL-API, einen Amazon Cognito Cognito-Benutzerpool und den Service integriert werden. AWS App Runner

AWS WAF verwendet Web-Zugriffskontrolllisten (ACLs), um eine Reihe von Ressourcen zu schützen. AWS Eine Web-ACL ist ein Regelwerk, das die Prüfkriterien und die damit verbundene Aktion definiert (Blockieren, Zulassen, Zählen oder Ausführen der Bot-Kontrolle), wenn eine Webanfrage die Kriterien erfüllt. AWS WAF stellt eine Reihe verwalteter Regeln bereit, die Schutz vor häufigen Sicherheitslücken in Anwendungen bieten. Diese Regeln werden von AWS Partnern kuratiert AWS und verwaltet. AWS WAF bietet auch eine leistungsstarke Regelsprache für die Erstellung benutzerdefinierter Regeln. Sie können benutzerdefinierte Regeln verwenden, um Prüfkriterien zu schreiben, die Ihren speziellen Anforderungen entsprechen. Beispiele hierfür sind IP-Einschränkungen, geografische Einschränkungen und benutzerdefinierte Versionen verwalteter Regeln, die besser zu Ihrem spezifischen Anwendungsverhalten passen.

AWS WAF bietet eine Reihe intelligenter, stufenweise verwalteter Regeln für allgemeine und gezielte Bots und den Schutz vor Kontoübernahmen (ATP). Ihnen werden eine Abonnementgebühr und eine Gebühr für die Datenverkehrs-Überprüfung berechnet, wenn Sie die Regelgruppen Bot Control und ATP verwenden. Wir empfehlen daher, dass Sie zuerst den Datenverkehr überwachen und sich erst dann für eine Option entscheiden. Sie können die kostenlos auf der AWS WAF Konsole verfügbaren Dashboards für Bot-Verwaltung und Kontoübernahme verwenden, um diese Aktivitäten

zu überwachen und dann zu entscheiden, ob Sie eine intelligente Regelgruppe benötigen. AWS WAF

In der AWS SRA AWS WAF ist das CloudFront in das Netzwerkkonto integriert. In dieser Konfiguration erfolgt die AWS WAF Regelverarbeitung an den Edge-Standorten statt innerhalb der VPC. Auf diese Weise kann bösartiger Datenverkehr näher am Endbenutzer gefiltert werden, der den Inhalt angefordert hat, und verhindert, dass bösartiger Datenverkehr in Ihr Kernnetzwerk gelangt.

Sie können vollständige AWS WAF Protokolle an einen S3-Bucket im Log Archive-Konto senden, indem Sie den kontoübergreifenden Zugriff auf den S3-Bucket konfigurieren. Weitere Informationen finden Sie im AWS re:POST-Artikel zu diesem Thema.

Designüberlegungen

- Als Alternative zur AWS WAF zentralen Bereitstellung im Netzwerkkonto lassen sich einige Anwendungsfälle besser durch die Bereitstellung AWS WAF im Anwendungskonto erfüllen. Sie können diese Option beispielsweise wählen, wenn Sie Ihre CloudFront Distributionen in Ihrem Anwendungskonto bereitstellen oder öffentlich zugängliche Application Load Balancer haben oder wenn Sie API Gateway vor Ihren Webanwendungen verwenden. Wenn Sie sich für die Bereitstellung AWS WAF in jedem Anwendungskonto entscheiden, verwenden Sie es, AWS Firewall Manager um die AWS WAF Regeln in diesen Konten über das zentrale Security Tooling-Konto zu verwalten.
- Sie können auch allgemeine AWS WAF Regeln auf der CloudFront Ebene und zusätzliche anwendungsspezifische AWS WAF Regeln auf einer regionalen Ressource wie dem Application Load Balancer oder dem API-Gateway hinzufügen.

AWS Shield

AWS Shieldist ein verwalteter DDo S-Protection-Dienst, der Anwendungen schützt, die auf. AWS Es gibt zwei Stufen von Shield: Shield Standard und Shield Advanced. Shield Standard bietet allen AWS Kunden Schutz vor den häufigsten Infrastrukturereignissen (Layer 3 und 4) ohne zusätzliche Kosten. Shield Advanced bietet ausgefeiltere automatische Abwehrmaßnahmen gegen unbefugte Ereignisse, die auf Anwendungen in geschützten Amazon- EC2, Elastic Load Balancing (Elastic Load Balancing) CloudFront AWS Global Accelerator, und Route 53-Hosting-Zonen abzielen. Wenn Sie Websites mit hoher Sichtbarkeit besitzen oder häufig DDo S-Angriffen ausgesetzt sind, können Sie die zusätzlichen Funktionen von Shield Advanced in Betracht ziehen.

Sie können die automatische Abwehr auf Anwendungsebene DDo S von Shield Advanced verwenden, um Shield Advanced so zu konfigurieren, dass es automatisch reagiert, um Angriffe der Anwendungsebene (Layer 7) gegen Ihre geschützten CloudFront Distributionen, Elastic Load Balancing (Elastic Load Balancing) -Load Balancer (Application, Network und Classic), Amazon Route 53-Hosting-Zonen, Amazon EC2 Elastic IP-Adressen und Standardbeschleuniger abzuwehren. AWS Global Accelerator Wenn Sie diese Funktion aktivieren, generiert Shield Advanced automatisch benutzerdefinierte AWS WAF Regeln zur Abwehr von DDo S-Angriffen. Shield Advanced bietet Ihnen auch Zugriff auf das AWS Shield Response Team (SRT). Sie können sich jederzeit an SRT wenden, um benutzerdefinierte Abwehrmaßnahmen für Ihre Anwendung oder während eines aktiven DDo S-Angriffs zu erstellen und zu verwalten. Wenn Sie möchten, dass SRT Ihre geschützten Ressourcen proaktiv überwacht und Sie während eines DDo S-Versuchs kontaktiert, sollten Sie die Aktivierung der Proactive Engagement-Funktion in Betracht ziehen.

Designüberlegungen

- Wenn Sie im Anwendungskonto über Workloads verfügen, denen mit dem Internet verbundene Ressourcen gegenüberstehen, z. B. CloudFront ein Application Load Balancer oder ein Network Load Balancer, konfigurieren Sie Shield Advanced im Anwendungskonto und fügen Sie diese Ressourcen zum Shield-Schutz hinzu. Sie können diese Optionen verwenden, um sie in großem Umfang AWS Firewall Manager zu konfigurieren.
- Wenn Sie mehrere Ressourcen im Datenfluss haben, z. B. eine CloudFront Verteilung vor einem Application Load Balancer, verwenden Sie nur die Einstiegspunktressource als geschützte Ressource. Dadurch wird sichergestellt, dass Sie Shield Data Transfer Out (DTO)-Gebühren nicht zweimal für zwei Ressourcen zahlen.
- Shield Advanced zeichnet Metriken auf, die Sie in Amazon überwachen können CloudWatch. (Weitere Informationen finden Sie CloudWatch in der AWS Dokumentation unter Monitoring with Amazon.) Richten Sie CloudWatch Alarme ein, um SNS-Benachrichtigungen an Ihr Sicherheitscenter zu erhalten, wenn ein DDo S-Ereignis erkannt wird. Bei einem vermuteten DDo S-Ereignis wenden Sie sich an das AWS Enterprise Support-Team, indem Sie ein Support-Ticket einreichen und diesem die höchste Priorität zuweisen. Das Enterprise Support Team wird das Shield Response Team (SRT) bei der Bearbeitung des Ereignisses einbeziehen. Darüber hinaus können Sie die AWS Shield Engagement Lambda-Funktion vorkonfigurieren, um ein Support-Ticket zu erstellen und eine E-Mail an das SRT-Team zu senden.

AWS Certificate Manager (ACM)

AWS Certificate Manager(ACM) ermöglicht die Bereitstellung, Verwaltung und Bereitstellung von öffentlichen und privaten TLS-Zertifikaten zur Verwendung mit AWS-Services und Ihren internen verbundenen Ressourcen. Mit ACM können Sie schnell ein Zertifikat anfordern, es auf ACM-integrierten AWS Ressourcen wie Elastic Load Balancing Balancing-Load Balancern, CloudFront Distributionen und APIs auf Amazon API Gateway bereitstellen und ACM die Zertifikatserneuerung überlassen. Wenn Sie öffentliche ACM-Zertifikate anfordern, müssen Sie weder ein key pair noch eine Certificate Signing Request (CSR) generieren, eine CSR an eine Zertifizierungsstelle (CA) senden oder das Zertifikat hochladen und installieren, wenn es empfangen wird. ACM bietet auch die Möglichkeit, von Drittanbietern ausgestellte TLS-Zertifikate zu importieren CAs und sie mit integrierten ACM-Diensten bereitzustellen. Wenn Sie ACM zur Verwaltung von Zertifikaten verwenden, werden private Schlüssel für Zertifikate sicher geschützt und gespeichert. Dabei werden bewährte Methoden zur Verschlüsselung und Schlüsselverwaltung angewendet. Bei ACM fallen keine zusätzlichen Gebühren für die Bereitstellung öffentlicher Zertifikate an, und ACM verwaltet den Erneuerungsprozess.

ACM wird im Netzwerkkonto verwendet, um ein öffentliches TLS-Zertifikat zu generieren, das wiederum von CloudFront Distributionen verwendet wird, um die HTTPS-Verbindung zwischen Zuschauern und herzustellen. CloudFront Weitere Informationen finden Sie in der CloudFront - Dokumentation.

> **Designüberlegung**
>
> Bei externen Zertifikaten muss sich ACM in demselben Konto befinden wie die Ressourcen, für die Zertifikate bereitgestellt werden. Zertifikate können nicht über Konten hinweg freigegeben werden.

Amazon Route 53

Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service. Sie können Route 53 zum Durchführen von drei wesentlichen Funktionen verwenden: Domain-Registrierung, DNS-Routing und Zustandsprüfung.

Sie können Route 53 als DNS-Dienst verwenden, um Domainnamen Ihren EC2 Instances, S3-Buckets, CloudFront Distributionen und anderen Ressourcen zuzuordnen. AWS Durch den verteilten Aufbau der AWS DNS-Server wird sichergestellt, dass Ihre Endbenutzer konsistent zu Ihrer

Anwendung weitergeleitet werden. Funktionen wie Route 53-Verkehrsfluss und Routingsteuerung helfen Ihnen dabei, die Zuverlässigkeit zu verbessern. Wenn Ihr primärer Anwendungsendpunkt nicht mehr verfügbar ist, können Sie Ihr Failover so konfigurieren, dass Ihre Benutzer an einen anderen Standort umgeleitet werden. Route 53 Resolver bietet rekursives DNS für Ihre VPC und lokale Netzwerke über AWS Direct Connect oder verwaltetes VPN. AWS

Durch die Verwendung des IAM-Dienstes mit Route 53 erhalten Sie eine genaue Kontrolle darüber, wer Ihre DNS-Daten aktualisieren kann. Sie können DNS-Sicherheitserweiterungen (DNSSEC) aktivieren, um es DNS-Resolvern zu ermöglichen, zu validieren, ob eine DNS-Antwort von Route 53 stammt und nicht manipuliert wurde.

Die Route 53 Resolver DNS Firewall bietet Schutz für ausgehende DNS-Anfragen von Ihrem. VPCs Diese Anforderungen verlaufen über Route 53 Resolver für die Auflösung von Domainnamen. Eine primäre Verwendung des DNS-Firewall-Schutzes besteht darin, die DNS-Exfiltration Ihrer Daten zu verhindern. Mit der DNS-Firewall können Sie die Domains überwachen und steuern, die Ihre Anwendungen abfragen können. Sie können den Zugriff auf die Domains verweigern, von denen Sie wissen, dass sie schlecht sind, und alle anderen Abfragen durchlaufen lassen. Alternativ können Sie allen Domains den Zugriff verweigern, außer jenen, denen Sie explizit vertrauen. Sie können die DNS-Firewall auch verwenden, um Auflösungsanforderungen an Ressourcen in privaten gehosteten Zonen (gemeinsam oder lokal) einschließlich VPC-Endpunktnamen zu blockieren. Sie kann auch Anfragen für öffentliche oder private EC2 Instanznamen blockieren.

Route-53-Resolver werden standardmäßig als Teil jeder VPC erstellt. In der AWS SRA wird Route 53 im Netzwerkkonto hauptsächlich für die DNS-Firewall-Funktion verwendet.

Designüberlegung

Die DNS-Firewall und AWS Network Firewall beide bieten die Filterung von Domainnamen, jedoch für unterschiedliche Arten von Datenverkehr. Sie können die DNS-Firewall und die Network Firewall zusammen verwenden, um die domänenbasierte Filterung für den Datenverkehr auf Anwendungsebene über zwei verschiedene Netzwerkpfade zu konfigurieren:

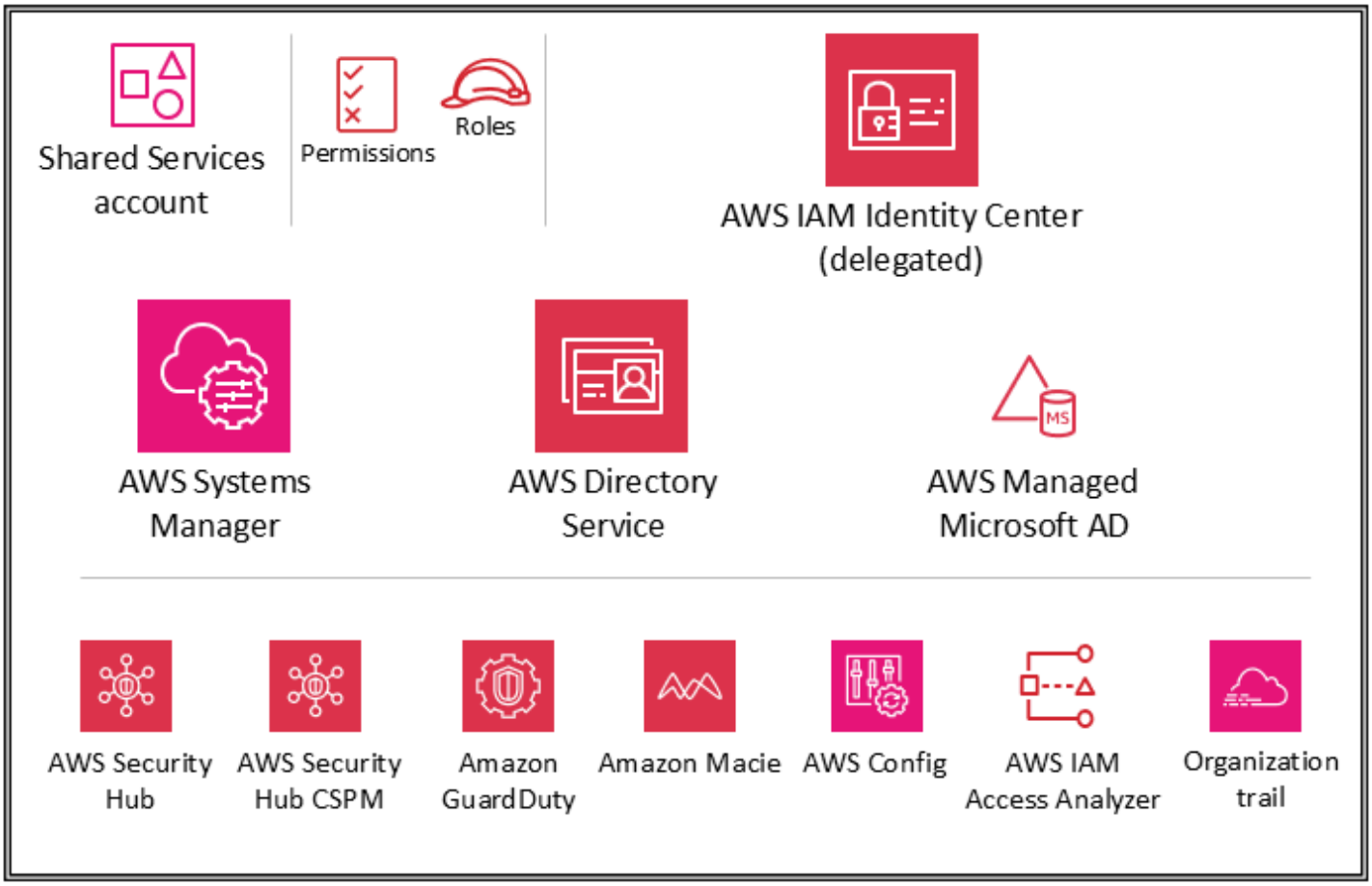
- Die DNS-Firewall bietet Filterung für ausgehende DNS-Abfragen, die den Route 53-Resolver von Anwendungen innerhalb Ihres Computers durchlaufen. VPCs Sie können die DNS-Firewall auch so konfigurieren, dass benutzerdefinierte Antworten für Abfragen an blockierte Domainnamen gesendet werden.

- Network Firewall bietet Filterung für den Datenverkehr auf Netzwerk- und Anwendungsebene, hat jedoch keine Einsicht in Abfragen, die von Route 53 Resolver durchgeführt werden.

Infrastructure OU — Shared Services-Konto

Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

Das folgende Diagramm zeigt die AWS Sicherheitsdienste, die im Shared Services-Konto konfiguriert sind.



Das Shared Services-Konto ist Teil der Infrastruktur-Organisationseinheit und dient dazu, die Dienste zu unterstützen, die mehrere Anwendungen und Teams zur Erzielung ihrer Ergebnisse verwenden. Zu dieser Kategorie gehören beispielsweise Verzeichnisdienste (Active Directory), Messaging-

Dienste und Metadatendienste. In der AWS SRA werden die gemeinsamen Dienste hervorgehoben, die Sicherheitskontrollen unterstützen. Die Netzwerkkonten sind zwar auch Teil der Infrastruktur-OU, sie wurden jedoch aus dem Shared Services-Konto entfernt, um die Aufgabentrennung zu unterstützen. Die Teams, die diese Dienste verwalten, benötigen weder Berechtigungen noch Zugriff auf die Netzwerkkonten.

AWS Systems Manager

AWS Systems Manager(das auch im Organisationsverwaltungskonto und im Anwendungskonto enthalten ist) bietet eine Reihe von Funktionen, mit denen Sie Ihre AWS Ressourcen einsehen und kontrollieren können. Eine dieser Funktionen, Systems Manager Explorer, ist ein anpassbares Operations-Dashboard, das Informationen über Ihre AWS Ressourcen meldet. Mithilfe AWS Organizations des Systems Manager Explorers können Sie Betriebsdaten für alle Konten in Ihrer AWS Organisation synchronisieren. Systems Manager wird im Shared Services-Konto über die delegierte Administratorfunktion in AWS Organizations bereitgestellt.

Systems Manager unterstützt Sie bei der Aufrechterhaltung von Sicherheit und Compliance, indem es Ihre verwalteten Instanzen scannt und festgestellte Richtlinienverstöße meldet (oder Korrekturmaßnahmen ergreift). Durch die Kopplung von Systems Manager mit entsprechenden Bereitstellungen in einzelnen Mitgliedern AWS-Konten (z. B. dem Anwendungskonto) können Sie die Erfassung von Instanzinventardaten koordinieren und Automatisierungen wie Patches und Sicherheitsupdates zentralisieren.

AWS Managed Microsoft AD

AWS Directory Service for Microsoft Active Directory, auch bekannt als AWS Managed Microsoft AD, ermöglicht Ihren verzeichnissensitiven Workloads und AWS Ressourcen die Nutzung von verwaltetem Active Directory. AWS Sie können AWS Managed Microsoft AD Amazon EC2 for Windows Server -, Amazon EC2 for Linux - und Amazon RDS for SQL Server-Instances zu Ihrer Domain hinzufügen und AWS End User Computing (EUC) -Services wie Amazon WorkSpaces mit Active Directory-Benutzern und -Gruppen nutzen.

AWS Managed Microsoft AD hilft Ihnen dabei, Ihr vorhandenes Active Directory auf AWS Cloud-Ressourcen zu erweitern und Ihre vorhandenen lokalen Benutzeranmeldedaten zu verwenden. Sie können auch Ihre lokalen Benutzer, Gruppen, Anwendungen und Systeme verwalten, ohne die Komplexität der Ausführung und Wartung eines lokalen, hochverfügbaren Active Directorys. Sie können Ihre vorhandenen Computer, Laptops und Drucker zu einer Domäne hinzufügen. AWS Managed Microsoft AD

AWS Managed Microsoft AD basiert auf Microsoft Active Directory und erfordert nicht, dass Sie Daten aus Ihrem vorhandenen Active Directory in die Cloud synchronisieren oder replizieren. Sie können vertraute Active Directory-Verwaltungstools und -funktionen wie Gruppenrichtlinienobjekte (GPOs), Domänenvertrauensstellungen, detaillierte Kennwortrichtlinien, gruppenverwaltete Dienstkonten (gMSAs), Schemaerweiterungen und Kerberos-basiertes Single Sign-On verwenden. Sie können auch Verwaltungsaufgaben delegieren und den Zugriff mithilfe von Active Directory-Sicherheitsgruppen autorisieren.

Mit der regionsübergreifenden Replikation können Sie ein einzelnes AWS Managed Microsoft AD Verzeichnis für mehrere bereitstellen und verwenden. AWS-Regionen Dies macht es für Sie einfacher und kostengünstiger, Ihre Microsoft Windows- und Linux-Workloads weltweit bereitzustellen und zu verwalten. Wenn Sie die automatische Replikationsfunktion für mehrere Regionen verwenden, erhalten Sie eine höhere Ausfallsicherheit, während Ihre Anwendungen für eine optimale Leistung ein lokales Verzeichnis verwenden.

AWS Managed Microsoft AD unterstützt das Lightweight Directory Access Protocol (LDAP) über SSL/TLS, auch bekannt als LDAPS, sowohl in Client- als auch in Serverrollen. AWS Managed Microsoft AD Unterstützt LDAPS über die Ports 636 (SSL) und 389 (TLS), wenn es als Server fungiert. Sie aktivieren die serverseitige LDAPS-Kommunikation, indem Sie auf Ihren AWS Managed Microsoft AD Domänencontrollern ein Zertifikat von einer Active Directory-Zertifikatsdienste (AD CS) AWS-Zertifizierungsstelle (CA) installieren. AWS Managed Microsoft AD Unterstützt LDAPS über die Ports 636 (SSL), wenn es als Client fungiert. Sie können die clientseitige LDAPS-Kommunikation aktivieren, indem Sie CA-Zertifikate von Ihren Serverzertifikatausstellern registrieren und dann LDAPS in AWS Ihrem Verzeichnis aktivieren.

In der AWS SRA Directory Service wird es innerhalb des Shared Services-Kontos verwendet, um Domänendienste für Microsoft-fähige Workloads über mehrere Mitgliedskonten hinweg bereitzustellen. AWS

> **Designüberlegung**
>
> Sie können Ihren lokalen Active Directory-Benutzern Zugriff darauf gewähren, sich mit ihren vorhandenen Active Directory-Anmeldeinformationen bei AWS-Managementkonsole und AWS Command Line Interface (AWS CLI) anzumelden, indem Sie IAM Identity Center verwenden und als Identitätsquelle auswählen. AWS Managed Microsoft AD Auf diese Weise können Ihre Benutzer bei der Anmeldung eine der ihnen zugewiesenen Rollen annehmen und entsprechend den für die Rolle definierten Berechtigungen auf die Ressourcen zugreifen

und Maßnahmen ergreifen. Eine alternative Option besteht darin, Ihren Benutzern AWS Managed Microsoft AD die Übernahme einer IAM-Rolle zu ermöglichen.

IAM Identity Center

Die AWS SRA verwendet die von unterstützte Funktion für delegierte Administratoren, AWS IAM Identity Center um den Großteil der Verwaltung von IAM Identity Center an das Shared Services-Konto zu delegieren. Auf diese Weise lässt sich die Anzahl der Benutzer einschränken, die Zugriff auf das Org Management-Konto benötigen. IAM Identity Center muss weiterhin im Org Management-Konto aktiviert sein, um bestimmte Aufgaben ausführen zu können, einschließlich der Verwaltung von Berechtigungssätzen, die im Org Management-Konto bereitgestellt werden.

Der Hauptgrund für die Verwendung des Shared Services-Kontos als delegierter Administrator für IAM Identity Center ist der Active Directory-Standort. Wenn Sie Active Directory als Ihre IAM Identity Center-Identitätsquelle verwenden möchten, müssen Sie das Verzeichnis in dem Mitgliedskonto suchen, das Sie als Ihr delegiertes IAM Identity Center-Administratorkonto festgelegt haben. In der AWS SRA wird das Shared Services-Konto gehostet AWS Managed Microsoft AD, sodass dieses Konto zum delegierten Administrator für IAM Identity Center ernannt wird.

IAM Identity Center unterstützt die gleichzeitige Registrierung eines einzelnen Mitgliedskontos als delegierter Administrator. Sie können ein Mitgliedskonto nur registrieren, wenn Sie sich mit den Anmeldeinformationen des Verwaltungskontos anmelden. Um die Delegierung zu aktivieren, müssen Sie die in der IAM Identity Center-Dokumentation aufgeführten Voraussetzungen berücksichtigen. Das delegierte Administratorkonto kann die meisten IAM Identity Center-Verwaltungsaufgaben ausführen, allerdings mit einigen Einschränkungen, die in der IAM Identity Center-Dokumentation aufgeführt sind. Der Zugriff auf das delegierte Administratorkonto für IAM Identity Center sollte streng kontrolliert werden.

Designüberlegungen

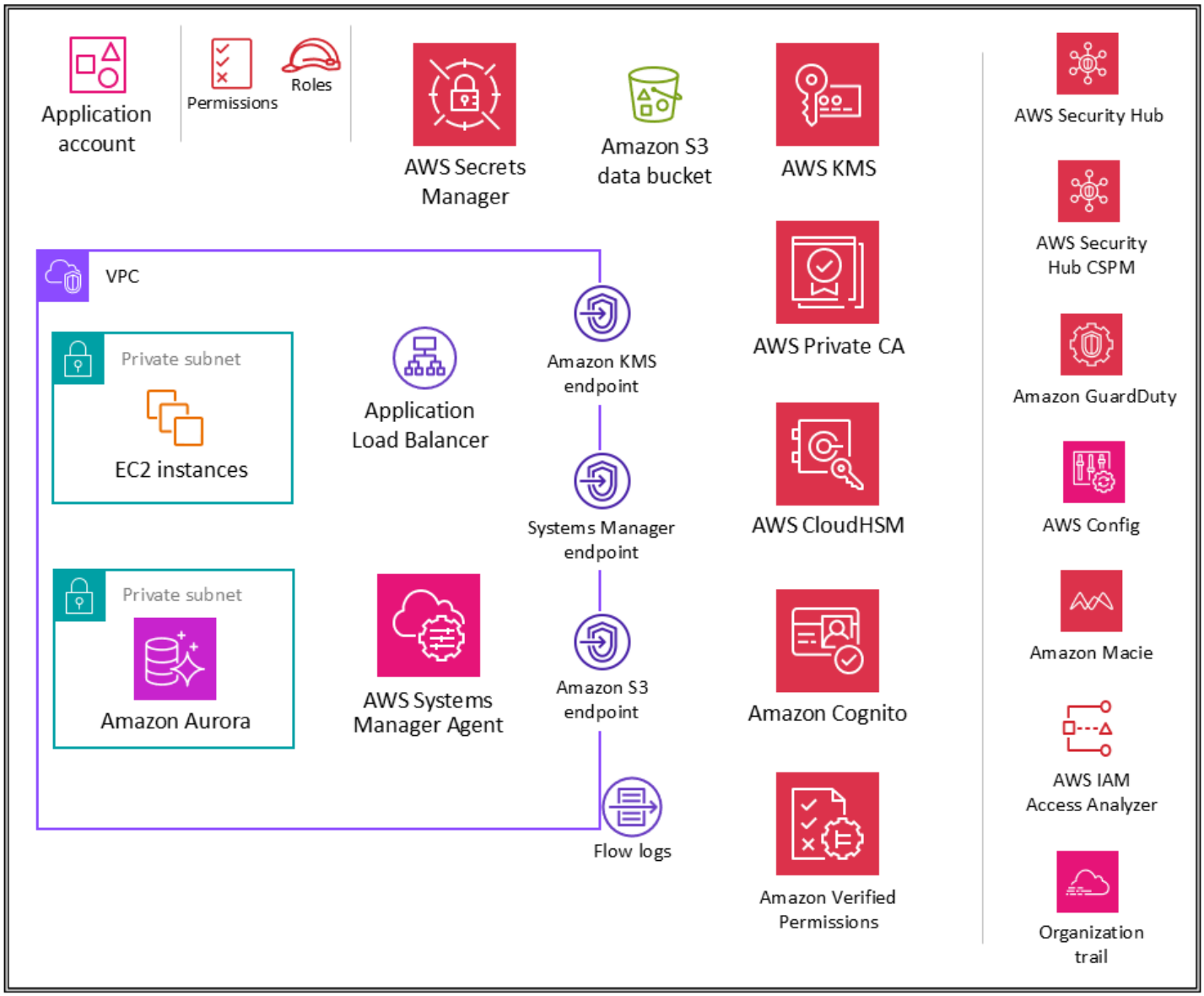
- Wenn Sie beschließen, die IAM Identity Center-Identitätsquelle von einer anderen Quelle auf Active Directory zu ändern oder sie von Active Directory auf eine andere Quelle zu ändern, muss sich das Verzeichnis in dem delegierten IAM Identity Center-Administrator-Mitgliedskonto befinden (diesem gehören), sofern eines vorhanden ist. Andernfalls muss es sich im Verwaltungskonto befinden.

- Sie können Ihre AWS Managed Microsoft AD innerhalb einer dedizierten VPC in einem anderen Konto hosten und dann AWS Resource Access Manager (AWS RAM) verwenden, um Subnetze von diesem anderen Konto für das delegierte Administratorkonto freizugeben. Auf diese Weise wird die AWS Managed Microsoft AD Instanz über das delegierte Administratorkonto gesteuert, aber aus Netzwerksicht verhält sie sich so, als ob sie in der VPC eines anderen Kontos bereitgestellt wäre. Dies ist hilfreich, wenn Sie über mehrere AWS Managed Microsoft AD Instances verfügen und diese lokal dort bereitstellen möchten, wo Ihr Workload ausgeführt wird, sie aber zentral über ein Konto verwalten möchten.
- Wenn Sie über ein eigenes Identitätsteam verfügen, das regelmäßig Aktivitäten zur Identitäts- und Zugriffsverwaltung durchführt, oder wenn Sie strenge Sicherheitsanforderungen haben, um Identitätsverwaltungsfunktionen von anderen Shared Services-Funktionen zu trennen, können Sie ein eigenes AWS-Konto Identitätsmanagement einrichten. In diesem Szenario bestimmen Sie dieses Konto als Ihren delegierten Administrator für IAM Identity Center, und es hostet auch Ihr Verzeichnis. AWS Managed Microsoft AD Sie können das gleiche Maß an logischer Isolierung zwischen Ihren Identity-Management-Workloads und anderen Shared Services-Workloads erreichen, indem Sie innerhalb eines einzigen Shared Service-Kontos detaillierte IAM-Berechtigungen verwenden.
- IAM Identity Center bietet derzeit keinen Support für mehrere Regionen. (Um IAM Identity Center in einer anderen Region zu aktivieren, müssen Sie zuerst Ihre aktuelle IAM Identity Center-Konfiguration löschen.) Darüber hinaus unterstützt es nicht die Verwendung verschiedener Identitätsquellen für verschiedene Gruppen von Konten und ermöglicht es Ihnen auch nicht, die Rechteverwaltung an verschiedene Teile Ihres Unternehmens (d. h. an mehrere delegierte Administratoren) oder an verschiedene Administratorgruppen zu delegieren. Wenn Sie eine dieser Funktionen benötigen, können Sie den IAM-Verbund verwenden, um Ihre Benutzeridentitäten innerhalb eines Identitätsanbieters (IdP) außerhalb von zu verwalten AWS und diesen externen Benutzeridentitäten die Erlaubnis zu erteilen, AWS Ressourcen in Ihrem Konto zu verwenden. IAM-Unterstützungen IdPs , die mit OpenID Connect (OIDC) oder SAML 2.0 kompatibel sind. Es hat sich bewährt, den SAML 2.0-Verbund mit externen Identitätsanbietern wie Active Directory Federation Service (AD FS), Okta, Azure Active Directory (Azure AD) oder Ping Identity zu verwenden, um Benutzern die Möglichkeit zu bieten, sich bei API-Vorgängen anzumelden oder diese aufzurufen. AWS-Managementkonsole AWS Weitere Informationen zum IAM-Verbund und zu Identitätsanbietern finden Sie in der IAM-Dokumentation unter Über den SAML 2.0-basierten Verbund.

Workloads OU — Anwendungskonto

Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

Das folgende Diagramm zeigt die AWS Sicherheitsdienste, die im Anwendungskonto konfiguriert sind (zusammen mit der Anwendung selbst).



Das Anwendungskonto hostet die primäre Infrastruktur und die Dienste für die Ausführung und Wartung einer Unternehmensanwendung. Das Anwendungskonto und die Organisationseinheit

Workloads dienen einigen primären Sicherheitszielen. Zunächst erstellen Sie für jede Anwendung ein separates Konto, um Grenzen und Kontrollen zwischen Workloads bereitzustellen und so Probleme mit der Vermischung von Rollen, Berechtigungen, Daten und Verschlüsselungsschlüsseln zu vermeiden. Sie möchten einen separaten Kontencontainer bereitstellen, in dem dem Anwendungsteam umfassende Rechte zur Verwaltung seiner eigenen Infrastruktur eingeräumt werden können, ohne andere zu beeinträchtigen. Als Nächstes fügen Sie eine Schutzebene hinzu, indem Sie dem Sicherheitsteam einen Mechanismus zur Überwachung und Erfassung von Sicherheitsdaten bereitstellen. Verwenden Sie einen Organisationsplan und lokale Bereitstellungen von Kontosicherheitsdiensten (Amazon GuardDuty, AWS Config, AWS Security Hub CSPM, Amazon EventBridge, IAM Access Analyzer), die vom Sicherheitsteam konfiguriert und überwacht werden. Schließlich ermöglichen Sie es Ihrem Unternehmen, Kontrollen zentral festzulegen. Sie passen das Anwendungskonto an die umfassendere Sicherheitsstruktur an, indem Sie es zu einem Mitglied der Workloads-Organisationseinheit machen, über die es die entsprechenden Serviceberechtigungen, Einschränkungen und Schutzmaßnahmen erbt.

Designüberlegung

In Ihrer Organisation haben Sie wahrscheinlich mehr als eine Geschäftsanwendung. Die Workloads OU ist für die Unterbringung der meisten Ihrer geschäftsspezifischen Workloads vorgesehen, einschließlich Produktions- und Nichtproduktionsumgebungen. Bei diesen Workloads kann es sich um eine Mischung aus kommerziellen off-the-shelf (COTS) Anwendungen und Ihren eigenen, intern entwickelten kundenspezifischen Anwendungen und Datendiensten handeln. Es gibt nur wenige Muster für die Organisation verschiedener Geschäftsanwendungen zusammen mit ihren Entwicklungsumgebungen. Ein Muster besteht darin, auf der OUs Grundlage Ihrer Entwicklungsumgebung mehrere untergeordnete Elemente zu haben, z. B. Produktion, Staging, Test und Entwicklung, und separate untergeordnete Elemente AWS-Konten unter denen zu verwenden OUs , die sich auf verschiedene Anwendungen beziehen. Ein weiteres gängiges Muster besteht darin, für jede Anwendung separate untergeordnete OUs Elemente zu verwenden und dann separate untergeordnete Elemente AWS-Konten für einzelne Entwicklungsumgebungen zu verwenden. Die genaue Organisationseinheit und Kontostruktur hängt von Ihrem Anwendungsdesign und den Teams ab, die diese Anwendungen verwalten. Denken Sie darüber nach, welche Sicherheitskontrollen Sie durchsetzen möchten, unabhängig davon, ob sie umgebungs- oder anwendungsspezifisch sind, da es einfacher ist, diese Kontrollen sofort zu implementieren. SCPs OUs Weitere Überlegungen zur auslastungsorientierten Organisation finden Sie OUs

im OUs Abschnitt „Anwendungen“ des AWS Whitepapers Organizing your environment using multiple accounts. AWS

Anwendung VPC

Die Virtual Private Cloud (VPC) im Anwendungskonto benötigt sowohl eingehenden Zugriff (für die einfachen Webdienste, die Sie modellieren) als auch ausgehenden Zugriff (für Anwendungsanforderungen oder AWS-Service -bedürfnisse). Standardmäßig sind Ressourcen innerhalb einer VPC untereinander routbar. Es gibt zwei private Subnetze: eines zum Hosten der EC2 Instances (Anwendungsschicht) und das andere für Amazon Aurora (Datenbankschicht). Die Netzwerksegmentierung zwischen verschiedenen Ebenen, z. B. der Anwendungs- und Datenbankebene, erfolgt über VPC-Sicherheitsgruppen, die den Datenverkehr auf Instanzebene einschränken. Aus Gründen der Ausfallsicherheit erstreckt sich der Workload über zwei oder mehr Availability Zones und verwendet zwei Subnetze pro Zone.

Designüberlegung

Sie können Traffic Mirroring verwenden, um Netzwerkdatenverkehr von einer elastic network interface von EC2 Instances zu kopieren. Anschließend können Sie den Datenverkehr zur Inhaltsinspektion, Bedrohungsüberwachung oder Fehlerbehebung an out-of-band Sicherheits- und Monitoring-Appliances weiterleiten. Möglicherweise möchten Sie beispielsweise den Traffic überwachen, der Ihre VPC verlässt, oder den Traffic, dessen Quelle sich außerhalb Ihrer VPC befindet. In diesem Fall spiegeln Sie den gesamten Datenverkehr mit Ausnahme des Datenverkehrs, der innerhalb Ihrer VPC fließt, und senden ihn an eine einzige Monitoring-Appliance. Amazon VPC-Flow-Logs erfassen keinen gespiegelten Datenverkehr; sie erfassen im Allgemeinen nur Informationen aus Paket-Headern. Traffic Mirroring bietet tiefere Einblicke in den Netzwerkverkehr, indem es Ihnen ermöglicht, den tatsächlichen Datenverkehrsinhalt, einschließlich der Nutzlast, zu analysieren. Aktivieren Sie Traffic Mirroring nur für die elastic network interface von EC2 Instances, die möglicherweise als Teil sensibler Workloads betrieben werden oder für die Sie im Falle eines Problems voraussichtlich detaillierte Diagnosen benötigen.

VPC-Endpunkte

VPC-Endpunkte bieten eine weitere Ebene der Sicherheitskontrolle sowie Skalierbarkeit und Zuverlässigkeit. Verwenden Sie diese, um Ihre Anwendungs-VPC mit anderen AWS-Services zu verbinden. (Im Anwendungskonto verwendet die AWS SRA VPC-Endpunkte für AWS KMS AWS Systems Manager, und Amazon S3.) Endpunkte sind virtuelle Geräte. Es handelt sich bei ihnen um horizontal skalierte, redundante und hochverfügbare VPC-Komponenten. Sie ermöglichen die Kommunikation zwischen Instances in Ihrer VPC und Services ohne Verfügbarkeitsrisiken oder Bandbreitenbeschränkungen für den Netzwerkverkehr. Sie können einen VPC-Endpunkt verwenden, um Ihre VPC privat mit unterstützten AWS-Services und VPC-Endpunktdiensten zu verbinden, die bereitgestellt werden, AWS PrivateLink ohne dass ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine Verbindung erforderlich ist. AWS Direct Connect Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit anderen AWS-Services zu kommunizieren. Der Verkehr zwischen Ihrer VPC und der anderen AWS-Service verlässt das Amazon-Netzwerk nicht.

Ein weiterer Vorteil der Verwendung von VPC-Endpunkten besteht darin, die Konfiguration von Endpunktrichtlinien zu ermöglichen. Eine VPC-Endpunktrichtlinie ist eine IAM-Ressourcenrichtlinie, die Sie einem Endpunkt beim Erstellen oder Ändern des Endpunkts zuordnen. Wenn Sie bei der Erstellung eines Endpunkts keine IAM-Richtlinie AWS anhängen, wird eine Standard-IAM-Richtlinie für Sie angehängt, die vollen Zugriff auf den Service ermöglicht. IAM-Benutzerrichtlinien oder servicespezifische Richtlinien (wie S3-Bucket-Richtlinien) werden durch Endpunktrichtlinien nicht überschrieben. Es handelt sich um eine separate IAM-Richtlinie zur Steuerung des Zugriffs vom Endpunkt auf den angegebenen Dienst. Auf diese Weise wird eine weitere Kontrollebene hinzugefügt, über die AWS Prinzipale mit Ressourcen oder Diensten kommunizieren können.

Amazon EC2

Die EC2Amazon-Instances, aus denen unsere Anwendung besteht, verwenden Version 2 des Instance Metadata Service (IMDSv2). IMDSv2 fügt Schutzmaßnahmen für vier Arten von Sicherheitslücken hinzu, die für den Zugriff auf das IMDS genutzt werden könnten: Firewalls für Website-Anwendungen, offene Reverse-Proxys, Sicherheitslücken bei serverseitiger Anforderungsfälschung (SSRF), offene Layer-3-Firewalls und. NATs Weitere Informationen finden Sie im Blogbeitrag Erweiterter Schutz vor offenen Firewalls, Reverse-Proxys und SSRF-Schwachstellen mit Verbesserungen am Instanz-Metadatendienst. EC2

Verwenden Sie separate VPCs (als Untergruppe der Kontogrenzen), um die Infrastruktur nach Workload-Segmenten zu isolieren. Verwenden Sie Subnetze, um Ihre Anwendungsschichten (z. B. Web, Anwendung und Datenbank) innerhalb einer einzelnen VPC zu isolieren. Verwenden Sie für

Ihre Instances private Subnetze, wenn Sie nicht direkt aus dem Internet erreichbar sein sollen. Um die EC2 Amazon-API von Ihrem privaten Subnetz aus aufzurufen, ohne ein Internet-Gateway zu verwenden, verwenden Sie AWS PrivateLink. Beschränken Sie den Zugriff auf Ihre Instances mithilfe von Sicherheitsgruppen. Verwenden Sie VPC Flow Logs, um den Traffic zu überwachen, der Ihre Instances erreicht. Verwenden Sie Session Manager, eine Funktion von AWS Systems Manager, um remote auf Ihre Instances zuzugreifen, anstatt eingehende SSH-Ports zu öffnen und SSH-Schlüssel zu verwalten. Verwenden Sie separate Amazon Elastic Block Store (Amazon EBS) -Volumes für das Betriebssystem und Ihre Daten. Sie können Ihr System so konfigurieren AWS-Konto, dass die Verschlüsselung der neuen EBS-Volumes und Snapshot-Kopien, die Sie erstellen, erzwungen wird.

> **Beispiel für eine Implementierung**
>
> Die AWS SRA-Codebibliothek bietet eine Beispielimplementierung der standardmäßigen Amazon EBS-Verschlüsselung in Amazon. EC2 Es zeigt, wie Sie die standardmäßige Amazon EBS-Verschlüsselung auf Kontoebene in jedem Unternehmen AWS-Konto und AWS-Region in der Organisation aktivieren können. AWS

AWS Nitro-Enklaven

AWS Nitro Enclaves ist eine EC2 Amazon-Funktion, mit der Sie isolierte Ausführungsumgebungen, sogenannte Enklaven, aus Instances erstellen können. EC2 Enklaven sind separate, gehärtete und stark eingeschränkte virtuelle Maschinen. Die CPU und der Speicher einer einzelnen übergeordneten EC2 Instance sind in isolierte Enklaven partitioniert. In jeder Enklave wird ein unabhängiger Kernel ausgeführt. Enklaven bieten nur sichere lokale Socket-Konnektivität mit ihrer übergeordneten Instanz. Sie verfügen über keinen persistenten Speicher, keinen interaktiven Zugriff oder kein externes Netzwerk. Benutzer können keine SSH-Verbindung zu einer Enklave herstellen, und die Prozesse, Anwendungen oder Benutzer (Root oder Administrator) der übergeordneten Instanz können nicht auf die Daten und Anwendungen in der Enklave zugreifen. Sie können Ihre sensibelsten Daten wie personenbezogene Daten (PII), Daten aus dem Gesundheitswesen, Finanzen und geistigem Eigentum innerhalb von Instanzen schützen. EC2 Nitro Enclaves ermöglicht es Ihnen, sich auf Ihre Anwendung zu konzentrieren, anstatt sich Gedanken über die Integration mit externen Diensten zu machen. Nitro Enclaves beinhaltet eine kryptografische Bescheinigung für Ihre Software, sodass Sie sicher sein können, dass nur autorisierter Code ausgeführt wird, sowie eine Integration mit der, AWS KMS sodass nur Ihre Enklaven auf vertrauliches Material zugreifen können. Dies trägt dazu bei, die Angriffsfläche für Ihre sensibelsten Datenverarbeitungsanwendungen zu reduzieren. Für die Verwendung von Nitro Enclaves fallen keine zusätzlichen Kosten an.

Die kryptografische Bescheinigung ist ein Verfahren, mit dem die Identität einer Enklave nachgewiesen wird. Der Bescheinigungsprozess wird über den Nitro Hypervisor durchgeführt, der ein unterschriebenes Bestätigungsdokument für die Enklave erstellt, um ihre Identität gegenüber einer anderen dritten Partei oder einem anderen Dienst nachzuweisen. Die Bescheinigungsdokumente enthalten wichtige Informationen über die Enklave, wie z. B. den öffentlichen Schlüssel der Enklave, Hashes des Enklave-Images und der Anwendungen und mehr.

Mit AWS Certificate Manager (ACM) für Nitro Enclaves können Sie öffentliche und private Zertifikate verwenden. SSL/TLS certificates with your web applications and web servers running on EC2 instances with Nitro Enclaves. SSL/TLS certificates are used to secure network communications and to establish the identity of websites over the internet and resources on private networks. ACM for Nitro Enclaves removes the time-consuming and error-prone manual process of purchasing, uploading, and renewing SSL/TLS ACM for Nitro Enclaves erstellt sichere private Schlüssel, verteilt das Zertifikat und seinen privaten Schlüssel an Ihre Enklave und verwaltet die Erneuerung von Zertifikaten. Mit ACM for Nitro Enclaves bleibt der private Schlüssel des Zertifikats in der Enklave isoliert, sodass die Instanz und ihre Benutzer nicht darauf zugreifen können. Weitere Informationen finden Sie unter AWS Certificate Manager Nitro Enclaves in der Nitro Enclaves-Dokumentation.

Application Load Balancer

Application Load Balancer verteilen den eingehenden Anwendungsdatenverkehr auf mehrere Ziele, z. B. EC2 Instances, in mehreren Availability Zones. In der AWS SRA sind die Anwendungsinstanzen die Zielgruppe für den Load Balancer. EC2 Die AWS SRA verwendet HTTPS-Listener, um sicherzustellen, dass der Kommunikationskanal verschlüsselt ist. Der Application Load Balancer verwendet ein Serverzertifikat, um die Front-End-Verbindung zu beenden und anschließend Anfragen von Clients zu entschlüsseln, bevor sie an die Ziele gesendet werden.

AWS Certificate Manager (ACM) ist nativ in Application Load Balancers integriert, und der AWS SRA verwendet ACM, um die erforderlichen öffentlichen X.509-Zertifikate (TLS-Server) zu generieren und zu verwalten. Sie können TLS 1.2 und starke Verschlüsselungen für Front-End-Verbindungen mithilfe der Application Load Balancer Balancer-Sicherheitsrichtlinie erzwingen. Weitere Informationen finden Sie im Elastic Load Balancing-Benutzerhandbuch.

Designüberlegungen

- Für allgemeine Szenarien, wie z. B. rein interne Anwendungen, die ein privates TLS-Zertifikat auf dem Application Load Balancer benötigen, können Sie ACM innerhalb dieses Kontos verwenden, um daraus ein privates Zertifikat zu generieren. AWS Private CAIn

der AWS SRA wird die private ACM-Stammzertifizierungsstelle im Security Tooling-Konto gehostet und kann, wie weiter oben im Abschnitt Security Tooling-Konto beschrieben, mit der gesamten AWS Organisation oder mit speziell AWS-Konten ausgestellten Endzertifikaten gemeinsam genutzt werden.

- Bei öffentlichen Zertifikaten können Sie ACM verwenden, um diese Zertifikate zu generieren und zu verwalten, einschließlich automatisierter Rotation. Alternativ können Sie Ihre eigenen Zertifikate generieren, indem Sie SSL/TLS Tools verwenden, um eine Certificate Signing Request (CSR) zu erstellen, die CSR von einer Zertifizierungsstelle (CA) signieren zu lassen, um ein Zertifikat zu erstellen, und dann das Zertifikat in ACM importieren oder das Zertifikat zur Verwendung mit dem Application Load Balancer in IAM hochladen. Wenn Sie ein Zertifikat in ACM importieren, müssen Sie das Ablaufdatum des Zertifikats überwachen und es verlängern, bevor es abläuft.
- Für zusätzliche Schutzebenen können Sie AWS WAF Richtlinien zum Schutz des Application Load Balancer bereitstellen. Edge-Richtlinien, Anwendungsrichtlinien und sogar private oder interne Ebenen zur Durchsetzung von Richtlinien erhöhen die Sichtbarkeit von Kommunikationsanfragen und sorgen für eine einheitliche Durchsetzung von Richtlinien. Weitere Informationen finden Sie im Blogbeitrag Deploying Defense in depth using Von AWS verwaltete Regeln for AWS WAF.

AWS Private CA

AWS Private Certificate Authority(AWS Private CA) wird im Anwendungskonto verwendet, um private Zertifikate zu generieren, die mit einem Application Load Balancer verwendet werden können. Es ist ein übliches Szenario, dass Application Load Balancers sichere Inhalte über TLS bereitstellen. Dazu müssen TLS-Zertifikate auf dem Application Load Balancer installiert sein. Für rein interne Anwendungen können private TLS-Zertifikate den sicheren Kanal bereitstellen.

In der AWS SRA AWS Private CA wird es im Security Tooling-Konto gehostet und über das Anwendungskonto gemeinsam genutzt. AWS RAM Auf diese Weise können Entwickler in einem Anwendungskonto ein Zertifikat von einer gemeinsamen privaten Zertifizierungsstelle anfordern. Durch die gemeinsame Nutzung CAs innerhalb Ihrer Organisation oder zwischen verschiedenen AWS-Konten Bereichen können Sie die Kosten und die Komplexität der Erstellung und Verwaltung von Duplikaten CAs in allen Ihren Systemen reduzieren AWS-Konten. Wenn Sie ACM verwenden, um private Zertifikate von einer gemeinsamen Zertifizierungsstelle auszustellen, wird das Zertifikat lokal im anfragenden Konto generiert, und ACM bietet die vollständige Lebenszyklusverwaltung und Verlängerung.

Amazon Inspector

Die AWS SRA verwendet Amazon Inspector, um EC2 Instances und Container-Images, die sich in der Amazon Elastic Container Registry (Amazon ECR) befinden, automatisch zu erkennen und auf Softwareschwachstellen und unbeabsichtigte Netzwerkbedrohungen hin zu scannen.

Amazon Inspector wird dem Anwendungskonto zugeordnet, da es Schwachstellen-Management-Services für EC2 Instances in diesem Konto bereitstellt. Darüber hinaus meldet Amazon Inspector unerwünschte Netzwerkpfade zu und von EC2 Instances.

Amazon Inspector in Mitgliedskonten wird zentral vom delegierten Administratorkonto verwaltet. In der AWS SRA ist das Security Tooling-Konto das delegierte Administratorkonto. Das delegierte Administratorkonto kann Ergebnisdaten und bestimmte Einstellungen für Mitglieder der Organisation verwalten. Dazu gehören das Anzeigen aggregierter Ergebnisdetails für alle Mitgliedskonten, das Aktivieren oder Deaktivieren von Scans für Mitgliedskonten und das Überprüfen gescannter Ressourcen innerhalb der Organisation. AWS

> **Designüberlegung**
>
> Sie können Patch Manager, eine Funktion von, verwenden, um On-Demand-Patches auszulösen AWS Systems Manager, um Zero-Day-Schwachstellen oder andere kritische Sicherheitslücken in Amazon Inspector zu beheben. Patch Manager hilft Ihnen dabei, diese Sicherheitslücken zu patchen, ohne auf Ihren normalen Patching-Zeitplan warten zu müssen. Die Behebung erfolgt mithilfe des Systems Manager Automation-Runbooks. Weitere Informationen finden Sie in der zweiteiligen Blogserie Automatisieren Sie das Schwachstellenmanagement und die Behebung von Sicherheitslücken AWS mithilfe von Amazon Inspector und. AWS Systems Manager

AWS Systems Manager

AWS Systems Managerist ein Programm AWS-Service , das Sie verwenden können, um Betriebsdaten aus mehreren Ressourcen einzusehen AWS-Services und betriebliche Aufgaben zu automatisieren. AWS Mit automatisierten Genehmigungsworkflows und Runbooks können Sie daran arbeiten, menschliche Fehler zu reduzieren und Wartungs- und Bereitstellungsaufgaben für AWS Ressourcen zu vereinfachen.

Zusätzlich zu diesen allgemeinen Automatisierungsfunktionen unterstützt Systems Manager eine Reihe von präventiven, detektiven und reaktionsschnellen Sicherheitsfunktionen. AWS Systems

Manager Agent (SSM Agent) ist Amazon-Software, die auf einer EC2 Instanz, einem lokalen Server oder einer virtuellen Maschine (VM) installiert und konfiguriert werden kann. SSM Agent ermöglicht es Systems Manager, diese Ressourcen zu aktualisieren, zu verwalten und zu konfigurieren. Systems Manager unterstützt Sie bei der Aufrechterhaltung von Sicherheit und Compliance, indem es diese verwalteten Instanzen scannt und alle Verstöße, die er in Ihren Patch-, Konfiguration- und benutzerdefinierten Richtlinien entdeckt, meldet (oder Korrekturmaßnahmen ergreift).

Die AWS SRA verwendet Session Manager, eine Funktion von Systems Manager, um ein interaktives, browserbasiertes Shell- und CLI-Erlebnis bereitzustellen. Dies ermöglicht eine sichere und überprüfbare Instanzverwaltung, ohne dass eingehende Ports geöffnet, Bastion-Hosts verwaltet oder SSH-Schlüssel verwaltet werden müssen. Die AWS SRA verwendet Patch Manager, eine Funktion von Systems Manager, um Patches auf EC2 Instanzen für Betriebssysteme und Anwendungen anzuwenden.

Die AWS SRA nutzt auch Automation, eine Funktion von Systems Manager, um allgemeine Wartungs- und Bereitstellungsaufgaben von EC2 Amazon-Instances und anderen AWS Ressourcen zu vereinfachen. Automatisierung kann übliche IT-Aufgaben vereinfachen, wie z. B. das Ändern des Zustands einer oder mehrerer Knoten (mithilfe einer Genehmigungs-Automatisierung) oder die Verwaltung von Knoten-Status gemäß einem Zeitplan. Systems Manager umfasst Funktionen, mit deren Hilfe Sie große Gruppen von Instances mithilfe von Tags und Geschwindigkeitskontrollen anvisieren können, um Änderungen entsprechend den von Ihnen festgelegten Grenzwerten durchzuführen. Automation bietet Automatisierungen mit einem Klick zur Vereinfachung komplexer Aufgaben wie der Erstellung goldener Amazon Machine Images (AMIs) und der Wiederherstellung nicht erreichbarer Instances. EC2 Darüber hinaus können Sie die Betriebssicherheit verbessern, indem Sie IAM-Rollen Zugriff auf bestimmte Runbooks gewähren, um bestimmte Funktionen auszuführen, ohne diesen Rollen direkt Berechtigungen zu erteilen. Wenn Sie beispielsweise möchten, dass eine IAM-Rolle berechtigt ist, bestimmte EC2 Instanzen nach Patch-Updates neu zu starten, Sie die Berechtigung aber nicht direkt dieser Rolle erteilen möchten, können Sie stattdessen ein Automatisierungs-Runbook erstellen und der Rolle die Berechtigungen erteilen, nur das Runbook auszuführen.

Designüberlegungen

- Systems Manager ist auf EC2 Instanzmetadaten angewiesen, um korrekt zu funktionieren. Systems Manager kann mithilfe von Version 1 oder Version 2 des Instanz-Metadatendienstes (IMDSv1 und IMDSv2) auf Instanzmetadaten zugreifen.

- Der SSM-Agent muss mit verschiedenen AWS-Services Ressourcen wie Amazon EC2 Messages, Systems Manager und Amazon S3 kommunizieren. Damit diese Kommunikation stattfinden kann, benötigt das Subnetz entweder eine ausgehende Internetverbindung oder die Bereitstellung geeigneter VPC-Endpunkte. Die AWS SRA verwendet VPC-Endpunkte für den SSM-Agent, um private Netzwerkpfade zu verschiedenen einzurichten. AWS-Services
- Automation lässt Sie bewährte Methoden mit Ihrer restlichen Organisation teilen. Sie können bewährte Methoden für die Ressourcenverwaltung in Runbooks erstellen und die Runbooks gruppenübergreifend gemeinsam nutzen. AWS-Regionen Sie können auch die zulässigen Werte für Runbook-Parameter einschränken. Für diese Anwendungsfälle müssen Sie möglicherweise Automatisierungs-Runbooks in einem zentralen Konto wie Security Tooling oder Shared Services erstellen und sie für den Rest der Organisation freigeben. AWS Zu den häufigsten Anwendungsfällen gehören die Möglichkeit, Patches und Sicherheitsupdates zentral zu implementieren, Abweichungen bei VPC-Konfigurationen oder S3-Bucket-Richtlinien zu beheben und EC2 Instances skalierbar zu verwalten. Einzelheiten zur Implementierung finden Sie in der Systems Manager Manager-Dokumentation.

Amazon Aurora

In der AWS SRA bilden Amazon Aurora und Amazon S3 die logische Datenschicht. Aurora ist eine vollständig verwaltete, mit MySQL und PostgreSQL kompatible relationale Datenbank-Engine. Eine Anwendung, die auf den EC2 Instances ausgeführt wird, kommuniziert bei Bedarf mit Aurora und Amazon S3. Aurora ist mit einem Datenbank-Cluster innerhalb einer DB-Subnetzgruppe konfiguriert.

Designüberlegung

Wie bei vielen Datenbankdiensten wird die Sicherheit für Aurora auf drei Ebenen verwaltet. Um zu kontrollieren, wer Amazon Relational Database Service (Amazon RDS) - Managementaktionen auf Aurora-DB-Clustern und DB-Instances ausführen kann, verwenden Sie IAM. Um zu steuern, welche Geräte und EC2 Instances Verbindungen zum Cluster-Endpunkt und Port der DB-Instance für Aurora-DB-Cluster in einer VPC öffnen können, verwenden Sie eine VPC-Sicherheitsgruppe. Um Anmeldungen und Berechtigungen für einen Aurora-DB-Cluster zu authentifizieren, können Sie den gleichen Ansatz wie bei einer eigenständigen DB-Instance von MySQL oder PostgreSQL verwenden, oder Sie können die IAM-Datenbankauthentifizierung für Aurora MySQL-Compatible Edition verwenden. Bei

letzterem Ansatz authentifizieren Sie sich bei Ihrem Aurora MySQL-kompatiblen DB-Cluster mithilfe einer IAM-Rolle und eines Authentifizierungstoken.

Amazon S3

Amazon S3 ist ein Objektspeicherservice, der branchenführende Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet. Es ist das Datenrückgrat vieler darauf basierender Anwendungen AWS, und angemessene Berechtigungen und Sicherheitskontrollen sind für den Schutz sensibler Daten von entscheidender Bedeutung. Empfohlene bewährte Sicherheitsmethoden für Amazon S3 finden Sie in der Dokumentation, in Online-Technikgesprächen und in ausführlicheren Informationen in Blogbeiträgen. Die wichtigste bewährte Methode besteht darin, übermäßig freizügigen Zugriff (insbesondere öffentlichen Zugriff) auf S3-Buckets zu blockieren.

AWS KMS

Die AWS SRA veranschaulicht das empfohlene Verteilungsmodell für die Schlüsselverwaltung, bei dem sich die zu AWS KMS key verschlüsselnde Ressource innerhalb derselben Ressource AWS-Konto befindet. Aus diesem Grund AWS KMS wird es im Anwendungskonto verwendet und ist zusätzlich zum Security Tooling-Konto enthalten. AWS KMS Wird im Anwendungskonto zur Verwaltung von Schlüsseln verwendet, die für die Anwendungsressourcen spezifisch sind. Sie können eine Aufgabentrennung implementieren, indem Sie mithilfe von Schlüsselrichtlinien lokalen Anwendungsrollen Schlüsselverwendungsberechtigungen erteilen und die Verwaltungs- und Überwachungsberechtigungen auf Ihre wichtigsten Verwalter beschränken.

Designüberlegung

In einem verteilten Modell liegt die Verantwortung für die AWS KMS Schlüsselverwaltung beim Anwendungsteam. Ihr zentrales Sicherheitsteam kann jedoch für die Steuerung und Überwachung wichtiger kryptografischer Ereignisse wie der folgenden verantwortlich sein:

- Das importierte Schlüsselmaterial in einem KMS-Schlüssel befindet kurz vor dem Ablaufdatum.
- Das Schlüsselmaterial in einem KMS-Schlüssel wurde automatisch rotiert.
- Der AKMS-Schlüssel wurde gelöscht.
- Es gibt eine hohe Rate an Entschlüsselungsfehlern.

AWS CloudHSM

AWS CloudHSMbietet verwaltete Hardware-Sicherheitsmodule (HSMs) in der AWS Cloud. Es ermöglicht Ihnen, Ihre eigenen Verschlüsselungsschlüssel mithilfe AWS von FIPS 140-2 Level 3 zu generieren und zu verwenden, auf HSMs die Sie den Zugriff kontrollieren. Sie können es verwenden AWS CloudHSM , um die SSL/TLS Verarbeitung für Ihre Webserver auszulagern. Dies reduziert die Belastung des Webservers und bietet zusätzliche Sicherheit, indem der private Schlüssel des Webservers gespeichert wird. AWS CloudHSM Sie könnten auch ein HSM AWS CloudHSM in der eingehenden VPC im Netzwerkkonto bereitstellen, um Ihre privaten Schlüssel zu speichern und Zertifikatsanfragen zu signieren, falls Sie als ausstellende Zertifizierungsstelle agieren müssen.

> **Designüberlegung**
>
> Wenn Sie eine strenge Anforderung für FIPS 140-2 Level 3 haben, können Sie auch festlegen, dass der AWS CloudHSM Cluster als benutzerdefinierter Schlüsselspeicher verwendet wird, anstatt den systemeigenen KMS-Schlüsselspeicher AWS KMS zu verwenden. Auf diese Weise profitieren Sie von der Integration zwischen Ihren Daten AWS KMS und AWS-Services der Verschlüsselung Ihrer Daten, während Sie gleichzeitig für den HSMs Schutz Ihrer KMS-Schlüssel verantwortlich sind. Dies kombiniert einen einzigen Mandanten HSMs unter Ihrer Kontrolle mit der Benutzerfreundlichkeit und Integration von. AWS KMS Um Ihre AWS CloudHSM Infrastruktur zu verwalten, müssen Sie eine Public-Key-Infrastruktur (PKI) einsetzen und über ein Team verfügen, das Erfahrung in der Verwaltung hat. HSMs

AWS Secrets Manager

AWS Secrets Managerhilft Ihnen dabei, die Anmeldeinformationen (Geheimnisse) zu schützen, die Sie für den Zugriff auf Ihre Anwendungen, Dienste und IT-Ressourcen benötigen. Mit diesem Service können Sie Datenbankanmeldedaten, API-Schlüssel und andere Geheimnisse während ihres gesamten Lebenszyklus effizient rotieren, verwalten und abrufen. Sie können hartcodierte Anmeldeinformationen in Ihrem Code durch einen API-Aufruf an Secrets Manager ersetzen, um das Geheimnis programmgesteuert abzurufen. Dadurch wird sichergestellt, dass das Geheimnis nicht von jemandem, der Ihren Code untersucht, kompromittiert werden kann, da das Geheimnis nicht mehr im Code enthalten ist. Darüber hinaus hilft Ihnen Secrets Manager dabei, Ihre Anwendungen zwischen Umgebungen (Entwicklung, Vorproduktion, Produktion) zu verschieben. Anstatt den Code zu ändern, können Sie sicherstellen, dass ein entsprechend benannter und referenzierter

Secret in der Umgebung verfügbar ist. Dies fördert die Konsistenz und Wiederverwendbarkeit des Anwendungscodes in verschiedenen Umgebungen und erfordert gleichzeitig weniger Änderungen und menschliche Interaktionen, nachdem der Code getestet wurde.

Mit Secrets Manager können Sie den Zugriff auf geheime Daten mithilfe detaillierter IAM-Richtlinien und ressourcenbasierter Richtlinien verwalten. Sie können zum Schutz von Geheimnissen beitragen, indem Sie sie mit Verschlüsselungsschlüsseln verschlüsseln, die Sie selbst verwenden. AWS KMS Secrets Manager lässt sich auch in AWS Protokollierungs- und Überwachungsdienste integrieren, um eine zentrale Prüfung zu ermöglichen.

Secrets Manager verwendet AWS KMS keys Umschlagverschlüsselung mit Datenschlüsseln, um jeden geheimen Wert zu schützen. Wenn Sie einen geheimen Schlüssel erstellen, können Sie einen beliebigen symmetrischen, vom Kunden verwalteten Schlüssel in der Region AWS-Konto und wählen, oder Sie können den AWS verwalteten Schlüssel für Secrets Manager verwenden.

Es hat sich bewährt, dass Sie Ihre Secrets überwachen können, um alle Änderungen daran zu protokollieren. Auf diese Weise können Sie sicherstellen, dass jede unerwartete Verwendung oder Änderung untersucht werden kann. Unerwünschte Änderungen können rückgängig gemacht werden. Secrets Manager unterstützt derzeit zwei AWS-Services , mit denen Sie Ihre Organisation und Aktivitäten überwachen können: AWS CloudTrail und AWS Config. CloudTrail erfasst alle API-Aufrufe für Secrets Manager als Ereignisse, einschließlich Aufrufe von der Secrets Manager-Konsole und von Codeaufrufen an den Secrets Manager APIs. CloudTrail Erfasst darüber hinaus andere verwandte (nicht API-bezogene) Ereignisse, die sich auf Ihre Sicherheit oder Konformität auswirken AWS-Konto oder Ihnen bei der Behebung betrieblicher Probleme helfen könnten. Dazu gehören Rotationsereignisse bei bestimmten Geheimnissen und das Löschen geheimer Versionen. AWS Config kann detektivische Kontrollen bereitstellen, indem Änderungen an Geheimnissen in Secrets Manager verfolgt und überwacht werden. Zu diesen Änderungen gehören die Beschreibung, die Rotationskonfiguration, die Tags und die Beziehung zu anderen AWS Quellen wie dem KMS-Verschlüsselungsschlüssel oder den AWS Lambda Funktionen, die für die geheime Rotation verwendet werden. Sie können Amazon EventBridge, das Benachrichtigungen über Konfiguration und Konformitätsänderungen von erhält, auch so konfigurieren AWS Config, dass bestimmte geheime Ereignisse für Benachrichtigungen oder Abhilfemaßnahmen weitergeleitet werden.

In der AWS SRA befindet sich Secrets Manager im Anwendungskonto, um lokale Anwendungsfälle zu unterstützen und Geheimnisse zu verwalten, die ihrer Verwendung nahe kommen. Hier wird ein Instanzprofil an die EC2 Instanzen im Anwendungskonto angehängt. Separate Secrets können dann in Secrets Manager konfiguriert werden, sodass das Instance-Profil geheime Daten abrufen kann, z. B. um der entsprechenden Active Directory- oder LDAP-Domäne beizutreten

und auf die Aurora-Datenbank zuzugreifen. Secrets Manager ist in Amazon RDS integriert, um Benutzeranmeldeinformationen zu verwalten, wenn Sie eine Amazon RDS-DB-Instance oder einen Multi-AZ-DB-Cluster erstellen, ändern oder wiederherstellen. Dies hilft Ihnen bei der Verwaltung der Erstellung und Rotation von Schlüsseln und ersetzt die hartcodierten Anmeldeinformationen in Ihrem Code durch programmatische API-Aufrufe an Secrets Manager.

> **Designüberlegung**
>
> Im Allgemeinen sollten Sie Secrets Manager in dem Konto konfigurieren und verwalten, das dem Ort, an dem die Secrets verwendet werden, am nächsten ist. Dieser Ansatz nutzt die lokalen Kenntnisse des Anwendungsfalls und bietet Anwendungsentwicklungsteams Geschwindigkeit und Flexibilität. Für streng kontrollierte Informationen, bei denen eine zusätzliche Kontrollebene angebracht sein könnte, können Geheimnisse zentral vom Secrets Manager im Security Tooling-Konto verwaltet werden.

Amazon Cognito

Mit Amazon Cognito können Sie Ihren Web- und mobilen Apps schnell und effizient Benutzerregistrierung, Anmeldung und Zugriffskontrolle hinzufügen. Amazon Cognito ist auf Millionen von Benutzern skalierbar und unterstützt die Anmeldung bei Anbietern sozialer Identitäten wie Apple, Facebook, Google und Amazon sowie bei Anbietern von Unternehmensidentitäten über SAML 2.0 und OpenID Connect. Die beiden Hauptkomponenten von Amazon Cognito sind Benutzerpools und Identitätspools. Benutzerpools sind Benutzerverzeichnisse, die Anmelde- und Anmeldeoptionen für Ihre Anwendungsbenutzer bieten. Mithilfe von Identitätspools können Sie Ihren Benutzern Zugriff auf andere gewähren. AWS-Services Sie können Identitäten-Pools und Benutzerpools getrennt oder zusammen verwenden. Allgemeine Nutzungsszenarien finden Sie in der Amazon Cognito Cognito-Dokumentation.

Amazon Cognito bietet eine integrierte und anpassbare Benutzeroberfläche für die Benutzerregistrierung und -anmeldung. Sie können Android, iOS und JavaScript SDKs Amazon Cognito verwenden, um Benutzerregistrierungs- und Anmeldeseiten zu Ihren Apps hinzuzufügen. Amazon Cognito Sync ist eine AWS-Service AND-Client-Bibliothek, die die geräteübergreifende Synchronisierung anwendungsbezogener Benutzerdaten ermöglicht.

Amazon Cognito unterstützt die Multi-Faktor-Authentifizierung und Verschlüsselung von Daten im Ruhezustand und Daten während der Übertragung. Amazon Cognito Cognito-Benutzerpools bieten erweiterte Sicherheitsfunktionen, um den Zugriff auf Benutzerkonten in Ihrer Anwendung zu schützen.

Diese erweiterten Sicherheitsfunktionen bieten eine risikobasierte adaptive Authentifizierung und Schutz vor der Verwendung kompromittierter Anmeldeinformationen.

Designüberlegungen

- Sie können eine AWS Lambda Funktion erstellen und diese Funktion dann bei Benutzerpoolvorgängen wie Benutzeranmeldung, Bestätigung und Anmeldung (Authentifizierung) mit einem Lambda-Trigger auslösen. Sie können Authentifizierungsaufforderungen hinzufügen, Benutzer migrieren und Verifizierungsnachrichten anpassen. Informationen zu allgemeinen Vorgängen und Benutzerabläufen finden Sie in der Amazon Cognito Cognito-Dokumentation. Amazon Cognito ruft Lambda-Funktionen synchron auf.
- Sie können Amazon Cognito Cognito-Benutzerpools verwenden, um kleine, mandantenfähige Anwendungen zu sichern. Ein häufiger Anwendungsfall für Multi-Tenant-Designs ist die Ausführung von Workloads, um das Testen mehrerer Versionen einer Anwendung zu unterstützen. Ein Design mit mehreren Mandanten ist auch nützlich, um eine einzelne Anwendung mit unterschiedlichen Datensätzen zu testen, was die volle Nutzung Ihrer Clusterressourcen ermöglicht. Stellen Sie jedoch sicher, dass die Anzahl der Mandanten und das erwartete Volumen mit den entsprechenden Amazon Cognito-Servicekontingenten übereinstimmen. Diese Kontingente werden für alle Mandanten in Ihrer Anwendung freigegeben.

Amazon Verified Permissions

Amazon Verified Permissions ist ein skalierbares Berechtigungsmanagement und ein detaillierter Autorisierungsservice für die von Ihnen erstellten Anwendungen. Entwickler und Administratoren können Cedar verwenden, eine speziell entwickelte und sicherheitsorientierte Open-Source-Richtliniensprache mit Rollen und Attributen, um detailliertere, kontextsensitive und richtlinienbasierte Zugriffskontrollen zu definieren. Entwickler können sicherere Anwendungen schneller erstellen, indem sie die Autorisierung externalisieren und die Richtlinienverwaltung und -verwaltung zentralisieren. Verified Permissions umfasst Schemadefinitionen, die Grammatik von Richtlinienerklärungen und automatische Argumentation, die sich auf Millionen von Berechtigungen erstrecken, sodass Sie die Prinzipien der Standardverweigerung und der geringsten Zugriffsrechte durchsetzen können. Der Service umfasst auch einen Evaluierungssimulator, mit dem Sie Ihre Autorisierungsentscheidungen und Autorenrichtlinien testen können. Diese Funktionen erleichtern die Implementierung eines detaillierten, detaillierten Autorisierungsmodells zur Unterstützung Ihrer Zero-Trust-Ziele. Verified

Permissions zentralisiert Berechtigungen in einem Richtlinienspeicher und hilft Entwicklern, diese Berechtigungen zu verwenden, um Benutzeraktionen in ihren Anwendungen zu autorisieren.

Sie können Ihre Anwendung über die API mit dem Dienst verbinden, um Benutzerzugriffsanfragen zu autorisieren. Für jede Autorisierungsanfrage ruft der Service die relevanten Richtlinien ab und bewertet diese Richtlinien, um anhand von Kontexteingaben wie Benutzern, Rollen, Gruppenmitgliedschaft und Attributen festzustellen, ob ein Benutzer eine Aktion an einer Ressource ausführen darf. Sie können verifizierte Berechtigungen konfigurieren und verbinden, an die Ihre Richtlinienverwaltungs- und Autorisierungsprotokolle gesendet werden sollen. AWS CloudTrail Wenn Sie Amazon Cognito als Identitätsspeicher verwenden, können Sie Verified Permissions integrieren und die ID- und Zugriffstoken verwenden, die Amazon Cognito bei den Autorisierungsentscheidungen in Ihren Anwendungen zurückgibt. Sie stellen Amazon Cognito Cognito-Token für Verified Permissions bereit. Verified Permissions verwendet die Attribute, die die Token enthalten, um den Principal darzustellen und die Rechte des Prinzipals zu identifizieren. Weitere Informationen zu dieser Integration finden Sie im AWS Blogbeitrag Vereinfachung der feinkörnigen Autorisierung mit Amazon Verified Permissions und Amazon Cognito.

Verified Permissions hilft Ihnen bei der Definition einer richtlinienbasierten Zugriffskontrolle (PBAC). PBAC ist ein Zugriffskontrollmodell, das mithilfe von Berechtigungen, die als Richtlinien ausgedrückt werden, bestimmt, wer auf welche Ressourcen in einer Anwendung zugreifen kann. PBAC vereint die rollenbasierte Zugriffskontrolle (RBAC) und die attributebasierte Zugriffskontrolle (ABAC), was zu einem leistungsfähigeren und flexibleren Zugriffskontrollmodell führt. Weitere Informationen über PBAC und darüber, wie Sie mithilfe von Verified Permissions ein Autorisierungsmodell entwerfen können, finden Sie im AWS Blogbeitrag Policy-based access control in application development with Amazon Verified Permissions.

In der AWS SRA befindet sich Verified Permissions im Anwendungskonto, um die Rechteverwaltung für Anwendungen durch die Integration mit Amazon Cognito zu unterstützen.

Mehrschichtiger Schutz

Das Anwendungskonto bietet die Möglichkeit, die Prinzipien der mehrschichtigen Verteidigung zu veranschaulichen, die dies AWS ermöglichen. Betrachten Sie die Sicherheit der EC2 Instanzen, die den Kern einer einfachen Beispielanwendung bilden, die in der AWS SRA dargestellt wird, und Sie können sehen, wie eine mehrschichtige Verteidigung AWS-Services zusammenarbeitet. Dieser Ansatz entspricht der strukturellen Sichtweise von AWS Sicherheitsdiensten, wie sie im Abschnitt Wenden Sie Sicherheitsdienste in Ihrem AWS Unternehmen weiter oben in diesem Handbuch beschrieben haben.

- Die innerste Schicht sind die EC2 Instanzen. Wie bereits erwähnt, enthalten EC2 Instances viele systemeigene Sicherheitsfunktionen, entweder standardmäßig oder als Optionen. Beispiele hierfür sind IMDSv2das Nitro-System und die Amazon EBS-Speicherverschlüsselung.
- Die zweite Schutzschicht konzentriert sich auf das Betriebssystem und die Software, die auf den EC2 Instances ausgeführt werden. Dienste wie Amazon Inspector AWS Systems Managerermöglichen es Ihnen, diese Konfigurationen zu überwachen, zu melden und Korrekturmaßnahmen zu ergreifen. Amazon Inspector überwacht Ihre Software auf Sicherheitslücken und Systems Manager unterstützt Sie bei der Aufrechterhaltung von Sicherheit und Compliance, indem verwaltete Instances auf ihren Patch - und Konfigurationsstatus überprüft und anschließend alle von Ihnen angegebenen Korrekturmaßnahmen gemeldet und ergriffen werden.
- Die Instances und die auf diesen Instances ausgeführte Software gehören zu Ihrer AWS Netzwerkinfrastruktur. Die AWS SRA nutzt nicht nur die Sicherheitsfunktionen von Amazon VPC, sondern nutzt auch VPC-Endpunkte, um private Konnektivität zwischen der VPC und dem Support AWS-Services bereitzustellen und um einen Mechanismus zur Platzierung von Zugriffsrichtlinien an der Netzwerkgrenze bereitzustellen.
- Die Aktivität und Konfiguration der EC2 Instances, Software-, Netzwerk- und IAM-Rollen und AWS-Konto-Ressourcen werden zusätzlich durch spezielle Services wie AWS Security Hub CSPM,, Amazon,, AWS Security Hub GuardDuty AWS CloudTrail AWS Config, IAM Access Analyzer und Amazon Macie überwacht.
- Darüber hinaus AWS RAM hilft Ihnen das Anwendungskonto dabei, zu kontrollieren, welche Ressourcen mit anderen Konten gemeinsam genutzt werden, und die Richtlinien zur IAM-Servicekontrolle helfen Ihnen dabei, einheitliche Berechtigungen im gesamten Unternehmen durchzusetzen. AWS

KI/ML für Sicherheit

Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

Künstliche Intelligenz und maschinelles Lernen (sind AI/ML) is transforming businesses. AI/ML seit über 20 Jahren ein Schwerpunkt von Amazon), und viele der Funktionen, die Kunden nutzen AWS, einschließlich Sicherheitsservices, basieren auf KI/ML. Dies schafft einen integrierten Mehrwert, da Sie sicher darauf aufbauen können, AWS ohne dass Ihre Sicherheits- oder Anwendungsentwicklungsteams über Fachkenntnisse in KI/ML verfügen müssen.

KI ist eine fortschrittliche Technologie, die es Maschinen und Systemen ermöglicht, Informationen zu entwickeln und Vorhersagen zu treffen. KI-Systeme lernen aus früheren Erfahrungen anhand von Daten, die sie nutzen oder anhand derer sie trainiert werden. ML ist einer der wichtigsten Aspekte der KI. ML ist die Fähigkeit von Computern, aus Daten zu lernen, ohne explizit programmiert zu werden. Bei der traditionellen Programmierung schreibt der Programmierer Regeln, die definieren, wie das Programm auf einem Computer oder einer Maschine funktionieren soll. In ML lernt das Modell die Regeln aus Daten. ML-Modelle können verborgene Muster in den Daten entdecken oder genaue Vorhersagen für neue Daten treffen, die beim Training nicht verwendet wurden. Vielfach AWS-Services einsetzbar AI/ML , um aus riesigen Datensätzen zu lernen und Sicherheitsrückschlüsse zu ziehen.

- Amazon Macie ist ein Datensicherheitsservice, der maschinelles Lernen und Musterabgleich verwendet, um Ihre sensiblen Daten zu erkennen und zu schützen. Macie erkennt automatisch eine große und ständig wachsende Liste sensibler Datentypen, darunter personenbezogene Daten (PII) wie Namen, Adressen und Finanzinformationen wie Kreditkartennummern. Außerdem erhalten Sie ständigen Einblick in Ihre Daten, die in Amazon Simple Storage Service (Amazon S3) gespeichert sind. Macie verwendet Natural Language Processing (NLP) und ML-Modelle, die anhand verschiedener Arten von Datensätzen trainiert wurden, um Ihre vorhandenen Daten zu verstehen und Geschäftswerte für die Priorisierung geschäftskritischer Daten zuzuweisen. Macie generiert dann Ergebnisse aus sensiblen Daten.
- Amazon GuardDuty ist ein Service zur Bedrohungserkennung, der ML, Anomalieerkennung und integrierte Bedrohungsinformationen verwendet, um kontinuierlich nach böswilligen Aktivitäten und unberechtigtem Verhalten zu suchen, um Ihre Instances AWS-Konten, serverlosen und Container-Workloads, Benutzer, Datenbanken und Speicher zu schützen. GuardDuty verwendet ML-

Techniken, die äußerst effektiv sind, um potenziell bösartige Benutzeraktivitäten von anomalem, aber harmlosem Betriebsverhalten innerhalb des Unternehmens zu unterscheiden. AWS-Konten Diese Funktion modelliert kontinuierlich API-Aufrufe innerhalb eines Kontos und berücksichtigt probabilistische Vorhersagen, um äußerst verdächtiges Benutzerverhalten genauer zu isolieren und Warnmeldungen zu erhalten. Dieser Ansatz hilft bei der Identifizierung bösartiger Aktivitäten im Zusammenhang mit bekannten Bedrohungstaktiken wie Entdeckung, Erstzugriff, Persistenz, Rechteerweiterung, Umgehung von Abwehrmaßnahmen, Zugriff auf Anmeldeinformationen, Auswirkung und Datenexfiltration. Weitere Informationen zur GuardDuty Verwendung von maschinellem Lernen finden Sie in der AWS re:INFORCE 2023 Breakout-Session Developing new findings using machine learning in Amazon GuardDuty (0). TDR31

Nachweisbare Sicherheit

AWS entwickelt automatisierte Argumentationswerkzeuge, die mathematische Logik verwenden, um kritische Fragen zu Ihrer Infrastruktur zu beantworten und Fehlkonfigurationen zu erkennen, die Ihre Daten potenziell preisgeben könnten. Diese Fähigkeit wird als nachweisbare Sicherheit bezeichnet, da sie ein höheres Maß an Sicherheit in der Cloud und in der Cloud bietet. Bei nachweisbarer Sicherheit kommt automatisiertes Denken zum Einsatz. Dabei handelt es sich um eine spezielle Disziplin der KI, bei der logische Schlussfolgerungen auf Computersysteme angewendet werden. Tools für automatisiertes Denken können beispielsweise Richtlinien und Konfigurationen der Netzwerkarchitektur analysieren und nachweisen, dass keine unbeabsichtigten Konfigurationen vorliegen, die potenziell anfällige Daten preisgeben könnten. Dieser Ansatz bietet das höchstmögliche Maß an Sicherheit für die kritischen Sicherheitsmerkmale der Cloud. Weitere Informationen finden Sie auf der AWS Website unter Bewährte Sicherheitsressourcen. Die folgenden AWS-Services und Funktionen verwenden derzeit automatisiertes Denken, um Ihnen dabei zu helfen, nachweisbare Sicherheit für Ihre Anwendungen zu erreichen:

- Amazon Verified Permissions ist ein skalierbares Berechtigungsmanagement und ein detaillierter Autorisierungsservice für die von Ihnen erstellten Anwendungen. Verified Permissions verwendet Cedar, eine Open-Source-Sprache für die Zugriffskontrolle, die mithilfe automatisierter Argumentation und Differenztests entwickelt wurde. Cedar ist eine Sprache, mit der Berechtigungen als Richtlinien definiert werden, die beschreiben, wer Zugriff auf welche Ressourcen haben sollte. Es ist auch eine Spezifikation für die Bewertung dieser Richtlinien. Verwenden Sie die Richtlinien von Cedar, um zu kontrollieren, was jeder Benutzer Ihrer Anwendung tun darf und auf welche Ressourcen er zugreifen darf. Bei den Richtlinien von Cedar handelt es sich um Zulassungs- oder Verbotserklärungen, die festlegen, ob ein Benutzer auf

eine Ressource einwirken kann. Richtlinien sind mit Ressourcen verknüpft, und Sie können einer Ressource mehrere Richtlinien zuordnen. Verbotene Richtlinien haben Vorrang vor Genehmigungsrichtlinien. Wenn ein Benutzer Ihrer Anwendung versucht, eine Aktion an einer Ressource auszuführen, sendet Ihre Anwendung eine Autorisierungsanfrage an die Cedar Policy Engine. Cedar bewertet die geltenden Richtlinien und gibt eine `ALLOW` `DENY` Oder-Entscheidung zurück. Cedar unterstützt Autorisierungsregeln für alle Arten von Prinzipalen und Ressourcen, ermöglicht eine rollen- und attributbasierte Zugriffskontrolle und unterstützt Analysen mithilfe automatisierter Argumentationstools, mit denen Sie Ihre Richtlinien optimieren und Ihr Sicherheitsmodell validieren können.

- AWS Identity and Access Management Access Analyzerhilft Ihnen dabei, das Berechtigungsmanagement zu optimieren. Sie können diese Funktion verwenden, um detaillierte Berechtigungen festzulegen, beabsichtigte Berechtigungen zu überprüfen und Berechtigungen zu verfeinern, indem Sie ungenutzten Zugriff entfernen. IAM Access Analyzer generiert eine detaillierte Richtlinie, die auf den in Ihren Protokollen erfassten Zugriffsaktivitäten basiert. Es bietet außerdem über 100 Richtlinienprüfungen, die Sie bei der Erstellung und Validierung Ihrer Richtlinien unterstützen. IAM Access Analyzer verwendet nachweisbare Sicherheit, um Zugriffspfade zu analysieren und umfassende Erkenntnisse für den öffentlichen und kontoübergreifenden Zugriff auf Ihre Ressourcen bereitzustellen. Dieses Tool basiert auf Zelkova, das IAM-Richtlinien in entsprechende logische Aussagen übersetzt und eine Reihe von allgemeinen und speziellen logischen Lösungsansätzen (Erfüllbarkeitsmodulo-Theorien) zur Lösung des Problems einsetzt. IAM Access Analyzer wendet Zelkova wiederholt auf eine Richtlinie mit immer spezifischeren Abfragen an, um Verhaltensklassen zu charakterisieren, die die Richtlinie basierend auf dem Inhalt der Richtlinie zulässt. Der Analyzer untersucht keine Zugriffsprotokolle, um festzustellen, ob eine externe Entität auf eine Ressource in Ihrer Vertrauenszone zugegriffen hat. Es wird ein Ergebnis generiert, wenn eine ressourcenbasierte Richtlinie den Zugriff auf eine Ressource ermöglicht, auch wenn die externe Entität nicht auf die Ressource zugegriffen hat. Weitere Informationen zu den Modulo-Theorien zur Erfüllbarkeit finden Sie unter Modulo-Theorien zur Erfüllbarkeit im Handbuch zur Zufriedenheit. *
- Amazon S3 Block Public Access ist eine Funktion von Amazon S3, mit der Sie mögliche Fehlkonfigurationen blockieren können, die zu einem öffentlichen Zugriff auf Ihre Buckets und Objekte führen könnten. Sie können Amazon S3 Block Public Access für Access Points, Buckets, Konten und die AWS Organisation aktivieren (was sich sowohl auf bestehende als auch auf neue Buckets im Konto auswirkt). Öffentlicher Zugriff auf Buckets und Objekte wird über Zugriffskontrolllisten (ACLs), Bucket-Richtlinien oder beides gewährt. Die Entscheidung, ob eine bestimmte Richtlinie oder ACL als öffentlich betrachtet wird, erfolgt mithilfe des automatisierten Argumentationssystems von Zelkova. Amazon S3 verwendet Zelkova, um jede Bucket-Richtlinie

zu überprüfen, und warnt Sie, wenn ein nicht autorisierter Benutzer in der Lage ist, Ihren Bucket zu lesen oder in ihn zu schreiben. Wenn ein Bucket als öffentlich gekennzeichnet ist, dürfen einige öffentliche Anfragen auf den Bucket zugreifen. Wenn ein Bucket als nicht öffentlich gekennzeichnet ist, werden alle öffentlichen Anfragen abgelehnt. Zelkova ist in der Lage, solche Entscheidungen zu treffen, weil sie über eine präzise mathematische Darstellung der IAM-Richtlinien verfügt. Sie erstellt für jede Richtlinie eine Formel und beweist einen Satz über diese Formel.

- Amazon VPC Network Access Analyzer ist eine Funktion von Amazon VPC, die Ihnen hilft, potenzielle Netzwerkpfade zu Ihren Ressourcen zu verstehen und potenzielle unbeabsichtigte Netzwerkzugriffe zu identifizieren. Network Access Analyzer hilft Ihnen dabei, die Netzwerksegmentierung zu überprüfen, den Internetzugang zu ermitteln und vertrauenswürdige Netzwerkpfade und Netzwerkzugriffe zu verifizieren. Diese Funktion verwendet automatische Argumentationsalgorithmen, um die Netzwerkpfade zu analysieren, die ein Paket zwischen Ressourcen in einem AWS Netzwerk nehmen kann. Anschließend werden Ergebnisse für Pfade generiert, die Ihren Netzwerkzugriffsbereichen entsprechen, die Muster für ausgehenden und eingehenden Datenverkehr definieren. Network Access Analyzer führt eine statische Analyse einer Netzwerkkonfiguration durch, was bedeutet, dass im Rahmen dieser Analyse keine Pakete im Netzwerk übertragen werden.
- Amazon VPC Reachability Analyzer ist eine Funktion von Amazon VPC, mit der Sie die Konnektivität in Ihrem Netzwerk debuggen, verstehen und visualisieren können. AWS Reachability Analyzer ist ein Tool zur Konfigurationsanalyse, mit dem Sie Konnektivitätstests zwischen einer Quellressource und einer Zielressource in Ihren virtuellen privaten Clouds () VPCs durchführen können. Wenn das Ziel erreichbar ist, erzeugt Reachability Analyzer hop-by-hop Details zum virtuellen Netzwerkpfad zwischen der Quelle und dem Ziel. Wenn das Ziel nicht erreichbar ist, identifiziert Reachability Analyzer die blockierende Komponente. Reachability Analyzer verwendet automatisiertes Denken, um praktikable Pfade zu identifizieren, indem er ein Modell der Netzwerkkonfiguration zwischen einer Quelle und einem Ziel erstellt. Anschließend wird anhand der Konfiguration geprüft, ob die Erreichbarkeit gewährleistet ist. Es sendet keine Pakete und analysiert auch nicht die Datenebene.

* Biere, A.M. Heule, H. van Maaren und T. Walsh. 2009. Handbuch zur Zufriedenheit. IOS Press, NLD.

Aufbau Ihrer Sicherheitsarchitektur — ein schrittweiser Ansatz

Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

Die von der AWS SRA empfohlene Sicherheitsarchitektur für mehrere Konten ist eine Basisarchitektur, mit der Sie Sicherheit frühzeitig in Ihren Entwurfsprozess integrieren können. Die Reise jedes Unternehmens in die Cloud ist einzigartig. Um Ihre Cloud-Sicherheitsarchitektur erfolgreich weiterzuentwickeln, müssen Sie sich den gewünschten Zielstatus vorstellen, Ihre aktuelle Cloud-Bereitschaft verstehen und einen agilen Ansatz verfolgen, um etwaige Lücken zu schließen. Die AWS SRA bietet einen Referenzzielstatus für Ihre Sicherheitsarchitektur. Durch die schrittweise Transformation können Sie schnell den Nutzen nachweisen und gleichzeitig die Notwendigkeit, weitreichende Prognosen zu treffen, auf ein Minimum reduzieren.

Das AWS Cloud Adoption Framework (AWS CAF) empfiehlt vier iterative und inkrementelle Phasen der Cloud-Transformation: Planung, Ausrichtung, Einführung und Skalierung. Wenn Sie in die Startphase eintreten und sich auf die Durchführung von Pilotinitiativen in der Produktion konzentrieren, sollten Sie sich auf den Aufbau einer starken Sicherheitsarchitektur als Grundlage für die Skalierungsphase konzentrieren, damit Sie über die technischen Fähigkeiten verfügen, Ihre geschäftskritischsten Workloads sicher zu migrieren und zu betreiben. Dieser schrittweise Ansatz eignet sich für Startups, kleine oder mittlere Unternehmen, die ihr Geschäft ausbauen möchten, oder für Unternehmen, die neue Geschäftsbereiche erwerben oder Fusionen und Übernahmen durchführen. Die AWS SRA hilft Ihnen dabei, diese grundlegende Sicherheitsarchitektur zu erreichen, sodass Sie Sicherheitskontrollen in Ihrem expandierenden Unternehmen einheitlich anwenden können. AWS Organizations Die Basisarchitektur besteht aus mehreren UND-Services AWS-Konten . Planung und Implementierung sollten ein mehrphasiger Prozess sein, sodass Sie sich über kleinere Meilensteine hinweg wiederholen können, um das größere Ziel, die Einrichtung Ihrer grundlegenden Sicherheitsarchitektur, zu erreichen. In diesem Abschnitt werden die typischen Phasen Ihrer Cloud-Reise anhand eines strukturierten Ansatzes beschrieben. Diese Phasen entsprechen den AWS Sicherheitsdesignprinzipien des Well-Architected Framework.

Phase 1: Erstellen Sie Ihre Organisationseinheit und Ihre Kontostruktur

Voraussetzung für ein solides Sicherheitsfundament ist eine gut durchdachte AWS Organisations- und Kontostruktur. Wie bereits im Abschnitt SRA-Bausteine dieses Handbuchs erläutert, können Sie verschiedene Geschäfts- und Sicherheitsfunktionen von Haus aus isolieren, wenn Sie mehrere AWS-Konten haben. Am Anfang mag das nach unnötiger Arbeit erscheinen, aber es ist eine Investition, die Ihnen hilft, schnell und sicher zu skalieren. In diesem Abschnitt wird auch erklärt AWS-Konten, wie Sie mehrere Konten verwalten können und wie Sie Funktionen für vertrauenswürdigen Zugriff und delegierte Administratoren verwenden können, um diese AWS-Services verschiedenen Konten zentral zu verwalten. AWS Organizations

Sie können die zuvor in diesem Handbuch beschriebene Methode verwenden AWS Control Tower, um Ihre landing zone zu orchestrieren. Wenn Sie derzeit ein einzelnes Konto verwenden AWS-Konto, finden Sie im AWS-Konten Leitfaden Umstellung auf mehrere Konten so früh wie möglich Informationen zur Migration zu mehreren Konten. Wenn Ihr Startup-Unternehmen derzeit beispielsweise Ideen entwickelt und Prototypen für Ihr Produkt entwickelt, sollten Sie darüber nachdenken AWS-Konto, eine Strategie für mehrere Konten zu verfolgen, bevor Sie Ihr Produkt auf den Markt bringen. Ebenso sollten kleine, mittlere und große Unternehmen damit beginnen, ihre Strategie für mehrere Konten zu entwickeln, sobald sie ihre ersten Produktionsworkloads planen. Beginnen Sie mit Ihrem Fundament OUs und AWS-Konten fügen Sie dann Ihre Workloads und Konten hinzu. OUs

Empfehlungen AWS-Konto und Empfehlungen zur Organisationsstruktur, die über die Bestimmungen der AWS SRA hinausgehen, finden Sie im Blogbeitrag Multi-Account-Strategie für kleine und mittlere Unternehmen. Denken Sie bei der Fertigstellung Ihrer Organisationseinheit und Ihrer Kontostruktur über die allgemeinen, unternehmensweiten Sicherheitskontrollen nach, die Sie mithilfe von Dienststeuerungsrichtlinien (SCPs), Ressourcenkontrollrichtlinien () und deklarativen Richtlinien durchsetzen möchten. RCPs

> **Designüberlegung**
>
> Replizieren Sie nicht die Berichtsstruktur Ihres Unternehmens, wenn Sie Ihre OU- und Kontostruktur entwerfen. Sie OUs sollten auf Workload-Funktionen und gemeinsamen Sicherheitskontrollen basieren, die für die Workloads gelten. Versuchen Sie nicht, Ihre gesamte Kontostruktur von Anfang an zu entwerfen. Konzentrieren Sie sich auf die Grundlagen und fügen Sie dann die Arbeitslast OUs hinzu OUs, wenn Sie sie benötigen. Sie

können Konten zwischen Konten verschieben OUs, um in den frühen Phasen Ihres Entwurfs mit alternativen Ansätzen zu experimentieren. Dies kann jedoch zu einem gewissen Aufwand bei der Verwaltung logischer Berechtigungen führen, abhängig von SCPs, RCPs, deklarativen Richtlinien und IAM-Bedingungen, die auf OU- und Kontopfaden basieren.

Beispiel für eine Implementierung

Die AWS SRA-Codebibliothek bietet eine Beispielimplementierung von Account Alternate Contacts. Diese Lösung legt die alternativen Ansprechpartner für Abrechnung, Betrieb und Sicherheit für alle Konten innerhalb einer Organisation fest.

Phase 2: Implementieren Sie ein starkes Identitätsfundament

Sobald Sie mehrere erstellt haben AWS-Konten, sollten Sie Ihren Teams Zugriff auf die AWS Ressourcen in diesen Konten gewähren. Es gibt zwei allgemeine Kategorien des Identitätsmanagements: Identitäts - und Zugriffsmanagement für Mitarbeiter und Kundenidentitäts- und Zugriffsmanagement (CIAM). Workforce IAM ist für Unternehmen gedacht, in denen sich Mitarbeiter und automatisierte Workloads anmelden müssen, um ihre Arbeit AWS zu erledigen. CIAM wird verwendet, wenn ein Unternehmen eine Möglichkeit benötigt, Benutzer zu authentifizieren, um Zugriff auf die Anwendungen des Unternehmens zu gewähren. Sie benötigen zunächst eine IAM-Strategie für die Belegschaft, damit Ihre Teams Anwendungen erstellen und migrieren können. Sie sollten immer IAM-Rollen anstelle von IAM-Benutzern verwenden, um menschlichen oder maschinellen Benutzern Zugriff zu gewähren. Folgen Sie den AWS SRA-Anweisungen zur Verwendung AWS IAM Identity Center innerhalb der Konten Org Management und Shared Services, um den Single Sign-On (SSO) -Zugriff auf Ihre Konten zentral zu verwalten. AWS-Konten Die Anleitung enthält auch Designüberlegungen für die Verwendung des IAM-Verbunds, wenn Sie IAM Identity Center nicht verwenden können.

Wenn Sie mit IAM-Rollen arbeiten, um Benutzern Zugriff auf AWS Ressourcen zu gewähren, sollten Sie IAM Access Analyzer und IAM Access Advisor verwenden, wie in den Abschnitten Security Tooling und Org Management dieses Handbuchs beschrieben. Diese Services helfen Ihnen dabei, die geringsten Rechte zu erreichen. Dabei handelt es sich um eine wichtige präventive Kontrolle, mit der Sie ein gutes Sicherheitsniveau aufbauen können.

Designüberlegung

Um die geringsten Rechte zu erreichen, sollten Sie Prozesse entwickeln, mit denen die Beziehungen zwischen Ihren Identitäten und den Berechtigungen, die sie für ein ordnungsgemäßes Funktionieren benötigen, regelmäßig überprüft und verstanden werden. Wenn Sie lernen, sollten Sie diese Berechtigungen verfeinern und sie schrittweise auf die geringstmöglichen Berechtigungen reduzieren. Aus Gründen der Skalierbarkeit sollten Ihre zentralen Sicherheits- und Anwendungsteams dafür gemeinsam verantwortlich sein. Verwenden Sie Funktionen wie ressourcenbasierte Richtlinien, Berechtigungsgrenzen, attributbasierte Zugriffskontrollen und Sitzungsrichtlinien, um Anwendungsbesitzern dabei zu helfen, eine detaillierte Zugriffskontrolle zu definieren.

Implementierungsbeispiele

Die AWS SRA-Codebibliothek bietet zwei Beispielimplementierungen, die für diese Phase gelten:

- Die IAM-Passwortrichtlinie legt die Kontopasswortrichtlinie für Benutzer so fest, dass sie den gängigen Compliance-Standards entspricht.
- Access Analyzer konfiguriert einen Analyzer auf Organisationsebene innerhalb eines delegierten Administratorkontos und einen Analyzer auf Kontoebene in jedem Konto.

Phase 3: Aufrechterhaltung der Rückverfolgbarkeit

Wenn Ihre Benutzer Zugriff auf die Software haben AWS und mit der Entwicklung beginnen, werden Sie wissen wollen, wer was, wann und von wo aus macht. Außerdem benötigen Sie Einblick in potenzielle Sicherheitsfehlkonfigurationen, Bedrohungen oder unerwartetes Verhalten. Ein besseres Verständnis von Sicherheitsbedrohungen ermöglicht es Ihnen, die geeigneten Sicherheitskontrollen zu priorisieren. Um die AWS Aktivitäten zu überwachen, folgen Sie den Empfehlungen der AWS SRA zur Einrichtung eines Organisationstrails, indem Sie Ihre Protokolle im Log Archive-Konto verwenden AWS CloudTrailund dort zentralisieren. Verwenden Sie AWS Security Hub CSPM für die Überwachung von Sicherheitsereignissen Amazon und Amazon Security Lake GuardDuty AWS Config, wie im Abschnitt Security Tooling-Konto beschrieben.

Designüberlegung

Wenn Sie mit der Nutzung von New beginnen AWS-Services, stellen Sie sicher, dass Sie die dienstspezifischen Protokolle für den Service aktivieren und diese als Teil Ihres zentralen Protokoll-Repositorys speichern.

Implementierungsbeispiele

Die AWS SRA-Codebibliothek enthält die folgenden Beispielimplementierungen, die für diese Phase gelten:

- Die Organisation CloudTrail erstellt einen Organisationspfad und legt Standardwerte für die Konfiguration von Datenereignissen fest (z. B. in Amazon S3 und AWS Lambda), um CloudTrail die Duplizierung der von konfigurierten Daten zu reduzieren. AWS Control Tower Diese Lösung bietet Optionen für die Konfiguration von Verwaltungsereignissen.
- AWS Config Das Control Tower Tower-Verwaltungskonto ermöglicht AWS Config im Verwaltungskonto die Überwachung der Ressourcen-Compliance.
- Mit Conformance Pack Organization Rules wird ein Conformance Pack für die Konten und angegebenen Regionen innerhalb einer Organisation bereitgestellt.
- AWS Config Aggregator stellt einen Aggregator bereit, indem er die Verwaltung an ein anderes Mitgliedskonto als das Auditkonto delegiert.
- Security Hub CSPM Organization konfiguriert Security Hub CSPM innerhalb eines delegierten Administratorkontos für die Konten und verwalteten Regionen innerhalb der Organisation.
- GuardDuty Die Organisation konfiguriert GuardDuty innerhalb eines delegierten Administratorkontos die Konten innerhalb einer Organisation.

Phase 4: Wenden Sie Sicherheit auf allen Ebenen an

Zu diesem Zeitpunkt sollten Sie über Folgendes verfügen:

- Die entsprechenden Sicherheitskontrollen für Ihre AWS-Konten.

- Eine klar definierte Konto- und Organisationsstruktur mit präventiven Kontrollen SCPs RCPs, die durch deklarative Richtlinien und IAM-Rollen und -Richtlinien mit den geringsten Rechten definiert sind.
- Die Fähigkeit, AWS Aktivitäten mithilfe AWS CloudTrail von Amazon zu protokollieren AWS Security Hub CSPM, Sicherheitsereignisse mithilfe von Amazon GuardDuty und AWS Config zu erkennen und mithilfe von Amazon Security Lake erweiterte Analysen an einem speziell für die Sicherheit erstellten Data Lake durchzuführen.

Planen Sie in dieser Phase, die Sicherheit auch auf anderen Ebenen Ihrer AWS Organisation anzuwenden, wie im Abschnitt Einführung von Sicherheitsdiensten in Ihrer AWS gesamten Organisation beschrieben. Sie können Sicherheitskontrollen für Ihre Netzwerkebene einrichten, indem Sie Dienste wie AWS WAF AWS Shield, AWS Firewall Manager, AWS Network Firewall, AWS Certificate Manager (ACM), Amazon CloudFront, Amazon Route 53 und Amazon VPC verwenden, wie im Abschnitt Netzwerkkonto beschrieben. Wenden Sie bei der Weiterentwicklung Ihres Technologie-Stacks Sicherheitskontrollen an, die für Ihren Workload oder Ihren Anwendungsstapel spezifisch sind. Verwenden Sie VPC-Endpunkte, Amazon Inspector, AWS Systems Manager AWS Secrets Manager, und Amazon Cognito, wie im Abschnitt Anwendungskonto beschrieben.

Designüberlegung

Berücksichtigen Sie bei der Gestaltung Ihrer Sicherheitskontrollen (Defense in Depth, DiD) Skalierungsfaktoren. Ihr zentrales Sicherheitsteam wird nicht über die Bandbreite oder das vollständige Verständnis dafür verfügen, wie sich jede Anwendung in Ihrer Umgebung verhält. Geben Sie Ihren Anwendungsteams die Möglichkeit, für die Identifizierung und Gestaltung der richtigen Sicherheitskontrollen für ihre Anwendungen verantwortlich und rechenschaftspflichtig zu sein. Das zentrale Sicherheitsteam sollte sich darauf konzentrieren, die richtigen Tools und Beratung bereitzustellen, um die Anwendungsteams zu unterstützen. Informationen zu den Skalierungsmechanismen, AWS mit denen ein eher nach links gerichteter Sicherheitsansatz eingeführt wird, finden Sie im Blogbeitrag How AWS built the Security Guardians program, a mechanism to distribution ownership.

Implementierungsbeispiele

Die AWS SRA-Codebibliothek enthält die folgenden Beispielimplementierungen, die für diese Phase gelten:

- EC2 Default EBS Encryption konfiguriert die standardmäßige Amazon EBS-Verschlüsselung in Amazon EC2 so, dass sie die Standardeinstellung innerhalb der bereitgestellten verwendet. AWS KMS key AWS-Regionen
- S3 Block Account Public Access konfiguriert die Block Public Access (BPA) -Einstellungen auf Kontoebene in Amazon S3 für Konten innerhalb der Organisation.
- Firewall Manager zeigt, wie eine Sicherheitsgruppenrichtlinie und AWS WAF Richtlinien für Konten innerhalb einer Organisation konfiguriert werden.
- Inspector Organization konfiguriert Amazon Inspector innerhalb eines delegierten Administratorkontos für Konten und verwaltete Regionen innerhalb der Organisation.

Phase 5: Schützen Sie Daten während der Übertragung und im Speicher

Ihre Geschäfts- und Kundendaten sind wertvolle Ressourcen, die Sie schützen müssen. AWS bietet verschiedene Sicherheitsdienste und -funktionen zum Schutz von Daten, die sich in Bewegung befinden und gespeichert werden. Verwenden Sie Amazon CloudFront mit AWS Certificate Manager, wie im Abschnitt Netzwerkkonto beschrieben, um Daten zu schützen, die während der Übertragung über das Internet gesammelt werden. Verwenden Sie für Daten, die innerhalb interner Netzwerke übertragen werden, einen Application Load Balancer mit AWS Private Certificate Authority, wie im Abschnitt Anwendungskonto beschrieben. AWS KMS und AWS CloudHSM unterstützen Sie bei der Verwaltung kryptografischer Schlüssel, um Daten im Speicher zu schützen.

Phase 6: Bereiten Sie sich auf Sicherheitsereignisse vor

Beim Betrieb Ihrer IT-Umgebung werden Sie auf Sicherheitsereignisse stoßen. Dabei handelt es sich um Veränderungen im täglichen Betrieb Ihrer IT-Umgebung, die auf einen möglichen Verstoß gegen Sicherheitsrichtlinien oder ein Versagen der Sicherheitskontrolle hinweisen. Eine ordnungsgemäße Rückverfolgbarkeit ist entscheidend, damit Sie so schnell wie möglich über ein Sicherheitsereignis informiert werden. Ebenso wichtig ist es, darauf vorbereitet zu sein, solche Sicherheitsereignisse zu analysieren und darauf zu reagieren, damit Sie geeignete Maßnahmen ergreifen können, bevor das Sicherheitsereignis eskaliert. Die Vorbereitung hilft Ihnen dabei, ein Sicherheitsereignis schnell zu beurteilen, um seine möglichen Auswirkungen zu verstehen.

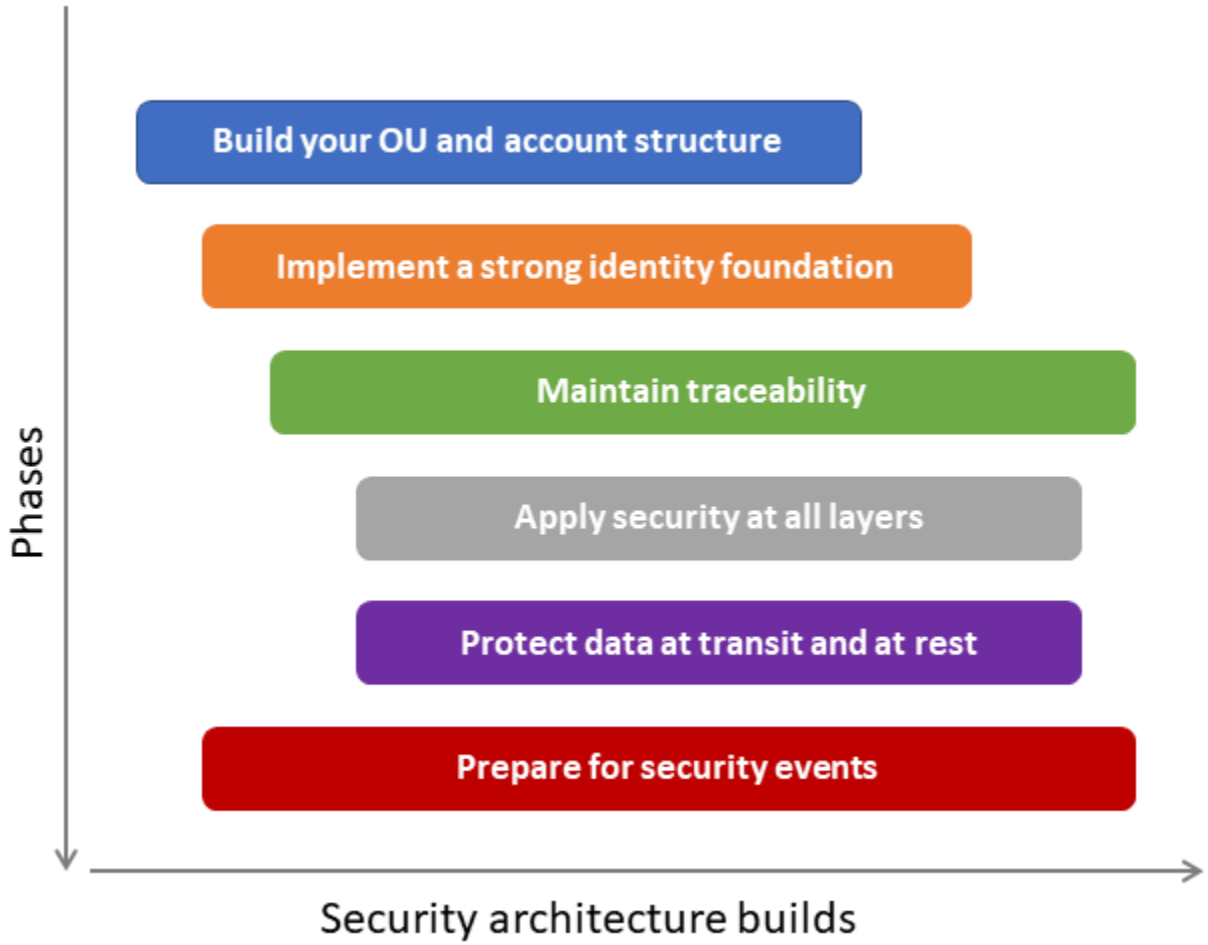
Die AWS SRA bietet Ihnen durch die Gestaltung des Security Tooling-Kontos und die Bereitstellung einheitlicher Sicherheitsdienste in allen Bereichen die Möglichkeit AWS-Konten, Sicherheitsereignisse in Ihrem gesamten Unternehmen zu erkennen. AWS Amazon Detective im Security Tooling-Konto hilft Ihnen dabei, ein Sicherheitsereignis zu analysieren und die Ursache zu identifizieren. Während einer Sicherheitsuntersuchung müssen Sie in der Lage sein, die relevanten Protokolle zu überprüfen, um den gesamten Umfang und den Zeitplan des Vorfalls aufzuzeichnen und zu verstehen. Protokolle sind auch für die Generierung von Warnmeldungen erforderlich, wenn bestimmte Aktionen von Interesse sind. Die AWS SRA empfiehlt ein zentrales Log Archive-Konto für die unveränderliche Speicherung aller Sicherheits- und Betriebsprotokolle. Sie können Protokolle abfragen, indem Sie CloudWatch Logs Insights für Daten verwenden, die in CloudWatch Protokollgruppen gespeichert sind, und Amazon Athena und Amazon OpenSearch Service für Daten, die in Amazon S3 gespeichert sind. Verwenden Sie Amazon Security Lake, um Sicherheitsdaten aus der AWS Umgebung, von SaaS-Anbietern (Software as a Service), vor Ort und anderen Cloud-Anbietern automatisch zu zentralisieren. Richten Sie Abonnenten im Security Tooling-Konto oder einem anderen speziellen Konto, wie von der AWS SRA beschrieben, ein, um diese Protokolle zur Untersuchung abzufragen.

AWS Security Incident Responsehilft Ihnen dabei, die Reaktion auf Sicherheitsvorfälle, deren Untersuchung und Behebung zu automatisieren. Es bietet vorgefertigte Playbooks und Workflows, mit denen Sie schnell und konsistent auf Sicherheitsereignisse reagieren können. Wenn die proaktive Reaktionsfunktion aktiviert ist, lässt sich Security Incident Response in Security Hub CSPM integrieren und GuardDuty löst automatisch Reaktionsworkflows aus, wenn Sicherheitslücken erkannt werden. Der Service hilft Ihnen dabei, Ihre Prozesse zur Reaktion auf Vorfälle in Ihrem gesamten Unternehmen zu standardisieren und zu automatisieren. AWS Wenn Sie zusätzliche Unterstützung benötigen, können Sie einen Fall mit Serviceunterstützung eröffnen, um sich an das AWS Customer Incident Response Team (CIRT) zu wenden.

Designüberlegungen

- Sie sollten sich von Beginn Ihrer Cloud-Reise an darauf vorbereiten, Sicherheitsereignisse zu erkennen und darauf zu reagieren. Um begrenzte Ressourcen besser zu nutzen, weisen Sie Ihren AWS Ressourcen Daten und Geschäftskritikalität zu, sodass Sie, wenn Sie ein Sicherheitsereignis erkennen, die Auswahl und Reaktion auf der Grundlage der Kritikalität der beteiligten Ressourcen priorisieren können.
- Die Phasen für den Aufbau Ihrer Cloud-Sicherheitsarchitektur, wie in diesem Abschnitt beschrieben, sind sequentieller Natur. Sie müssen jedoch nicht auf den vollständigen Abschluss einer Phase warten, bevor Sie mit der nächsten Phase beginnen. Wir empfehlen

Ihnen, einen iterativen Ansatz zu wählen, bei dem Sie beginnen, an mehreren Phasen parallel zu arbeiten und jede Phase weiterzuentwickeln, während Sie Ihre Cloud-Sicherheitslage weiterentwickeln. Während Sie die verschiedenen Phasen durchlaufen, wird sich Ihr Design weiterentwickeln. Erwägen Sie, die in der folgenden Abbildung vorgeschlagene Reihenfolge an Ihre speziellen Bedürfnisse anzupassen.



Beispiel für eine Implementierung

Die AWS SRA-Codebibliothek bietet eine Beispielimplementierung einer Detective Organization, die Amazon Detective automatisch aktiviert, indem sie die Verwaltung an ein Konto delegiert (z. B. Audit oder Security Tooling) und Detective für bestehende und future Konten konfiguriert. AWS Organizations

AWS Checkliste für bewährte SRA-Praktiken

Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

In diesem Abschnitt werden die Best Practices für AWS SRA, die in diesem Leitfaden beschrieben werden, in einer Checkliste zusammengefasst, die Sie beim Aufbau Ihrer Version der Sicherheitsarchitektur befolgen können. AWS Verwenden Sie diese Liste als Referenz und nicht als Ersatz für die Lektüre des Leitfadens. Die Checkliste ist gruppiert AWS-Service nach. Wenn Sie Ihre bestehende AWS Umgebung anhand der SRA-Checkliste für bewährte Methoden programmgesteuert überprüfen möchten, können Sie AWS SRA Verify verwenden.

SRA Verify ist ein Tool zur Sicherheitsbewertung, mit dem Sie beurteilen können, ob Ihr Unternehmen die SRA in mehreren Regionen AWS einhält. AWS-Konten Es orientiert sich direkt an den AWS SRA-Empfehlungen, indem es automatisierte Prüfungen bereitstellt, mit denen Ihre Implementierung anhand der AWS SRA-Richtlinien validiert wird. Mit dem Tool können Sie überprüfen, ob Ihre Sicherheitsdienste gemäß der Referenzarchitektur ordnungsgemäß konfiguriert sind. Es bietet detaillierte Ergebnisse und umsetzbare Schritte zur Problembehebung, um sicherzustellen, dass Ihre AWS Umgebung den bewährten Sicherheitsmethoden entspricht. SRA Verify ist so konzipiert, dass es AWS CodeBuild im Auditkonto der Organisation (Security Tooling) ausgeführt wird. Sie können es auch lokal ausführen oder mithilfe der SRA Verify-Bibliothek erweitern.

> **Note**
>
> SRA Verify enthält Prüfungen für mehrere Dienste, enthält jedoch möglicherweise nicht für alle Aspekte des AWS SRA eine Prüfung. Weitere Informationen finden Sie in den Leitfäden in der AWS SRA-Bibliothek.

AWS Organizations

- AWS Organizations ist mit allen Funktionen aktiviert.
- Dienststeuerungsrichtlinien (SCPs) werden verwendet, um Richtlinien zur Zugriffskontrolle für IAM-Prinzipale zu definieren.

- Ressourcenkontrollrichtlinien (RCPs) werden verwendet, um Richtlinien für die Zugriffskontrolle für AWS Ressourcen zu definieren.
- Deklarative Richtlinien werden verwendet, um Ihre gewünschte Konfiguration für eine bestimmte Größe in Ihrem gesamten Unternehmen zentral AWS-Service zu deklarieren und durchzusetzen.
- Drei grundlegende Konten (Sicherheit, Infrastruktur und Workload) OUs werden für die Gruppierung von Mitgliedskonten eingerichtet, die grundlegende Dienste bereitstellen.
- Das Security Tooling-Konto wird unter der Security OU erstellt. Dieses Konto ermöglicht die zentrale Verwaltung von AWS Sicherheitsdiensten und anderen Sicherheitstools von Drittanbietern.
- Das Log Archive-Konto wird unter der Security OU erstellt. Dieses Konto stellt ein streng kontrolliertes zentrales Protokoll-Repository mit Anwendungsprotokollen AWS-Services und Anwendungsprotokollen bereit.
- Das Netzwerkkonto wird unter der Infrastruktur-OU erstellt. Dieses Konto verwaltet das Gateway zwischen Ihrer Anwendung und dem breiteren Internet. Es isoliert die Netzwerkdienste, die Konfiguration und den Betrieb von den Workloads, der Sicherheit und anderen Infrastrukturen der einzelnen Anwendungen.
- Das Shared Service-Konto wird unter der Infrastruktur-OU erstellt. Dieses Konto unterstützt die Dienste, die mehrere Anwendungen und Teams verwenden, um ihre Ergebnisse zu erzielen.
- Das Anwendungskonto wird unter der Workloads OU erstellt. Dieses Konto hostet die primäre Infrastruktur und die Dienste für den Betrieb und die Wartung einer Unternehmensanwendung. Dieses Handbuch bietet eine Darstellung, aber in der Praxis wird es mehrere Konten OUs und Mitgliedskonten geben, die nach Anwendungen, Entwicklungsumgebungen und anderen Sicherheitsaspekten getrennt sind.
- Alternative Kontaktinformationen für Abrechnung, Betrieb und Sicherheit für alle Mitgliedskonten sind konfiguriert.

AWS CloudTrail

- Es ist ein Organisationspfad konfiguriert, der die Übermittlung von CloudTrail Verwaltungsereignissen im Verwaltungskonto und in allen Mitgliedskonten einer AWS Organisation ermöglicht.
- Der Organisationspfad ist als regionsübergreifender Pfad konfiguriert.
- Der Organization Trail ist so konfiguriert, dass Ereignisse aus globalen Ressourcen erfasst werden.
- Zusätzliche Pfade zur Erfassung bestimmter Datenereignisse werden nach Bedarf konfiguriert, um sensible AWS Ressourcenaktivitäten zu überwachen.

- Das Security Tooling-Konto ist als delegierter Administrator des Organisationstrails eingerichtet.
- Der Organization Trail ist so konfiguriert, dass er automatisch für alle neuen Mitgliedskonten aktiviert wird.
- Der Organization Trail ist so konfiguriert, dass Protokolle in einem zentralen S3-Bucket veröffentlicht werden, der im Log Archive-Konto gehostet wird.
- Für den Organization Trail ist die Überprüfung der Protokolldateien aktiviert, um die Integrität der Protokolldateien zu überprüfen.
- Der Organization Trail ist zur Aufbewahrung von CloudWatch Protokollen in Logs integriert.
- Der Organization Trail wird mithilfe eines vom Kunden verwalteten Schlüssels verschlüsselt.
- Der zentrale S3-Bucket, der für das Protokoll-Repository im Log Archive-Konto verwendet wird, ist mit einem vom Kunden verwalteten Schlüssel verschlüsselt.
- Der zentrale S3-Bucket, der für das Log-Repository im Log Archive-Konto verwendet wird, ist aus Gründen der Unveränderlichkeit mit S3 Object Lock konfiguriert.
- Die Versionierung ist für den zentralen S3-Bucket aktiviert, der für das Log-Repository im Log Archive-Konto verwendet wird.
- Für den zentralen S3-Bucket, der für das Protokoll-Repository im Log Archive-Konto verwendet wird, ist eine Ressourcenrichtlinie definiert, die das Hochladen von Objekten nur anhand des Organisationstrails über die Ressource Amazon Resource Name (ARN) einschränkt.

AWS Security Hub CSPM

- Security Hub CSPM ist für alle Mitgliedskonten und das Verwaltungskonto aktiviert.
- AWS Config ist für alle Mitgliedskonten als Voraussetzung für Security Hub CSPM aktiviert.
- Das Security Tooling-Konto ist als delegierter Administrator von Security Hub CSPM eingerichtet.
- Amazon GuardDuty und Amazon Detective haben dasselbe delegierte Administratorkonto wie Security Hub CSPM, um eine reibungslose Serviceintegration zu gewährleisten.
- Die zentrale Konfiguration wird verwendet, um Security Hub CSPM über mehrere AWS-Konten und hinweg einzurichten und zu verwalten. AWS-Regionen
- Alle OU- und Mitgliedskonten werden vom delegierten Administrator von Security Hub CSPM als zentral verwaltet eingestuft.
- Security Hub CSPM wird automatisch für alle neuen Mitgliedskonten aktiviert.
- Security Hub CSPM wird automatisch für die Konfiguration neuer Standards aktiviert.

- Die CSPM-Ergebnisse von Security Hub aus allen Regionen werden in einer einzigen Heimatregion zusammengefasst.
- Die CSPM-Ergebnisse von Security Hub aus allen Mitgliedskonten werden im Security Tooling-Konto zusammengefasst.
- Der FSBP-Standard (AWS Foundational Best Practices) in Security Hub CSPM ist für alle Mitgliedskonten aktiviert.
- Der CIS AWS Foundation Benchmark-Standard in Security Hub CSPM ist für alle Mitgliedskonten aktiviert.
- Andere Security Hub CSPM-Standards sind je nach Bedarf aktiviert.
- Eine Security Hub CSPM-Automatisierungsregel wird verwendet, um Ergebnisse mit Ressourcenkontext anzureichern.
- Die automatische Reaktions- und Problembehebungsfunktion von Security Hub CSPM wird verwendet, um benutzerdefinierte EventBridge Regeln zu erstellen, um automatische Maßnahmen gegen bestimmte Ergebnisse zu ergreifen.

AWS Config

- Der AWS Config Rekorder ist für alle Mitgliedskonten und das Verwaltungskonto aktiviert.
- Der AWS Config Rekorder ist für alle Regionen aktiviert.
- Der S3-Bucket für den AWS Config Lieferkanal ist im Log Archive-Konto zentralisiert.
- Das AWS Config delegierte Administratorkonto ist auf das Security Tooling-Konto festgelegt.
- AWS Config hat einen Organisationsaggregator eingerichtet. Der Aggregator umfasst alle Regionen.
- AWS Config Konformitätspakete werden vom delegierten Administratorkonto aus einheitlich für alle Mitgliedskonten bereitgestellt.
- AWS Config Regelergebnisse werden automatisch an Security Hub CSPM gesendet.

Amazon GuardDuty

- GuardDuty Der Detektor ist für alle Mitgliedskonten und das Verwaltungskonto aktiviert.
- GuardDuty Der Detektor ist für alle Regionen aktiviert.
- GuardDuty Der Detektor wird automatisch für alle neuen Mitgliedskonten aktiviert.

- GuardDuty Die delegierte Verwaltung ist auf das Security Tooling-Konto festgelegt.
- GuardDuty grundlegende Datenquellen wie CloudTrail Verwaltungsereignisse, VPC-Flussprotokolle und Route 53 Resolver-DNS-Abfrageprotokolle sind aktiviert.
- GuardDuty S3-Schutz ist aktiviert.
- GuardDuty Der Malware-Schutz für EBS-Volumes ist aktiviert.
- GuardDuty Der Malware-Schutz für S3 ist aktiviert.
- GuardDuty Der RDS-Schutz ist aktiviert.
- GuardDuty Lambda-Schutz ist aktiviert.
- GuardDuty Der EKS-Schutz ist aktiviert.
- GuardDuty EKS Runtime Monitoring ist aktiviert.
- GuardDuty Die erweiterte Bedrohungserkennung ist aktiviert.
- GuardDuty Die Ergebnisse werden zur Aufbewahrung in einen zentralen S3-Bucket im Log Archive-Konto exportiert.

IAM

- IAM-Benutzer werden nicht verwendet.
- Die zentrale Verwaltung des Root-Zugriffs für Mitgliedskonten wird durchgesetzt.
- Die zentrale Aufgabe für privilegierte Root-Benutzer für das Verwaltungskonto wird vom delegierten Administrator durchgesetzt.
- Die zentrale Verwaltung des Root-Zugriffs wird an das Security Tooling-Konto delegiert.
- Alle Root-Anmeldeinformationen für Mitgliedskonten werden entfernt.
- Alle AWS-Konto Passwortrichtlinien für Mitglieder und Verwaltung entsprechen den Sicherheitsstandards der Organisation.
- Der IAM Access Advisor wird verwendet, um die zuletzt verwendeten Informationen für IAM-Gruppen, Benutzer, Rollen und Richtlinien zu überprüfen.
- Berechtigungsgrenzen werden verwendet, um die maximal möglichen Berechtigungen für IAM-Rollen einzuschränken.

IAM Access Analyzer

- IAM Access Analyzer ist für alle Mitgliedskonten und das Verwaltungskonto aktiviert.

- Der delegierte Administrator von IAM Access Analyzer ist auf das Security Tooling-Konto eingestellt.
- Der externe Zugriffsanalysator von IAM Access Analyzer ist mit der Vertrauenszone der Organisation in jeder Region konfiguriert.
- Der externe Zugriffsanalysator von IAM Access Analyzer ist mit der Vertrauenszone für Konten in jeder Region konfiguriert.
- Der interne Zugriffsanalysator von IAM Access Analyzer ist mit der Vertrauenszone der Organisation in jeder Region konfiguriert.
- Der interne Zugriffsanalysator von IAM Access Analyzer ist mit der Vertrauenszone für Konten in jeder Region konfiguriert.
- Der IAM Access Analyzer Analyzer Analyzer für ungenutzten Zugriff für das aktuelle Konto wird erstellt.
- Der IAM Access Analyzer Analyzer für ungenutzten Zugriff für die aktuelle Organisation wird erstellt.

Amazon Detective

- Detective ist für alle Mitgliedskonten aktiviert.
- Detective ist automatisch für alle neuen Mitgliedskonten aktiviert.
- Detective ist für alle Regionen aktiviert.
- Der delegierte Detective Administrator ist auf das Security Tooling-Konto eingestellt.
- Der delegierte CSPM-Administrator Detective und Security Hub ist auf dasselbe Security Tooling-Konto eingestellt. GuardDuty
- Detective ist in Security Lake für die Speicherung und Analyse von Rohprotokollen integriert.
- Detective ist GuardDuty für die Erfassung von Erkenntnissen integriert.
- Detective nimmt Amazon EKS-Auditprotokolle zur Analyse auf.
- Detective nimmt die CSPM-Protokolle von Security Hub zur Analyse auf.

AWS Firewall Manager

- Die Sicherheitsrichtlinien von Firewall Manager sind festgelegt.
- Der delegierte Administrator von Firewall Manager ist auf das Security Tooling-Konto eingestellt.

- AWS Config ist als Voraussetzung aktiviert.
- Es werden mehrere Firewall Manager Manager-Administratoren mit eingeschränktem Geltungsbereich pro OU, Konto und Region eingerichtet.
- Eine Firewall Manager AWS WAF Manager-Sicherheitsrichtlinie ist definiert.
- Eine AWS WAF zentrale Protokollierungsrichtlinie von Firewall Manager ist definiert.
- Eine Firewall Manager Shield Advanced-Sicherheitsrichtlinie ist definiert.
- Eine Sicherheitsrichtlinie für Firewall Manager Manager-Sicherheitsgruppen ist definiert.

Amazon Inspector

- Amazon Inspector ist für alle Mitgliedskonten aktiviert.
- Amazon Inspector wird automatisch für jedes neue Mitgliedskonto aktiviert.
- Der von Amazon Inspector delegierte Administrator ist auf das Security Tooling-Konto eingestellt.
- Die Suche nach EC2 Sicherheitslücken in Amazon Inspector ist aktiviert.
- Das Scannen nach Sicherheitslücken in ECR-Bildern in Amazon Inspector ist aktiviert.
- Die Amazon Inspector Lambda-Funktion und der Layer-Schwachstellen-Scan sind aktiviert.
- Das Scannen von Amazon Inspector Lambda-Code ist aktiviert.
- Das Sicherheitsscannen von Amazon Inspector ist aktiviert.

Amazon Macie

- Macie ist für die entsprechenden Mitgliedskonten aktiviert.
- Macie wird automatisch für entsprechende neue Mitgliedskonten aktiviert.
- Der delegierte Macie-Administrator ist auf das Security Tooling-Konto eingestellt.
- Die Ergebnisse von Macie werden in einen zentralen S3-Bucket im Log-Archive-Konto exportiert.
- S3-Buckets, in denen Macie-Ergebnisse gespeichert werden, werden mit einem vom Kunden verwalteten Schlüssel verschlüsselt.
- Die Macie-Richtlinie und die Klassifizierungsrichtlinie werden in Security Hub CSPM veröffentlicht.

Amazon Security Lake

- Die Security Lake-Organisationskonfiguration ist aktiviert.

- Der delegierte Security Lake-Administrator ist auf das Security Tooling-Konto eingestellt.
- Die Security Lake-Organisationskonfiguration ist für neue Mitgliedskonten aktiviert.
- Das Security Tooling-Konto ist als Abonnent für den Datenzugriff eingerichtet, um die Analyse von Protokollen durchzuführen.
- Das Security Tooling-Konto ist als Abonnent für Datenabfragen eingerichtet, um die Analyse von Protokollen durchzuführen.
- Eine CloudTrail Verwaltungsprotokollquelle ist für Security Lake in allen oder bestimmten aktiven Mitgliedskonten aktiviert.
- Eine VPC-Flow-Protokollquelle ist für Security Lake in allen oder bestimmten aktiven Mitgliedskonten aktiviert.
- Eine Route 53-Protokollquelle ist für Security Lake in allen oder bestimmten aktiven Mitgliedskonten aktiviert.
- CloudTrail Das Datenereignis für eine S3-Protokollquelle ist für Security Lake in allen oder bestimmten aktiven Mitgliedskonten aktiviert.
- Eine Lambda-Ausführungsprotokollquelle ist für Security Lake in allen oder bestimmten aktiven Mitgliedskonten aktiviert.
- Eine Amazon EKS-Audit-Protokollquelle ist für Security Lake in allen oder bestimmten aktiven Mitgliedskonten aktiviert.
- Eine Security Hub Hub-Ergebnisprotokollquelle ist für Security Lake in allen oder bestimmten aktiven Mitgliedskonten aktiviert.
- Eine AWS WAF Protokollquelle ist für Security Lake in allen oder bestimmten aktiven Mitgliedskonten aktiviert.
- Die SQS-Warteschlangen von Security Lake im delegierten Administratorkonto sind mit einem vom Kunden verwalteten Schlüssel verschlüsselt.
- Die Security Lake SQS-Warteschlange für unzustellbare Briefe im delegierten Administratorkonto ist mit einem vom Kunden verwalteten Schlüssel verschlüsselt.
- Der Security Lake S3-Bucket ist mit einem vom Kunden verwalteten Schlüssel verschlüsselt.
- Der Security Lake S3-Bucket verfügt über eine Ressourcenrichtlinie, die den direkten Zugriff nur durch Security Lake einschränkt.

AWS WAF

- Alle CloudFront Distributionen sind verknüpft mit. AWS WAF

- Alle Amazon API Gateway APIs Gateway-REST-Dateien sind verknüpft mit AWS WAF.
- Alle Application Load Balancer sind verknüpft mit AWS WAF.
- Alle AWS AppSync GraphQL APIs sind verknüpft mit AWS WAF.
- Alle Amazon Cognito Cognito-Benutzerpools sind verknüpft mit AWS WAF.
- Alle AWS App Runner Dienste sind verknüpft mit AWS WAF.
- Alle AWS Verified Access Instanzen sind verknüpft mit AWS WAF.
- Alle AWS Amplify Anwendungen sind verknüpft mit AWS WAF.
- AWS WAF Die Protokollierung ist aktiviert.
- AWS WAF Protokolle werden in einem S3-Bucket im Log Archive-Konto zentralisiert.

AWS Shield Advanced

- Das Shield Advanced-Abonnement ist aktiviert und so eingestellt, dass es für alle Anwendungskonten mit öffentlich zugänglichen Ressourcen automatisch verlängert wird.
- Shield Advanced ist für alle CloudFront Distributionen konfiguriert.
- Shield Advanced ist für alle Application Load Balancer konfiguriert.
- Shield Advanced ist für alle Network Load Balancer konfiguriert.
- Shield Advanced ist für alle von Route 53 gehosteten Zonen konfiguriert.
- Shield Advanced ist für alle Elastic IP-Adressen konfiguriert.
- Shield Advanced ist für alle Global Accelerators konfiguriert.
- CloudWatch Alarme werden für CloudFront und Route 53-Ressourcen konfiguriert, die durch Shield Advanced geschützt sind.
- Der Zugriff auf das Shield Response Team (SRT) ist konfiguriert.
- Das proaktive Engagement von Shield Advanced ist aktiviert.
- Die proaktiven Engagement-Kontakte von Shield Advanced sind konfiguriert.
- Für geschützte Shield Advanced-Ressourcen ist eine benutzerdefinierte AWS WAF Regel konfiguriert.
- Bei geschützten Shield Advanced-Ressourcen ist die automatische Risikominderung auf Anwendungsebene DDo S aktiviert.

AWS Reaktion auf Sicherheitsvorfälle

- AWS Security Incident Response ist für die gesamte AWS Organisation aktiviert.
- Der delegierte AWS Security Incident Response-Administrator ist auf das Security Tooling-Konto eingestellt.
- Der Workflow zur proaktiven Reaktion und Alert-Triaging ist aktiviert.
- AWS Maßnahmen zur Eindämmung durch das Customer Incident Response Team (CIRT) sind autorisiert.

AWS Audit Manager

- Audit Manager ist für alle Mitgliedskonten aktiviert.
- Audit Manager wird automatisch für neue Mitgliedskonten aktiviert.
- Der delegierte Administrator von Audit Manager ist auf das Security Tooling-Konto eingestellt.
- AWS Config ist als Voraussetzung für Audit Manager aktiviert.
- Ein vom Kunden verwalteter Schlüssel wird für Daten verwendet, die in Audit Manager gespeichert sind.
- Das Standardziel für Bewertungsberichte ist konfiguriert.

IAM-Ressourcen

Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

AWS Identity and Access Management (IAM) ist zwar kein Service, der in einem herkömmlichen Architekturdiagramm enthalten ist, betrifft aber jeden Aspekt der AWS Organisation AWS-Konten, und. AWS-Services Sie können keine bereitstellen, AWS-Services ohne zuerst IAM-Entitäten zu erstellen und Berechtigungen zu erteilen. Eine vollständige Erläuterung von IAM würde den Rahmen dieses Dokuments sprengen, aber dieser Abschnitt enthält wichtige Zusammenfassungen von Empfehlungen für bewährte Verfahren und Hinweise auf zusätzliche Ressourcen.

- Bewährte Methoden für IAM finden Sie in der AWS Dokumentation unter Bewährte Methoden zur Sicherheit in IAM, in IAM-Artikeln im AWS Sicherheitsblog und in re:Invent-Präsentationen.AWS
- Die AWS Well-Architected-Sicherheitssäule beschreibt die wichtigsten Schritte im Prozess der Rechteverwaltung: Definition von Berechtigungsbarrieren, Gewährung von Zugriff mit geringsten Rechten, Analyse des öffentlichen und kontoübergreifenden Zugriffs, sichere gemeinsame Nutzung von Ressourcen, kontinuierliche Reduzierung von Berechtigungen und Einrichtung eines Notfallzugriffsprozesses.
- Die folgende Tabelle und die zugehörigen Hinweise bieten einen allgemeinen Überblick über empfohlene Anleitungen zu den verfügbaren IAM-Berechtigungsrichtlinien und deren Verwendung in Ihrer Sicherheitsarchitektur. Weitere Informationen finden Sie im Video AWS re:Invent 2020 zur Auswahl der richtigen Mischung von IAM-Richtlinien.

Anwendungsfall oder Richtlinie	Effect (Effekt)	Verwaltet von	Zweck	Bezieht sich auf	Wirkt	Eingesetzt in
Richtlinien zur Servicesteuerung (SCPs)	Restrict	Zentrales Team, z. B. Plattform- oder Sicherheitsteam [1]	Leitplanken, Unternehmensführung	Organisation, Organisationseinheit, Konto	Alle Principals in Organisation, OU und Konten	Konto für die Unternehmensverwaltung [2]

Richtlinien zur Ressourcenkontrolle (RCPs)	Restrict	Zentrales Team, z. B. Plattform- oder Sicherheitsteam [1]	Leitplanken, Unternehmensführung	Organisation, Organisationseinheit, Konto	Ressourcen in Mitgliedskonten [12]	Konto für die Unternehmensverwaltung [2]
Grundlegende Richtlinien zur Kontoautomatisierung (die IAM-Rollen, die von der Plattform für den Betrieb eines Kontos verwendet werden)	Gewähren und einschränken	Zentrales Team, z. B. Plattform-, Sicherheits- oder IAM-Team [1]	Berechtigungen für (grundlegende) Automatisierungsrollen ohne Arbeitslast [3]	Einzelkonto [4]	Prinzipale, die bei der Automatisierung innerhalb eines Mitgliedskontos verwendet werden	Mitgliedskonten

Grundlegende Personalrichtlinien (die IAM-Rollen, die Benutzern Berechtigungen zur Ausführung ihrer Arbeit gewähren)	Gewähren und einschränken	Zentrales Team, z. B. Plattform-, Sicherheits- oder IAM-Team [1]	Berechtigungen für menschliche Rollen [5]	Einzelkonto [4]	Verbundprinzipale [5] und IAM-Benutzer [6]	Mitgliedskonten
Berechtigungsgrenzen (maximale Berechtigungen, die ein autorisierter Entwickler einem anderen Principal zuweisen kann)	Restrict	Zentrales Team, z. B. Plattform-, Sicherheits- oder IAM-Team [1]	Leitplanken für Anwendungsrollen (müssen angewendet werden)	Einzelkonto [4]	Einzelne Rollen für eine Anwendung oder einen Workload in diesem Konto [7]	Mitgliedskonten

Richtlinien für Maschinenrollen für Anwendungen (Rolle, die der von Entwicklern bereitgestellten Infrastruktur zugewiesen ist)	Gewähren und einschränken	An Entwickler delegiert [8]	Genehmigung für die Anwendung oder den Workload [9]	Einzelkonto	Ein Principal in diesem Konto	Konten von Mitgliedern
Ressourcenrichtlinien	Gewähren und einschränken	An Entwickler delegiert [8,10]	Berechtigungen für Ressourcen	Einzelkonto	Ein Principal in einem Konto [11]	Konten von Mitgliedern
Zentrale Root-Benutzerverwaltung	Gewähren und einschränken	Zentrales Team, z. B. Plattform-, Sicherheits- oder IAM-Team [1]	Verwalten Sie die Root-Benutzer von Mitgliedskonten zentral und nach Bedarf	Organisation	Alle Root-Benutzer in Mitgliedskonten	Organisationsverwaltungskonto, delegiertes Administratorkonto

Hinweise aus der Tabelle:

1. Unternehmen verfügen über viele zentralisierte Teams (z. B. Teams für Cloud-Plattformen, Sicherheitsoperationen oder Identitäts- und Zugriffsmanagement), die die Zuständigkeiten dieser unabhängigen Kontrollen aufteilen und die Richtlinien gegenseitig überprüfen. Die Beispiele in

der Tabelle sind Platzhalter. Sie müssen die wirksamste Aufgabentrennung für Ihr Unternehmen festlegen.

2. Um es verwenden zu können SCPs, müssen Sie alle darin enthaltenen Funktionen aktivieren AWS Organizations.
3. Für die Automatisierung sind im Allgemeinen allgemeine Basisrollen und -richtlinien erforderlich, z. B. Berechtigungen für die Pipeline, Bereitstellungstools, Überwachungstools (z. B. AWS Lambda und AWS-Config-Regeln) und andere Berechtigungen. Diese Konfiguration wird in der Regel bereitgestellt, wenn das Konto bereitgestellt wird.
4. Diese beziehen sich zwar auf eine Ressource (z. B. eine Rolle oder eine Richtlinie) in einem einzelnen Konto, können jedoch mithilfe von repliziert oder für mehrere Konten bereitgestellt werden. AWS CloudFormation StackSets
5. Definieren Sie grundlegende menschliche Rollen und Richtlinien, die von einem zentralen Team auf alle Mitgliedskonten angewendet werden (häufig während der Kontobereitstellung). Beispiele hierfür sind die Entwickler im Plattformteam, das IAM-Team und die Sicherheitsprüfungsteams.
6. Verwenden Sie nach Möglichkeit einen Identitätsverbund (anstelle von lokalen IAM-Benutzern).
7. Berechtigungsgrenzen werden von delegierten Administratoren verwendet. Diese IAM-Richtlinie definiert die maximalen Berechtigungen und setzt andere Richtlinien außer Kraft (einschließlich `"*:*"` Richtlinien, die alle Aktionen für Ressourcen zulassen). Berechtigungsgrenzen sollten in den grundlegenden Personalrichtlinien als Voraussetzung für die Erstellung von Rollen (z. B. Rollen für die Leistung von Arbeitslasten) und das Anhängen von Richtlinien erforderlich sein. Zusätzliche Konfigurationen, z. B. die SCPs Erzwingung der Festlegung von Rechtegrenzen.
8. Dies setzt voraus, dass ausreichend Schutzmaßnahmen (z. B. SCPs und Rechtegrenzen) bereitgestellt wurden.
9. Diese optionalen Richtlinien könnten während der Kontobereitstellung oder als Teil des Anwendungsentwicklungsprozesses bereitgestellt werden. Die Genehmigung zum Erstellen und Anhängen dieser Richtlinien unterliegt den eigenen Berechtigungen des Anwendungsentwicklers.
10. Zusätzlich zu den lokalen Kontoberechtigungen verwaltet ein zentrales Team (z. B. das Cloud-Plattform-Team oder das Security Operations Team) häufig einige ressourcenbasierte Richtlinien, um einen kontenübergreifenden Zugriff für die Verwaltung der Konten zu ermöglichen (z. B. um Zugriff auf S3-Buckets für die Protokollierung zu gewähren).
11. Eine ressourcenbasierte IAM-Richtlinie kann sich auf jeden Prinzipal in jedem Konto beziehen, um den Zugriff auf dessen Ressourcen zu gewähren oder zu verweigern. Sie kann sich sogar auf anonyme Principals beziehen, um den öffentlichen Zugriff zu ermöglichen.

12 RCPs gelten für Ressourcen für eine Teilmenge von. AWS-Services Weitere Informationen finden Sie RCPs in der AWS Organizations Dokumentation unter Liste AWS-Services dieser Unterstützungen.

Um das Risiko eines böswilligen oder unbeabsichtigten Missbrauchs von Berechtigungen zu verringern, ist es von entscheidender Bedeutung, sicherzustellen, dass IAM-Identitäten nur über die Berechtigungen verfügen, die für eine genau abgegrenzte Reihe von Aufgaben erforderlich sind. Für die Einrichtung und Beibehaltung eines Modells mit den geringsten Rechten ist ein wohlüberlegter Plan zur kontinuierlichen Aktualisierung, Bewertung und Reduzierung übermäßiger Rechte erforderlich. Hier sind einige zusätzliche Empfehlungen für diesen Plan:

- Verwenden Sie das Governance-Modell Ihrer Organisation und die etablierte Risikobereitschaft, um spezifische Leitplanken und Genehmigungsgrenzen festzulegen.
- Implementieren Sie Least-Privilegien in einem kontinuierlich iterativen Prozess. Dies ist keine einmalige Übung.
- Wird verwendet SCPs , um umsetzbare Risiken zu reduzieren. Dabei handelt es sich um breit angelegte Leitplanken und nicht um eng begrenzte Kontrollen.
- Verwenden Sie Rechtegrenzen, um die IAM-Verwaltung sicherer zu delegieren.
  - Stellen Sie sicher, dass die delegierten Administratoren den Rollen und Benutzern, die sie erstellen, die entsprechende IAM-Grenzrichtlinie zuordnen.
- Verwenden Sie als defense-in-depth Ansatz (in Verbindung mit identitätsbasierten Richtlinien) ressourcenbasierte IAM-Richtlinien, um einen umfassenden Zugriff auf Ressourcen zu verweigern.
- Verwenden Sie IAM Access Advisor, IAM Access Analyzer und zugehörige Tools AWS CloudTrail, um regelmäßig den Nutzungsverlauf und die erteilten Berechtigungen zu analysieren. Korrigieren Sie sofort offensichtliche Überberechtigungen.
- Richten Sie allgemeine Aktionen gegebenenfalls auf bestimmte Ressourcen ein, anstatt ein Sternchen als Platzhalter für alle Ressourcen zu verwenden.
- Implementieren Sie einen Mechanismus, um IAM-Richtlinienausnahmen auf der Grundlage von Anfragen schnell zu identifizieren, zu überprüfen und zu genehmigen.

Code-Repository für AWS SRA-Beispiele

Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

Um Ihnen den Einstieg in die Erstellung und Implementierung der Leitlinien in der AWS SRA zu erleichtern, wird dieser Leitfaden von einem Infrastructure-as-Code-Repository (IaC) unter https://github.com/aws-samples/aws-security-reference-architecture-examples begleitet. Dieses Repository enthält Code, der Entwicklern und Ingenieuren bei der Implementierung einiger der in diesem Dokument vorgestellten Anleitungen und Architekturmuster hilft. Dieser Code basiert auf den Erfahrungen der Berater von AWS Professional Services mit Kunden aus erster Hand. Die Vorlagen sind allgemeiner Natur — sie dienen eher der Veranschaulichung eines Implementierungsmusters als der Bereitstellung einer vollständigen Lösung. Die AWS-Service Konfigurationen und Ressourcenbereitstellungen sind bewusst sehr restriktiv. Möglicherweise müssen Sie diese Lösungen modifizieren und an Ihre Umgebung und Ihre Sicherheitsanforderungen anpassen.

Das AWS SRA-Code-Repository bietet Codebeispiele sowohl mit Terraform-Bereitstellungsoptionen als AWS CloudFormation auch mit Terraform-Optionen. Die Lösungsmuster unterstützen zwei Umgebungen: eine erfordert AWS Control Tower und die andere ohne. AWS Organizations AWS Control Tower Die erforderlichen Lösungen in diesem Repository AWS Control Tower wurden in einer AWS Control Tower Umgebung mithilfe von und Customizations for AWS Control Tower (cFcT) bereitgestellt AWS CloudFormation und getestet. Lösungen, die dies nicht erfordern AWS Control Tower , wurden in einer AWS Organizations Umgebung getestet, indem AWS CloudFormation Die cFCT-Lösung hilft Kunden dabei, schnell eine sichere AWS Umgebung mit mehreren Konten einzurichten, die auf AWS bewährten Verfahren basiert. Sie hilft, Zeit zu sparen, indem sie die Einrichtung einer Umgebung für die Ausführung sicherer und skalierbarer Workloads automatisiert und gleichzeitig eine erste Sicherheitsbasis durch die Erstellung von Konten und Ressourcen implementiert. AWS Control Tower bietet außerdem eine Basisumgebung für den Einstieg in eine Architektur mit mehreren Konten, Identitäts- und Zugriffsmanagement, Governance, Datensicherheit, Netzwerkdesign und Protokollierung. Die Lösungen im AWS SRA-Repository bieten zusätzliche Sicherheitskonfigurationen zur Implementierung der in diesem Dokument beschriebenen Muster.

Hier finden Sie eine Zusammenfassung der Lösungen im AWS SRA-Repository. Jede Lösung enthält eine `README.md` Datei mit Details.

- Die CloudTrail Organisationslösung erstellt einen Organisationspfad innerhalb des Org Management-Kontos und delegiert die Verwaltung an ein Mitgliedskonto, z. B. das Audit- oder das Security Tooling-Konto. Dieser Trail wird mit einem vom Kunden verwalteten Schlüssel verschlüsselt, der im Security Tooling-Konto erstellt wurde, und überträgt die Protokolle an einen S3-Bucket im Log Archive-Konto. Optional können Datenereignisse für Amazon S3 und AWS Lambda Funktionen aktiviert werden. Ein Organisations-Trail protokolliert Ereignisse für alle Mitglieder AWS-Konten der AWS Organisation und verhindert gleichzeitig, dass Mitgliedskonten die Konfigurationen ändern.
- Die GuardDuty Organization-Lösung ermöglicht Amazon GuardDuty , die Verwaltung an das Security Tooling-Konto zu delegieren. Es konfiguriert GuardDuty innerhalb des Security Tooling-Kontos für alle bestehenden und future AWS Organisationskonten. Die GuardDuty Ergebnisse werden außerdem mit einem KMS-Schlüssel verschlüsselt und an einen S3-Bucket im Log Archive-Konto gesendet.
- Die Security Hub CSPM Organization-Lösung konfiguriert Security Hub CSPM, indem sie die Verwaltung an das Security Tooling-Konto delegiert. Es konfiguriert Security Hub CSPM innerhalb des Security Tooling-Kontos für alle bestehenden und future Unternehmenskonten. AWS Die Lösung bietet auch Parameter für die Synchronisierung der aktivierten Sicherheitsstandards für alle Konten und Regionen sowie für die Konfiguration eines Regionsaggregators innerhalb des Security Tooling-Kontos. Die Zentralisierung von Security Hub CSPM innerhalb des Security Tooling-Kontos bietet einen kontoübergreifenden Überblick über die Einhaltung von Sicherheitsstandards und die Ergebnisse von Integrationen von Drittanbietern. AWS-Services AWS Partner
- Die Inspector-Lösung konfiguriert Amazon Inspector innerhalb des delegierten Administratorkontos (Security Tooling) für alle Konten und kontrollierten Regionen innerhalb der Organisation. AWS
- Die Firewall Manager-Lösung konfiguriert AWS Firewall Manager Sicherheitsrichtlinien, indem sie die Verwaltung an das Security Tooling-Konto delegiert und Firewall Manager mit einer Sicherheitsgruppenrichtlinie und mehreren Richtlinien konfiguriert. AWS WAF Die Sicherheitsgruppenrichtlinie erfordert eine maximal zulässige Sicherheitsgruppe innerhalb einer VPC (vorhanden oder von der Lösung erstellt), die von der Lösung bereitgestellt wird.
- Die Macie Organization-Lösung ermöglicht Amazon Macie, indem sie die Verwaltung an das Security Tooling-Konto delegiert. Es konfiguriert Macie innerhalb des Security Tooling-Kontos für alle bestehenden und future AWS Organisationskonten. Macie ist außerdem so konfiguriert, dass es seine Erkennungsergebnisse an einen zentralen S3-Bucket sendet, der mit einem KMS-Schlüssel verschlüsselt ist.
- AWS Config:

  - Die Config Aggregator-Lösung konfiguriert einen AWS Config Aggregator, indem sie die Verwaltung an das Security Tooling-Konto delegiert. Die Lösung konfiguriert dann einen AWS Config Aggregator innerhalb des Security Tooling-Kontos für alle bestehenden und future Konten in der Organisation. AWS
  - Die Conformance Pack Organization Rules-Lösung wird bereitgestellt, AWS-Config-Regeln indem die Verwaltung an das Security Tooling-Konto delegiert wird. Anschließend erstellt es ein Organization Conformance Pack innerhalb des delegierten Administratorkontos für alle vorhandenen und future Konten in der AWS Organisation. Die Lösung ist so konfiguriert, dass sie die Beispielvorlage für das Konformitätspaket Operational Best Practices for Encryption and Key Management bereitstellt.
  - Die AWS Config Control Tower Management Account-Lösung aktiviert AWS Config das AWS Control Tower Verwaltungskonto und aktualisiert den AWS Config Aggregator im Security Tooling-Konto entsprechend. Die Lösung verwendet die AWS Control Tower CloudFormation Vorlage für die Aktivierung AWS Config als Referenz, um die Konsistenz mit den anderen Konten in der AWS Organisation sicherzustellen.
- IAM:
  - Die Access Analyzer-Lösung ermöglicht IAM Access Analyzer, indem sie die Verwaltung an das Security Tooling-Konto delegiert. Anschließend konfiguriert es einen IAM Access Analyzer auf Organisationsebene innerhalb des Security Tooling-Kontos für alle vorhandenen und future Konten in der Organisation. AWS Die Lösung stellt außerdem IAM Access Analyzer für alle Mitgliedskonten und Regionen bereit, um die Analyse von Berechtigungen auf Kontoebene zu unterstützen.
  - Die IAM Password Policy-Lösung aktualisiert die AWS-Konto Passwortrichtlinie für alle Konten in einer Organisation. AWS Die Lösung bietet Parameter für die Konfiguration der Passwortrichtlinieneinstellungen, damit Sie sich an die branchenüblichen Compliance-Standards anpassen können.
- Die EC2 Standard-EBS-Verschlüsselungslösung ermöglicht die standardmäßige Amazon EBS-Verschlüsselung auf Kontoebene innerhalb jedes Unternehmens AWS-Konto . AWS-Region AWS Sie erzwingt die Verschlüsselung neuer EBS-Volumes und -Snapshots, die Sie erstellen. Amazon EBS verschlüsselt beispielsweise die EBS-Volumes, die beim Starten einer Instance erstellt werden, und die Snapshots, die Sie aus einem unverschlüsselten Snapshot kopieren.
- Die S3 Block Account Public Access-Lösung ermöglicht Einstellungen auf Amazon S3 S3-Kontoebene innerhalb jedes AWS-Konto Unternehmens. AWS Die Amazon S3 Block Public Access-Funktion bietet Einstellungen für Zugriffspunkte, Buckets und Konten, mit denen Sie den öffentlichen Zugriff auf Amazon-S3-Ressourcen verwalten können. Standardmäßig erlauben neue

Buckets, Zugriffspunkte und Objekte keinen öffentlichen Zugriff. Benutzer können jedoch Bucket-Richtlinien, Zugriffspunkt-Richtlinien oder Objektberechtigungen ändern, um öffentlichen Zugriff zu ermöglichen. Die Einstellungen von Amazon S3 Block Public Access setzen diese Richtlinien und Berechtigungen außer Kraft, sodass Sie den öffentlichen Zugriff auf diese Ressourcen einschränken können.

- Die Detective Organization-Lösung automatisiert die Aktivierung von Amazon Detective, indem sie die Verwaltung an ein Konto (z. B. das Audit- oder Security Tooling-Konto) delegiert und Detective für alle bestehenden und future Konten konfiguriert. AWS Organizations
- Die Shield Advanced-Lösung automatisiert die Bereitstellung von AWS Shield Advanced , um einen erweiterten DDo S-Schutz für Ihre Anwendungen zu AWS bieten.
- Die AMI Bakery Organization-Lösung hilft dabei, den Prozess für die Erstellung und Verwaltung von standardmäßigen, gehärteten Amazon Machine Image (AMI) -Images zu automatisieren. Dies gewährleistet Konsistenz und Sicherheit in Ihren AWS Instances und vereinfacht die Bereitstellungs- und Wartungsaufgaben.
- Die Patch Manager-Lösung hilft dabei, das Patch-Management für mehrere AWS-Konten Benutzer zu optimieren. Sie können diese Lösung verwenden, um den AWS Systems Manager Agenten (SSM Agent) auf allen verwalteten Instanzen zu aktualisieren und kritische und wichtige Sicherheitspatches und Bugfixes auf markierten Windows- und Linux-Instanzen zu scannen und zu installieren. Die Lösung konfiguriert auch die Einstellung für die Standard-Host-Management-Konfiguration, um die Erstellung neuer Konten zu erkennen AWS-Konten und die Lösung automatisch für diese Konten bereitzustellen.

Mitwirkende

Hauptautor:

- Avik Mukherjee, Senior Security SA AWS

Mitwirkende:

- Jason Hurst, leitender Sicherheitsermittler bei AWS CIRT
- Abhishek Panday, Hauptproduktmanager — Technik AWS
- Itay Meller, leitender Spezialist SA AWS
- Jonathan VanKim, AWS Principal Security SA
- Josh Du Lac, Stratege für AWS Unternehmenssicherheit
- James Thompson, AWS leitender Lösungsarchitekt
- Jeremy Girven, AWS Spezialist SA
- Rodney Underkoffler, Senior Specialist SA AWS
- Farhan Farooq, leitender Lösungsarchitekt AWS
- Prashob Krishnan, technischer Kundenbetreuer AWS
- Meg Peddada, leitende Sicherheitsberaterin AWS
- Ashwin Phadke, leitender Lösungsarchitekt AWS
- Sowjanya Rajavaram, Senior Security SA AWS
- Tomek Jakubowski, leitender Berater AWS
- Arun Thomas, leitender Lösungsarchitekt AWS
- Ross Warren, Architekt für AWS Produktlösungen
- Scott Conklin, AWS leitender Berater
- Ilya Epshteyn, leitender Manager, Identitätslösungen AWS
- Michael Haken, leitender Technologe AWS
- Mehial Mendrin, leitender Berater AWS
- Christopher Evensen, AWS leitender technischer Kundenbetreuer

Überprüfung von:

- Eric Rose, AWS Principal Security SA
- Manoj Kumar, Lieferberater AWS

Technisches Schreiben:

- Handan Selamoglu, leitender technischer Redakteur AWS

Anhang: AWS Sicherheits-, Identitäts- und Compliance-Services

Beeinflussen Sie die future der AWS Security Reference Architecture (AWS SRA), indem Sie an einer kurzen Umfrage teilnehmen.

Eine Einführung oder Auffrischung finden Sie unter Sicherheit, Identität und Compliance AWS auf der AWS Website. Dort finden Sie eine Liste der Lösungen AWS-Services , die Ihnen helfen, Ihre Workloads und Anwendungen in der Cloud zu schützen. Diese Dienste sind in fünf Kategorien unterteilt: Datenschutz, Identitäts- und Zugriffsmanagement, Netzwerk- und Anwendungsschutz, Bedrohungserkennung und kontinuierliche Überwachung sowie Compliance und Datenschutz.

Datenschutz — AWS bietet Dienste, mit denen Sie Ihre Daten, Konten und Workloads vor unbefugtem Zugriff schützen können.

- Amazon Macie — Entdecken, klassifizieren und schützen Sie sensible Daten mit Sicherheitsfunktionen, die auf maschinellem Lernen basieren.
- AWS KMS— Erstellen und kontrollieren Sie die Schlüssel, die zur Verschlüsselung Ihrer Daten verwendet werden.
- AWS CloudHSM— Verwalten Sie Ihre Hardware-Sicherheitsmodule (HSMs) im AWS Cloud.
- AWS Certificate Manager— Bereitstellung, Verwaltung und Bereitstellung von SSL/TLS Zertifikaten zur Verwendung mit AWS-Services.
- AWS Secrets Manager— Rotation, Verwaltung und Abruf von Datenbankanmeldedaten, API-Schlüsseln und anderen Geheimnissen während ihres gesamten Lebenszyklus.

Identitäts- und Zugriffsmanagement — AWS Identitätsdienste ermöglichen Ihnen die sichere und skalierbare Verwaltung von Identitäten, Ressourcen und Berechtigungen.

- IAM — Kontrollieren Sie den Zugriff auf AWS-Services und Ressourcen sicher.
- IAM Identity Center — Verwalten Sie den SSO-Zugriff auf mehrere AWS-Konten Geschäftsanwendungen zentral.
- Amazon Cognito — Fügen Sie Benutzerregistrierung, Anmeldung und Zugriffskontrolle zu Ihren Web- und Mobilanwendungen hinzu.

- AWS Directory Service— Verwenden Sie verwaltetes Microsoft Active Directory in der AWS Cloud.
- AWS RAM— Teilen Sie AWS Ressourcen einfach und sicher.
- AWS Organizations— Implementieren Sie eine richtlinienbasierte Verwaltung für mehrere. AWS-Konten
- Von Amazon verifizierte Berechtigungen — Verwalten Sie skalierbare, detaillierte Berechtigungen und Autorisierungen in Ihren benutzerdefinierten Anwendungen.

Netzwerk- und Anwendungsschutz — Mit diesen Servicekategorien können Sie detaillierte Sicherheitsrichtlinien an Netzwerkkontrollpunkten in Ihrem Unternehmen durchsetzen. AWS-Services helfen Ihnen dabei, den Datenverkehr zu untersuchen und zu filtern, um unbefugten Zugriff auf Ressourcen auf Host-, Netzwerk- und Anwendungsebene zu verhindern.

- AWS Shield— Schützen Sie Ihre Webanwendungen, die weiterlaufen, mit Managed S Protection. AWS DDo
- AWS WAF— Schützen Sie Ihre Webanwendungen vor gängigen Web-Exploits und sorgen Sie für Verfügbarkeit und Sicherheit.
- AWS Firewall Manager— Konfigurieren und verwalten Sie AWS WAF anwendungsübergreifende AWS-Konten Regeln von einem zentralen Standort aus.
- AWS Systems Manager— Konfiguration und Verwaltung von Amazon EC2- und lokalen Systemen, um Betriebssystem-Patches anzuwenden, sichere System-Images zu erstellen und sichere Betriebssysteme zu konfigurieren.
- Amazon VPC — Stellen Sie einen logisch isolierten Bereich bereit, in AWS dem Sie AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können.
- AWS Network Firewall— Implementieren Sie wichtige Netzwerkschutzmaßnahmen für Ihr. VPCs
- Amazon Route 53 DNS-Firewall — Schützen Sie Ihre ausgehenden DNS-Anfragen vor Ihren VPCs.
- AWS Verified Access— Bieten Sie sicheren Zugriff auf Ihre Anwendungen, ohne virtuelle private Netzwerke (VPNs) zu benötigen.
- Amazon VPC Lattice — Vereinfachen Sie service-to-service Konnektivität, Sicherheit und Überwachung.

Bedrohungserkennung und kontinuierliche Überwachung — AWS Überwachungs- und Erkennungsservices bieten Anleitungen zur Identifizierung potenzieller Sicherheitsvorfälle in Ihrer AWS Umgebung.

- AWS Security Hub CSPM— Sehen und verwalten Sie Sicherheitswarnungen und automatisieren Sie Konformitätsprüfungen von einem zentralen Ort aus.
- AWS Security Hub— Korrelieren und ergänzen Sie die Sicherheitsergebnisse, um kritische Sicherheitsprobleme in Ihren Konten zu priorisieren und. AWS-Regionen
- Amazon GuardDuty — Schützen Sie Ihre AWS-Konten Workloads mit intelligenter Bedrohungserkennung und kontinuierlicher Überwachung.
- Amazon Inspector — Automatisieren Sie Sicherheitsbewertungen, um die Sicherheit und Konformität Ihrer Anwendungen zu verbessern, die auf bereitgestellt werden AWS.
- AWS Config— Erfassen und bewerten Sie die Konfigurationen Ihrer AWS Ressourcen, um Compliance-Prüfungen, die Nachverfolgung von Ressourcenänderungen und Sicherheitsanalysen zu ermöglichen.
- AWS-Config-Regeln— Erstellen Sie Regeln, die automatisch auf Änderungen in Ihrer Umgebung reagieren, z. B. das Isolieren von Ressourcen, das Anreichern von Ereignissen mit zusätzlichen Daten oder das Wiederherstellen eines zweifelsfrei funktionierenden Zustands der Konfiguration.
- AWS Security Incident Response— Automatisieren Sie die Reaktion, Untersuchung und Behebung von Sicherheitsvorfällen mit vorgefertigten Playbooks und Workflows.
- AWS CloudTrail— Verfolgen Sie die Benutzeraktivitäten und die API-Nutzung, um die Unternehmensführung sowie die Betriebs- und Risikoprüfung Ihres Systems zu ermöglichen. AWS-Konto
- Amazon Detective — Analysieren und visualisieren Sie Sicherheitsdaten, um schnell der Ursache potenzieller Sicherheitsprobleme auf den Grund zu gehen.
- AWS Lambda— Führen Sie Code aus, ohne Server bereitzustellen oder zu verwalten, sodass Sie Ihre programmierte, automatisierte Reaktion auf Vorfälle skalieren können.

Compliance und Datenschutz — AWS bietet Ihnen einen umfassenden Überblick über Ihren Compliance-Status und überwacht Ihre Umgebung kontinuierlich mithilfe automatisierter Konformitätsprüfungen, die auf den AWS bewährten Verfahren und Industriestandards basieren, die Ihr Unternehmen befolgt.

- AWS Artifact— Verwenden Sie ein kostenloses Self-Service-Portal, um bei Bedarf Zugriff auf AWS Sicherheits- und Compliance-Berichte und ausgewählte Online-Vereinbarungen zu erhalten.
- AWS Audit Manager— Überprüfen Sie Ihre AWS Nutzung kontinuierlich, um die Bewertung von Risiken und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

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
Umstrukturierung und Aktualisierung der Inhalte	• Anleitung für Security Hub und AWS Nitro Enclaves hinzugefügt. • Die AWS SRA wurde neu strukturiert, um sich auf die Kernarchitektur zu konzentrieren, und die vertieften Abschnitte wurden in separate Leitfäden für Identitätsmanagement, Perimetersicherheit, Cyberforensik, generative KI und IoT verschoben. • Bestehende Leitlinien wurden aktualisiert und enthalten nun zusätzliche Informationen für AWS CloudTrail Detective AWS Firewall Manager, Amazon GuardDuty, IAM Access Analyzer, Amazon Security Lake AWS Shield Advanced, und AWS Audit Manager. AWS Config	22. Dezember 2025
Wichtige Updates	• Es wurden Informationen zur neuen zentralisierten	29. August 2025

IAM-Zugriffsverwaltung für Root-Benutzer, zu Richtlinien zur Ressourcenkontrolle (RCPs) und zu deklarativen Richtlinien hinzugefügt.

- Die Security Hub CSPM-Verweise auf das neue Security Hub CSPM wurden aktualisiert.
- Beinhaltet neue Servicefunktionen für Amazon GuardDuty und Security Hub CSPM.
- AWS Security Incident Response Serviceanleitung hinzugefügt.
- Die detaillierten IAM-Leitlinien wurden aktualisiert und umfassen nun auch VPC Lattice für machine-to-machine das Identitätsmanagement.
- Es wurde eine neue ausführliche Anleitung hinzugefügt: SRA for IoT.

Ergänzungen und Klarstellungen	• Im Bereich Security Tooling-Konto wurden die AWS KMS Leitlinien aktualisiert. • Im Abschnitt Kundenidentitätsverwaltung wurden die Informationen zur Autorisierung von API Gateway erweitert. • Der Abschnitt Generative KI wurde aktualisiert, um Überlegungen zum Design von Organisationseinheiten und Konten hinzuzufügen. • Im Abschnitt AWS SRA-Code-Repository wurden Informationen zur neuen Patch Management-Lösung hinzugefügt.	12. September 2024

Wichtige Updates	• Zwei Abschnitte mit detaillierter Architekturberatung wurden hinzugefügt: Generative KI mit Amazon Bedrock und Identitätsmanagement. • Die AWS Identity and Access Management Access Analyzer CloudFrontBereiche Amazon Detective, Amazon Inspector AWS ArtifactAWS Config,,, Amazon Security Lake und Amazon wurden mit neuen Servicefunktionen aktualisiert. AWS Security Hub CSPM • Der Abschnitt zum AWS SRA-Code-Repository wurde um die neue Terraform-Bereitstellungsoption und die Hinzufügung von AMI AWS Shield Advanced Bakery-Lösungen erweitert.	7. Juni 2024

Wichtige Updates	• Die Abschnitte Netzwerkkonto und Anwendungskonto wurden aktualisiert, um Architekturrichtlinien für Amazon Verified Permissions und Amazon VPC Lattice hinzuzufügen. AWS Verified Access • Es wurden detaillierte Architekturanleitungen hinzugefügt, die auf Sicherheitsfunktionen basieren. • Es wurden neue Hinweise hinzugefügt, wie AI/ML mit AWS-Services dieser Methode bessere Sicherheitsergebnisse erzielt werden können. • Es wurden Hinweise zur schrittweisen Planung Ihrer Sicherheitsarchitektur hinzugefügt.	4. November 2023
Hinzufügung von Security Lake	Die Abschnitte Security Tooling-Konto und Log Archive-Konto wurden aktualisiert, um Designrichtlinien für Amazon Security Lake hinzuzufügen.	22. September 2023

Kleinere Updates	• Bestehende Leitlinien wurden aktualisiert, um neuen AWS-Services Funktionen und bewährten Methoden Rechnung zu tragen. • Aktualisierte Architekt urrichtlinien für AWS CloudTrail AWS IAM Identity Center, und Edge-Sich erheit.	10. Mai 2023
Umfrage	Es wurde eine kurze Umfrage hinzugefügt, um besser zu verstehen, wie Sie die AWS SRA in Ihrer Organisation einsetzen.	14. Dezember 2022
Quelldateien für Referenza rchitekturdiagramme	Im Abschnitt AWS Sicherhei tsreferenzarchitektur wurde eine Download-Datei hinzugefügt, die die Architekt urdiagramme für dieses Handbuch in bearbeitbarem PowerPoint Format bereitstellt.	17. November 2022
Updates für den Abschnitt Sicherheitsgrundlagen	Im Abschnitt Sicherhei tsgrundlagen wurden die Informationen zu den Säulen und Prinzipien des Sicherhei tsdesigns von Well-Architected Framework aktualisiert.	27. September 2022

Wichtige Ergänzungen und Updates	• Es wurden Informationen zur Verwendung der AWS SRA und wichtige Implementierungsrichtlinien hinzugefügt. • Architekturberatung für weitere Anwendungen AWS-Services wie AWS Artifact Amazon Inspector AWS RAM, Amazon Route 53,,, AWS Control Tower AWS Audit Manager Directory Service, Amazon Cognito und Network Access Analyzer hinzugefügt. • Bestehende Leitlinien wurden aktualisiert, um neuen AWS-Service Funktionen und bewährten Methoden Rechnung zu tragen.	25. Juli 2022
—	Erste Veröffentlichung	23. Juni 2021

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

Siehe 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 verarbeitet Transaktionen von verbindenden Anwendungen, 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.

maßgebliche 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 Einführung der Cloud (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 normalerweise 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 AWS für die 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 wird allgemein als Pipeline beschrieben. CI/CD kann 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 Abweichung 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.

Einsatz

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, z. B. unbeabsichtigte Fehlkonfigurationen oder ein Malware-Angriff.

Notfallwiederherstellung (DR)

Die Strategie und der Prozess, mit denen Sie Ausfallzeiten und Datenverluste aufgrund einer Katastrophe 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 Sicherheitsepen 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 CSPM, 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.

Daten zurückhalten

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 Infrastruktur als Code.

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

Siehe 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

Siehe Labelbasierte 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 Verfolgung, 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 Mitglied einer Organisation sein.

MES

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.

EICHE

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.

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. Diese Entität ist in der Regel ein 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 der Kontrolle entspricht, 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).

RAG

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 für die Erholungszeit.

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-Managementkonsole 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 Amazon EC2 EC2-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.

Eingabeaufforderung ohne Zwischenfälle

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.