Aufbau eines skalierbaren Vulnerability Management-Programms auf AWS

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: Aufbau eines skalierbaren Vulnerability Management-Programms auf AWS

Table of Contents

Aufbau eines skalierbaren Vulnerability Management-Programms auf AWS

Anna McAbee und Megan O'Neil, Amazon Web Services ()AWS

Oktober 2023 (Geschichte der Dokumente)

Abhängig von der zugrunde liegenden Technologie, die Sie verwenden, können in einer Cloud-Umgebung verschiedene Tools und Scans zu Sicherheitsergebnissen führen. Ohne Prozesse zur Verarbeitung dieser Erkenntnisse können sie sich anhäufen, was oft zu Tausenden bis Zehntausenden von Ergebnissen in kurzer Zeit führt. Mit einem strukturierten Schwachstellen-Management-Programm und einer ordnungsgemäßen Operationalisierung Ihrer Tools kann Ihr Unternehmen jedoch eine große Anzahl von Erkenntnissen aus unterschiedlichen Quellen verarbeiten und analysieren.

Das Vulnerability Management konzentriert sich auf die Entdeckung, Priorisierung, Bewertung, Behebung und Meldung von Sicherheitslücken. Das Patch-Management konzentriert sich dagegen auf das Patchen oder Aktualisieren von Software, um Sicherheitslücken zu beseitigen oder zu beheben. Das Patch-Management ist nur ein Aspekt des Schwachstellenmanagements. Im Allgemeinen empfehlen wir, sowohl einen patch-in-place Prozess (auch mitigate-in-placeProzess genannt) für kritische Patch-Now-Szenarien als auch einen Standardprozess einzurichten, den Sie regelmäßig ausführen, um gepatchte Amazon Machine Images (AMIs), Container oder Softwarepakete zu veröffentlichen. Diese Prozesse tragen dazu bei, Ihr Unternehmen darauf vorzubereiten, schnell auf eine Zero-Day-Sicherheitslücke zu reagieren. Bei kritischen Systemen in einer Produktionsumgebung kann die Verwendung eines patch-in-place Prozesses schneller und zuverlässiger sein als die Einführung eines neuen AMI für die gesamte Flotte. Für regelmäßig geplante Patches, wie Betriebssystem- (OS) und Softwarepatches, empfehlen wir, dass Sie beim Erstellen und Testen standardmäßige Entwicklungsprozesse verwenden, genau wie bei jeder Änderung auf Softwareebene. Dies bietet eine bessere Stabilität für Standardbetriebsmodi. Sie können Patch Manager, eine Funktion von AWS Systems Manager oder andere Produkte von Drittanbietern als patch-in-place Lösungen verwenden. Weitere Informationen zur Verwendung von Patch Manager finden Sie unter Patch-Management im AWS Cloud Adoption Framework: Operations Perspective. Außerdem können Sie EC2 Image Builder verwenden, um die Erstellung, Verwaltung und Bereitstellung von benutzerdefinierten Images und up-to-date Server-Images zu automatisieren.

Der Aufbau eines skalierbaren Vulnerability Management-Programms AWS beinhaltet neben Cloud-Konfigurationsrisiken auch die Verwaltung herkömmlicher Software- und Netzwerkschwachstellen.

Ein Cloud-Konfigurationsrisiko, wie z. B. ein unverschlüsselter Amazon Simple Storage Service (Amazon S3) -Bucket, sollte einem ähnlichen Triage- und Behebungsprozess folgen wie eine Softwareschwachstelle. In beiden Fällen muss das Anwendungsteam für die Sicherheit seiner Anwendung, einschließlich der zugrunde liegenden Infrastruktur, verantwortlich sein und dafür verantwortlich sein. Diese Eigentumsverteilung ist entscheidend für ein effektives und skalierbares Schwachstellen-Management-Programm.

In diesem Leitfaden wird erläutert, wie die Identifizierung und Behebung von Sicherheitslücken optimiert werden kann, um das Gesamtrisiko zu reduzieren. Verwenden Sie die folgenden Abschnitte, um Ihr Schwachstellen-Management-Programm aufzubauen und weiterzuentwickeln:

1. Vorbereitung — Bereiten Sie Ihre Mitarbeiter, Prozesse und Technologien darauf vor, Sicherheitslücken in Ihrer Umgebung zu identifizieren, zu bewerten und zu beheben.
2. Triage und Behebung — Leite die Sicherheitsergebnisse an die relevanten Beteiligten weiter, identifiziere die geeigneten Abhilfemaßnahmen und ergreife dann die entsprechenden Abhilfemaßnahmen.
3. Berichterstattung und Verbesserung — Verwenden Sie Berichtsmechanismen, um Verbesserungsmöglichkeiten zu identifizieren, und führen Sie anschließend Ihr Schwachstellen-Management-Programm weiter aus.

Der Aufbau eines Cloud-Vulnerability Management-Programms erfordert oft mehrere Wiederholungen. Priorisieren Sie die Empfehlungen in diesem Leitfaden und überprüfen Sie regelmäßig Ihren Backlog, um über technologische Veränderungen und Ihre Geschäftsanforderungen auf dem Laufenden zu bleiben.

Zielgruppe

Dieser Leitfaden richtet sich an große Unternehmen mit drei Hauptteams, die für sicherheitsrelevante Erkenntnisse verantwortlich sind: ein Sicherheitsteam, ein Cloud Center of Excellence (CCoE) oder ein Cloud-Team und Anwendungs- (oder Entwickler -) Teams. Dieser Leitfaden verwendet die gängigsten Betriebsmodelle von Unternehmen und baut auf diesen Betriebsmodellen auf, um eine effizientere Reaktion auf Sicherheitserkenntnisse zu ermöglichen und die Sicherheitsergebnisse zu verbessern. Organizations, die AWS dies verwenden, haben möglicherweise unterschiedliche Strukturen und Betriebsmodelle. Sie können jedoch viele der Konzepte in diesem Handbuch ändern, um sie an unterschiedliche Betriebsmodelle und kleinere Organisationen anzupassen.

Ziele

Dieser Leitfaden kann Ihnen und Ihrer Organisation helfen:

- Entwickeln Sie Richtlinien, um das Schwachstellenmanagement zu optimieren und die Rechenschaftspflicht sicherzustellen
- Richten Sie Mechanismen ein, um die Verantwortung für die Sicherheit auf die Anwendungsteams zu verteilen
- Konfigurieren Sie die relevanten AWS-Services Komponenten gemäß den Best Practices für ein skalierbares Schwachstellenmanagement
- Verteilen Sie die Eigentumsrechte an den Sicherheitsergebnissen
- Richten Sie Mechanismen ein, um über Ihr Schwachstellen-Management-Programm zu berichten und es weiterzuentwickeln
- Verbessern Sie die Sichtbarkeit von Sicherheitslücken und verbessern Sie die allgemeine Sicherheitslage

Bereiten Sie Ihr skalierbares Vulnerability Management-Programm vor

Zur Vorbereitung eines skalierbaren Schwachstellen-Management-Programms gehören die Schulung der Mitarbeiter, die Entwicklung von Prozessen und die Implementierung der richtigen Technologie gemäß den bewährten Verfahren. Mitarbeiter, Prozesse und Technologien sind für ein effektives Schwachstellen-Management-Programm gleichermaßen wichtig, und Sie müssen sie eng integrieren, um Sicherheitslücken in großem Umfang zu managen.

In diesem Abschnitt des Leitfadens werden die grundlegenden Maßnahmen beschrieben, die Sie ergreifen können, um Ihr skalierbares Schwachstellen-Management-Programm vorzubereiten. AWS

Themen

Definieren Sie einen Plan für das Schwachstellenmanagement

Der erste Schritt bei der Vorbereitung Ihres Cloud-Vulnerability Management-Programms ist die Definition Ihres Schwachstellen-Management-Plans. Dieser Plan umfasst die Richtlinien und Prozesse, denen Ihr Unternehmen folgt. Dieser Plan sollte dokumentiert und für alle Beteiligten zugänglich sein. Ein Schwachstellenmanagementplan ist ein Dokument auf hoher Ebene, das in der Regel die folgenden Abschnitte umfasst:

- Ziele und Umfang — Erläutern Sie die Ziele, Funktionen und den Umfang des Schwachstellenmanagements.
- Rollen und Zuständigkeiten — Führen Sie die Akteure des Schwachstellenmanagements auf und erläutern Sie deren Zuständigkeiten.

- Definitionen des Schweregrads und der Priorisierung von Sicherheitslücken — Legen Sie fest, wie der Schweregrad einer Sicherheitslücke klassifiziert und wie sie priorisiert werden soll.
- Service Level Agreements (SLAs) für die Behebung — Definieren Sie für jeden Schweregrad, wie viel Zeit dem Eigentümer der Behebung maximal zur Verfügung steht, um eine Sicherheitslücke zu beheben. Da die Einhaltung von SLAs ein integraler Bestandteil eines effektiven und skalierbaren Schwachstellen-Management-Programms ist, sollten Sie sich überlegen, wie Sie nachverfolgen können, ob Sie diese SLAs einhalten.
- Ausnahmeprozess — Erläutern Sie den Prozess der Einreichung, Genehmigung und Aktualisierung von Ausnahmen. Dieser Prozess sollte sicherstellen, dass Ausnahmen legitim und zeitgebunden sind und nachverfolgt werden.
- Informationsquellen zu Sicherheitslücken — Führen Sie die Quellen oder Tools auf, die zu Sicherheitsergebnissen führen. Weitere Informationen dazu AWS-Services , die Quellen für Sicherheitserkenntnisse sein könnten, finden Sie Sicherheitsdienste konfigurieren AWS in diesem Handbuch.

Obwohl diese Abschnitte in Unternehmen unterschiedlicher Größe und Branche üblich sind, ist der Schwachstellen-Management-Plan jedes Unternehmens einzigartig. Sie müssen einen Plan für das Schwachstellenmanagement erstellen, der für Ihr Unternehmen am besten geeignet ist. Gehen Sie davon aus, dass Sie Ihren Plan im Laufe der Zeit wiederholen werden, um die gewonnenen Erkenntnisse und die sich weiterentwickelnden Technologien zu berücksichtigen.

Verteilen Sie die Eigentumsrechte an

Das Modell der AWS gemeinsamen Verantwortung definiert, wie AWS und die Kunden gemeinsam die Verantwortung für Cloud-Sicherheit und Compliance übernehmen. In diesem Modell wird die Infrastruktur AWS gesichert, auf der alle in der angebotenen Dienste ausgeführt werden AWS Cloud, und die AWS Kunden sind für den Schutz ihrer Daten und Anwendungen verantwortlich.

Sie können dieses Modell innerhalb Ihres Unternehmens widerspiegeln und die Verantwortlichkeiten zwischen Ihren Cloud- und Anwendungsteams verteilen. Auf diese Weise können Sie Ihre Cloud-Sicherheitsprogramme effektiver skalieren, da die Anwendungsteams die Verantwortung für bestimmte Sicherheitsaspekte ihrer Anwendungen übernehmen. Die einfachste Interpretation des Modells der gemeinsamen Verantwortung ist, dass Sie für die Sicherheit dieser Ressource verantwortlich sind, wenn Sie Zugriff auf die Konfiguration der Ressource haben.

Ein wichtiger Teil der Verteilung von Sicherheitsaufgaben auf Anwendungsteams ist die Entwicklung von Self-Service-Sicherheitstools, die Ihren Anwendungsteams bei der Automatisierung helfen. Anfänglich kann dies eine gemeinsame Anstrengung sein. Das Sicherheitsteam kann Sicherheitsanforderungen in Tools zum Scannen von Code umsetzen, und dann können Anwendungsteams diese Tools verwenden, um Lösungen zu entwickeln und mit ihrer internen Entwickler-Community zu teilen. Dies trägt zu einer höheren Effizienz anderer Teams bei, die ähnliche Sicherheitsanforderungen erfüllen müssen.

In der folgenden Tabelle werden die Schritte zur Verteilung der Eigentumsrechte an die Anwendungsteams beschrieben und es werden Beispiele aufgeführt.

Schritt	Aktion	Beispiel
1	Definieren Sie Ihre Sicherheitsanforderungen — Was möchten Sie erreichen ? Dies kann auf einen Sicherheitsstandard oder eine Compliance-Anforderung zurückzuführen sein.	Ein Beispiel für eine Sicherheitsanforderung ist der Zugriff mit den geringsten Rechten für Anwendungsidentitäten.
2	Kontrollen für eine Sicherheitsanforderung aufzählen — Was bedeutet diese Anforderung eigentlich aus Kontrollsicht? Was muss ich tun, um dies zu erreichen?	Um die geringste Zugriffsberechtigung für Anwendungsidentitäten zu erreichen, gibt es im Folgenden zwei Beispiele für Steuerelemente: • Verwenden Sie AWS Identity and Access Management (IAM-) Rollen • Verwenden Sie in IAM-Richtlinien keine Platzhalter
3	Dokumentierter Leitfaden für die Kontrollen — Welche Hinweise können Sie Entwicklern mit diesen	Zunächst könnten Sie mit der Dokumentation einfacher Beispielrichtlinien beginnen, darunter sichere

Schritt	Aktion	Beispiel
	Kontrollen geben, um sie bei der Einhaltung der Kontrollen zu unterstützen?	und unsichere IAM-Richt linien und Bucket-Richtlinien für Amazon Simple Storage Service (Amazon S3). Als Nächstes können Sie Lösungen zum Scannen von Richtlinien in CI/CD-Pipelines (Continuous Integration and Continuous Delivery) einbetten , z. B. mithilfe von Regeln für die proaktive Bewertung.AWS Config
4	Wiederverwendbare Artefakte entwickeln — Können Sie es anhand der Anleitung noch einfacher machen und wiederverwendbare Artefakte für Entwickler entwickeln?	Sie könnten Infrastructure-as-Code (IaC) erstellen, um IAM-Richtlinien bereitzustellen, die dem Prinzip der geringste n Rechte folgen. Sie können diese wiederverwendbaren Artefakte in einem Code-Repo sitory speichern.

Self-Service funktioniert möglicherweise nicht für alle Sicherheitsanforderungen, aber er kann für Standardszenarien funktionieren. Wenn Unternehmen diese Schritte befolgen, können sie ihre Anwendungsteams in die Lage versetzen, einen größeren Teil ihrer eigenen Sicherheitsaufgaben auf skalierbare Weise zu übernehmen. Insgesamt führt das Modell der verteilten Verantwortung in vielen Organisationen zu mehr kollaborativen Sicherheitspraktiken.

Entwickeln Sie ein Programm zur Offenlegung von Sicherheitslücken

Als defense-in-depthAnsatz für das Schwachstellenmanagement sollten Sie ein Programm zur Offenlegung von Sicherheitslücken einrichten, damit Personen innerhalb oder außerhalb Ihres Unternehmens Sicherheitslücken oder -risiken melden können.

Richten Sie für Personen innerhalb Ihres Unternehmens ein Verfahren zur Meldung von Risiken oder Sicherheitslücken ein. Dies kann über ein Ticketsystem oder per E-Mail erfolgen. Unabhängig davon, für welchen Prozess Sie sich entscheiden, ist es wichtig, dass Ihre Mitarbeiter sich des Prozesses bewusst sind und alle Sicherheitslücken oder Risiken, auf die sie stoßen, problemlos melden können.

Richten Sie für Personen außerhalb Ihres Unternehmens eine externe Webseite ein, auf der potenzielle Sicherheitslücken gemeldet werden können. Ein Beispiel finden Sie auf der Webseite AWS Vulnerability Reporting. Diese Webseite sollte auch Offenlegungsrichtlinien enthalten, um die Daten und Vermögenswerte Ihres Unternehmens zu schützen. Ein Programm zur Offenlegung von Sicherheitslücken sollte potenziell schädliche Aktivitäten nicht fördern. Daher ist es wichtig, dass Sie klare Richtlinien mit Richtlinien haben. Der Aufbau eines ausgereiften, verantwortungsvollen Offenlegungsprogramms ist ein Ziel, das Sie im Zuge der Weiterentwicklung Ihres Programms anstreben sollten. Die meisten beginnen nicht mit einem externen Offenlegungsprogramm, und es braucht Zeit, bis es richtig ist.

Bereite deine AWS Umgebung vor

Stellen Sie vor der Implementierung von Tools für das Schwachstellenmanagement sicher, dass Ihre AWS Umgebung so konzipiert ist, dass sie ein skalierbares Schwachstellen-Management-Programm unterstützt. Die Struktur der Tagging-Richtlinien von Ihnen AWS-Konten und Ihrer Organisation kann den Aufbau eines skalierbaren Schwachstellen-Management-Programms vereinfachen.

Entwickeln Sie eine Struktur AWS-Konto

AWS Organizationshilft dabei, eine AWS Umgebung zentral zu verwalten und zu steuern, wenn Ihr Unternehmen wächst und seine AWS Ressourcen skaliert. Eine Organisation in AWS Organizations konsolidiert Sie AWS-Konten in logische Gruppen oder Organisationseinheiten, sodass Sie sie als eine einzige Einheit verwalten können. Sie verwalten AWS Organizations von einem speziellen Konto aus, dem sogenannten Verwaltungskonto. Weitere Informationen zu finden Sie unter Terminologie und Konzepte für AWS Organizations.

Wir empfehlen Ihnen, Ihre Umgebung mit AWS mehreren Konten in AWS Organizations zu verwalten. Auf diese Weise können Sie ein vollständiges Inventar der Konten und Ressourcen Ihres Unternehmens erstellen. Dieses vollständige Asset-Inventar ist ein wichtiger Aspekt des Schwachstellenmanagements. Anwendungsteams sollten keine Konten verwenden, die sich außerhalb des Unternehmens befinden.

AWS Control Towerhilft Ihnen bei der Einrichtung und Verwaltung einer Umgebung AWS mit mehreren Konten und folgt dabei den vorgeschriebenen Best Practices. Wenn Sie noch keine Umgebung mit mehreren Konten eingerichtet haben, AWS Control Tower ist dies ein guter Ausgangspunkt.

Wir empfehlen, die spezielle Kontostruktur und die in der AWS Security Reference Architecture (AWS SRA) beschriebenen bewährten Methoden zu verwenden. Das Security Tooling-Konto sollte als delegierter Administrator für Ihre Sicherheitsdienste dienen. Weitere Informationen zur Konfiguration Ihrer Vulnerability Management-Tools in diesem Konto finden Sie weiter unten in diesem Handbuch. Hosten Sie Anwendungen in speziellen Konten in der Workloads Organization Unit (OU). Dadurch wird eine starke Isolierung auf Workload-Ebene und explizite Sicherheitsgrenzen für jede Anwendung eingeführt. Informationen zu den Entwurfsprinzipien und den Vorteilen eines Ansatzes mit mehreren Konten finden Sie unter Organizing Your AWS Environment Using Multi-Accounts (AWS Whitepaper).

Eine gezielte Kontostruktur und die zentrale Verwaltung von Sicherheitsdiensten von einem speziellen Konto aus sind wichtige Aspekte eines skalierbaren Schwachstellen-Management-Programms.

Definieren, implementieren und durchsetzen

Tags sind Schlüssel-Wert-Paare, die als Metadaten für die Organisation Ihrer AWS Ressourcen dienen. Weitere Informationen finden Sie unter Markieren Ihrer AWS -Ressourcen. Sie können Tags verwenden, um Geschäftskontext bereitzustellen, z. B. Geschäftseinheit, Anwendungsinhaber, Umgebung und Kostenstelle. Die folgende Tabelle zeigt eine Reihe von Beispiel-Tags.

Schlüssel	Wert
BusinessUnit	HumanResources
CostCenter	CC101
ApplicationTeam	HumanResourcesTechnology
Umgebung	Produktion

Mithilfe von Stichwörtern können Sie Ergebnisse priorisieren. Es kann dir zum Beispiel helfen:

- Identifizieren Sie den Besitzer einer Ressource, der für das Patchen einer Sicherheitslücke verantwortlich ist
- Verfolgen Sie, welche Anwendungen oder Geschäftsbereiche über eine große Anzahl von Ergebnissen verfügen
- Erhöhen Sie den Schweregrad der Ergebnisse bei bestimmten Datenklassifizierungen, z. B. bei personenbezogenen Daten (PII) oder Daten der Zahlungskartenbranche (PCI)
- Identifizieren Sie den Datentyp in der Umgebung, z. B. Testdaten in einer untergeordneten Entwicklungsumgebung oder Produktionsdaten

Folgen Sie den Anweisungen unter Aufbau Ihrer Tagging-Strategie in Best Practices for Tagging Resources (Whitepaper), damit Sie effektives Tagging in großem Umfang erreichen können. AWS AWS

Überwachen Sie die Sicherheitsbulletins AWS

Wir empfehlen dringend, die AWS Sicherheitsbulletins regelmäßig und regelmäßig zu überprüfen. Sicherheitsbulletins können Sie über neue sicherheitsrelevante Sicherheitslücken, betroffene Dienste und entsprechende Updates informieren. Sie können auch einen RSS-Feed für die Sicherheitsbulletins abonnieren und im Rahmen Ihres Schwachstellen-Management-Programms einen Prozess zur Erfassung und Behebung dieser Bulletins einrichten.

Sicherheitsdienste konfigurieren AWS

AWS bietet eine Vielzahl von Sicherheitsdiensten, die zum Schutz Ihrer AWS Umgebung entwickelt wurden. Für Ihr Vulnerability Management-Programm empfehlen wir, dass Sie AWS-Services in jedem Konto Folgendes aktivieren:

- Amazon GuardDuty hilft Ihnen dabei, aktive Bedrohungen in Ihrer Umgebung zu erkennen. Ein GuardDuty Ergebnis könnte Ihnen helfen, eine unbekannte Sicherheitslücke zu identifizieren, die in Ihrer Umgebung ausgenutzt wurde. Es könnte Ihnen auch helfen, die Auswirkungen einer nicht gepatchten Sicherheitsanfälligkeit zu verstehen.
- AWS Healthbietet fortlaufenden Einblick in die Leistung Ihrer Ressourcen und die Verfügbarkeit Ihrer Konten AWS-Services .
- AWS Identity and Access Management Access Analyzeranalysiert die ressourcenbasierten Richtlinien in Ihrer AWS Umgebung, um Ressourcen zu identifizieren, die gemeinsam mit einer

externen Entität genutzt werden. Auf diese Weise können Sie Sicherheitslücken identifizieren, die durch unbeabsichtigten Zugriff auf Ihre Ressourcen und Daten entstehen. Für jede Instance einer Ressource, die außerhalb Ihres Kontos geteilt wird, generiert IAM Access Analyzer ein Ergebnis.

- Amazon Inspector ist ein Schwachstellen-Management-Service, der Ihre AWS Workloads kontinuierlich auf Software-Schwachstellen und unbeabsichtigte Netzwerkbedrohungen überprüft.
- AWS Security Hubhilft Ihnen dabei, Ihre AWS Umgebung anhand der Sicherheitsstandards der Branche zu überprüfen und Risiken bei der Cloud-Konfiguration zu identifizieren. Es bietet auch einen umfassenden Überblick über Ihren AWS Sicherheitsstatus, indem es die Ergebnisse anderer AWS Sicherheitsdienste und Sicherheitstools von Drittanbietern zusammenfasst.

In diesem Abschnitt wird beschrieben, wie Sie Amazon Inspector und Security Hub aktivieren und konfigurieren, damit Sie ein skalierbares Schwachstellen-Management-Programm einrichten können.

Verwendung von Amazon Inspector in Ihrem Vulnerability Management-Programm

Amazon Inspector ist ein Schwachstellen-Management-Service, der Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Amazon Elastic Container Registry (Amazon ECR) Container-Images und AWS Lambda Funktionen kontinuierlich auf Softwareschwachstellen und unbeabsichtigte Netzwerkgefährdung überprüft. Mit Amazon Inspector können Sie sich einen Überblick verschaffen und die Behebung von Softwareschwachstellen in Ihren AWS Umgebungen priorisieren.

Amazon Inspector bewertet Ihre Umgebung kontinuierlich während des gesamten Lebenszyklus Ihrer Ressourcen. Als Reaktion auf Änderungen, die zu einer neuen Sicherheitslücke führen könnten, werden Ressourcen automatisch erneut gescannt. Es scannt beispielsweise erneut, wenn Sie ein neues Paket auf einer EC2-Instance installieren, wenn Sie einen Patch installieren oder wenn ein neues CVE (Common Vulnerabilities and Exposures) veröffentlicht wird, das sich auf die Ressource auswirkt. Wenn Amazon Inspector eine Sicherheitslücke oder einen offenen Netzwerkpfad identifiziert, wird ein Ergebnis generiert, das Sie untersuchen können. Das Ergebnis bietet umfassende Informationen über die Sicherheitsanfälligkeit, einschließlich der folgenden Informationen:

- Amazon Inspector-Risikobewertung
- Bewertung des Common Vulnerability Scoring System (CVSS)
- Betroffene Ressource

- Schwachstelleninformationen über das CVE von Amazon Recorded Future, und Cybersecurity and Infrastructure Security Agency (CISA)
- Empfehlungen zur Problembehebung

Anweisungen zur Einrichtung von Amazon Inspector finden Sie unter Erste Schritte mit Amazon Inspector. Der Schritt Amazon Inspector aktivieren in diesem Tutorial bietet zwei Konfigurationsoptionen: eine eigenständige Kontoumgebung und eine Umgebung mit mehreren Konten. Wir empfehlen die Verwendung der Umgebungsoption mit mehreren Konten, wenn Sie mehrere AWS-Konten Mitglieder einer Organisation überwachen möchten. AWS Organizations

Wenn Sie Amazon Inspector für eine Umgebung mit mehreren Konten einrichten, bestimmen Sie ein Konto in der Organisation als delegierten Amazon Inspector-Administrator. Der delegierte Administrator kann die Ergebnisse und einige Einstellungen für Organisationsmitglieder verwalten. Der delegierte Administrator kann beispielsweise die Details der aggregierten Ergebnisse für alle Mitgliedskonten einsehen, Scans für Mitgliedskonten aktivieren oder deaktivieren und gescannte Ressourcen überprüfen. Die AWS SRA empfiehlt, dass Sie ein Security Tooling-Konto erstellen und es als delegierten Amazon Inspector-Administrator verwenden.

Verwendung AWS Security Hub in Ihrem Vulnerability Management-Programm

Der Aufbau eines skalierbaren Schwachstellen-Management-Programms AWS beinhaltet neben Cloud-Konfigurationsrisiken auch das Management herkömmlicher Software- und Netzwerkschwachstellen. AWS Security Hubhilft Ihnen dabei, Ihre AWS Umgebung anhand der Sicherheitsstandards der Branche zu überprüfen und Risiken bei der Cloud-Konfiguration zu identifizieren. Security Hub bietet auch einen umfassenden Überblick über Ihren Sicherheitsstatus, AWS indem es Sicherheitsergebnisse von anderen Sicherheitsdiensten und AWS Sicherheitstools von Drittanbietern zusammenfasst.

In den folgenden Abschnitten finden Sie bewährte Methoden und Empfehlungen für die Einrichtung von Security Hub zur Unterstützung Ihres Vulnerability Management-Programms:

- Security Hub einrichten
- Security Hub Hub-Standards aktivieren
- Verwaltung der Security Hub Hub-Ergebnisse
- Zusammenfassung der Ergebnisse anderer Sicherheitsdienste und -tools

Security Hub einrichten

Anweisungen zur Einrichtung finden Sie unter Einrichtung AWS Security Hub. Um Security Hub verwenden zu können, müssen Sie es aktivieren AWS Config. Weitere Informationen finden Sie unter Aktivierung und Konfiguration AWS Config in der Security Hub Hub-Dokumentation.

Wenn Sie integriert sind AWS Organizations, bestimmen Sie über das Organisationsverwaltungskonto ein Konto als delegierten Security Hub-Administrator. Eine Anleitung finden Sie unter Den delegierten Security Hub-Administrator benennen. Die AWS SRA empfiehlt, dass Sie ein Security Tooling-Konto erstellen und es als delegierten Security Hub-Administrator verwenden.

Der delegierte Administrator hat automatisch Zugriff darauf, Security Hub für alle Mitgliedskonten in der Organisation zu konfigurieren und die mit diesen Konten verknüpften Ergebnisse einzusehen. Wir empfehlen Ihnen, AWS Config Security Hub in allen AWS-Regionen Ihren zu aktivieren AWS-Konten. Sie können Security Hub so konfigurieren, dass neue Organisationskonten automatisch als Security Hub Hub-Mitgliedskonten behandelt werden. Anweisungen finden Sie unter Mitgliedskonten verwalten, die zu einer Organisation gehören.

Security Hub Hub-Standards aktivieren

Security Hub generiert Ergebnisse, indem es automatisierte und kontinuierliche Sicherheitsprüfungen anhand von Sicherheitskontrollen durchführt. Die Kontrollen sind mit einem oder mehreren Sicherheitsstandards verknüpft. Mithilfe der Kontrollen können Sie feststellen, ob die Anforderungen eines Standards erfüllt werden.

Wenn Sie einen Standard in Security Hub aktivieren, aktiviert Security Hub automatisch die Kontrollen, die für den Standard gelten. Security Hub verwendet AWS Config Regeln, um die meisten Sicherheitsprüfungen für Kontrollen durchzuführen. Sie können die Security Hub Hub-Standards jederzeit aktivieren oder deaktivieren. Weitere Informationen finden Sie unter Sicherheitskontrollen und -standards unter AWS Security Hub. Eine vollständige Liste der Standards finden Sie unter Security Hub Hub-Standardreferenz.

Wenn Ihr Unternehmen noch keinen bevorzugten Sicherheitsstandard hat, empfehlen wir die Verwendung des FSBP-Standards (AWS Foundational Security Best Practices). Dieser Standard wurde entwickelt, um zu erkennen, wann AWS-Konten und welche Ressourcen von den bewährten Sicherheitsmethoden abweichen. AWS kuratiert diesen Standard und aktualisiert ihn regelmäßig, um neue Funktionen und Dienste abzudecken. Nach der Prüfung der FSBP-Ergebnisse sollten Sie erwägen, andere Standards zu aktivieren.

Verwaltung der Security Hub Hub-Ergebnisse

Security Hub bietet mehrere Funktionen, die Ihnen helfen, große Mengen von Erkenntnissen aus Ihrem gesamten Unternehmen zu verarbeiten und den Sicherheitsstatus Ihrer AWS Umgebung zu verstehen. Um Ihnen bei der Verwaltung der Ergebnisse zu helfen, empfehlen wir, die folgenden beiden Security Hub Hub-Funktionen zu aktivieren:

- Verwenden Sie die regionsübergreifende Aggregation, um Ergebnisse zu aggregieren, Updates und Erkenntnisse zu finden, den Compliance-Status und Sicherheitswerte aus mehreren Regionen in einer einzigen Aggregationsregion AWS-Regionen zu kontrollieren.
- Verwenden Sie konsolidierte Kontrollergebnisse, um das Auffinden von Ergebnissen zu reduzieren, indem Sie doppelte Ergebnisse entfernen. Wenn konsolidierte Kontrollbefunde in Ihrem Konto aktiviert sind, generiert Security Hub für jede Sicherheitsüberprüfung einer Kontrolle ein einzelnes neues Ergebnis oder ein Befundupdate, auch wenn eine Kontrolle für mehrere aktivierte Standards gilt.

Zusammenfassung der Ergebnisse anderer Sicherheitsdienste und -tools

Zusätzlich zur Generierung von Sicherheitsergebnissen können Sie Security Hub verwenden, um Funddaten aus verschiedenen AWS-Services und unterstützten Sicherheitslösungen von Drittanbietern zu aggregieren. Dieser Abschnitt konzentriert sich auf das Senden von Sicherheitsergebnissen an Security Hub. Im nächsten Abschnitt,Bereiten Sie sich auf die Zuordnung von Sicherheitsergebnissen vor, wird erläutert, wie Sie Security Hub in Produkte integrieren können, die Erkenntnisse von Security Hub erhalten können.

Es gibt viele AWS-Services Produkte von Drittanbietern und Open-Source-Lösungen, die Sie in Security Hub integrieren können. Wenn Sie gerade erst anfangen, empfehlen wir Folgendes:

1. Integriert aktivieren AWS-Services — Die meisten AWS-Service Integrationen, die Ergebnisse an Security Hub senden, werden automatisch aktiviert, nachdem Sie sowohl Security Hub als auch den integrierten Dienst aktiviert haben. Für Ihr Vulnerability Management-Programm empfehlen wir, Amazon Inspector GuardDuty AWS Health, Amazon und IAM Access Analyzer in jedem Konto zu aktivieren. Diese Dienste senden ihre Ergebnisse automatisch an Security Hub. Eine vollständige Liste der unterstützten AWS-Service Integrationen finden Sie unter Die Ergebnisse AWS-Services an Security Hub senden.

> **Note**
>
> AWS Health sendet Ergebnisse an Security Hub, wenn eine der folgenden Bedingungen erfüllt ist:
>
> - Der Befund steht im Zusammenhang mit einem AWS Sicherheitsdienst
> - Der Typcode des Befundes enthält die Wörter`security`,`abuse`, oder `certificate`
> - Der AWS Health Suchdienst ist oder `risk abuse`

2. Integrationen von Drittanbietern einrichten — Eine Liste der derzeit unterstützten Integrationen finden Sie unter Verfügbare Produktintegrationen von Drittanbietern. Wählen Sie alle zusätzlichen Tools aus, die Ergebnisse an Security Hub senden oder Ergebnisse von Security Hub empfangen können. Möglicherweise verfügen Sie bereits über einige dieser Tools von Drittanbietern. Folgen Sie den Produktanweisungen, um die Integration mit Security Hub zu konfigurieren.

Bereiten Sie sich auf die Zuordnung von Sicherheitsergebnissen vor

In diesem Abschnitt richten Sie die Tools ein, die Ihre Teams zur Verwaltung und Zuweisung von Sicherheitsergebnissen verwenden. Dieser Abschnitt umfasst die folgenden Optionen:

- Managen Sie die Ergebnisse in bestehenden Tools und Workflows— Diese Option lässt sich in bestehende Systeme integrieren, AWS Security Hub mit denen Ihre Teams ihre täglichen Aufgaben verwalten, z. B. einen Produkt-Backlog. Diese Option wird Teams empfohlen, die über etablierte Tools zur Verwaltung ihrer Workflows verfügen.
- Ergebnisse im Security Hub verwalten— Mit dieser Option werden Benachrichtigungen für Security Hub-Ereignisse so konfiguriert, dass das entsprechende Team eine Warnung erhält und das Ergebnis in Security Hub bearbeiten kann.

Entscheiden Sie, welcher Workflow für Ihre Teams am besten geeignet ist, und stellen Sie sicher, dass Sicherheitsfeststellungen umgehend ihren jeweiligen Eigentümern übermittelt werden.

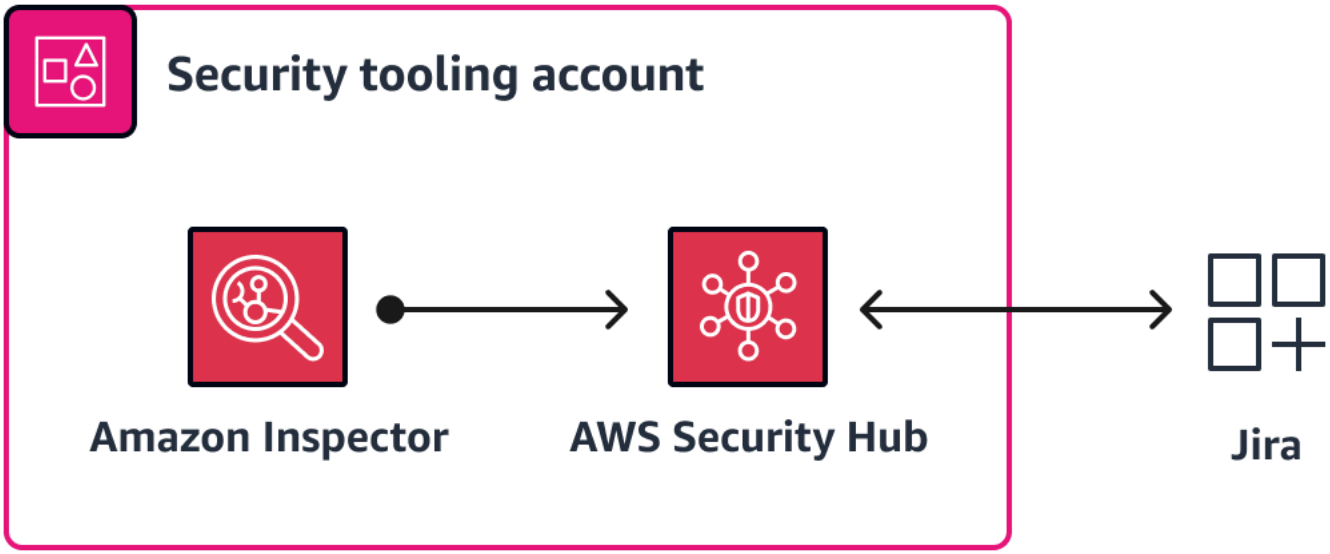
Managen Sie die Ergebnisse in bestehenden Tools und Workflows

Wir empfehlen zusätzliche Security Hub Hub-Integrationen für Unternehmen, die über etablierte Tools verfügen, mit denen Teams ihre täglichen Aufgaben verwalten oder ausführen können. Sie können Security Hub-Suchdaten in mehrere Technologieplattformen importieren. Beispiele sind unter anderem:

- SIEM-Systeme (Security Information and Event Management) helfen Sicherheitsteams dabei, betriebliche Sicherheitsereignisse zu analysieren. SIEM-Systeme ermöglichen eine Echtzeitanalyse von Sicherheitswarnungen, die von Anwendungen und Netzwerkhardware generiert werden.
- GRC-Systeme (Governance, Risk and Compliance) unterstützen Compliance- und Governance-Teams bei der Überwachung und Berichterstattung über Risikomanagementdaten. GRC-Tools sind Softwareanwendungen, mit denen Unternehmen Richtlinien verwalten, Risiken einschätzen, den Benutzerzugriff kontrollieren und die Einhaltung von Vorschriften optimieren können. Sie könnten GRC-Tools verwenden, um Geschäftsprozesse zu integrieren, Kosten zu senken und die Effizienz zu verbessern.
- Produkt-Backlog- und Ticketsysteme helfen Anwendungs- und Cloud-Teams dabei, Funktionen zu verwalten und Entwicklungsaufgaben zu priorisieren. Atlassian Jiraund Microsoft Azure DevOpssind Beispiele für diese Systeme.

Durch die direkte Integration der Security Hub Hub-Ergebnisse in diese bestehenden Unternehmenssysteme können die Mean Time to Recovery (MTTR) und die Sicherheitsergebnisse verbessert werden, da sich der tägliche Betriebsablauf nicht ändern muss. Teams können viel schneller reagieren und aus Sicherheitsergebnissen lernen, da sie keine separaten Workflows und Tools verwenden müssen. Durch die Integration wird die Bearbeitung von Sicherheitslücken zu einem Teil des normalen Standardworkflows.

Security Hub lässt sich in mehrere Partnerprodukte von Drittanbietern integrieren. Eine vollständige Liste und Anweisungen finden Sie unter Verfügbare Produktintegrationen von Drittanbietern in der Security Hub Hub-Dokumentation. Zu den gängigen Integrationen gehören Atlassian - Jira Service ManagementBidirektionale Integration AWS Security Hub mit Jira Software und. ServiceNow – ITSM Das folgende Diagramm zeigt, wie Sie Amazon Inspector so konfigurieren können, dass Ergebnisse an Security Hub gesendet werden, und anschließend Security Hub so konfigurieren können, dass alle Ergebnisse an gesendet Jira werden.



Ergebnisse im Security Hub verwalten

Mithilfe von EventBridgeAmazon-Regeln und Amazon Simple Notification Service (Amazon SNS) - Themen können Sie ein cloudbasiertes Benachrichtigungssystem für Security Hub Hub-Ergebnisse erstellen. Dieses System benachrichtigt das entsprechende Team über ein Ergebnis, wenn es erstellt wird. Für diesen Ansatz ist die unter beschriebene Strategie mit mehreren Konten von Entwickeln Sie eine Struktur AWS-Konto entscheidender Bedeutung, da die Anwendungen in spezielle Konten aufgeteilt sind. Auf diese Weise können Sie bei jedem Ergebnis die richtigen Teams benachrichtigen.

Sicherheits- oder Cloud-Teams können sich dafür entscheiden, Ereignisse von allen zu erhalten AWS-Konten. Erstellen Sie in diesem Fall eine EventBridge Regel innerhalb des delegierten Security Hub-Administratorkontos und abonnieren Sie ein Amazon SNS SNS-Thema, das diese Teams benachrichtigt. Für Anwendungsteams müssen Sie eine EventBridge Regel und ein SNS-Thema in ihren jeweiligen Anwendungskonten konfigurieren. Wenn innerhalb eines Anwendungskontos ein Security Hub Hub-Befund auftritt, wird das zuständige Team über den Befund informiert.

Security Hub sendet bereits automatisch alle neuen Ergebnisse und alle Aktualisierungen vorhandener Ergebnisse EventBridge als Security Hub Hub-Ergebnisse — Importierte Ereignisse. Jedes Ereignis „Security Hub Hub-Ergebnisse — Importiert“ enthält ein einzelnes Ergebnis. Sie können Filter auf EventBridge Regeln anwenden, sodass ein Ergebnis die Regel nur dann auslöst, wenn das Ergebnis den Filtern entspricht. Anweisungen finden Sie unter Konfiguration einer EventBridge Regel für automatisch gesendete Ergebnisse. Weitere Informationen zum Erstellen und Abonnieren von Amazon SNS-Themen finden Sie unter Amazon SNS konfigurieren.

Beachten Sie bei der Verwendung dieses Ansatzes Folgendes:

- Erstellen Sie für Anwendungsteams EventBridge Regeln für die einzelnen Anwendungen AWS-Konto und den AWS-Region Ort, an dem die Anwendung gehostet wird.
- Für Sicherheits- und Cloud-Teams erstellen Sie EventBridge Regeln im delegierten Security Hub-Administratorkonto. Dadurch werden die Teams über alle Ergebnisse in den Mitgliedskonten informiert.
- Amazon SNS sendet jeden Tag eine Benachrichtigung, wenn der Status der Sicherheitsfeststellung lautet`NEW`. Wenn Sie die täglichen Benachrichtigungen ausschalten möchten, können Sie eine benutzerdefinierte AWS Lambda Funktion erstellen, die den Status des Ergebnisses von `NEW` zu ändert, `NOTIFIED` nachdem der Amazon SNS SNS-Abonnent die Benachrichtigung erhalten hat.

Prüfung und Behebung von Sicherheitslücken in Ihrer Umgebung AWS

Bei der Prüfung eines Sicherheitsproblems wird das Ergebnis an den entsprechenden Beteiligten weitergeleitet, das Ergebnis bewertet und priorisiert und anschließend behoben. In diesem Abschnitt werden die einzelnen Schritte detailliert beschrieben und Empfehlungen zur Skalierbarkeit und Effizienz gegeben. Er enthält auch Beispiele zur Veranschaulichung des Triage- und Problembehebungsprozesses.

Themen

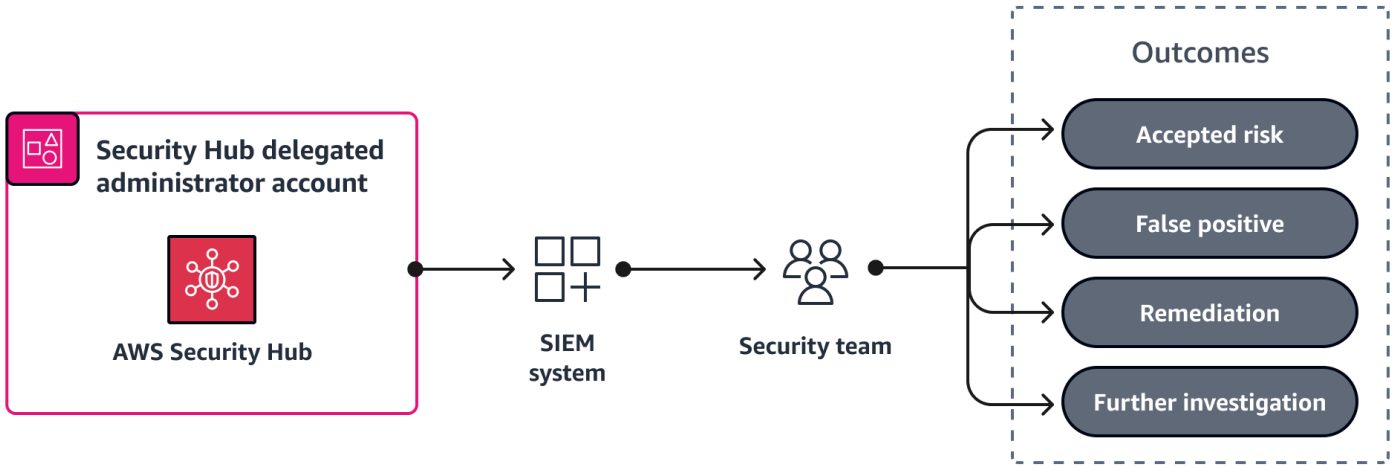
Definieren Sie die Verantwortung für die Sicherheitsergebnisse

Die Definition eines Eigentümermodells zur Prüfung von Sicherheitsergebnissen kann eine Herausforderung sein, muss es aber nicht sein. Die Sicherheitslandschaft ändert sich ständig, und die Praktiker müssen flexibel sein, um sich an diese Veränderungen anzupassen. Verfolgen Sie einen flexiblen Ansatz bei der Entwicklung Ihres Eigentumsmodells für Sicherheitserkenntnisse. Ihr erstes Modell sollte es Ihren Teams ermöglichen, sofort zu handeln. Wir empfehlen, mit der grundlegenden Eigentümerlogik zu beginnen und diese Logik im Laufe der Zeit zu verfeinern. Wenn Sie die Definition der perfekten Besitzkriterien verzögern, wird die Anzahl der Sicherheitsfeststellungen weiter zunehmen.

Um die Zuordnung der Ergebnisse zu den entsprechenden Teams und Ressourcen zu erleichtern, empfehlen wir die AWS Security Hub Integration in alle vorhandenen Systeme, die Ihre Teams zur Verwaltung ihrer täglichen Aufgaben verwenden. Sie können Security Hub beispielsweise in SIEM-Systeme (Security Information and Event Management) oder in Produkt-Backlog- und Ticketing-Systeme integrieren. Weitere Informationen finden Sie unter Bereiten Sie sich auf die Zuordnung von Sicherheitsergebnissen vor in diesem Handbuch.

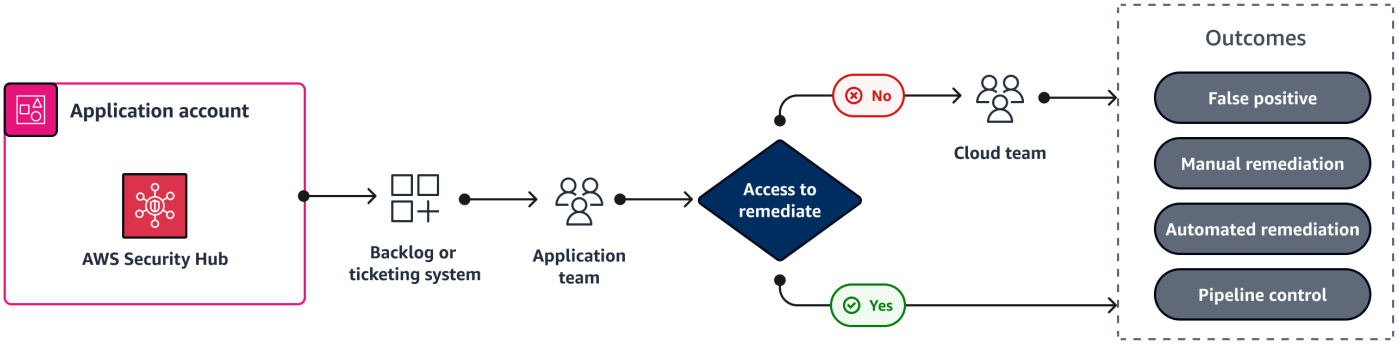
Im Folgenden finden Sie ein Beispiel für ein Eigentümermodell, das Sie als Ausgangspunkt verwenden können:

- Das Sicherheitsteam überprüft potenziell aktive Bedrohungen und hilft bei der Bewertung und Priorisierung von Sicherheitsergebnissen. Das Sicherheitsteam verfügt über das Fachwissen und die Tools, um den Kontext angemessen zu bewerten. Sie kennen die zusätzlichen sicherheitsrelevanten Daten, die ihnen helfen, Sicherheitslücken zu bewerten und zu priorisieren und Ereignisse zur Erkennung von Bedrohungen zu untersuchen. Wenn Sie den Schweregrad ermitteln oder zusätzliche Anpassungen vornehmen müssen, lesen Sie den Beurteilen und priorisieren Sie die Sicherheitsergebnisse Abschnitt in diesem Handbuch. Ein Beispiel finden Sie Beispiel für ein Sicherheitsteam in diesem Handbuch.



- Verteilung der Sicherheitsergebnisse zwischen den Cloud- und Anwendungsteams — Wie im Verteilen Sie die Eigentumsrechte an Abschnitt beschrieben, ist das Team, das Zugriff auf die Konfiguration der Ressource hat, für deren sichere Konfiguration verantwortlich. Die Anwendungsteams sind für die Sicherheitsfeststellungen im Zusammenhang mit den Ressourcen verantwortlich, die sie erstellen und konfigurieren, und das Cloud-Team ist für die Sicherheitsfeststellungen im Zusammenhang mit den weitreichenden Konfigurationen verantwortlich. In den meisten Fällen haben Anwendungsteams keinen Zugriff darauf, weitreichende Konfigurationen wie Service Control Policies (SCPs) AWS Control TowerAWS Organizations, netzwerkbezogene VPC-Konfigurationen und AWS-Services IAM Identity Center zu ändern.AWS

  In Umgebungen mit mehreren Konten, in denen Anwendungen in spezielle Konten aufgeteilt werden, können Sie in der Regel sicherheitsrelevante Ergebnisse für das Konto in das Backlog- oder Ticketsystem der Anwendung integrieren. Von diesem System aus kann das Cloud-Team oder das Anwendungsteam das Ergebnis bearbeiten. Beispiele finden Sie Beispiel für ein Anwendungsteam in Beispiel für ein Cloud-Team oder in diesem Handbuch.



- Weisen Sie die verbleibenden, ungelösten Probleme dem Cloud-Team zu — Die verbleibenden Ergebnisse können sich auf Standardeinstellungen oder weitreichende Konfigurationen beziehen, mit denen sich das Cloud-Team befassen kann. Dieses Team verfügt wahrscheinlich über das meiste historische Wissen und verfügt über die meisten Möglichkeiten, das Problem zu lösen. Insgesamt handelt es sich dabei in der Regel um eine deutlich kleinere Teilmenge der Gesamtergebnisse.

Beurteilen und priorisieren Sie die Sicherheitsergebnisse

Eine wichtige Komponente eines effektiven Schwachstellenmanagementprogramms ist die Fähigkeit, Sicherheitsergebnisse zu bewerten und zu priorisieren. Hier kommt es ins Spiel, den Kontext und die Unternehmensgeschichte einzubeziehen und die Erkennungssysteme zu optimieren. Die Priorisierung von Sicherheitsergebnissen hilft dabei, die angemessene Reaktionsgeschwindigkeit festzulegen.

Für Amazon Inspector und Amazon GuardDuty enthalten die Ergebnisse eine Bezeichnung oder Bewertung des Schweregrads. AWS Security Hub Wir empfehlen, der Untersuchung aller kritischen und schwerwiegenden Ergebnisse in Security Hub Priorität einzuräumen, einschließlich der Ergebnisse im Zusammenhang mit dem Standard Foundational Security Best Practices (FSBP), Amazon Inspector und. GuardDuty Bei der Suche nach Schweregraden werden die Bewertungen wie folgt ermittelt:

- Der Amazon Inspector-Score ist ein stark kontextualisierter Wert für jedes Ergebnis. Er wird berechnet, indem die Basisscore-Informationen des Common Vulnerability Scoring System (CVSS) mit den Ergebnissen zur Erreichbarkeit des Netzwerks und Daten zur Ausnutzbarkeit korreliert werden. Anhand dieser Bewertung können Sie die Ergebnisse priorisieren, um sich auf die kritischsten Ergebnisse und anfälligsten Ressourcen zu konzentrieren. Zusätzlich zur Bewertung bietet Amazon Inspector auch erweiterte Schwachstelleninformationen zu Common Vulnerabilities

and Exposures (CVE). Dies ist eine Zusammenfassung der verfügbaren Informationen über das CVE von Amazon sowie branchenübliche Sicherheitsinformationsquellen wie Recorded Future und Cybersecurity and Infrastructure Security Agency (CISA). Amazon Inspector kann beispielsweise die Namen bekannter Malware-Kits angeben, mit denen eine Sicherheitslücke ausgenutzt wird. Weitere Informationen finden Sie unter Vulnerability Intelligence.

- Jedem GuardDuty Befund ist ein Schweregrad und ein Wert zugewiesen, der das potenzielle Risiko des Ergebnisses für Ihre Umgebung widerspiegelt. Diese Stufe und dieser Wert werden von AWS Sicherheitstechnikern festgelegt. Ein `High` Schweregrad weist beispielsweise darauf hin, dass eine Ressource gefährdet ist und aktiv für nicht autorisierte Zwecke genutzt wird. Wir empfehlen Ihnen, die GuardDuty Feststellung eines `High` Schweregrads als Priorität zu behandeln und sofort Abhilfe zu schaffen, um eine weitere unbefugte Nutzung zu verhindern.
- Der Schweregrad einer Sicherheitslücke hängt von der Schwierigkeit der Ausnutzung und der Wahrscheinlichkeit einer Sicherheitslücke ab. Der Schwierigkeitsgrad wird durch den Grad an Raffinesse oder Komplexität bestimmt, der erforderlich ist, um die Schwachstelle zur Ausführung eines Bedrohungsszenarios auszunutzen. Die Wahrscheinlichkeit einer Gefährdung gibt an, wie wahrscheinlich es ist, dass das Bedrohungsszenario zu einer Störung oder einem Angriff auf Ihre Ressourcen AWS-Services oder Ihre Ressourcen führt.

Um die Ergebnisse zu optimieren, können Sie bestimmte Ergebnisse direkt in der jeweiligen Servicekonsole oder mithilfe der API des Dienstes unterdrücken oder archivieren. Darüber hinaus können Sie mithilfe von Automatisierungsregeln Änderungen an den Ergebnissen in Security Hub vornehmen. GuardDuty und die Ergebnisse von Amazon Inspector werden automatisch an Security Hub gesendet. Sie können Automatisierungsregeln verwenden, um Ergebnisse anhand von von Ihnen definierter Kriterien in nahezu Echtzeit automatisch zu aktualisieren (z. B. durch Änderung des Schweregrads) oder zu unterdrücken. Bei der Erstellung von Automatisierungsregeln empfehlen wir, der Regelbeschreibung Kontext hinzuzufügen, z. B. das Erstellungs- oder Änderungsdatum, wer sie erstellt hat und warum die Regel benötigt wird. Diese Informationen sind oft hilfreich für future Nachschlagewerke.

Korrigieren Sie Sicherheitslücken

Nach der Bewertung und Priorisierung eines Fehlers besteht die nächste Maßnahme darin, den Fehler zu beheben. Es gibt viele verschiedene Maßnahmen, die Sie ergreifen können, um ein Ergebnis zu korrigieren. Bei Softwareschwachstellen können Sie das Betriebssystem aktualisieren oder einen Patch installieren. Um die Ergebnisse der Cloud-Konfiguration zu ermitteln, können Sie

die Ressourcenkonfiguration aktualisieren. Im Allgemeinen können die Maßnahmen, die Sie zur Problembehebung ergreifen, zu einem der folgenden Ergebnisse zusammengefasst werden:

- Manuelle Behebung — Sie beheben die Sicherheitsanfälligkeit manuell, indem Sie beispielsweise die Eigenschaften einer AWS Ressource ändern, um die Verschlüsselung zu aktivieren. Wenn das Ergebnis von einem verwalteten Check in Security Hub stammt, enthält das Ergebnis einen Link zu Anweisungen zur manuellen Behebung des Ergebnisses.
- Wiederverwendbares Artefakt — Sie aktualisieren die Infrastruktur als Code (IaC), um die Sicherheitslücke zu beheben, und wissen, dass andere von einer ähnlichen Lösung profitieren könnten. Erwägen Sie, die aktualisierte IaC und eine kurze Zusammenfassung der Lösung in ein internes gemeinsam genutztes Code-Repository hochzuladen.
- Automatisierte Behebung — Die Sicherheitsanfälligkeit wird automatisch mithilfe von Mechanismen behoben, die Sie erstellt haben.
- Pipeline-Kontrolle — Sie wenden innerhalb Ihrer CI/CD-Pipeline (Continuous Integration and Continuous Delivery) eine Kontrolle an, die eine Implementierung verhindert, falls die Sicherheitslücke vorhanden ist.
- Akzeptiertes Risiko — Sie ergreifen keine Maßnahmen oder implementieren keine Ausgleichsmaßnahmen und akzeptieren das Risiko, das die Sicherheitslücke darstellt. Verfolgen Sie das akzeptierte Risiko an einem dafür vorgesehenen Ort, z. B. in einem Risikoregister.
- Falsch positiv — Sie ergreifen keine Maßnahmen, da Sie festgestellt haben, dass das Ergebnis eine Sicherheitslücke nicht korrekt identifiziert hat.

Eine vollständige Liste der verschiedenen Maßnahmen, die Sie ergreifen können, und der Tools, die Sie zur Behebung einer Sicherheitsanfälligkeit verwenden können, ist in diesem Handbuch nicht enthalten. Es gibt jedoch einige Dienste und Tools, mit denen Sie Sicherheitslücken in großem Umfang beheben können und die es wert sind, erwähnt zu werden, darunter:

- Patch Manager, eine Funktion von AWS Systems Manager, automatisiert den Prozess des Patchens verwalteter Knoten sowohl mit sicherheitsrelevanten Updates als auch mit anderen Arten von Updates. Sie können Patchmanager verwenden, um Patches sowohl für Betriebssysteme als auch für Anwendungen durchzuführen.
- AWS Firewall Managerhilft Ihnen bei der zentralen Konfiguration und Verwaltung von Firewallregeln für Ihre Konten und Anwendungen in. AWS Organizations Wenn neue Anwendungen erstellt werden, erleichtert Firewall Manager die Einhaltung der Vorschriften für neue Anwendungen und Ressourcen, indem gemeinsame Sicherheitsregeln durchgesetzt werden.

- Automated Security Response on AWS ist eine AWS Lösung, die mit Security Hub zusammenarbeitet und vordefinierte Reaktions- und Abhilfemaßnahmen bietet, die auf branchenüblichen Compliance-Standards und Best Practices für Sicherheitsbedrohungen basieren.

Beispiele für die Suche und Behebung von Sicherheitslücken

Dieser Abschnitt enthält Beispiele für den Triage-Prozess für die Sicherheits-, Cloud- und Anwendungsteams. Es werden die Arten von Ergebnissen erörtert, mit denen sich jedes Team üblicherweise befasst, und es wird ein Beispiel dafür gegeben, wie darauf reagiert werden kann. Umfassende Anleitungen zur Problembehebung sind ebenfalls enthalten.

In diesem Abschnitt sind die folgenden Beispiele enthalten:

- Beispiel für ein Sicherheitsteam: Erstellen einer Security Hub Hub-Automatisierungsregel
- Beispiel für ein Cloud-Team: VPC-Konfigurationen ändern
- Beispiel für ein Anwendungsteam: Eine Regel erstellen AWS Config

Beispiel für ein Sicherheitsteam: Erstellen einer Security Hub Hub-Automatisierungsregel

Das Sicherheitsteam erhält Erkenntnisse im Zusammenhang mit der Erkennung von Bedrohungen, einschließlich der GuardDuty Ergebnisse von Amazon. Eine vollständige Liste der GuardDuty Findetypen, die nach AWS Ressourcentyp kategorisiert sind, finden Sie in der GuardDuty Dokumentation unter Finding types. Sicherheitsteams müssen mit all diesen Befundtypen vertraut sein.

In diesem Beispiel akzeptiert das Sicherheitsteam die Höhe des damit verbundenen Risikos für Sicherheitslücken in einer Anlage AWS-Konto , die ausschließlich zu Lernzwecken verwendet wird und keine wichtigen oder sensiblen Daten enthält. Der Name dieses Kontos ist`sandbox`, und die Konto-ID ist`123456789012`. Das Sicherheitsteam kann eine AWS Security Hub Automatisierungsregel erstellen, die alle GuardDuty Ergebnisse dieses Kontos unterdrückt. Sie können entweder eine Regel anhand einer Vorlage erstellen, die viele gängige Anwendungsfälle abdeckt, oder sie können eine benutzerdefinierte Regel erstellen. In Security Hub empfehlen wir, eine Vorschau der Ergebnisse der Kriterien anzuzeigen, um sicherzustellen, dass die Regel die beabsichtigten Ergebnisse zurückgibt.

> **Note**
>
> In diesem Beispiel wird die Funktionalität von Automatisierungsregeln verdeutlicht. Wir empfehlen nicht, alle GuardDuty Ergebnisse für ein Konto zu unterdrücken. Der Kontext ist wichtig, und jedes Unternehmen muss anhand von Datentyp, Klassifizierung und Schutzmaßnahmen entscheiden, welche Ergebnisse unterdrückt werden sollen.

Die folgenden Parameter wurden verwendet, um diese Automatisierungsregel zu erstellen:

- Regel:
  - Der Name der Regel ist `Suppress findings from Sandbox account`
  - Die Beschreibung der Regel ist `Date: 06/25/23 Authored by: John Doe Reason: Suppress GuardDuty findings from the sandbox account`
- Kriterien:
  - `AwsAccountId` = `123456789012`
  - `ProductName` = `GuardDuty`
  - `WorkflowStatus` = `NEW`
  - `RecordState` = `ACTIVE`
- Automatisierte Aktion:
  - `Workflow.status` ist `SUPPRESSED`

Weitere Informationen finden Sie unter Automatisierungsregeln in der Security Hub Hub-Dokumentation. Sicherheitsteams haben viele Möglichkeiten, die Ergebnisse erkannter Bedrohungen zu untersuchen und zu korrigieren. Umfassende Anleitungen finden Sie im Leitfaden zur Reaktion auf AWS Sicherheitsvorfälle. Wir empfehlen, diesen Leitfaden zu lesen, um sicherzustellen, dass Sie über solide Verfahren zur Reaktion auf Vorfälle verfügen.

Beispiel für ein Cloud-Team: VPC-Konfigurationen ändern

Das Cloud-Team ist dafür verantwortlich, Sicherheitsfeststellungen zu analysieren und zu korrigieren, die gemeinsame Trends aufweisen, wie z. B. Änderungen der AWS Standardeinstellungen, die möglicherweise nicht zu Ihrem Anwendungsfall passen. Diese Ergebnisse wirken sich in der Regel auf viele AWS-Konten unserer Ressourcen aus, z. B. VPC-Konfigurationen, oder sie beinhalten eine

Einschränkung, die für die gesamte Umgebung gelten sollte. In den meisten Fällen nimmt das Cloud-Team manuelle, einmalige Änderungen vor, z. B. das Hinzufügen oder Aktualisieren einer Richtlinie.

Nachdem Ihr Unternehmen eine AWS Umgebung für einige Zeit genutzt hat, stellen Sie möglicherweise fest, dass sich eine Reihe von Anti-Pattern-Angriffen herausbilden. Ein Anti-Pattern ist eine häufig verwendete Lösung für ein wiederkehrendes Problem, bei dem die Lösung kontraproduktiv, ineffektiv oder weniger wirksam als eine Alternative ist. Als Alternative zu diesen Anti-Pattern kann Ihr Unternehmen umgebungsweite Einschränkungen verwenden, die effektiver sind, wie z. B. AWS Organizations Service Control Policies (SCPs) oder IAM Identity Center-Berechtigungssätze. SCPs und Berechtigungssätze können zusätzliche Einschränkungen für Ressourcentypen vorsehen, z. B. verhindern, dass Benutzer einen öffentlichen Amazon Simple Storage Service (Amazon S3) -Bucket konfigurieren. Obwohl es verlockend sein kann, alle möglichen Sicherheitskonfigurationen einzuschränken, gibt es Richtliniengrößenbeschränkungen für SCPs und Berechtigungssätze. Wir empfehlen einen ausgewogenen Ansatz für präventive und detektive Kontrollen.

Im Folgenden sind einige Kontrollen aus dem FSBP-Standard (AWS Security Hub Foundational Security Best Practices) aufgeführt, für die das Cloud-Team möglicherweise verantwortlich ist:

- [EC2.2] Die VPC-Standardsicherheitsgruppe sollte eingehenden und ausgehenden Datenverkehr nicht zulassen
- [EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren
- [CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem multiregionalen Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst
- [Config.1] AWS Config sollte aktiviert sein

In diesem Beispiel befasst sich das Cloud-Team mit einem Ergebnis für die FSBP-Steuerung EC2.2. In der Dokumentation zu diesem Steuerelement wird empfohlen, nicht die Standardsicherheitsgruppe zu verwenden, da sie einen breiten Zugriff über die Standardregeln für eingehende und ausgehende Nachrichten ermöglicht. Da die Standardsicherheitsgruppe nicht gelöscht werden kann, wird empfohlen, die Regeleinstellungen zu ändern, um den eingehenden und ausgehenden Verkehr einzuschränken. Um dieses Problem effizient zu lösen, sollte das Cloud-Team etablierte Mechanismen verwenden, um die Sicherheitsgruppenregeln für alle VPCs zu ändern, da jede VPC über diese Standardsicherheitsgruppe verfügt. In den meisten Fällen verwalten Cloud-Teams VPC-

Konfigurationen mithilfe von AWS Control TowerAnpassungen oder einem IaC-Tool (Infrastructure as Code) wie oder. HashiCorp TerraformAWS CloudFormation

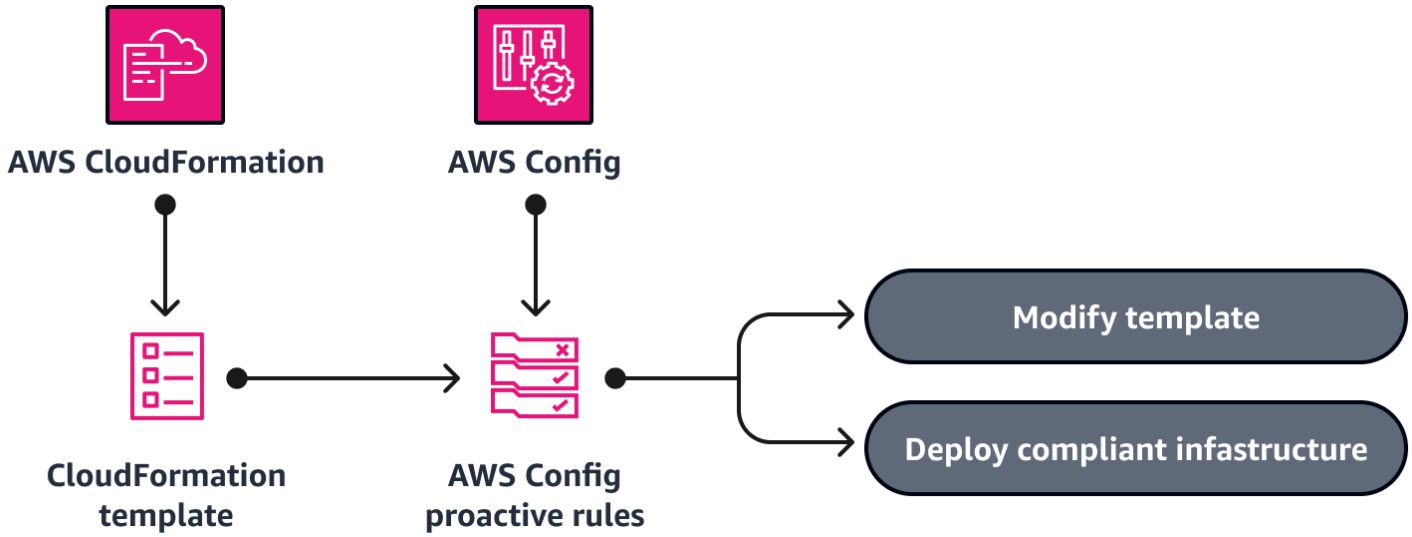
Beispiel für ein Anwendungsteam: Eine Regel erstellen AWS Config

Im Folgenden sind einige Kontrollen des Sicherheitsstandards Security Hub Foundational Security Best Practices (FSBP) aufgeführt, für die das Anwendungs- oder Entwicklungsteam möglicherweise verantwortlich ist:

- [CloudFront.1] Für CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [EC2.19] Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko ermöglichen
- [CodeBuild.1] CodeBuild GitHub oder Bitbucket-Quell-Repository-URLs sollten OAuth verwenden
- [ECS.4] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden
- [ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden

In diesem Beispiel befasst sich das Anwendungsteam mit einem Ergebnis für die FSBP-Steuerung EC2.19. Dieses Steuerelement prüft, ob uneingeschränkter eingehender Datenverkehr für die Sicherheitsgruppen für die angegebenen Ports zugänglich ist, die das höchste Risiko aufweisen. Diese Kontrolle schlägt fehl, wenn eine der Regeln in einer Sicherheitsgruppe eingehenden Datenverkehr von `0.0.0.0/0` oder `::/0` für diese Ports zulässt. In der Dokumentation zu diesem Steuerelement wird empfohlen, die Regeln zu löschen, die diesen Datenverkehr zulassen.

Dies geht nicht nur auf die individuelle Sicherheitsgruppenregel ein, sondern ist auch ein hervorragendes Beispiel für ein Ergebnis, das zu einer neuen AWS Config Regel führen sollte. Durch die Verwendung des proaktiven Testmodus können Sie verhindern, dass in future riskante Sicherheitsgruppenregeln eingesetzt werden. Im proaktiven Modus werden Ressourcen vor ihrer Bereitstellung bewertet, sodass Sie falsch konfigurierte Ressourcen und die damit verbundenen Sicherheitserkenntnisse verhindern können. Bei der Implementierung eines neuen Dienstes oder einer neuen Funktionalität können Anwendungsteams im Rahmen ihrer CI/CD-Pipeline (Continuous Integration and Continuous Delivery) Regeln im proaktiven Modus ausführen, um Ressourcen zu identifizieren, die nicht den Vorschriften entsprechen. Die folgende Abbildung zeigt, wie Sie eine proaktive AWS Config Regel verwenden können, um zu überprüfen, ob die in einer AWS CloudFormation Vorlage definierte Infrastruktur konform ist.



In diesem Beispiel kann eine weitere wichtige Effizienz erzielt werden. Wenn ein Anwendungsteam eine proaktive AWS Config Regel erstellt, kann es sie in einem gemeinsamen Code-Repository teilen, sodass andere Anwendungsteams sie verwenden können.

Jedes Ergebnis, das mit einem Security Hub-Steuerelement verknüpft ist, enthält Details zum Ergebnis und einen Link zu den Anweisungen zur Behebung des Problems. Cloud-Teams können zwar auf Ergebnisse stoßen, die gegebenenfalls eine manuelle, einmalige Behebung erfordern, wir empfehlen jedoch, proaktive Prüfungen durchzuführen, um Probleme so früh wie möglich im Entwicklungsprozess zu identifizieren.

Melden Sie Ihr Vulnerability Management-Programm und verbessern Sie es

Effektive Berichterstattung für das Schwachstellenmanagement beinhaltet die Überprüfung von Daten, die Überwachung von Trends und den Wissensaustausch. Dies sorgt für Transparenz und hilft Teams, die Sicherheitslage ihrer Organisation in der zu verbessern AWS Cloud.

Führen Sie monatliche Besprechungen zum Thema Security Operations durch

Monatliche Treffen zur Sicherheitsabteilung sind ein wirksamer Mechanismus, um die kontinuierliche Eigenverantwortung, Rechenschaftspflicht und Abstimmung zwischen den Teams zu fördern. Bei dem Treffen überprüfen die Beteiligten aus den Sicherheits-, Cloud- und Anwendungsteams die Daten auf herausragende Sicherheitsfeststellungen, Ergebnisse außerhalb von Service Level Agreements (SLAs) und die Teams, die die meisten Ergebnisse erzielt haben.

Diese Treffen helfen Ihren Teams dabei, Antimuster zu erkennen, z. B. Möglichkeiten, weitere Einschränkungen einzuführen. Präventive Kontrollen und Automatisierungsmöglichkeiten können ebenfalls entdeckt und gemeinsam genutzt werden. Die Treffen helfen auch dabei, herauszufinden, was innerhalb des Vulnerability Management-Programms gut funktioniert und was nicht, sodass Sie Verbesserungen vornehmen können.

Durch die Überprüfung von Daten, die Identifizierung von Anti-Pattern und Problemen und den Austausch von Informationen über Kontrollen und Automatisierungen können Teams wertvolle Erkenntnisse gewinnen und fortlaufend Verbesserungen vornehmen, um ihre Sicherheitslage zu stärken und ihre sicherheitsrelevanten SLAs zu reduzieren.

Nutzen Sie die Erkenntnisse von Security Hub, um Anti-Pattern zu identifizieren

AWS Security Hub Einblicke können Ihnen auch dabei helfen, Antimuster zu identifizieren und Ihre Fortschritte bei der Behebung von Ergebnissen zu verfolgen. Ein Security Hub Hub-Einblick ist eine Sammlung verwandter Ergebnisse. Es identifiziert einen Sicherheitsbereich, der Aufmerksamkeit und Intervention erfordert. Einblicke in Security Hub können Ihnen helfen, spezifische Anforderungen zu

identifizieren und Berichte zu erstellen. Security Hub bietet mehrere integrierte, verwaltete Einblicke. Um Sicherheitsprobleme zu verfolgen, die für Ihre AWS Umgebung und Nutzung spezifisch sind, können Sie benutzerdefinierte Einblicke erstellen.

Schlussfolgerung und nächste Schritte

Zusammenfassend lässt sich sagen, dass ein effektives Schwachstellen-Management-Programm eine gründliche Vorbereitung erfordert und dass Sie die richtigen Tools und Integrationen einsetzen, diese Tools fein abstimmen, Probleme effizient analysieren und kontinuierlich berichten und Verbesserungen vornehmen. Wenn Unternehmen die Best Practices in diesem Leitfaden befolgen, können sie ein skalierbares Schwachstellen-Management-Programm aufbauen AWS , um ihre Cloud-Umgebungen zu schützen.

Sie können dieses Programm um zusätzliche sicherheitsrelevante Sicherheitslücken und Erkenntnisse erweitern, z. B. Sicherheitslücken in Anwendungen. AWS Security Hub unterstützt benutzerdefinierte Produktintegrationen. Erwägen Sie, Security Hub als Integrationspunkt für zusätzliche Sicherheitstools und -produkte zu verwenden. Diese Integration ermöglicht es Ihnen, die Prozesse und Workflows zu nutzen, die Sie bereits in Ihrem Schwachstellen-Management-Programm eingerichtet haben, wie z. B. die direkte Integration mit Produkt-Backlogs und die monatlichen Besprechungen zur Sicherheitsüberprüfung.

In der folgenden Tabelle sind die in diesem Leitfaden beschriebenen Phasen und Maßnahmen zusammengefasst.

Phase	Aktionselemente
Vorbereitung	• Definieren Sie einen Plan für das Schwachstellenmanagement. • Verteilen Sie die Verantwortung für die Ergebnisse. • Entwickeln Sie ein Programm zur Offenlegung von Sicherheitslücken • Entwickeln Sie eine AWS-Konto Struktur. • Definieren, implementieren und erzwingen Sie Tags. • Überwachen Sie AWS Sicherheitsbulletins. • Aktivieren Sie Amazon Inspector mit einem delegierten Administrator.

Phase	Aktionselemente
	• Aktivieren Sie Security Hub mit einem delegierten Administrator. • Aktivieren Sie die Security Hub Hub-Stand ards. • Richten Sie die regionsübergreifende Aggregation von Security Hub ein. • Ermöglichen Sie konsolidierte Kontrolle rgebnisse in Security Hub. • Einrichtung und Verwaltung von Security Hub Hub-Integrationen, einschließlich entsprech ender nachgelagerter Integrationen mit SIEM-, GRC- oder Produkt-Backlog- oder Ticketsystemen
Triage und behebe	• Leitet die Ergebnisse auf der Grundlage einer Strategie für mehrere Konten weiter. • Leiten Sie die Ergebnisse an Sicherheits-, Cloud- und Anwendungs- oder Entwickle rteams weiter. • Passen Sie die Sicherheitsergebnisse an, um sicherzustellen, dass sie für Ihre spezifische Umgebung umsetzbar sind. • Entwickeln Sie, wenn möglich, automatisierte Behebungsmechanismen. • Implementieren Sie nach Möglichkeit CI/CD-Pipeline-Kontrollen oder andere Schutzmaß nahmen, um Sicherheitslücken zu verhinder n. • Verwenden Sie Security Hub Hub-Autom atisierungsregeln, um Ergebnisse zu eskalieren oder zu unterdrücken.

Phase	Aktionselemente
Bericht erstatten und verbessern	• Halten Sie monatliche Treffen zum Thema Security Operations ab. • Nutzen Sie die Erkenntnisse von Security Hub, um Anti-Pattern zu identifizieren.

Ressourcen

AWS Servicedokumentation

- Produktintegrationen ()AWS Security Hub
- Integration AWS Security Hub in Jira Service Management Cloud ()AWS Security Hub
- Automatisierungsregeln (AWS Security Hub)
- Regeln für die proaktive Bewertung (AWS Config)
- Patch-Manager (AWS Systems Manager)

Andere AWS Ressourcen

- Bewährte Methoden für das Markieren von AWS Ressourcen (AWS Whitepaper)
- Automatisierte Sicherheitsreaktion auf AWS (AWS Lösungsbibliothek)
- AWS Leitfaden zur Reaktion auf Sicherheitsvorfälle (AWS Technischer Leitfaden)
- AWS Sicherheitsbulletins

Dokumentverlauf

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

Änderung	Beschreibung	Datum
Erste Veröffentlichung	—	12. Oktober 2023

AWS Glossar zu präskriptiven Leitlinien

Im Folgenden finden Sie häufig verwendete Begriffe in Strategien, Leitfäden und Mustern von AWS Prescriptive Guidance. 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 SQL Postgre-Compatible 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 (AmazonRDS) 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 Kundenbeziehungsmanagementsystem (CRM) 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 ein 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 Transaktionen von verbindenden Anwendungen verarbeitet, während Daten in die Zieldatenbank repliziert werden. Die Zieldatenbank akzeptiert während der Migration keine Transaktionen.

Aggregatfunktion

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

AI

Siehe künstliche Intelligenz.

AIOps

Siehe Operationen im Bereich künstliche Intelligenz.

Anonymisierung

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

Anti-Muster

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

Anwendungssteuerung

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

Anwendungsportfolio

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

künstliche Intelligenz (KI)

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

Operationen mit künstlicher Intelligenz (AIOps)

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

Asymmetrische Verschlüsselung

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

Atomarität, 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 ABACfür 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 Cloud-Einführung ()AWS CAF

Ein Framework mit Richtlinien und bewährten Verfahren AWS , das Unternehmen bei der Entwicklung eines effizienten und effektiven Plans für die erfolgreiche Umstellung auf die Cloud unterstützt. AWS CAFgliedert 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 AWS CAF bietet es Anleitungen zur Personalentwicklung, Schulung und Kommunikation, um das Unternehmen auf eine erfolgreiche

Cloud-Einführung vorzubereiten. Weitere Informationen finden Sie AWS CAFauf der Website und im AWS CAFWhitepaper.

AWS Rahmen für die Qualifizierung der Arbeitslast ()AWS WQF

Ein Tool, das Workloads bei der Datenbankmigration bewertet, Migrationsstrategien empfiehlt und Arbeitsschätzungen bereitstellt. AWS WQFist in AWS Schema Conversion Tool ()AWS SCT enthalten. 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 Anrufe und ähnliche Aktionen 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, die als bösartige Bots bezeichnet werden, 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 für die AWS Cloud-Einführung.

Bereitstellung auf Kanaren

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

CCoE

Weitere Informationen finden Sie im Cloud Center of Excellence.

CDC

Siehe Erfassung von Änderungsdaten.

Erfassung von Änderungsdaten (CDC)

Der Prozess der Nachverfolgung von Änderungen an einer Datenquelle, z. B. einer Datenbanktabelle, und der Aufzeichnung von Metadaten zu der Änderung. Sie können es CDC für

verschiedene Zwecke verwenden, z. B. zur 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 CCoEBeiträgen 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 einerCCoE, 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 or Bitbucket Cloud. Jede Version des Codes wird als Zweig bezeichnet. 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. AWS Panorama Bietet beispielsweise Geräte an, die CV zu lokalen Kameranetzwerken hinzufügen, und Amazon SageMaker stellt Bildverarbeitungsalgorithmen für CV bereit.

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.

Datenbank für das Konfigurationsmanagement () 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 Phase der Migration, die sich CMDB in der Phase der Portfolioerkennung und -analyse befindet.

Konformitätspaket

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

Kontinuierliche Bereitstellung und kontinuierliche Integration (CI/CD)

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

CV

Siehe Computer Vision.

D

Daten im Ruhezustand

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

Datenklassifizierung

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

Datendrift

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

Daten während der Übertragung

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

Datennetz

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

Datenminimierung

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

Datenperimeter

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

Vorverarbeitung der Daten

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

Herkunft der Daten

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

betroffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

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

Datenbankdefinitionssprache (DDL)

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

Sprache zur Datenbankmanipulation (DML)

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

DDL

Siehe Datenbankdefinitionssprache.

Deep-Ensemble

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

Deep Learning

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

defense-in-depth

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

delegierter Administrator

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

Bereitstellung

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

Entwicklungsumgebung

Siehe Umgebung.

Detektivische Kontrolle

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

Abbildung des Wertstroms in der Entwicklung (DVSM)

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

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

digitaler Zwilling

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

Maßtabelle

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

Katastrophe

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

Disaster Recovery (DR)

Die Strategie und der Prozess, 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 dazu, wie Sie domänengesteuertes Design mit dem Strangler-Fig-Muster verwenden können, finden Sie unter Modernizing legacy Microsoft. ASP NET(ASMX) schrittweise 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 der Wertströme in der Entwicklung.

E

EDA

Siehe explorative Datenanalyse.

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.

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 Dienst, den Sie in einer virtuellen privaten 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) Prinzipalen erstellen AWS PrivateLink und diesen Berechtigungen gewähren. Diese Konten oder Prinzipale können sich privat mit Ihrem Endpunktdienst verbinden, indem sie VPC Schnittstellenendpunkte erstellen. Weitere Informationen finden Sie unter Create an Endpoint Service in der Dokumentation zu Amazon Virtual Private Cloud (AmazonVPC).

Unternehmensressourcenplanung (ERP)

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

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 AWS CAF Sicherheitsepen 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

Weitere Informationen finden Sie unter 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. EDAwird 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.

FGAC

Siehe Feinkörnige 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.

G

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.

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 Regel auf hoher Ebene, die dabei hilft, Ressourcen, Richtlinien und die Einhaltung von Vorschriften in allen Organisationseinheiten zu regeln (). OUs Präventiver Integritätsschutz setzt Richtlinien durch, um die Einhaltung von Standards zu gewährleisten. Sie werden mithilfe von Dienststeuerungsrichtlinien und IAM Berechtigungsgrenzen implementiert. Detektivischer Integritätsschutz erkennt Richtlinienverstöße und Compliance-Probleme und generiert Warnmeldungen zur Abhilfe. Sie werden mithilfe von AWS Config, AWS Security Hub, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector und benutzerdefinierten AWS Lambda Prüfungen implementiert.

H

HEKTAR

Siehe Hochverfügbarkeit.

Heterogene Datenbankmigration

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

hohe Verfügbarkeit (HA)

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

historische Modernisierung

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

Homogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank in eine Zieldatenbank, die dieselbe Datenbank-Engine verwendet (z. B. Microsoft SQL Server zu Amazon RDS for 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 Principals zugeordnet ist und deren Berechtigungen innerhalb der AWS Cloud Umgebung definiert.

Leerlaufanwendung

Eine Anwendung mit einer durchschnittlichen CPU Speicherauslastung 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.

eingehend (Eingang) VPC

In einer Architektur AWS mit mehreren Konten, VPC die Netzwerkverbindungen von außerhalb einer Anwendung akzeptiert, überprüft und weiterleitet. In der AWS Sicherheitsreferenzarchitektur wird empfohlen, Ihr Netzwerkkonto mit eingehenden und ausgehenden Daten sowie Inspektionen 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 () IIoT

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).

Inspektion VPC

In einer Architektur AWS mit mehreren Konten, eine zentrale Architektur, 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 von Modellen für maschinelles Lernen mit. AWS

IoT

Siehe Internet der Dinge.

IT-Informationsbibliothek (ITIL)

Eine Reihe von bewährten Methoden für die Bereitstellung von IT-Services und die Abstimmung dieser Services auf die Geschäftsanforderungen. ITILbietet die Grundlage fürITSM.

IT-Servicemanagement (ITSM)

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 Operations Integration Guide.

ITIL

Weitere Informationen finden Sie in der IT-Informationsbibliothek.

ITSM

Siehe IT-Servicemanagement.

L

Labelbasierte Zugriffskontrolle () LBAC

Eine Implementierung der obligatorischen Zugriffskontrolle (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..

Große Migration

Eine Migration von 300 oder mehr Servern.

LBAC

Weitere Informationen finden Sie unter Label-basierte Zugriffskontrolle.

Geringste Berechtigung

Die bewährte Sicherheitsmethode, bei der nur die für die Durchführung einer Aufgabe erforderlichen Mindestberechtigungen erteilt werden. Weitere Informationen finden Sie in der Dokumentation unter Anwenden von Berechtigungen mit den geringsten Rechten. IAM

Lift and Shift

Siehe 7 Rs.

Little-Endian-System

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

Niedrigere Umgebungen

Siehe Umwelt.

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.

Fertigungsleitsystem () MES

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

MAP

Siehe Migration Acceleration Program.

Mechanismus

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

Mitgliedskonto

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

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. MAPumfasst 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 von Migration Factory gehören in der Regel Betriebsanalysten 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.

Bewertung des Migrationsportfolios () MPA

Ein Online-Tool, das Informationen zur Validierung des Geschäftsszenarios für die Migration auf das bereitstellt. AWS Cloud MPAbietet eine detaillierte Portfoliobewertung (richtige Servergröße, Preisgestaltung, TCO Vergleiche, Analyse der Migrationskosten) sowie Migrationsplanung (Analyse und Datenerfassung von Anwendungen, Gruppierung von Anwendungen, Priorisierung der Migration und Wellenplanung). Das MPATool (Anmeldung erforderlich) steht allen AWS Beratern und APN Partnerberatern kostenlos zur Verfügung.

Bewertung der Eignung für die Migration (MRA)

Der Prozess der Gewinnung von Erkenntnissen über den Cloud-Bereitschaftsstatus eines Unternehmens, der Identifizierung von Stärken und Schwächen und der Erstellung eines Aktionsplans zur Schließung festgestellter Lücken unter Verwendung von AWS CAF. Weitere Informationen finden Sie im Benutzerhandbuch für Migration Readiness. MRAist die erste Phase der AWS Migrationsstrategie.

Migrationsstrategie

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

ML

Siehe maschinelles Lernen.

Modernisierung

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

Bewertung der Modernisierungsfähigkeit

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

Monolithische Anwendungen (Monolithen)

Anwendungen, die als ein einziger Service mit eng gekoppelten Prozessen ausgeführt werden. Monolithische Anwendungen haben verschiedene Nachteile. Wenn ein Anwendungs-Feature stark nachgefragt wird, muss die gesamte Architektur skaliert werden. Das Hinzufügen oder Verbessern der Feature einer monolithischen Anwendung wird ebenfalls komplexer, wenn die Codebasis wächst. Um diese Probleme zu beheben, können Sie eine Microservices-Architektur verwenden. Weitere Informationen finden Sie unter Zerlegen von Monolithen in Microservices.

MPA

Siehe Bewertung des Migrationsportfolios.

MQTT

Siehe Message Queuing-Telemetrietransport.

Mehrklassen-Klassifizierung

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

veränderbare Infrastruktur

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

O

OAC

Siehe Origin Access Control.

OAI

Siehe Zugriffsidentität von Origin.

OCM

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 betrieblicher 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 Offene Prozesskommunikation — Einheitliche Architektur.

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 betrieblicher Ebene () OLA

Eine Vereinbarung, in der klargestellt wird, welche funktionalen IT-Gruppen sich gegenseitig versprechen, um eine Vereinbarung auf Serviceniveau zu unterstützen (). SLA

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 Änderungsmanagement (OCM)

Ein Framework für das Management wichtiger, disruptiver Geschäftstransformationen aus Sicht der Mitarbeiter, der Kultur und der Führung. OCMunterstützt Unternehmen bei der Vorbereitung und Umstellung auf neue Systeme und Strategien, indem es die Einführung von Veränderungen beschleunigt, Übergangsprobleme angeht und kulturelle und organisatorische Veränderungen vorantreibt. In der AWS Migrationsstrategie wird dieses Framework als Mitarbeiterbeschleunigung bezeichnet, da bei Projekten zur Cloud-Einführung die Geschwindigkeit des Wandels erforderlich ist. Weitere Informationen finden Sie im OCMLeitfaden.

ursprüngliche Zugriffskontrolle (OAC)

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

ursprüngliche Zugriffsidentität () OAI

In CloudFront, eine Option zur Zugriffsbeschränkung, um Ihre Amazon S3 S3-Inhalte zu sichern. Wenn Sie es verwendenOAI, 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, welche eine detailliertere und erweiterte Zugriffskontrolle bietet.

ORR

Siehe Überprüfung der Betriebsbereitschaft.

NICHT

Siehe Betriebstechnologie.

ausgehend (Ausgang) VPC

In einer Architektur AWS mit mehreren Konten eine, VPC die Netzwerkverbindungen verarbeitet, die von einer Anwendung aus initiiert werden. In der AWS Security Reference Architecture wird empfohlen, Ihr Netzwerkkonto mit eingehenden und ausgehenden Daten und Inspektionen einzurichten, 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 zugewiesen wird, um die maximalen Berechtigungen festzulegen, die der Benutzer oder die Rolle haben kann. Weitere Informationen finden Sie in der IAM Dokumentation unter Grenzen von Berechtigungen.

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 hierfür PII sind Namen, Adressen und Kontaktinformationen.

PII

Siehe persönlich identifizierbare Informationen.

Playbook

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

PLC

Siehe programmierbare Logiksteuerung.

PLM

Siehe Produktlebenszyklusmanagement.

policy

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

Polyglotte Beharrlichkeit

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

Portfoliobewertung

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

predicate

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

Prädikat Pushdown

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

Präventive Kontrolle

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

Prinzipal

Eine Entität AWS , die Aktionen ausführen und auf Ressourcen zugreifen kann. Bei dieser Entität handelt es sich in der Regel um einen Root-Benutzer für einen AWS-Konto, eine IAM Rolle oder

einen Benutzer. Weitere Informationen finden Sie in der IAM Dokumentation unter Principal in Roles (Begriffe und Konzepte).

Datenschutz durch Design

Ein Ansatz in der Systemtechnik, der den Datenschutz während des gesamten Engineering-Prozesses berücksichtigt.

Privat gehostete Zonen

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

proaktive Steuerung

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

Produktlebenszyklusmanagement (PLM)

Das Management von Daten und Prozessen für ein Produkt während seines gesamten Lebenszyklus, von der Konstruktion, Entwicklung und Markteinführung über Wachstum und Reife bis hin zu Verkauf und Verkauf.

Produktionsumgebung

Siehe Umgebung.

programmierbare Logiksteuerung (PLC)

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

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 Microservice-basierten System kann ein Microservice beispielsweise Ereignismeldungen in einem Kanal veröffentlichen MES, 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 SQL relationalen 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

RACIMatrix

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

Ransomware

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

RASCIMatrix

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.

Ziel des Wiederherstellungspunkts (RPO)

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

Ziel für die Wiederherstellungszeit (RTO)

Die maximal zulässige Verzögerung zwischen der Unterbrechung des Dienstes 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.

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

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 RASCIMatrix bezeichnet, und wenn Sie sie ausschließen, wird sie als RACIMatrix 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.

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, die über definierte Zugriffsregeln verfügen. RCACbesteht aus Zeilenberechtigungen und Spaltenmasken.

RPO

Siehe Recovery Point Objective.

RTO

Siehe Ziel der Wiederherstellungszeit.

Runbook

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

S

SAML2.0

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

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.

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 (SIEM)

Tools und Dienste, die Systeme zur Verwaltung von Sicherheitsinformationen (SIM) und zur Verwaltung von Sicherheitsereignissen (SEM) kombinieren. Ein SIEM System sammelt, überwacht und analysiert Daten von Servern, Netzwerken, Geräten und anderen Quellen, um Bedrohungen und Sicherheitsverletzungen zu erkennen und Warnmeldungen zu generieren.

Automatisierung von Sicherheitsreaktionen

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

Serverseitige Verschlüsselung

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

Richtlinie zur Dienststeuerung (SCP)

Eine Richtlinie, die eine zentrale Kontrolle über die Berechtigungen für alle Konten in einer Organisation in AWS Organizations ermöglicht. SCPsDefinieren 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

Der 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.

Vereinbarung zum Servicelevel () 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.

Indikator für das Serviceniveau () SLI

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

Ziel auf Serviceniveau () 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, wohingegen 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.

zentraler Fehlerpunkt (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.

SLO

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.

SPOF

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 Modernizing legacy MicrosoftASP. NET(ASMX) schrittweise Webservices mithilfe von Containern und Amazon API Gateway.

Subnetz

Ein Bereich von IP-Adressen in IhremVPC. 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.

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.

VPCPeering

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

Schwachstelle

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

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.

WORM

Sehen, einmal schreiben, viele lesen.

WQF

Siehe AWSWorkload-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.

Zombie-Anwendung

Eine Anwendung mit einer durchschnittlichen CPU Speicherauslastung von unter 5 Prozent. 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.