AWS Leitfaden zur Entscheidungsfindung

Auswahl von AWS Sicherheits-, Identitäts- und Governance-Diensten

Auswahl von AWS Sicherheits-, Identitäts- und Governance-Diensten: AWS Leitfaden zur Entscheidungsfindung

Table of Contents

Leitfaden zur Entscheidungsfindung 1
Einführung 1
Verstehen 2
Gemeinsame Verantwortlichkeit 2
Kombinieren Sie AWS Tools und Services 3
Erwägen Sie 8
Klicken Sie auf 12
Identitäts- und Zugriffsverwaltung 13
Datenschutz 14
Netzwerk- und Anwendungsschutz 15
Erkennung und Reaktion 15
Unternehmensführung und Einhaltung von Vorschriften 17
Verwenden Sie 18
Identitäts- und Zugriffsverwaltung 18
Datenschutz 21
Netzwerk- und Anwendungsschutz 26
Erkennung und Reaktion 28
Unternehmensführung und Compliance 33
Erkunden 35
Dokumentverlauf 37
..... xxxviii

Auswahl von AWS Sicherheits-, Identitäts- und Governance-Diensten

Den ersten Schritt machen

Zeit zum Lesen	27 Minuten	
Zweck	Wir helfen Ihnen dabei, herauszufinden, welche AWS Sicherheits-, Identitäts- und Governance-Services für Ihr Unternehmen am besten geeignet sind.	
Letzte Aktualisierung	30. Dezember 2024	
Abgedeckte Dienstleistungen	• AWS Artifact • AWS Audit Manager • AWS Certificate Manager • AWS CloudHSM • AWS CloudTrail • Amazon Cognito • AWS Config • AWS Control Tower • Amazon Detective • AWS Firewall Manager • Amazon GuardDuty • AWS IAM • AWS IAM Identity Center • Amazon Inspector	• AWS KMS • Amazon Macie • AWS Network Firewall • AWS Organizations • AWS Payment Cryptography • AWS Private CA • AWS RAM • AWS Secrets Manager • AWS Security Hub • Amazon Security Lake • AWS Reaktion auf Sicherheitsvorfälle • AWS Shield • AWS WAF

Einführung

Sicherheit, Identität und Governance in der Cloud sind wichtige Komponenten für Sie, um die Integrität und Sicherheit Ihrer Daten und Dienste zu erreichen und aufrechtzuerhalten. Dies ist

besonders relevant, da immer mehr Unternehmen zu Cloud-Anbietern wie Amazon Web Services (AWS) migrieren.

Dieser Leitfaden hilft Ihnen bei der Auswahl der AWS Sicherheits-, Identitäts- und Governance-Dienste und Tools, die für Ihre Bedürfnisse und Ihr Unternehmen am besten geeignet sind.

Lassen Sie uns zunächst untersuchen, was wir mit Sicherheit, Identität und Governance meinen:

- Cloud-Sicherheit bezieht sich auf den Einsatz von Maßnahmen und Praktiken zum Schutz digitaler Ressourcen vor Bedrohungen. Dies umfasst sowohl die physische Sicherheit von Rechenzentren als auch Cybersicherheitsmaßnahmen zum Schutz vor Online-Bedrohungen. AWS priorisiert Sicherheit durch verschlüsselte Datenspeicherung, Netzwerksicherheit und kontinuierliche Überwachung potenzieller Bedrohungen.
- Identitätsdienste helfen Ihnen dabei, Identitäten, Ressourcen und Berechtigungen auf sichere und skalierbare Weise zu verwalten. AWS bietet Identitätsdienste, die für Anwendungen mit Personal- und Kundenkontakt sowie für die Verwaltung des Zugriffs auf Ihre Workloads und Anwendungen konzipiert sind.
- Cloud-Governance besteht aus einer Reihe von Regeln, Prozessen und Berichten, die Ihr Unternehmen dabei unterstützen, bewährte Verfahren zu befolgen. Sie können Cloud-Governance für Ihre AWS Ressourcen einrichten, integrierte Best Practices und Standards verwenden und Compliance- und Auditprozesse automatisieren. Compliance in der Cloud bezieht sich auf die Einhaltung von Gesetzen und Vorschriften zum Datenschutz und zur Privatsphäre. AWS Compliance-Programme bieten Informationen über die Zertifizierungen, Vorschriften und Rahmenbedingungen, mit denen sie AWS übereinstimmen.

Dieses kurze one-and-a-half Video fasst zusammen, wie wir starke Sicherheit in unserem Kern AWS aufbauen.

Machen Sie sich mit AWS Sicherheits-, Identitäts- und Governance-Services vertraut

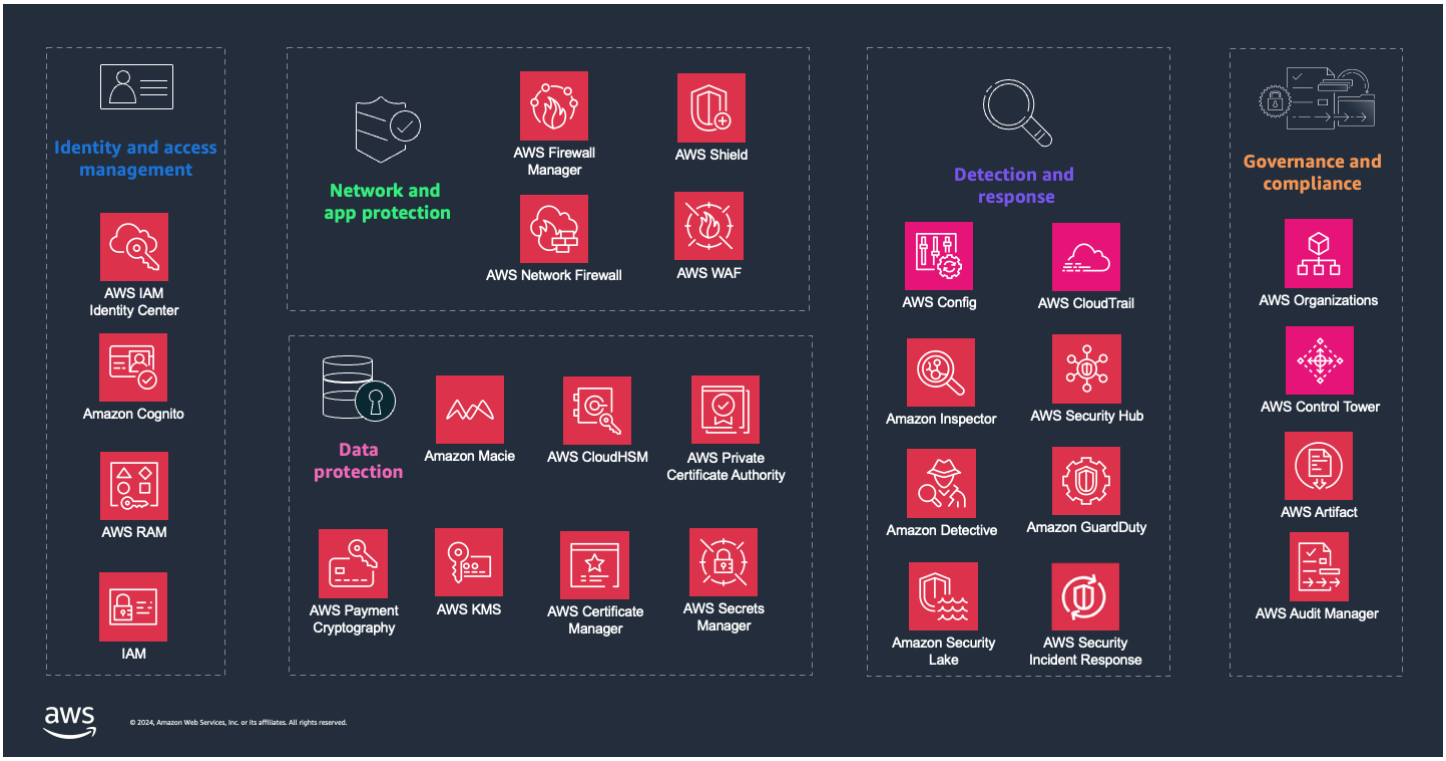
Sicherheit und Compliance sind gemeinsame Aufgaben

Bevor Sie sich für Ihre AWS Sicherheits-, Identitäts- und Governance-Services entscheiden, sollten Sie sich darüber im Klaren sein, dass Sie und Sie für Sicherheit und Compliance gemeinsam verantwortlich sind AWS.

Die Art dieser gemeinsamen Verantwortung trägt dazu bei, Ihre betriebliche Belastung zu verringern, und bietet Ihnen Flexibilität und Kontrolle über Ihren Einsatz. Diese Differenzierung der Verantwortung wird allgemein als Sicherheit „der“ Cloud und Sicherheit „in“ der Cloud bezeichnet.

Wenn Sie dieses Modell kennen, können Sie die Bandbreite der verfügbaren Optionen verstehen und verstehen, wie die jeweiligen Optionen AWS-Services zusammenpassen.

Sie können AWS Tools und Services kombinieren, um Ihre Workloads zu schützen



Wie im vorherigen Diagramm dargestellt, AWS bietet es Tools und Dienste für fünf Bereiche, mit denen Sie zuverlässige Sicherheit, Identitätsmanagement und Governance in der Cloud erreichen und aufrechterhalten können. Sie können diese fünf AWS-Services Domänen verwenden, um Ihnen dabei zu helfen, Folgendes zu tun:

- Entwickeln Sie einen mehrschichtigen Ansatz zum Schutz Ihrer Daten und Umgebungen
- Stärken Sie Ihre Cloud-Infrastruktur gegen sich entwickelnde Bedrohungen
- Halten Sie sich an strenge regulatorische Standards

Weitere Informationen zur AWS Sicherheit, einschließlich der Sicherheitsdokumentation für AWS-Services, finden Sie unter AWS Sicherheitsdokumentation.

In den folgenden Abschnitten untersuchen wir die einzelnen Domänen genauer.

Machen Sie sich mit AWS Identitäts- und Zugriffsverwaltungsdiensten vertraut

Im Mittelpunkt der AWS Sicherheit steht das Prinzip der geringsten Rechte: Einzelpersonen und Dienste haben nur den Zugriff, den sie benötigen. AWS IAM Identity Centerwird AWS-Service für die Verwaltung des Benutzerzugriffs auf AWS Ressourcen empfohlen. Sie können diesen Dienst verwenden, um den Zugriff auf Ihre Konten und die Berechtigungen innerhalb dieser Konten, einschließlich Identitäten von externen Identitätsanbietern, zu verwalten.

In der folgenden Tabelle sind die in diesem Handbuch erörterten Angebote zur Identitäts- und Zugriffsverwaltung zusammengefasst:

AWS IAM Identity Center

: AWS IAM Identity Centerhilft Ihnen dabei, Ihre Identitätsquelle zu verbinden oder Benutzer zu erstellen. Sie können den Zugriff Ihrer Mitarbeiter auf mehrere AWS-Konten Anwendungen zentral verwalten.

Amazon Cognito

: Amazon Cognito bietet ein Identitätstool für Web- und mobile Apps, mit dem Benutzer über das integrierte Benutzerverzeichnis, Ihr Unternehmensverzeichnis und Kundenidentitätsanbieter authentifiziert und autorisiert werden können.

AWS RAM

: AWS RAMhilft Ihnen dabei AWS-Konten, Ihre Ressourcen sicher innerhalb Ihrer Organisation und mit IAM-Rollen und -Benutzern gemeinsam zu nutzen.

IAM

: IAM ermöglicht eine sichere, detaillierte Kontrolle über den Zugriff auf Workload-Ressourcen. AWS

Machen Sie sich mit Datenschutzdiensten vertraut AWS

Datenschutz ist in der Cloud von entscheidender Bedeutung und AWS bietet Dienste, mit denen Sie Ihre Daten, Konten und Workloads schützen können. Beispielsweise trägt die Verschlüsselung Ihrer Daten sowohl bei der Übertragung als auch bei der Speicherung dazu bei, sie vor unbefugtem Zugriff zu schützen. Mit AWS Key Management Service(AWS KMS) und können AWS CloudHSMSie die kryptografischen Schlüssel, die Sie zum Schutz Ihrer Daten verwenden, erstellen und steuern.

In der folgenden Tabelle sind die in diesem Leitfaden erörterten Datenschutzangebote zusammengefasst:

Amazon Macie

Amazon Macie erkennt sensible Daten mithilfe von maschinellem Lernen und Musterabgleich und ermöglicht einen automatisierten Schutz vor den damit verbundenen Risiken.

AWS KMS

AWS KMSerstellt und kontrolliert die kryptografischen Schlüssel, die Sie zum Schutz Ihrer Daten verwenden.

AWS CloudHSM

AWS CloudHSMstellt hochverfügbare, cloudbasierte Hardware-Sicherheitsmodule bereit (HSMs).

AWS Certificate Manager

AWS Certificate Managerbewältigt die Komplexität der Erstellung, Speicherung und Erneuerung von öffentlichen und privaten SSL/TLS X.509-Zertifikaten und Schlüsseln.

AWS Private CA

AWS Private CAhilft Ihnen bei der Erstellung privater Zertifizierungsstellenhierarchien, einschließlich Stamm- und untergeordneter Zertifizierungsstellen (). CAs

AWS Secrets Manager

AWS Secrets Managerhilft Ihnen dabei, Datenbankanmeldedaten, Anwendungsanmeldedaten, OAuth Token, API-Schlüssel und andere Geheimnisse zu verwalten, abzurufen und zu rotieren.

AWS Payment Cryptography

AWS Payment Cryptographybietet Zugriff auf kryptografische Funktionen und Schlüsselverwaltung, die bei der Zahlungsabwicklung gemäß den PCI-Standards (Payment Card Industry) verwendet werden.

Verstehen Sie die Dienste für den AWS Netzwerk- und Anwendungsschutz

AWS bietet verschiedene Dienste zum Schutz Ihrer Netzwerke und Anwendungen. AWS Shieldbietet Ihnen Schutz vor Distributed-Denial-of-Service (DDoS) -Angriffen und AWS WAFhilft Ihnen, Webanwendungen vor gängigen Internet-Exploit-Angriffen zu schützen.

In der folgenden Tabelle sind die in diesem Handbuch erörterten Angebote zum Schutz von Netzwerken und Anwendungen zusammengefasst:

AWS Firewall Manager

AWS Firewall Managervereinfacht zum Schutz Ihre Verwaltungs- und Wartungsaufgaben für mehrere Konten und Ressourcen.

AWS Network Firewall

AWS Network Firewallbietet mit Ihrer VPC eine statusbehaftete, verwaltete Netzwerk-Firewall sowie einen Service zur Erkennung und Verhinderung von Eindringlingen.

AWS Shield

AWS Shieldbietet Schutz vor DDo S-Angriffen auf AWS Ressourcen auf Netzwerk-, Transport- und Anwendungsebene.

AWS WAF

AWS WAFbietet eine Firewall für Webanwendungen, mit der Sie die HTTP (S) -Anfragen überwachen können, die an Ihre geschützten Webanwendungsressourcen weitergeleitet werden.

Machen Sie sich mit AWS Erkennungs- und Reaktionsdiensten vertraut

AWS bietet Tools, mit denen Sie die Sicherheitsabläufe in Ihrer AWS Umgebung optimieren können, auch in Umgebungen mit mehreren Konten. Sie können Amazon GuardDuty beispielsweise für die intelligente Bedrohungserkennung verwenden, und Sie können Amazon Detective verwenden, um Sicherheitsergebnisse zu identifizieren und zu analysieren, indem Sie Protokolldaten sammeln. AWS Security Hubunterstützt mehrere Sicherheitsstandards und bietet einen Überblick über Sicherheitswarnungen und den Compliance-Status in allen Bereichen AWS-Konten. AWS CloudTrailverfolgt die Benutzeraktivitäten und die Nutzung der API (Application Programming Interface), was für das Verständnis und die Reaktion auf Sicherheitsereignisse von entscheidender Bedeutung ist.

In der folgenden Tabelle sind die in diesem Leitfaden erörterten Erkennungs- und Reaktionsangebote zusammengefasst:

AWS Config

AWS Configbietet einen detaillierten Überblick über die Konfiguration der AWS Ressourcen in Ihrem AWS-Konto.

AWS CloudTrail

AWS CloudTrailzeichnet Aktionen auf, die von einem Benutzer, einer Rolle oder ausgeführt wurden AWS-Service.

AWS Security Hub

AWS Security Hubbietet einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS.

Amazon GuardDuty

Amazon überwacht Ihre Workloads AWS-Konten, Laufzeitaktivitäten und Daten GuardDuty kontinuierlich auf böswillige Aktivitäten.

Amazon Inspector

Amazon Inspector scannt Ihre AWS Workloads auf Softwareschwachstellen und unbeabsichtigte Netzwerkgefährdung.

Amazon Security Lake

Amazon Security Lake zentralisiert automatisch Sicherheitsdaten aus AWS Umgebungen, SaaS-Anbietern, lokalen Umgebungen, Cloud-Quellen und Quellen von Drittanbietern in einem Data Lake.

Amazon Detective

Amazon Detective hilft Ihnen, die Ursache von Sicherheitserkenntnissen oder verdächtigen Aktivitäten zu analysieren, zu untersuchen und schnell zu identifizieren.

AWS Security Incident Response

AWS Reaktion auf Sicherheitsvorfälle

Hilft Ihnen, sich schnell auf Sicherheitsvorfälle vorzubereiten, darauf zu reagieren und Anleitungen zu erhalten, um sich nach Sicherheitsvorfällen zu erholen.

Verstehen Sie die AWS Governance- und Compliance-Services

AWS bietet Tools, mit denen Sie Ihre Sicherheits-, Betriebs-, Compliance- und Kostenstandards einhalten können. Sie können es beispielsweise verwenden, AWS Control Towerum eine Umgebung mit mehreren Konten mit vorgeschriebenen Kontrollen einzurichten und zu verwalten. Mit AWS Organizationskönnen Sie eine richtlinienbasierte Verwaltung für mehrere Konten in Ihrem Unternehmen einrichten.

AWS bietet Ihnen außerdem einen umfassenden Überblick über Ihren Compliance-Status und überwacht Ihre Umgebung kontinuierlich mithilfe automatisierter Konformitätsprüfungen, die auf den AWS bewährten Verfahren und Industriestandards basieren, die Ihr Unternehmen befolgt. AWS ArtifactErmöglicht beispielsweise den Zugriff auf Compliance-Berichte auf Abruf und AWS Audit Managerautomatisiert die Erfassung von Nachweisen, sodass Sie leichter beurteilen können, ob Ihre Kontrollen effektiv funktionieren.

In der folgenden Tabelle sind die in diesem Leitfaden erörterten Governance- und Compliance-Angebote zusammengefasst:

AWS Organizations

AWS Organizationshilft Ihnen dabei, mehrere AWS-Konten zu einer Organisation zu konsolidieren, die Sie erstellen und zentral verwalten.

AWS Control Tower

AWS Control Towerhilft Ihnen bei der Einrichtung und Verwaltung einer Umgebung AWS mit mehreren Konten, die auf bewährten Methoden basiert.

AWS Artifact

AWS Artifactbietet auf Abruf Downloads von AWS Sicherheits- und Compliance-Dokumenten.

AWS Audit Manager

AWS Audit Manager

Unterstützt Sie dabei, Ihre AWS Nutzung kontinuierlich zu überprüfen, um die Bewertung von Risiken und der Einhaltung von Vorschriften zu vereinfachen.

Berücksichtigen Sie AWS Sicherheits-, Identitäts- und Governance-Kriterien

Die Wahl der richtigen Sicherheits-, Identitäts- und Governance-Services AWS hängt von Ihren spezifischen Anforderungen und Anwendungsfällen ab. Wenn Sie sich für einen AWS Sicherheitsservice entscheiden, erhalten Sie einen Entscheidungsbaum, anhand dessen Sie entscheiden können, ob AWS-Services der Einsatz in den Bereichen Sicherheit, Identität und Governance für Ihr Unternehmen geeignet ist. Darüber hinaus finden Sie hier einige Kriterien, die Sie bei Ihrer Entscheidung, welche Dienste Sie nutzen möchten, berücksichtigen sollten.

Security requirements and threat landscape

Führen Sie eine umfassende Bewertung der spezifischen Sicherheitslücken und Bedrohungen Ihres Unternehmens durch. Dazu gehört die Identifizierung der Arten von Daten, mit denen Sie umgehen, z. B. persönliche Kundeninformationen, Finanzunterlagen oder firmeneigene Geschäftsdaten. Machen Sie sich mit den jeweiligen potenziellen Risiken vertraut.

Bewerten Sie Ihre Anwendungs- und Infrastrukturarchitektur. Stellen Sie fest, ob Ihre Anwendungen öffentlich zugänglich sind und welche Art von Web-Traffic sie verarbeiten. Dies berücksichtigt Ihren Bedarf an Diensten, z. B. AWS WAF zum Schutz vor Internet-Ausbeutung. Denken Sie bei internen Anwendungen daran, wie wichtig die interne Bedrohungserkennung und die kontinuierliche Überwachung mit Amazon sind GuardDuty, um ungewöhnliche Zugriffsmuster oder nicht autorisierte Bereitstellungen zu identifizieren.

Denken Sie abschließend an die Raffinesse Ihrer bestehenden Sicherheitsvorkehrungen und das Fachwissen Ihres Sicherheitsteams. Wenn Ihr Team nur über begrenzte Ressourcen verfügt, können Sie mit Services, die mehr Automatisierung und Integration bieten, effektive Sicherheitsverbesserungen erzielen, ohne Ihr Team zu überfordern. Zu den Services gehören AWS Shield beispielsweise DDo der Schutz von Betriebssystemen und AWS Security Hub die zentralisierte Sicherheitsüberwachung.

Compliance and regulatory requirements

Identifizieren Sie die relevanten Gesetze und Standards für Ihre Branche oder geografische Region, z. B. die Allgemeine Datenschutzverordnung (DSGVO), den US-amerikanischen Health Insurance Portability and Accountability Act von 1996 (HIPAA) oder den Payment Card Industry Data Security Standard (PCI DSS).

AWS bietet Dienste wie AWS Config AWS Artifact an, mit denen Sie die Einhaltung verschiedener Standards verwalten können. Mit AWS Config können Sie die Konfigurationen Ihrer AWS Ressourcen beurteilen, prüfen und bewerten, sodass Sie leichter sicherstellen können, dass interne Richtlinien und behördliche Anforderungen eingehalten werden. AWS Artifact bietet On-Demand-Zugriff auf AWS Compliance-Dokumente und unterstützt Sie bei Audits und Compliance-Berichten.

Die Auswahl von Services, die Ihren spezifischen Compliance-Anforderungen entsprechen, kann Ihrem Unternehmen helfen, gesetzliche Anforderungen zu erfüllen und eine sichere und vertrauenswürdige Umgebung für Ihre Daten aufzubauen. Erfahren Sie mehr über AWS Compliance-Programme.

Scalability and flexibility

Überlegen Sie, wie und wie schnell Ihr Unternehmen wachsen wird. Wählen Sie AWS-Services diese Option, damit Ihre Sicherheitsmaßnahmen nahtlos mit Ihrer Infrastruktur mitwachsen und sich an neue Bedrohungen anpassen können.

Um Ihnen eine schnelle Skalierung zu ermöglichen, AWS Control Tower orchestriert es die Funktionen mehrerer anderer Anbieter AWS-Services, darunter AWS Organizations AWS IAM Identity Center, sodass Sie in weniger als einer Stunde eine landing zone einrichten können. Control Tower richtet Ressourcen in Ihrem Namen ein und verwaltet sie.

AWS entwickelt außerdem viele Dienste so, dass sie sich automatisch an den Traffic und die Nutzungsmuster einer Anwendung anpassen, z. B. Amazon GuardDuty zur Erkennung von Bedrohungen und AWS WAF zum Schutz von Webanwendungen. Wenn Ihr Unternehmen wächst, wachsen diese Services mit, ohne dass manuelle Anpassungen erforderlich sind oder Engpässe entstehen.

Darüber hinaus ist es wichtig, dass Sie Ihre Sicherheitskontrollen an Ihre Geschäftsanforderungen und Bedrohungslandschaften anpassen können. Erwägen Sie die Verwaltung Ihrer Konten mit AWS Organizations, sodass Sie die Ressourcen von mehr als 40 Diensten über mehrere Konten hinweg verwalten können. Dies gibt den einzelnen Anwendungsteams die Flexibilität und Transparenz, um Sicherheitsanforderungen zu verwalten, die für ihre Arbeitslast spezifisch sind, und bietet ihnen gleichzeitig Kontrolle und Transparenz gegenüber zentralisierten Sicherheitsteams.

Wenn Sie Skalierbarkeit und Flexibilität berücksichtigen, können Sie sicherstellen, dass Ihre Sicherheitsvorkehrungen robust und reaktionsschnell sind und dynamische Geschäftsumgebungen unterstützen können.

Integration with existing systems

Erwägen Sie Sicherheitsmaßnahmen, die Ihren aktuellen Betrieb verbessern, anstatt ihn zu stören. Denken Sie beispielsweise an Folgendes:

- Optimieren Sie Ihre Arbeitsabläufe, indem Sie Sicherheitsdaten und Warnmeldungen aus AWS-Services bestehenden SIEM-Systemen (Security Information and Event Management) zusammenführen und diese analysieren.
- Verschaffen Sie sich einen einheitlichen Überblick über Sicherheitsbedrohungen und Sicherheitslücken sowohl in lokalen als auch in lokalen AWS Umgebungen.

- AWS CloudTrail Integrieren Sie es in bestehende Protokollverwaltungslösungen, um eine umfassende Überwachung der Benutzeraktivitäten und der API-Nutzung in Ihrer gesamten AWS Infrastruktur und vorhandenen Anwendungen zu gewährleisten.
- Untersuchen Sie, wie Sie die Ressourcennutzung optimieren und Sicherheitsrichtlinien in allen Umgebungen einheitlich anwenden können. Auf diese Weise können Sie das Risiko von Sicherheitslücken verringern.

Cost and budget considerations

Prüfen Sie die Preismodelle für jeden Service, den Sie in Betracht ziehen. AWS Gebühren basieren häufig auf der Nutzung, z. B. der Anzahl der API-Aufrufe, dem verarbeiteten Datenvolumen oder der Menge der gespeicherten Daten. Amazon GuardDuty berechnet beispielsweise Gebühren auf der Grundlage der Menge der Protokolldaten, die für die Erkennung von Bedrohungen analysiert wurden, während die AWS WAF Rechnungen auf der Anzahl der bereitgestellten Regeln und der Anzahl der eingegangenen Webanfragen basieren.

Schätzen Sie Ihre erwartete Nutzung ab, um die Kosten genau prognostizieren zu können. Berücksichtigen Sie sowohl den aktuellen Bedarf als auch potenzielles Wachstum oder Nachfragespitzen. Skalierbarkeit ist beispielsweise ein wichtiges Merkmal von AWS-Services, kann aber auch zu höheren Kosten führen, wenn sie nicht sorgfältig verwaltet wird. Verwenden Sie die AWS -Preisrechner, um verschiedene Szenarien zu modellieren und ihre finanziellen Auswirkungen zu bewerten.

Bewerten Sie die Gesamtbetriebskosten (TCO), die sowohl direkte als auch indirekte Kosten umfassen, z. B. den Zeit- und Ressourcenaufwand für Verwaltung und Wartung. Wenn Sie sich für Managed Services entscheiden, können Sie die Betriebskosten senken, dies kann jedoch mit einem höheren Preis verbunden sein.

Schließlich sollten Sie Ihre Sicherheitsinvestitionen auf der Grundlage einer Risikobewertung priorisieren. Nicht alle Sicherheitsdienste werden für Ihre Infrastruktur gleichermaßen wichtig sein. Konzentrieren Sie Ihr Budget daher auf die Bereiche, die den größten Einfluss auf die Risikominderung und die Einhaltung von Vorschriften haben. Ein ausgewogenes Verhältnis zwischen Kosteneffektivität und dem Sicherheitsniveau, das Sie benötigen, ist der Schlüssel zu einer erfolgreichen AWS Sicherheitsstrategie.

Organizational structure and access needs

Beurteilen Sie, wie Ihre Organisation strukturiert ist und funktioniert und wie Ihre Zugriffsanforderungen je nach Team, Projekt oder Standort variieren können. Dies berücksichtigt,

wie Sie Benutzeridentitäten verwalten und authentifizieren, Rollen zuweisen und Zugriffskontrollen in Ihrer AWS gesamten Umgebung durchsetzen. Implementieren Sie bewährte Methoden, z. B. die Anwendung von Berechtigungen mit den geringsten Rechten und die Anforderung einer Multi-Faktor-Authentifizierung (MFA).

Die meisten Unternehmen benötigen eine Umgebung mit mehreren Konten. Informieren Sie sich über bewährte Methoden für diese Art von Umgebung und ziehen Sie in Betracht, diese AWS Control Tower zu verwenden AWS Organizations und Ihnen bei der Implementierung zu helfen.

Ein weiterer Aspekt, den Sie berücksichtigen sollten, ist die Verwaltung von Anmeldeinformationen und Zugriffsschlüsseln. Erwägen Sie die Verwendung von IAM Identity Center für die Zentralisierung der Zugriffsverwaltung für mehrere AWS-Konten und geschäftliche Anwendungen, was sowohl die Sicherheit als auch den Benutzerkomfort verbessert. Um Ihnen zu helfen, den Zugriff auf alle Konten Ihres Unternehmens reibungslos zu verwalten, lässt sich IAM Identity Center mit integrieren. AWS Organizations

Prüfen Sie außerdem, wie sich diese Identitäts- und Zugriffsverwaltungsdienste in Ihre vorhandenen Verzeichnisdienste integrieren lassen. Wenn Sie bereits über einen Identitätsanbieter verfügen, können Sie ihn mithilfe von SAML 2.0 oder OpenID Connect (OIDC) in IAM Identity Center integrieren. IAM Identity Center unterstützt auch die SCIM-Bereitstellung (System for Cross-Domain Identity Management), damit Ihre Verzeichnisse synchronisiert bleiben. Auf diese Weise können Sie eine nahtlose und sichere Benutzererfahrung beim Zugriff auf Ressourcen gewährleisten. AWS

Wählen Sie einen AWS Sicherheits-, Identitäts- und Governance-Service

Nachdem Sie nun die Kriterien für die Bewertung Ihrer Sicherheitsoptionen kennen, können Sie entscheiden, welche AWS Sicherheitsdienste für Ihre Unternehmensanforderungen am besten geeignet sein könnten.

In der folgenden Tabelle wird dargestellt, welche Dienste für welche Umstände optimiert sind. Anhand der Tabelle können Sie den Service ermitteln, der für Ihr Unternehmen und Ihren Anwendungsfall am besten geeignet ist.

Note

[1] Integriert mit AWS Security Hub (vollständige Liste)
[2] Integriert in Amazon GuardDuty (vollständige Liste)
[3] Integriert in Amazon Security Lake (vollständige Liste)

Wählen Sie AWS Identitäts- und Zugriffsverwaltungsdienste

Gewähren Sie den entsprechenden Personen den entsprechenden Zugriff auf Systeme, Anwendungen und Daten.

Wann sollten Sie es verwenden?	Wofür ist es optimiert?	Sicherheits-, Identitäts- und Governance-Dienste
Verwenden Sie diese Dienste, um den Zugriff für Ihre Kunden, Mitarbeiter und Workloads sicher zu verwalten und zu steuern.	Hilft Ihnen dabei, Ihre Identität squellen zu verbinden oder Benutzer zu erstellen. Sie können den Zugriff Ihrer Mitarbeiter auf mehrere AWS Konten und Anwendungen zentral verwalten.	AWS IAM Identity Center
	Optimiert für die Authentif izierung und Autorisierung von Benutzern für Web- und Mobilanwendungen.	Amazon Cognito
	Optimiert für die sichere gemeinsame Nutzung von Ressourcen innerhalb von. AWS	AWS RAM
	Ermöglicht eine sichere, detaillierte Kontrolle über den Zugriff auf AWS Workload-Ressourcen.	ICH BIN 1

Wählen Sie AWS Datenschutzdienste

Automatisieren und vereinfachen Sie Datenschutz- und Sicherheitsaufgaben, die von der Schlüsselverwaltung und der Erkennung sensibler Daten bis hin zur Verwaltung von Anmeldeinformationen reichen.

Wann sollten Sie es verwenden?	Wofür ist es optimiert?	Dienstleistungen im Bereich Datenschutz
Verwenden Sie diese Dienste, um die Vertraulichkeit, Integrität und Verfügbarkeit sensibler Daten, die in AWS Umgebungen gespeichert und verarbeitet werden, zu gewährleisten und aufrechtz uerhalten.	Optimiert für die Erkennung sensibler Daten.	Amazon Macie 1
	Optimiert für kryptografische Schlüssel.	AWS KMS
	Optimiert für HSMs.	AWS CloudHSM
	Optimiert für private SSL/ TLS X.509-Zertifikate und Schlüssel.	AWS Certificate Manager
	Optimiert für die Erstellun g privater Zertifizierungsste llenhierarchien.	AWS Private CA
	Optimiert für Datenbank anmeldedaten, Anwendung sanmeldedaten, OAuth Token, API-Schlüssel und andere Geheimnisse.	AWS Secrets Manager
	Optimiert für den Zugriff auf kryptografische Funktionen und die Schlüsselverwaltun g, die bei der Zahlungsa bwicklung gemäß den PCI-Standards verwendet werden.	AWS Payment Cryptography

Wählen Sie Dienste für den AWS Netzwerk- und Anwendungsschutz

Schützen Sie Ihre Internetressourcen zentral vor gängigen Betriebssystem DDo - und Anwendungsangriffen.

Wann sollten Sie es verwenden?	Wofür ist es optimiert?	Dienste für den Netzwerk- und Anwendungsschutz
Verwenden Sie diese Dienste, um detaillierte Sicherheitsrichtlinien an jedem Netzwerkkontrollpunkt durchzusetzen.	Optimiert für die zentrale Konfiguration und Verwaltung von Firewallregeln.	AWS Firewall Manager[1]
	Optimiert für die Bereitste llung einer zustandsorientiert en, verwalteten Netzwerk-Firewall und eines Dienstes zur Erkennung und Abwehr von Eindringlingen.	AWS Network Firewall
	Optimiert für den Schutz vor DDo S-Angriffen auf AWS Ressourcen auf Netzwerk-, Transport- und Anwendung sebene.	AWS Shield
	Optimiert für die Bereitstellung einer Firewall für Webanwend ungen.	AWS WAF

Wählen Sie AWS Erkennungs- und Reaktionsdienste

Identifizieren und priorisieren Sie kontinuierlich Sicherheitsrisiken und integrieren Sie gleichzeitig bewährte Sicherheitsmethoden frühzeitig.

Wann sollten Sie es verwenden?	Wofür ist es optimiert?	Erkennungs- und Reaktionsdienste
Verwenden Sie diese Dienste, um Sicherheitsrisiken für Ihre Konten zu erkennen und darauf zu reagieren, sodass Sie Ihre Workloads in großem Umfang schützen können.	Optimiert für die Automatisierung von Sicherheitsprüfungen und die Zentralisierung von Sicherheitswarnungen mit AWS Integrationen von Drittanbietern.	AWS Security Hub[2, 3]
	Optimiert für die Bewertung, Prüfung und Evaluierung der Konfiguration Ihrer Ressourcen.	AWS Config[1]
	Optimiert für die Protokollierung von Ereignissen aus anderen Quellen AWS-Services als Prüfpfad.	AWS CloudTrail
	Optimiert für intelligente Bedrohungserkennung und detaillierte Berichterstattung.	Amazon GuardDuty [1]
	Optimiert für das Schwachstellenmanagement.	Amazon Inspector [1]
	Optimiert für die Zentralisierung von Sicherheitsdaten.	Amazon Security Lake [1]
	Optimiert für die Aggregation und Zusammenfassung potenzieller Sicherheitsprobleme.	Amazon Detective [1, 2, 3]
	Optimiert für die Unterstützung bei der Analyse von Ergebnissen, der Eskalatio	AWS Reaktion auf Sicherheitsvorfälle

Wann sollten Sie es verwenden?	Wofür ist es optimiert?	Erkennungs- und Reaktionsdienste
	n von Sicherheitsereignissen und der Verwaltung von Fällen, die Ihre sofortige Aufmerksamkeit erfordern.	

Entscheiden Sie sich für AWS Governance- und Compliance-Services

Richten Sie Cloud-Governance für Ihre Ressourcen ein und automatisieren Sie Ihre Compliance- und Auditprozesse.

Wann sollten Sie es verwenden?	Wofür ist es optimiert?	Dienstleistungen im Bereich Unternehmensführung und Compliance
Nutzen Sie diese Services, um Sie bei der Implementierung von Best Practices zu unterstützen und bei der Nutzung die Branchenstandards einzuhalten AWS.	Optimiert für die zentrale Verwaltung mehrerer Konten und die konsolidierte Abrechnung.	AWS Organizations
	Optimiert für die Bereitstellung von On-Demand-Downloads von AWS Sicherheits- und Compliance-Dokumenten.	AWS Artifact
	Optimiert für die Prüfung der AWS Nutzung.	AWS Audit Manager[1]
	Optimiert für die Einrichtung und Verwaltung einer Umgebung AWS mit mehreren Konten.	AWS Control Tower

Nutzen Sie AWS Sicherheits-, Identitäts- und Governance-Dienste

Sie sollten jetzt genau wissen, was die einzelnen AWS Sicherheits-, Identitäts- und Governance-Dienste (und die unterstützenden AWS Tools und Dienste) tun und welche für Sie geeignet sein könnten.

Um zu erfahren, wie Sie die einzelnen verfügbaren AWS Sicherheits-, Identitäts- und Governance-Dienste verwenden können, und mehr über sie erfahren, haben wir einen Weg bereitgestellt, um zu untersuchen, wie die einzelnen Dienste funktionieren. In den folgenden Abschnitten finden Sie Links zu ausführlicher Dokumentation, praktischen Tutorials und Ressourcen, die Ihnen den Einstieg erleichtern.

Verwenden Sie AWS Identitäts- und Zugriffsverwaltungsdienste

In den folgenden Tabellen sind einige nützliche Ressourcen zur Identitäts- und Zugriffsverwaltung aufgeführt, die nach Diensten geordnet sind und Ihnen den Einstieg erleichtern sollen.

AWS IAM Identity Center

- AWS IAM Identity Center aktivieren

  Aktivieren Sie IAM Identity Center und beginnen Sie, es mit Ihrem zu verwenden. AWS Organizations

  Den Leitfaden erkunden
- Konfigurieren Sie den Benutzerzugriff mit dem standardmäßigen IAM Identity Center-Verzeichnis

  Verwenden Sie das Standardverzeichnis als Identitätsquelle und richten Sie den Benutzerzugriff ein und testen Sie ihn.

  Erste Schritte mit dem Tutorial
- Verwenden von Active Directory als Identitätsquelle

  Vervollständigen Sie die Grundkonfiguration für die Verwendung von Active Directory als IAM Identity Center-Identitätsquelle.

  Erste Schritte mit dem Tutorial
- Konfigurieren Sie SAML und SCIM mit Okta und IAM Identity Center

Richten Sie eine SAML-Verbindung mit Okta und IAM Identity Center ein.

Erste Schritte mit dem Tutorial

Amazon Cognito

- Erste Schritte mit Amazon Cognito

  Erfahren Sie mehr über die häufigsten Amazon Cognito Cognito-Aufgaben.

  Den Leitfaden erkunden
- Tutorial: Einen Benutzerpool erstellen

  Erstellen Sie einen Benutzerpool, über den sich Ihre Benutzer bei Ihrer Web- oder Mobil-App anmelden können.

  Erste Schritte mit dem Tutorial
- Tutorial: Einen Identitätspool erstellen

  Erstellen Sie einen Identitätspool, der es Ihren Benutzern ermöglicht, temporäre AWS Anmeldeinformationen für den Zugriff zu erhalten AWS-Services.

  Erste Schritte mit dem Tutorial
- Amazon Cognito Cognito-Workshop

  Üben Sie, Amazon Cognito zu verwenden, um eine Authentifizierungslösung für eine hypothetische Tierhandlung zu entwickeln.

  Erste Schritte mit dem Tutorial

AWS RAM

- Erste Schritte mit AWS RAM

  Erfahren Sie mehr über AWS RAM Begriffe und Konzepte.

  Den Leitfaden erkunden
- Mit gemeinsam genutzten AWS Ressourcen arbeiten

Teilen Sie AWS Ressourcen, die Sie besitzen, und greifen Sie auf AWS Ressourcen zu, die mit Ihnen geteilt wurden.

Den Leitfaden erkunden

- Verwaltung von Berechtigungen im AWS RAM

  Erfahren Sie mehr über die beiden Arten verwalteter Berechtigungen: AWS verwaltete Berechtigungen und vom Kunden verwaltete Berechtigungen.

  Den Leitfaden erkunden

- Konfigurieren Sie den detaillierten Zugriff auf Ihre Ressourcen, die über AWS RAM gemeinsam genutzt werden

  Verwenden Sie vom Kunden verwaltete Berechtigungen, um Ihren Ressourcenzugriff individuell anzupassen und die bewährte Methode der geringsten Zugriffsrechte zu nutzen.

  Lesen Sie den Blog

IAM

- Erste Schritte mit IAM

  Erstellen Sie IAM-Rollen, -Benutzer und -Richtlinien mithilfe von. AWS Management Console

  Erste Schritte mit dem Tutorial

- Delegieren Sie den Zugriff mithilfe von Rollen AWS-Konten

  Verwenden Sie eine Rolle, um den Zugriff auf Ressourcen in anderen Bereichen als Produktion und Entwicklung zu delegieren AWS-Konten , die Sie besitzen.

  Erste Schritte mit dem Tutorial

- Erstellen Sie eine vom Kunden verwaltete Richtlinie

  Verwenden Sie die AWS Management Console , um eine vom Kunden verwaltete Richtlinie zu erstellen, und fügen Sie diese Richtlinie dann einem IAM-Benutzer in Ihrem AWS-Konto hinzu.

  Erste Schritte mit dem Tutorial

- Definieren Sie Berechtigungen für den Zugriff auf AWS Ressourcen auf der Grundlage von Tags

  Erstellen und testen Sie eine Richtlinie, die es IAM-Rollen mit Prinzipal-Tags ermöglicht, auf Ressourcen mit passenden Tags zuzugreifen.

  Erste Schritte mit dem Tutorial
- Bewährte Sicherheitsmethoden in IAM

  Tragen Sie zur Sicherung Ihrer AWS Ressourcen bei, indem Sie bewährte IAM-Praktiken anwenden.

  Den Leitfaden erkunden

Nutzen Sie AWS Datenschutzdienste

Der folgende Abschnitt enthält Links zu detaillierten Ressourcen, in denen der AWS Datenschutz beschrieben wird.

Macie

- Erste Schritte mit Amazon Macie

  Aktivieren Sie Macie für Sie AWS-Konto, bewerten Sie Ihren Amazon S3 S3-Sicherheitsstatus und konfigurieren Sie wichtige Einstellungen und Ressourcen für die Erkennung und Meldung sensibler Daten in Ihren S3-Buckets.

  Den Leitfaden erkunden
- Überwachung von Datensicherheit und Datenschutz mit Amazon Macie

  Verwenden Sie Amazon Macie, um die Amazon S3 S3-Datensicherheit zu überwachen und Ihren Sicherheitsstatus zu bewerten.

  Den Leitfaden erkunden
- Analyse der Ergebnisse von Amazon Macie

  Überprüfen, analysieren und verwalten Sie die Ergebnisse von Amazon Macie.

  Den Leitfaden erkunden

- Abrufen sensibler Datenproben mit Amazon Macie Macie-Ergebnissen

  Verwenden Sie Amazon Macie, um Stichproben sensibler Daten abzurufen und offenzulegen, die aufgrund von Einzelbefunden gemeldet wurden.

  Den Leitfaden erkunden
- Erkennung sensibler Daten mit Amazon Macie

  Automatisieren Sie die Erkennung, Protokollierung und Berichterstattung sensibler Daten in Ihrem Amazon S3 S3-Datenbestand.

  Den Leitfaden erkunden

AWS KMS

- Erste Schritte mit AWS KMS

  Verwalten Sie KMS-Schlüssel mit symmetrischer Verschlüsselung, von der Erstellung bis zur Löschung.

  Den Leitfaden erkunden
- Schlüssel für spezielle Zwecke

  Erfahren Sie mehr über die verschiedenen Schlüsseltypen, die zusätzlich zur symmetrischen Verschlüsselung KMS-Schlüssel AWS KMS unterstützt werden.

  Den Leitfaden erkunden
- Skalieren Sie Ihre Funktionen zur Verschlüsselung im Ruhezustand mit AWS KMS

  Erfahren Sie mehr über die Optionen zur Verschlüsselung im Ruhezustand, die in dieser Datei verfügbar sind AWS.

  Den Workshop erkunden

AWS CloudHSM

- Erste Schritte mit AWS CloudHSM

  Erstellen, initialisieren und aktivieren Sie einen AWS CloudHSM Cluster.

Den Leitfaden erkunden

- Cluster verwalten AWS CloudHSM

  Connect zu Ihrem AWS CloudHSM Cluster und den verschiedenen administrativen Aufgaben bei der Verwaltung Ihres Clusters her.

  Den Leitfaden erkunden

- HSM-Benutzer verwalten und Schlüssel eingeben AWS CloudHSM

  Erstellen Sie Benutzer und Schlüssel auf dem HSMs in Ihrem Cluster.

  Den Leitfaden erkunden

- Automatisieren Sie die Bereitstellung eines NGINX-Webservices mithilfe von Amazon ECS mit TLS-Offload in CloudHSM

  Verwenden Sie diese AWS CloudHSM Option, um Ihre privaten Schlüssel für Ihre Websites zu speichern, die in der Cloud gehostet werden.

  Lesen Sie den Blog

AWS Certificate Manager

- Ein öffentliches Zertifikat beantragen

  Verwenden Sie die AWS Certificate Manager (ACM-) Konsole oder AWS CLI um ein öffentliches ACM-Zertifikat anzufordern.

  Den Leitfaden erkunden

- Bewährte Methoden für AWS Certificate Manager

  Lernen Sie bewährte Verfahren kennen, die auf realen Erfahrungen von aktuellen ACM-Kunden basieren.

  Den Leitfaden erkunden

- Wie verwendet man, AWS Certificate Manager um Kontrollen bei der Ausstellung von Zertifikaten durchzusetzen

Verwenden Sie IAM-Bedingungsschlüssel, um sicherzustellen, dass Ihre Benutzer TLS-Zertifikate gemäß den Richtlinien Ihrer Organisation ausstellen oder anfordern.

Lesen Sie den Blog

AWS Private CA

- Planen Sie Ihren AWS Private CA Einsatz

  Bereiten Sie AWS Private CA sich auf die Nutzung vor, bevor Sie eine private Zertifizierungsstelle einrichten.

  Den Leitfaden erkunden

- AWS Private CA Verwaltung

  Erstellen Sie eine vollständig AWS gehostete Hierarchie von Stamm- und untergeordneten Zertifizierungsstellen für den internen Gebrauch in Ihrer Organisation.

  Den Leitfaden erkunden

- Verwaltung von Zertifikaten

  Führen Sie grundlegende Aufgaben zur Zertifikatsverwaltung durch AWS Private CA, z. B. das Ausstellen, Abrufen und Auflisten von privaten Zertifikaten.

  Den Leitfaden erkunden

- AWS Private CA Workshop

  Entwickeln Sie praktische Erfahrungen mit verschiedenen Anwendungsfällen privater Zertifizierungsstellen.

  Den Workshop erkunden

- So vereinfachen Sie die Bereitstellung von Zertifikaten in Active Directory mit AWS Private CA

  Wird verwendet AWS Private CA , um Zertifikate für Benutzer und Computer in Ihrer Microsoft Active Directory-Umgebung einfacher bereitzustellen.

  Lesen Sie den Blog

- Wie erzwingt man DNS-Namensbeschränkungen in AWS Private CA

Wenden Sie mithilfe des Dienstes DNS-Namenseinschränkungen auf eine untergeordnete AWS Private CA Zertifizierungsstelle an.

Lesen Sie den Blog

AWS Secrets Manager

- AWS Secrets Manager Konzepte

  Führen Sie grundlegende Aufgaben zur Zertifikatsverwaltung durch AWS Private CA, z. B. das Ausstellen, Abrufen und Auflisten von privaten Zertifikaten.

  Den Leitfaden erkunden

- Richten Sie eine wechselnde Benutzerrotation ein für AWS Secrets Manager

  Richten Sie eine abwechselnde Benutzerrotation für ein Geheimnis ein, das Datenbankanmeldedaten enthält.

  Den Leitfaden erkunden

- Verwenden von AWS Secrets Manager Geheimnissen mit Kubernetes

  Zeigen Sie Geheimnisse aus Secrets Manager als Dateien an, die mithilfe des AWS Secrets and Configuration Provider (ASCP) in Amazon EKS-Pods gemountet wurden.

  Den Leitfaden erkunden

AWS Payment Cryptography

- Erste Schritte mit AWS Payment Cryptography

  Erstellen Sie Schlüssel und verwenden Sie sie für verschiedene kryptografische Operationen.

  Den Leitfaden erkunden

- AWS Payment Cryptography FAQs

  Verstehe die Grundlagen von. AWS Payment Cryptography

  Erkunden Sie die FAQs

Nutzen Sie AWS Netzwerk- und Anwendungsschutzdienste

Die folgenden Tabellen enthalten Links zu ausführlichen Ressourcen, in denen der AWS Netzwerk- und Anwendungsschutz beschrieben wird.

AWS Firewall Manager

- Erste Schritte mit AWS Firewall Manager Richtlinien

  Wird verwendet AWS Firewall Manager , um verschiedene Arten von Sicherheitsrichtlinien zu aktivieren.

  Den Leitfaden erkunden
- Wie können Sicherheitsgruppen kontinuierlich überwacht und eingeschränkt werden mit AWS Firewall Manager

  Wird verwendet AWS Firewall Manager , um Sicherheitsgruppen einzuschränken und sicherzustellen, dass nur die erforderlichen Ports geöffnet sind.

  Lesen Sie den Blog
- Wird verwendet AWS Firewall Manager , um Schutz in großem Umfang bereitzustellen in AWS Organizations

  Wird verwendet AWS Firewall Manager , um Sicherheitsrichtlinien in Ihrem Unternehmen bereitzustellen und zu verwalten AWS Organizations.

  Lesen Sie den Blog

AWS Network Firewall

- Erste Schritte mit AWS Network Firewall

  Konfigurieren und implementieren Sie eine AWS Network Firewall Firewall für eine VPC mit einer grundlegenden Internet-Gateway-Architektur.

  Den Leitfaden erkunden
- AWS Network Firewall Werkstatt

  Stellen Sie einen bereit, AWS Network Firewall indem Sie Infrastruktur als Code verwenden.

Den Workshop erkunden

- Praktische Einführung in die AWS Network Firewall flexible Regel-Engine — Teil 1

  Stellen Sie eine Demonstration von AWS Network Firewall in Ihrem bereit AWS-Konto , um mit der Regel-Engine zu interagieren.

  Lesen Sie den Blog

- Praktische Einführung in die AWS Network Firewall flexible Regel-Engine — Teil 2

  Erstellen Sie eine Firewall-Richtlinie mit einer strengen Regelreihenfolge und legen Sie eine oder mehrere Standardaktionen fest.

  Lesen Sie den Blog

- Bereitstellungsmodelle für AWS Network Firewall

  Lernen Sie Bereitstellungsmodelle für gängige Anwendungsfälle kennen, bei denen Sie AWS Network Firewall den Datenverkehrspfad erweitern können.

  Lesen Sie den Blog

- Bereitstellungsmodelle für AWS Network Firewall mit VPC-Routing-Verbesserungen

  Verwenden Sie erweiterte VPC-Routing-Primitive, um AWS Network Firewall zwischen Workloads in verschiedenen Subnetzen derselben VPC einzufügen.

  Lesen Sie den Blog

AWS Shield

- Wie AWS Shield funktioniert

  Erfahren Sie, wie AWS Ressourcen auf der Netzwerk AWS Shield Standard - AWS Shield Advanced und Transportebene (Schicht 3 und 4) sowie auf der Anwendungsebene (Schicht 7) vor DDo S-Angriffen geschützt werden.

  Den Leitfaden erkunden

- Erste Schritte mit AWS Shield Advanced

  Verwenden Sie AWS Shield Advanced zunächst die Shield Advanced-Konsole.

Den Leitfaden erkunden

- AWS Shield Advanced Werkstatt

  Schützen Sie im Internet exponierte Ressourcen vor DDo S-Angriffen, überwachen Sie DDo S-Angriffe auf Ihre Infrastruktur und benachrichtigen Sie die entsprechenden Teams.

  Den Workshop erkunden

AWS WAF

- Erste Schritte mit AWS WAF

  Richten Sie eine Web-ACL ein AWS WAF, erstellen Sie sie und schützen Sie Amazon, CloudFront indem Sie Regeln und Regelgruppen hinzufügen, um Webanfragen zu filtern.

  Erste Schritte mit dem Tutorial
- Analysieren von AWS WAF Protokollen in Amazon CloudWatch Logs

  Richten Sie die native AWS WAF Protokollierung in CloudWatch Amazon-Protokollen ein und visualisieren und analysieren Sie die Daten in den Protokollen.

  Lesen Sie den Blog
- Visualisieren Sie AWS WAF Protokolle mit einem CloudWatch Amazon-Dashboard

  Verwenden Sie Amazon CloudWatch , um AWS WAF Aktivitäten mithilfe von CloudWatch Metriken, Contributor Insights und Logs Insights zu überwachen und zu analysieren.

  Lesen Sie den Blog

Verwenden Sie AWS Erkennungs- und Reaktionsdienste

Die folgenden Tabellen enthalten Links zu detaillierten Ressourcen, in denen AWS Erkennungs- und Reaktionsdienste beschrieben werden.

AWS Config

- Erste Schritte mit AWS Config

  Richten Sie ein AWS Config und arbeiten Sie mit AWS SDKs.

Den Leitfaden erkunden

- Workshop zu Risiko und Compliance

  Automatisieren Sie AWS Config Steuerungen mithilfe von AWS Managed Config Rules.

  Den Workshop erkunden

- AWS Config Bibliothek des Rule Development Kit: Regeln in großem Maßstab erstellen und anwenden

  Verwenden Sie das Rule Development Kit (RDK), um eine benutzerdefinierte AWS Config Regel zu erstellen und sie zusammen mit dem RDKLib bereitzustellen.

  Lesen Sie den Blog

AWS CloudTrail

- Event-Historie anzeigen

  Überprüfen Sie die AWS API-Aktivität in Ihrem AWS-Konto für Dienste, die Folgendes unterstützen CloudTrail.

  Erste Schritte mit dem Tutorial

- Erstellen Sie einen Pfad, um Verwaltungsereignisse zu protokollieren

  Erstellen Sie einen Pfad, um Verwaltungsereignisse in allen Regionen zu protokollieren.

  Erste Schritte mit dem Tutorial

AWS Security Hub

- Aktiviert AWS Security Hub

  AWS Security Hub Mit AWS Organizations oder in einem eigenständigen Konto aktivieren.

  Den Leitfaden erkunden

- Regionsübergreifende Aggregation

  Aggregieren Sie AWS Security Hub Ergebnisse aus mehreren AWS-Regionen Aggregationsregionen in einer einzigen Aggregationsregion.

Den Leitfaden erkunden

- AWS Security Hub Werkstatt

  Erfahren Sie, wie Sie die Sicherheitslage Ihrer AWS Umgebungen nutzen AWS Security Hub , verwalten und verbessern können.

  Den Workshop erkunden

- Drei wiederkehrende Security Hub Hub-Nutzungsmuster und wie man sie einsetzt

  Erfahren Sie mehr über die drei häufigsten AWS Security Hub Nutzungsmuster und wie Sie Ihre Strategie zur Identifizierung und Verwaltung von Ergebnissen verbessern können.

  Lesen Sie den Blog

Amazon GuardDuty

- Erste Schritte mit Amazon GuardDuty

  Aktivieren Sie Amazon GuardDuty, generieren Sie Stichprobenergebnisse und richten Sie Benachrichtigungen ein.

  Erkunden Sie das Tutorial

- EKS-Schutz bei Amazon GuardDuty

  Verwenden Sie Amazon GuardDuty , um Ihre Amazon Elastic Kubernetes Service (Amazon EKS) Audit-Logs zu überwachen.

  Den Leitfaden erkunden

- Lambda-Schutz bei Amazon GuardDuty

  Identifizieren Sie potenzielle Sicherheitsbedrohungen, wenn Sie eine AWS Lambda Funktion aufrufen.

  Den Leitfaden erkunden

- GuardDuty Amazon RDS-Schutz

Verwenden Sie Amazon GuardDuty , um die Anmeldeaktivitäten des Amazon Relational Database Service (Amazon RDS) im Hinblick auf potenzielle Zugriffsbedrohungen auf Ihre Amazon Aurora Aurora-Datenbanken zu analysieren und zu profilieren.

Den Leitfaden erkunden

- Amazon S3 S3-Schutz bei Amazon GuardDuty

  Wird GuardDuty zur Überwachung von CloudTrail Datenereignissen und zur Identifizierung potenzieller Sicherheitsrisiken in Ihren S3-Buckets verwendet.

  Den Leitfaden erkunden

- Erkennung und Reaktion auf Bedrohungen mit Amazon GuardDuty und Amazon Detective

  Lernen Sie die Grundlagen von Amazon GuardDuty und Amazon Detective kennen.

  Den Workshop erkunden

Amazon Inspector

- Erste Schritte mit Amazon Inspector

  Aktivieren Sie Amazon Inspector-Scans, um die Ergebnisse in der Konsole zu verstehen.

  Erste Schritte mit dem Tutorial

- Schwachstellenmanagement mit Amazon Inspector

  Verwenden Sie Amazon Inspector, um EC2 Amazon-Instances und Container-Images in Amazon Elastic Container Registry (Amazon ECR) auf Softwareschwachstellen zu scannen.

  Den Workshop erkunden

- So scannen Sie EC2 AMIs mit Amazon Inspector

  Erstellen Sie eine Lösung, indem Sie mehrere verwenden AWS-Services , um Ihre AMIs nach bekannten Sicherheitslücken zu durchsuchen.

  Lesen Sie den Blog

Amazon Security Lake

- Erste Schritte mit Amazon Security Lake

  Aktivieren Sie Amazon Security Lake und beginnen Sie mit der Nutzung.

  Den Leitfaden erkunden
- Verwaltung mehrerer Konten mit AWS Organizations

  Sammeln Sie Sicherheitsprotokolle und Ereignisse von mehreren AWS-Konten.

  Den Leitfaden erkunden
- Erfassung, Transformation und Bereitstellung von Ereignissen, die von Amazon Security Lake veröffentlicht werden, an Amazon Service OpenSearch

  Erfassen, transformieren und liefern Sie Amazon Security Lake-Daten an Amazon OpenSearch Service, damit Ihre SecOps Teams sie verwenden können.

  Lesen Sie den Blog
- So visualisieren Sie die Ergebnisse von Amazon Security Lake mit QuickSight

  Abfragen und Visualisieren von Daten aus Amazon Security Lake mithilfe von Amazon Athena undQuickSight.

  Lesen Sie den Blog

Amazon Detective

- Begriffe und Konzepte von Amazon Detective

  Lernen Sie die wichtigsten Begriffe und Konzepte kennen, die für das Verständnis von Amazon Detective wichtig sind, und erfahren Sie, wie Amazon Detective funktioniert.

  Den Leitfaden erkunden
- Amazon Detective einrichten

  Aktivieren Sie Amazon Detective über die Amazon Detective-Konsole, die Amazon Detective API oder AWS CLI.

  Den Leitfaden erkunden

- Erkennung und Reaktion auf Bedrohungen mit Amazon GuardDuty und Amazon Detective

  Lernen Sie die Grundlagen von Amazon GuardDuty und Amazon Detective kennen.

  Den Workshop erkunden

Nutzen Sie AWS Governance- und Compliance-Dienste

Die folgenden Tabellen enthalten Links zu detaillierten Ressourcen, in denen Unternehmensführung und Compliance beschrieben werden.

AWS Organizations

- Eine Organisation erstellen und konfigurieren

  Erstellen Sie Ihre Organisation und konfigurieren Sie sie mit zwei AWS Mitgliedskonten.

  Erste Schritte mit dem Tutorial
- Dienste, die funktionieren mit AWS Organizations

  Finden AWS-Services Sie heraus, mit welchen Services Sie sie nutzen können AWS Organizations und welche Vorteile die Nutzung der einzelnen Services auf unternehmensweiter Ebene bietet.

  Den Leitfaden erkunden
- Organisieren Sie Ihre AWS Umgebung mithilfe mehrerer Konten

  Implementieren Sie bewährte Verfahren und aktuelle Empfehlungen für die Organisation Ihrer gesamten AWS Umgebung.

  Lesen Sie das Whitepaper

AWS Artifact

- Erste Schritte mit AWS Artifact

  Laden Sie Sicherheits- und Compliance-Berichte herunter, verwalten Sie rechtliche Vereinbarungen und verwalten Sie Benachrichtigungen.

  Den Leitfaden erkunden

- Verwaltung von Vereinbarungen in AWS Artifact

  Verwenden Sie den, AWS Management Console um Vereinbarungen für Ihr Konto oder Ihre Organisation zu überprüfen, zu akzeptieren und zu verwalten.

  Den Leitfaden erkunden
- Bereiten Sie sich auf ein Audit in AWS Teil 1 vor — AWS Audit Manager und AWS Artifact AWS Config

  Wird verwendet AWS-Services , um Ihnen zu helfen, die Erfassung von Nachweisen zu automatisieren, die bei Audits verwendet werden.

  Lesen Sie den Blog

AWS Audit Manager

- AWS Audit Manager aktivieren

  Aktivieren Sie Audit Manager mithilfe der AWS Management Console, der Audit Manager API oder der AWS CLI.

  Den Leitfaden erkunden
- Tutorial für Audit-Verantwortliche: Eine Bewertung erstellen

  Erstellen Sie eine Bewertung mithilfe des Audit Manager Sample Framework.

  Den Leitfaden erkunden
- Tutorial für Delegierte: Überprüfung eines Kontrollsatzes

  Prüfen Sie einen Kontrollsatz, der Ihnen von einem Prüfungsverantwortlichen in Audit Manager mitgeteilt wurde.

  Den Leitfaden erkunden

AWS Control Tower

- Erste Schritte mit AWS Control Tower

  Richten Sie eine Umgebung mit mehreren Konten, eine sogenannte landing zone, ein und starten Sie sie, die vorgeschriebenen Best Practices befolgt.

Den Leitfaden erkunden

- Modernisierung der Kontoverwaltung mit Amazon Bedrock und AWS Control Tower

  Richten Sie ein Konto für Sicherheitstools ein und nutzen Sie generative KI, um den Einrichtungs- und Verwaltungsprozess zu beschleunigen. AWS-Konto

  Lesen Sie den Blog

- Aufbau einer gut strukturierten AWS GovCloud (US-) Umgebung mit AWS Control Tower

  Richten Sie Ihre Governance in den Regionen AWS GovCloud (USA) ein, einschließlich der Steuerung Ihrer AWS Workloads mithilfe von Organisationseinheiten (OUs) und. AWS-Konten

  Lesen Sie den Blog

Informieren Sie sich über AWS Sicherheits-, Identitäts- und Governance-Dienste

Editable architecture diagrams

Referenzarchitekturdiagramme

Sehen Sie sich Referenzarchitekturdiagramme an, die Sie bei der Entwicklung Ihrer Sicherheits-, Identitäts- und Governance-Strategie unterstützen.

Erkunden Sie die Referenzarchitekturen für Sicherheit, Identität und Governance

Ready-to-use code

Ausgewählte Lösung	AWS Lösungen
Einblicke in die Sicherheit auf AWS Stellen Sie AWS integrierten Code bereit, der Ihnen hilft, Daten in Amazon Security Lake zu visualisieren, um Sicherheitsereignisse schneller untersuchen und darauf reagieren zu können.	Entdecken Sie vorkonfigurierte, einsatzbe reite Lösungen und deren Implementierungsle itfäden, entwickelt von. AWS Entdecken Sie alle AWS Sicherheits-, Identitäts- und Governance-Lösungen

Erkunden Sie diese Lösung

Documentation

Whitepapers zu Sicherheit, Identität und Unternehmensführung

In unseren Whitepapers finden Sie weitere Einblicke und bewährte Verfahren zur Auswahl, Implementierung und Nutzung der Sicherheits-, Identitäts- und Governance-Services, die am besten zu Ihrem Unternehmen passen.

Entdecken Sie Whitepapers zu Sicherheit, Identität und Unternehmensführung

AWS Blog zum Thema Sicherheit

Entdecken Sie Blogbeiträge, die sich mit bestimmten Sicherheitsanwendungsfällen befassen.

Erkunden Sie den AWS Sicherheits-Blog

Dokumentverlauf

In der folgenden Tabelle werden die wichtigen Änderungen an diesem Entscheidungsleitfaden beschrieben. Für Benachrichtigungen über Aktualisierungen dieses Handbuchs können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
re:Invent-Update	Es wurden Informationen zur Reaktion auf AWS Sicherheitsvorfälle und hinzugefügt. AWS Payment Cryptography Aktualisierte Serviceinformationen für AWS Identity and Access Management und AWS IAM Identity Center.	30. Dezember 2024
Video-Update	Aktualisiertes Einführungsvideo mit einem aktuellen Lightning Talk von Re:inForce 2024.	25. Juni 2024
Es wurden Governance-Dienste hinzugefügt	Der Geltungsbereich des Dokuments wurde um die Verwaltung erweitert, einschließlich der Hinzufügung von AWS CloudTrail AWS Control Tower, und AWS Organizations. Die Grafiken wurden aktualisiert, um dem neuen Geltungsbereich Rechnung zu tragen. Bewährte Verfahren für Identitäten wurden klargestellt. Redaktionelle Änderungen im gesamten Dokument.	7. Juni 2024
Erste Veröffentlichung	Leitfaden zuerst veröffentlicht.	21. März 2024

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.