

AW261 Security Engineering on AWS

Kurzbeschreibung:

Sicherheit ist ein zentrales Anliegen sowohl für bestehende Kunden in der Cloud als auch für Unternehmen, die eine Cloud-Einführung in Erwägung ziehen. Die Zunahme von Cyberangriffen und Datenlecks bleibt für die meisten Fachkräfte der Branche ein zentrales Thema. Der Kurs **AW261 Security Engineering on AWS** greift diese Bedenken auf, indem er Ihnen hilft, ein besseres Verständnis dafür zu entwickeln, wie Sie sicher mit Amazon Web Services (AWS) arbeiten und aufbauen.

In diesem Kurs **AW261 Security Engineering on AWS** lernen Sie die Verwaltung von Identitäten und Rollen, das Management und die Bereitstellung von Accounts sowie das Monitoring der API-Aktivität auf Anomalien. Außerdem lernen Sie, wie Sie Daten schützen, die in AWS gespeichert sind. Der Kurs **AW261 Security Engineering on AWS** zeigt, wie Sie Logs erzeugen, sammeln und überwachen können, um Sicherheitsvorfälle zu identifizieren. Schließlich befassen Sie sich mit der Erkennung und Untersuchung von Sicherheitsvorfällen mit AWS-Services.

Der Kurs **AW261 Security Engineering on AWS** setzt sich aus einer Präsentation und Übungen zusammen, um das Erlernete praktisch anzuwenden. Die Kursunterlagen (E-Book) sind in englischer Sprache, die Kurssprache ist deutsch.

Zielgruppe:

Dieser Kurs **AW261 Security Engineering on AWS** richtet sich an:

- Security Engineers
- Security Architects
- Cloud Architects
- Cloud Operators in allen globalen Segmenten

Voraussetzungen:

Um an dem Kurs **AW261 Security Engineering on AWS** bei qSkills teilnehmen zu können, sollten Sie das folgende AWS-Training besucht haben:

- Security Fundamentals (digital)
- [AW120 AWS Security Essentials](#)
- [AW200 Architecting on AWS](#)

Darüber hinaus sollten Sie folgende Voraussetzungen erfüllen:

- Erfahrung im Umgang mit Governance-, Risiko- und Compliance-Vorschriften sowie Kontrollzielen
- Praxiserfahrung im Umgang mit IT-Sicherheitsverfahren
- Praxiserfahrung im Umgang mit IT- Infrastrukturkonzepten
- Verständnis von Cloud Computing-Konzepten

Sonstiges:

Dauer: 3 Tage

Preis: 2685 Euro plus Mwst.

Ziele:

In diesem Kurs **AW261 Security Engineering on AWS** lernen Sie:

- Die AWS Cloud Security auf Basis des CIA-Dreiecks zu verstehen
- Authentifizierung und Autorisierung mit IAM zu erstellen und zu analysieren
- Accounts mit geeigneten AWS-Services zu verwalten und bereitzustellen
- Möglichkeiten zur Geheimnisverwaltung mit AWS-Services zu identifizieren
- Sensible Informationen zu überwachen und Daten durch Verschlüsselung und Zugriffskontrollen zu schützen
- AWS-Services zu identifizieren, die Angriffe von außen adressieren
- Logs zu generieren, zu sammeln und zu überwachen
- Indikatoren für Sicherheitsvorfälle zu identifizieren
- Bedrohungen zu untersuchen und mit AWS-Services zu beheben

Der Kurs **AW261 Security Engineering on AWS** unterstützt Sie bei der Vorbereitung auf folgende Prüfung:
AWS Certified Security – Specialty

Inhalte/Agenda:

- **◆ Überblick und Wiederholung zur Sicherheit**
 - ◆ Sicherheit in der AWS Cloud erläutern
 - ◆ Das AWS Shared Responsibility Model erläutern
 - ◆ IAM, Datenschutz sowie Erkennung und Reaktion auf Bedrohungen zusammenfassen
 - ◆ Interaktionsmöglichkeiten mit AWS über Konsole, CLI und SDKs beschreiben
 - ◆ MFA als zusätzliche Schutzmaßnahme beschreiben
 - ◆ Schutz des Root-User-Kontos und von Access Keys erklären
- **◆ Absicherung der Einstiegspunkte in AWS**
 - ◆ Einsatz von Multi-Factor Authentication (MFA) als zusätzliche Schutzmaßnahme beschreiben
 - ◆ Schutz des Root-User-Kontos und von Access Keys beschreiben
 - ◆ IAM-Richtlinien, Rollen, Richtlinienkomponenten und Berechtigungsgrenzen beschreiben
 - ◆ Protokollierung und Analyse von API-Anfragen mit AWS CloudTrail erläutern sowie Zugriffshistorie anzeigen und analysieren
 - ◆ Hands-on Lab: Einsatz von Identity- und Resource-Based Policies
- **◆ Account-Management und Bereitstellung in AWS**
 - ◆ Verwaltung mehrerer AWS-Accounts mit AWS Organizations und AWS Control Tower erläutern
 - ◆ Implementierung von Multi-Account-Umgebungen mit AWS Control Tower erläutern
 - ◆ Zugriff auf AWS-Services über Identity Provider und Broker demonstrieren
 - ◆ Einsatz von AWS IAM Identity Center (Nachfolger von AWS Single Sign-On) und AWS Directory Service erläutern
 - ◆ Verwaltung von Domain-Benutzerzugriffen mit Directory Service und IAM Identity Center demonstrieren
 - ◆ Hands-on Lab: Verwaltung von Domain-Benutzerzugriffen mit AWS Directory Service
- **◆ Geheimnisverwaltung in AWS**
 - ◆ Funktionen von AWS KMS, CloudHSM, AWS Certificate Manager (ACM) und AWS Secrets Manager beschreiben und auflisten
 - ◆ Erstellung eines Multi-Region AWS KMS-Schlüssels demonstrieren
 - ◆ Verschlüsselung eines Secrets in AWS Secrets Manager mit einem AWS KMS-Schlüssel demonstrieren
 - ◆ Nutzung eines verschlüsselten Secrets zur Verbindung mit einer Amazon RDS-Datenbank in mehreren AWS-Regionen demonstrieren
 - ◆ Hands-on Lab: Lab 3 – Verschlüsselung von Secrets in Secrets Manager mit AWS KMS
- **◆ Datensicherheit**
 - ◆ Überwachung von Daten auf sensible Informationen mit Amazon Macie
 - ◆ Schutz von Daten im Ruhezustand durch Verschlüsselung und Zugriffskontrollen beschreiben
 - ◆ AWS-Services zur Replikation von Daten für Schutzmaßnahmen identifizieren
 - ◆ Schutz von archivierten Daten bestimmen
 - ◆ Hands-on Lab: Lab 4 – Datensicherheit in Amazon S3
- **◆ Infrastruktur-Edge-Schutz**
 - ◆ Funktionen in AWS zum Aufbau sicherer Infrastrukturen beschreiben
 - ◆ AWS-Services zur Erhöhung der Resilienz bei Angriffen beschreiben
 - ◆ AWS-Services identifizieren, die Workloads vor externen Bedrohungen schützen
 - ◆ Funktionen von AWS Shield und AWS Shield Advanced vergleichen
 - ◆ Erläutern, wie eine zentrale Bereitstellung mit AWS Firewall Manager die Sicherheit verbessert
 - ◆ Hands-on Lab: Lab 5 – Einsatz von AWS WAF zur Abwehr von schädlichem Datenverkehr
- **◆ Monitoring und Log-Erfassung in AWS**
 - ◆ Nutzen der Log-Generierung und -Erfassung identifizieren
 - ◆ Einsatz von Amazon VPC Flow Logs zur Überwachung von sicherheitsrelevanten Ereignissen
 - ◆ Überwachung von Abweichungen vom Basisverhalten erläutern
 - ◆ Amazon EventBridge-Ereignisse beschreiben
 - ◆ Amazon CloudWatch-Metriken und -Alarmer beschreiben
 - ◆ Optionen und Techniken zur Log-Analyse auflisten
 - ◆ Einsatzszenarien für VPC Traffic Mirroring identifizieren
 - ◆ Hands-on Lab: Lab 6 – Überwachung und Reaktion auf Sicherheitsvorfälle
- **◆ Reaktion auf Bedrohungen**
 - ◆ Klassifizierung von Vorfällen in der Incident Response
 - ◆ Workflows der Incident Response verstehen

- ◇ Informationsquellen für Incident Response mit AWS-Services identifizieren
- ◇ Vorbereitung auf Sicherheitsvorfälle verstehen
- ◇ Bedrohungen mit AWS-Services erkennen
- ◇ Sicherheitsmeldungen analysieren und darauf reagieren
- ◇ Hands-on Lab: Lab 7 – Incident Response