AW920 AWS Security Best Practices

Kurzbeschreibung:

Derzeit kann der durchschnittliche Schaden eines Sicherheitsvorfalls über 4 Millionen US-Dollar betragen. Der Kurs **AW920 AWS Security Best Practices** bietet einen Überblick über einige der bewährten Methoden der Branche zur Nutzung von AWS-Sicherheitsfunktionen und Kontrolltypen.

Dieser Kurs **AW920 AWS Security Best Practices** hilft Ihnen, Ihre Verantwortlichkeiten zu verstehen, und liefert wertvolle Leitlinien, wie Sie Ihre Workloads sicher betreiben können. Sie lernen, wie Sie Ihre Netzwerkinfrastruktur mit durchdachten Architekturentscheidungen absichern. Zudem erfahren Sie, wie Sie Ihre Compute-Ressourcen härten und sicher verwalten können.

Schließlich lernen Sie durch ein Verständnis des Monitorings und der Alarmierung in AWS, wie Sie verdächtige Ereignisse erkennen und entsprechende Alarme auslösen können, um im Falle einer potenziellen Kompromittierung schnell mit dem Incident-Response-Prozess beginnen zu können.

Dieser Kurs **AW920 AWS Security Best Practices** beinhaltet Präsentationen, Demonstrationen und praktische Übungen (Hands-on Labs).

Zielgruppe:

Dieser Kurs **AW920 AWS Security Best Practices** richtet sich an:

- Solutions Architects
- Cloud Engineers einschließlich Security Engineers
- Delivery- und Implementation Engineers
- Professional Services sowie Mitglieder von Cloud Center of Excellence (CCOE)

Voraussetzungen:

Um an dem Kurs **AW920 AWS Security Best Practices** bei qSkills teilnehmen zu können, sollten Sie die folgenden AWS-Trainings besucht haben:

- AWS Security Fundamentals
- AW120 AWS Security Essentials

Sonstiges:

Dauer: 1 Tage

Preis: 750 Euro plus Mwst.

Ziele:

In diesem Kurs **AW920 AWS Security Best Practices** lernen Sie:

- Eine sichere Netzwerkinfrastruktur zu entwerfen und umzusetzen
- Compute-Sicherheit zu entwerfen und umzusetzen
- Eine Logging-Lösung zu entwerfen und umzusetzen

Inhalte/Agenda:

- **Überblick über AWS-Sicherheit**
  - ◊ Shared Responsibility Model
  - ◊ Herausforderungen für Kunden
  - ◊ Frameworks und Standards
  - ◊ Einführung von Best Practices
  - ◊ Compliance in AWS
  - ◊
- **Netzwerksicherheit**
  - ◊ Flexibilität und Sicherheit
  - ◊ Sicherheit innerhalb der Amazon Virtual Private Cloud (Amazon VPC)
  - ◊ Sicherheitsservices
  - ◊ Sicherheitslösungen von Drittanbietern
  - ◊
- **Lab 1: Netzwerksteuerung**
  - ◊ Aufbau einer Netzwerkinfrastruktur mit drei Sicherheitszonen
  - ◊ Umsetzung der Netzwerksegmentierung mit Security Groups, Network Access Control Lists (NACLs) sowie öffentlichen und privaten Subnetzen
  - ◊ Monitoring des Netzwerkverkehrs zu Amazon Elastic Compute Cloud (EC2)-Instanzen mithilfe von VPC Flow Logs
  - ◊
- **Sicherheit für Amazon EC2**
  - ◊ Compute-Hardening
  - ◊ Verschlüsselung von Amazon Elastic Block Store (EBS)
  - ◊ Sicheres Management und Wartung
  - ◊ Erkennung von Schwachstellen
  - ◊ Nutzung von AWS Marketplace
  - ◊
- **Lab 2: Absicherung des Ausgangspunkts (EC2)**
  - ◊ Erstellung eines benutzerdefinierten Amazon Machine Image (AMI)
  - ◊ Bereitstellung einer neuen EC2-Instanz auf Basis eines benutzerdefinierten AMIs
  - ◊ Patchen einer EC2-Instanz mit AWS Systems Manager
  - ◊ Verschlüsselung eines EBS-Volumes
  - ◊ Verständnis der Funktionsweise von EBS-Verschlüsselung und ihrer Auswirkungen auf andere Vorgänge
  - ◊ Nutzung von Security Groups zur Beschränkung des Datenverkehrs zwischen EC2-Instanzen auf verschlüsselten Verkehr
  - ◊
- **Monitoring und Alarmierung**
  - ◊ Protokollierung des Netzwerkverkehrs
  - ◊ Protokollierung von Benutzer- und API-Verkehr
  - ◊ Sichtbarkeit mit Amazon CloudWatch
  - ◊ Erweiterung von Monitoring und Alarmierung
  - ◊ Verifizierung der AWS-Umgebung
  - ◊
- **Sicherheitsmonitoring**
  - ◊ Konfiguration einer Amazon Linux 2-Instanz zur Übertragung von Logdateien an Amazon CloudWatch
  - ◊ Erstellung von Amazon CloudWatch Alarms und Benachrichtigungen zur Überwachung fehlgeschlagener Anmeldeversuche
  - ◊ Erstellung von Amazon CloudWatch Alarms zur Überwachung des Datenverkehrs über ein NAT-Gateway
  - ◊