# *AW920 AWS Security Best Practices*

**Kurzbeschreibung:**

In dem Kurs „AWS Security Best Practices” erhalten die Teilnehmer einen Überblick über Best Practices für den Einsatz von AWS-Sicherheits- und Kontrolltypen. Ziel ist es, die Verantwortlichkeiten und Richtlinien zu verstehen.

**Zielgruppe:**

- Lösungsarchitekten
- Cloud-Ingenieure
- einschließlich Sicherheitsingenieure, Bereitstellungs- und Implementierungsingenieure, Professional Services

**Voraussetzungen:**

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

- "AWS Security Fundamentals"
- "AWS Security Essentials"

**Sonstiges:**

**Dauer:** 1 Tage

**Preis:** 750 Euro plus Mwst.

**Ziele:**

- Lernen Sie eine sichere Netzwerkinfrastruktur zu entwerfen und zu implementieren
- Entwurf und Implementierung von Rechensicherheit
- Protokollierungslösungen entwerfen und implementieren

**Inhalte/Agenda:**

- ♦ Das eintägige Training „AWS Security Best Practices“ gibt Einblicke in branchenübliche Best Practices für den Einsatz von AWS Sicherheits- und Kontrolltypen, um die Arbeitslast sicher zu halten. Die Teilnehmer lernen Verantwortlichkeiten und Richtlinien verstehen.

  Die Sicherung der Netzwerkinfrastruktur durch Designoptionen sowie die Verwaltung der Rechenressourcen werden in diesem Training ebenfalls behandelt.

  Sie erfahren wie Sie mit Hilfe der AWS-Überwachung und -Warnungen potentiell verdächtige Ereignisse erkennen können und wie im Falle einer potentiellen Gefährdung zu reagieren ist.

  Dieser Kurs setzt sich aus einer Präsentation, Demonstrationen und praktischen Übungen zusammen, um das Erlernte praktisch anzuwenden.

  Die Kursunterlagen (E-Book) sind in englischer Sprache, die Kurssprache ist deutsch.

♦ **Modul 0: Einführung**

♦ **Module 1: AWS Security Overview**

♦
- ◊ Shared responsibility model
- ◊ Customer challenges
- ◊ Frameworks and standards
- ◊ Establishing best practices
- ◊ Compliance in AWS

♦ **Module 2: Securing the Network**

♦
- ◊ Flexible and secure
- ◊ Security inside the Amazon Virtual Private Cloud (Amazon VPC)
- ◊ Security services
- ◊ Third-party security solutions

♦ **Lab 1: Controlling the Network**

♦
- ◊ Create a three-security zone network infrastructure
- ◊ Implement network segmentation using security groups, Network Access Control Lists (NACLs), and public and private subnets
- ◊ Monitor network traffic to Amazon Elastic Compute Cloud (EC2) instances using VPC flow logs

♦ **Module 3: Amazon EC2 Security**

♦
- ◊ Compute hardening
- ◊ Amazon Elastic Block Store (EBS) encryption
- ◊ Secure management and maintenance
- ◊ Detecting vulnerabilities
- ◊ Using AWS Marketplace

♦ **Lab 2: Securing the starting point (EC2)**

♦
- ◊ Create a custom Amazon Machine Image (AMI)
- ◊ Deploy a new EC2 instance from a custom AMI
- ◊ Patch an EC2 instance using AWS Systems Manager
- ◊ Encrypt an EBS volume
- ◊ Understand how EBS encryption works and how it impacts other operations
- ◊ Use security groups to limit traffic between EC2 instances to only that which is encrypted

♦ **Module 4: Monitoring and Alerting**

♦
- ◊ Logging network traffic
- ◊ Logging user and Application Programming Interface (API) traffic
- ◊ Visibility with Amazon CloudWatch
- ◊ Enhancing monitoring and alerting
- ◊ Verifying your AWS environment

♦ **Lab 3: Security Monitoring**

♦
- ◊ Configure an Amazon Linux 2 instance to send log files to Amazon CloudWatch
- ◊

◊ Create Amazon CloudWatch alarms and notifications to monitor for failed login attempts
◊ Create Amazon CloudWatch alarms to monitor network traffic through a Network Address Translation (NAT) gateway
◊