



AWS Security Best Practices

Derzeit können die durchschnittlichen Kosten einer Sicherheitsverletzung mehr als 4 Millionen US-Dollar betragen. Best Practices für AWS-Sicherheit bietet einen Überblick über einige der Best Practices der Branche für die Verwendung von AWS-Sicherheits- und Kontrolltypen.

Dieser Kurs hilft Ihnen, Ihre Verantwortlichkeiten zu verstehen, und bietet gleichzeitig wertvolle Richtlinien, wie Sie Ihre Workloads sicher und geschützt halten können. Sie erfahren, wie Sie Ihre Netzwerkinfrastruktur mit fundierten Gestaltungsmöglichkeiten sichern. Außerdem erfahren Sie, wie Sie Ihre Compute-Ressourcen härten und sicher verwalten können. Schließlich können Sie durch das Verständnis der AWS-Überwachung und -Warnung verdächtige Ereignisse erkennen und warnen, damit Sie im Falle einer potenziellen Gefährdung schnell mit dem Reaktionsprozess beginnen können.

Dieser Kurs umfasst Präsentationen, Demonstrationen und praktische Übungen.

Kursinhalt

- Module 1: AWS Security Overview
- Module 2: Securing the Network
- Module 3: Amazon EC2 Security
- Module 4: Monitoring and Alerting
- Lab 3: Security Monitoring

Auf die Labs haben Sie nach dem Kurs noch weitere 14 Tage Zugriff. So können Sie Übungen wiederholen oder individuell vertiefen.

E-Book Die englischsprachigen Original-Unterlagen von Amazon Web Services erhalten Sie als E-Book.

Zielgruppe

Dieser Kurs richtet sich an Lösungsarchitekten, Cloud-Ingenieure, einschließlich Sicherheitsingenieure, Bereitstellungs- und Implementierungsingenieure, Professional Services und Cloud Center of Excellence (CCOE).

Voraussetzungen

Vor der Teilnahme an diesem Kurs sollten Sie folgende Kurse absolviert haben:

- AWS Security Fundamentals
- AWS Security Essentials

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/AWSB

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

AWS Security Best Practices

Training		Preise zzgl. MwSt.
Termine in Deutschland	1 Tag	CHF 875,-
Online Training	1 Tag	CHF 875,-
Termin/Kursort	Kurssprache Deutsch	
16.09.-16.09.24	16.09.-16.09.24	

Stand 12.03.2024



Inhaltsverzeichnis

AWS Security Best Practices

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.

