



# Security Engineering on AWS

# Security Engineering on AWS

In diesem Kurs wird erläutert, wie AWS-Sicherheitsservices effizient zur Bewahrung von Sicherheit und Compliance in der AWS-Cloud genutzt werden können. Der Schwerpunkt liegt auf den von AWS empfohlenen, bewährten Sicherheitsmethoden, die für höhere Sicherheit Ihrer Daten und Systeme in der Cloud sorgen. Der Kurs beleuchtet die Sicherheitsfunktionen wichtiger AWS-Services wie Datenverarbeitungs-, Speicher-, Netzwerk- und Datenbankservices. Er behandelt auch die üblichen Sicherheitskontrollziele und die Standards zur Einhaltung gesetzlicher Vorschriften und erläutert Anwendungsfälle für laufende regulierte Verarbeitungslasten auf AWS für verschiedene Branchen weltweit. Außerdem lernen Sie, wie man AWS-Services und -Tools zur Automatisierung und fortlaufenden Überwachung nutzt – und dadurch Sicherheitsvorgänge zuverlässiger macht denn je.

### Kursinhalt

- Anpassung und Nutzung des AWS-Modells zur Shared Security Responsibility
- Benutzeridentität- und Zugriffsverwaltung in der AWS-Cloud
- Verwendung von AWS-Sicherheitsservices wie AWS Identity and Access Management, Amazon Virtual Private Cloud, AWS Config, AWS CloudTrail, AWS Key Management Service, AWS CloudHSM und AWS Trusted Advisor
- Implementieren besserer Sicherheitskontrollen für Ressourcen in der AWS-Cloud
- Verwaltung und Überwachung von AWS-Ressourcen aus der Sicherheitsperspektive
- Überwachung und Protokollierung des Zugriffs und der Nutzung von Datenverarbeitungs-, Speicherungs-, Netzwerk- und Datenbankservices in AWS
- Anpassung und Nutzung des AWS-Modells zur Shared Compliance Responsibility
- Identifizieren von AWS-Services und -Tools zur Automatisierung, Überwachung und Verwaltung von Sicherheitsvorgängen in AWS
- Verwaltung von Sicherheitsvorfällen in der AWS-Cloud

Auf die Labs haben Sie nach dem Kurs noch weitere 4 Wochen 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 ist konzipiert für:

- Sicherheitsfachleute
- Sicherheitsarchitekten
- Sicherheitsanalysten
- Sicherheitsprüfer
- Personen, die für die Leitung, Überwachung und das Testen der IT-Infrastruktur einer Organisation, sowie für die Sicherstellung von deren Konformität mit Sicherheits-, Risiko- und Compliance-Richtlinien zuständig sind

### Voraussetzungen

Wir empfehlen, dass die Teilnehmer an diesem Kurs die folgenden Voraussetzungen erfüllen:

- Besuch des Kurses Grundlagen der AWS-Sicherheit
- Erfahrung mit Governance-, Risiko- und Compliance-Vorschriften sowie Kontrollzielen
- Praktische Erfahrung mit IT-Sicherheitsverfahren
- Praktische Erfahrung mit IT-Infrastrukturkonzepten
- Verständnis von Cloud Computing-Konzepten

Bestandteil der Schulung sind praktische Labor-Übungen mit der AWS Umgebung. Um diese erfolgreich durchführen zu können, ist ein internetfähiges Notebook (Windows, Linux, MacOS) Voraussetzung.

**Wichtig:** Bitte bringen Sie daher Ihr Notebook zum Kurs mit! Falls dies nicht möglich ist, nehmen Sie bitte mit uns vorher Kontakt auf.

### Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: [www.experteach.at/go/AWSE](http://www.experteach.at/go/AWSE)

### 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.

Training	Preise zzgl. MwSt.	
<b>Termine in Deutschland</b>	<b>3 Tage</b>	<b>€ 2.685,-</b>
<b>Online Training</b>	<b>3 Tage</b>	<b>€ 2.685,-</b>
<b>Termin/Kursort</b>	Kurs Sprache Deutsch	
08.10.-10.10.24	ON Online	26.03.-28.03.25
26.11.-28.11.24	HY Hamburg	26.03.-28.03.25
26.11.-28.11.24	HY Online	

Stand 02.10.2024



# Inhaltsverzeichnis

## Security Engineering on AWS

### Module 1: Security Overview and Review

Explain Security in the AWS Cloud.  
Explain AWS Shared Responsibility Model.  
Summarize IAM, Data Protection, and Threat Detection and Response.  
State the different ways to interact with AWS using the console, CLI, and SDKs.  
Describe how to use MFA for extra protection.  
State how to protect the root user account and access keys.

### Module 2: Securing Entry Points on AWS

Describe how to use multi-factor authentication (MFA) for extra protection.  
Describe how to protect the root user account and access keys.  
Describe IAM policies, roles, policy components, and permission boundaries.  
Explain how API requests can be logged and viewed using AWS CloudTrail and how to view and analyze access history.  
Hands-On Lab: Using Identity and Resource Based Policies.

### Module 3: Account Management and Provisioning on AWS

Explain how to manage multiple AWS accounts using AWS Organizations and AWS Control Tower.  
Explain how to implement multi-account environments with AWS Control Tower.  
Demonstrate the ability to use identity providers and brokers to acquire access to AWS services.  
Explain the use of AWS IAM Identity Center (successor to AWS Single Sign-On) and AWS Directory Service.  
Demonstrate the ability to manage domain user access with Directory Service and IAM Identity Center.  
Hands-On Lab: Managing Domain User Access with AWS Directory Service

### Module 4: Secrets Management on AWS

Describe and list the features of AWS KMS, CloudHSM, AWS Certificate Manager (ACM), and AWS Secrets Manager.  
Demonstrate how to create a multi-Region AWS KMS key.  
Demonstrate how to encrypt a Secrets Manager

secret with an AWS KMS key.  
Demonstrate how to use an encrypted secret to connect to an Amazon Relational Database Service (Amazon RDS) database in multiple AWS Regions  
Hands-on lab: Lab 3: Using AWS KMS to Encrypt Secrets in Secrets Manager

### Module 5: Data Security

Monitor data for sensitive information with Amazon Macie.  
Describe how to protect data at rest through encryption and access controls.  
Identify AWS services used to replicate data for protection.  
Determine how to protect data after it has been archived.  
Hands-on lab: Lab 4: Data Security in Amazon S3

### Module 6: Infrastructure Edge Protection

Describe the AWS features used to build secure infrastructure.  
Describe the AWS services used to create resiliency during an attack.  
Identify the AWS services used to protect workloads from external threats.  
Compare the features of AWS Shield and AWS Shield Advanced.  
Explain how centralized deployment for AWS Firewall Manager can enhance security.  
Hands-on lab: Lab 5: Using AWS WAF to Mitigate Malicious Traffic

### Module 7: Monitoring and Collecting Logs on AWS

Identify the value of generating and collecting logs.  
Use Amazon Virtual Private Cloud (Amazon VPC) Flow Logs to monitor for security events.  
Explain how to monitor for baseline deviations.  
Describe Amazon EventBridge events.  
Describe Amazon CloudWatch metrics and alarms.  
List log analysis options and available techniques.  
Identify use cases for using virtual private cloud (VPC) Traffic Mirroring.  
Hands-on lab: Lab 6: Monitoring for and Responding to Security Incidents

### Module 8: Responding to Threats

Classify incident types in incident response.  
Understand incident response workflows.  
Discover sources of information for incident response

using AWS services.  
Understand how to prepare for incidents.  
Detect threats using AWS services.  
Analyze and respond to security findings.  
Hands-on lab: Lab 7: Incident Response

