Security Engineering on AWS

Security is a concern for both customers in the cloud, and those considering cloud adoption. An increase in cyberattacks and data leaks remains top of mind for most industry personnel. The Security Engineering on AWS course addresses these concerns by helping you better understand how to interact and build with Amazon Web Services (AWS) in a secure way.

In this course, you will learn about managing identities and roles, managing and provisioning accounts, and monitoring API activity for anomalies. You will also learn about how to protect data stored on AWS. The course explores how you can generate, collect, and monitor logs to help identify security incidents. Finally, you will review detecting and investigating security incidents with AWS services.

The final day is an AWS Jam, a gamified event, with teams competing to score points by completing a series of challenges according to established best practices based on concepts covered in the course. You get to experience a wide range of AWS services in a series of real-world scenarios that represent common operational and troubleshooting tasks. The end result is developing, enhancing, and validating your skillsets in the AWS Cloud through real-world problem solving, exploring new services, features, and understanding how they interoperate.

Course Contents
• Module 1: Security Overview and Review
• Module 2: Securing Entry Points on AWS
• Module 3: Account Management and Provisioning on AWS
• Module 4: Secrets Management on AWS
• Module 5: Data Security
• Module 6: Infrastructure Edge Protection
• Module 7: Monitoring and Collecting Logs on AWS
• Module 8: Responding to Threats

You have access to the labs for another 14 days after the course. This way you can repeat exercises or deepen them individually.

E-Book You will receive the original course documentation by Amazon Web Services as an e-book.

Target Group
• Security engineers
• Security architects
• Cloud architects
• Cloud operators working across all global segments

Prerequisites
Completed the following courses:

• AWS Security Essentials
• Architecting on AWS

and

• Working knowledge of IT security practices and infrastructure concepts
• Familiarity with the AWS Cloud

Practical lab exercises with the AWS environment are part of the training. In order to be able to carry out these successfully, an internet-capable notebook (Windows, Linux, MacOS) is a prerequisite.

Important: Therefore, please bring your notebook to the course! If this is not possible, please contact us in advance.

Alternatives
Book this course together with *AWS Jam for Security Engineering on AWS – Practical day for Team-based learning* as *Security Engineering on AWS with AWS Jam* for the discounted price of **€ 3.175,-**.

Status 06/17/2025

This Course in the Web
You can find the up-to-date information and options for ordering under the following link:
www.experteach-training.com/go/**AWSE**

Reservation
On our Website, you can reserve a course seat for 7 days free of charge and in an non-committal manner. This can also be done by phone under +49 6074/4868-0.

Guaranteed Course Dates
To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

Your Tailor-Made Course!
We can precisely customize this course to your project and the corresponding requirements.

Training		Prices, excl. of V.A.T.
Classes in Germany	**3 Days**	**€ 2,685**
Online Training	**3 Days**	**€ 2,685**

Date/course venue		Course language German 🇩🇪	
23/09-25/09/25	Frankfurt	24/03-26/03/26	Frankfurt
23/09-25/09/25	Online	24/03-26/03/26	Online
16/12-18/12/25	Frankfurt	30/06-02/07/26	Frankfurt
16/12-18/12/25	Online	30/06-02/07/26	Online

Amazon Web Services (AWS)

ExperTeach

Table of Contents
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