



# AWS Security Best Practices

Currently, the average cost of a security breach can exceed \$4 million. Best Practices for AWS Security provides an overview of some of the industry's best practices for using AWS security and control types.

This course will help you understand your responsibilities while providing valuable guidance on how to keep your workloads safe and secure. You will learn how to secure your network infrastructure with sound design options. You'll also learn how to harden and securely manage your compute resources. Finally, by understanding AWS monitoring and alerting, you will be able to detect and alert suspicious events so that you can quickly begin the response process in the event of a potential compromise.

This course includes presentations, demonstrations and practical exercises.

### Course Contents

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

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

This course is aimed at solution architects, cloud engineers, including security engineers, deployment engineers, professional services and cloud centres of excellence (CCOE).

### Prerequisites

Before attending this course you should have completed the following courses:

- AWS Security Fundamentals
- AWS Security Essentials

### This Course in the Web



You can find the up-to-date information and options for ordering under the following link:

[www.expertech-training.com/go/AWSB](http://www.expertech-training.com/go/AWSB)

### Reservation

On our Website, you can reserve a course seat for 7 days free of charge and in a 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.

# AWS Security Best Practices

Training	Prices, excl. of V.A.T.	
Classes in Germany	1 Day	€ 795
Online Training	1 Day	€ 795
Date/course venue	Course language German	
16/09-16/09/24	16/09-16/09/24	

Status 03/12/2024



# Table of Contents

## 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.

