AWS Security Best Practices – Intensive Training («AWSB09»)

Do you need to know how to establish and maintain a secure posture in the AWS Cloud? The AWS Security Best Practices course will help you learn to design and implement solutions to keep your workloads safe and secure.

Duration: 1 day
Price: 900.–
Course documents: Digital original AWS courseware

Content

Currently, the average cost of a security breach can be upwards of $4 million. *AWS Security Best Practices* provides an overview of some of the industry best practices for using AWS security and control types. This course helps you understand your responsibilities while providing valuable guidelines for how to keep your workload safe and secure.
You will learn how to secure your network infrastructure using sound design options. You will also learn how you can harden your compute resources and manage them securely. Finally, by understanding AWS monitoring and alerting, you can detect and alert on suspicious events to help you quickly begin the response process in the event of a potential compromise.

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

Key Learnings

- Designing and implementing a secure network infrastructure
- Designing and implementing compute security
- Designing and implementing a logging solution

Target audience

This course is intended for the following job roles:

- Solution Architect
- Cyber Security
- CloudOps
- DevOps

Why should you attend this specific course? What are my benefits from taking this course? The **Voice of the Instructor answers these questions**. We have asked our instructor team to write a short text about WHY this course is very relevant for the respective job roles and what you can expect from attending the course. You can find this section in the course description under the «*Additional Information*» section.

Requirements

We recommend that attendees of this course have attended the following course (or equivalent knowledge):

- AWS Security Essentials – Intensive Training («AWSE04»)

Additional information

Voice of the Instructor

Participating in the «AWS Security Best Practices» course can offer several benefits for individuals and organizations. Here are a few reasons why you should consider participating:

1. Enhanced Security Knowledge: The course will provide you with a comprehensive understanding of AWS security best practices. You will learn about various security concepts, techniques, and tools specific to the AWS environment. This knowledge will enable you to effectively secure your

AWS infrastructure and applications, reducing the risk of security breaches and unauthorized access.

2. Protecting Data and Assets: AWS is a leading cloud service provider, hosting a vast amount of sensitive data and critical infrastructure for organizations worldwide. By participating in the course, you'll gain insights into securing your AWS resources, protecting your data from unauthorized access, implementing encryption, and establishing secure network configurations. This will help safeguard your organization's assets, maintain customer trust, and comply with relevant security regulations.
3. Mitigating Security Risks: As cyber threats continue to evolve, it's crucial to stay updated on the latest security practices. The course will cover common security risks and vulnerabilities specific to AWS and guide you on how to mitigate them effectively. You'll learn about best practices for identity and access management, network security, monitoring and logging, incident response, and more. By applying these best practices, you can proactively reduce security risks and respond appropriately to potential incidents.
4. Industry Recognition and Career Advancement: AWS certifications and training carry significant weight in the IT industry. By participating in the «AWS Security Best Practices» course, you'll gain valuable knowledge and skills that can be showcased on your resume or professional profile. This can differentiate you from others, increase your marketability, and open up career opportunities in cloud security and AWS-focused roles.
5. Compliance and Audit Readiness: Many industries have specific compliance requirements, such as HIPAA for healthcare or GDPR for data privacy. The «AWS Security Best Practices» course will guide you on aligning your AWS security measures with relevant compliance standards. You'll learn about implementing necessary controls, conducting audits, and maintaining documentation, ensuring your organization remains compliant and avoids penalties.

Remember, the security landscape is constantly evolving, and staying up to date with the latest best practices is essential. By participating in the «AWS Security Best Practices» course, you'll equip yourself with the knowledge and skills necessary to secure your AWS infrastructure, protect your data, and confidently navigate the challenges of cloud security.

Further courses

- Security Engineering on AWS – Intensive Training («AWSS04»)
- Advanced Architecting on AWS with JAM – Intensive Training («AWSA2J»)
- AWS Security Governance at Scale – Intensive Training («AWSE07»)
- Advanced Architecting on AWS – Intensive Training («AWSA02»)

Any questions?

We are happy to advise you on +41 44 447 21 21 or info@digicomp.ch. You can find detailed information about dates on www.digicomp.ch/courses-digital-transformation-technologies/cloud/amazon-web-services-aws/aws-devops/course-aws-security-best-practices-intensive-training