AWS Security Essentials – Intensive Training («AWSE04»)

This course covers fundamental AWS cloud security concepts, including AWS access control, data encryption methods, and how network access to your AWS infrastructure can be secured.

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

Content

Based on the AWS Shared Security Model, you learn where you are responsible for implementing security in the AWS Cloud and what security-oriented services are available to you. Learn also why and how the security services can help meet the security needs of your organization. This course enables you to dive deep, ask questions, work through solutions, and get feedback from AWS-accredited instructors with deep technical knowledge. This fundamental level course is part of the AWS Training and Certification Security learning path.

Module 1: Security on AWS

- Security design principles in the AWS Cloud
- AWS Shared Responsibility Model

Module 2: Security OF the Cloud

- AWS Global Infrastructure
- Data center security
- Compliance and governance

Module 3: Security IN the Cloud – Part 1

- Identity and access management
- Data protection essentials
- Lab 01 – Introduction to security policies

Module 4: Security IN the Cloud – Part 2

- Securing your infrastructure
- Monitoring and detective controls
- Lab 02 – Securing VPC resources with Security Groups

Module 5: Security IN the Cloud – Part 3

- DDoS mitigation
- Incident response essentials
- Lab 03 – Remediating issues with AWS Config Conformance Packs

Module 6: Course Wrap Up

- AWS Well-Architected tool overview
- Next Steps

Key Learnings

- Identifying security benefits and responsibilities of using the AWS Cloud
- Describing the access control and management features of AWS
- Explaining the available methods for providing encryption of data in transit and data at rest when storing data in AWS
- Describing how to secure network access to AWS resources
- Determining which AWS services can be used for monitoring and incident response

Methodology & didactics

These hybrid courses come in 1 instructor-led full day sessions with the instructor supervising the participants live. Each course consits of theory parts with live demos and practical lab exercises. The courses can be attended either on-site at a physical Digicomp location or virtually via Zoom. Please also refer to each course's description for specific details regarding the prerequisites and the covered topics.

Target audience

This course is intended for the following job roles:

- Solution Architect
- Cyber Security
- CloudOps
- DevOps

Requirements

We recommend that attendees of this course have the following prerequisites:

- Working knowledge of IT security practices

and have attended the following course or equivalent knowledge is required:

- AWS Technical Essentials – Intensive Training («AWSE01»)

Certification

There is no official certification related to this course.

Further courses

- AWS Security Governance at Scale – Intensive Training («AWSE07»)
- AWS Security Best Practices – Intensive Training («AWSB09»)
- Architecting on AWS with JAM – Intensive Training («AWSA1J»)
- Architecting on AWS with Best Practice – Intensive Training («AWSA10»)
- AWS Cloud for Finance Professionals – Intensive Training («AWSF01»)
- Architecting on AWS – Intensive Training («AWSA01»)
- Security Engineering on AWS – Intensive Training («AWSS04»)

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-itprovider/amazon-web-services-aws/aws-foundation/course-aws-security-essentials-intensive-training