AWS – Amazon Web Services Security Essentials

Description

This 1-day 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. 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 and why and how the security services can help meet the security needs of your organization.

Course Content
Module 1: Security on AWS

- 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

Module 4: Security IN the Cloud - Part 2

- Securing your infrastructure
- Monitoring and detective controls

Module 5: Security IN the Cloud - Part 3

- DDoS mitigation
- Incident response essentials

Module 6: Course Wrap Up

- AWS Well-Architected tool overview

Lab / Exercises

- Official AWS Labs

Documentation

- Digital courseware included

Participant profiles

- IT business-level professionals interested in cloud security practices
- Security professionals with minimal working knowledge of AWS

Prerequisites

- Working knowledge of IT security practices and infrastructure concepts, familiarity with cloud computing concepts.

Objectives

- Identify security benefits and responsibilities when using the AWS Cloud
- Describe the access control and management features of AWS
- Understand the different data encryption methods to secure sensitive data
- Describe how to secure network access to your AWS resources
- Determine which AWS services can be used for security logging and monitoring

Niveau
Fondamental
Classroom Registration Price (CHF)
-1
Virtual Classroom Registration Price (CHF)
850
Duration (in Days)
1
Reference
AWS-04