AWS Security Essentials

Length: 1 days
Format: Live Remote
Time: Day

About This Course

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.

We will address your security responsibilities in the AWS cloud and provide a brief introduction to the different security-oriented AWS services available.

Required Exams

Audience Profile

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

Course Objectives

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

Outline

Module : Security on AWS * Security design principles in the AWS Cloud
* AWS Shared Responsibility Model

Module : Security OF the Cloud * AWS Global Infrastructure
* Data Center Security
* Compliance and Governance

Module : Security IN the Cloud - Part 1 * Identity and Access Management
* Data Protection

Module : Security IN the Cloud - Part 2 * Securing your infrastructure
* Monitoring and detective controls

Module : Security IN the Cloud – Part 3 * DDoS mitigation
* Incident response essentials

Module : Course Wrap Up * AWS Well-Architected tool overview

Lab Outline

* Lab 01 - Introduction to Security Policies
* Lab 02 - Securing VPC Resources with Security Groups
* Lab 03 - Automating Incident Response with AWS Config and AWS Lambda

Follow-Course

Security Engineering On AWS