Security Engineering on AWS

Course ID #: 7000-075-ZZ-Z
Hours: 21

Course Content

Course Description:

This course demonstrates how to efficiently use AWS security services to stay secure in the AWS Cloud. The course focuses on the security practices that AWS recommends for enhancing the security of your data and systems in the cloud. The course highlights the security features of AWS key services including compute, storage, networking, and database services. You will also learn how to leverage AWS services and tools for automation, continuous monitoring and logging, and responding to security incidents.

Course Objectives:

Upon completion, students will be able to:

- Assimilate and leverage the AWS shared security responsibility model
- Architect and build AWS application infrastructures that are protected against the most common security threats
- Protect data at rest and in transit with encryption
- Apply security checks and analyses in an automated and reproducible manner
- Configure authentication for resources and applications in the AWS Cloud
- Gain insight into events by capturing, monitoring, processing, and analyzing logs
- Identify and mitigate incoming threats against applications and data
- Perform security assessments to ensure that common vulnerabilities are patched and security best practices are applied

Target Audience:

This course is for:

- Security engineers
- Security architects
- Security operations
- Information security

Prerequisites:

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

- AWS Cloud Practitioner Essentials
- AWS Security Fundamentals
- Architecting on AWS
- Working knowledge of IT security practices and infrastructure concepts
- Familiarity with cloud computing concepts

Security Engineering on AWS

Course ID #: 7000-075-ZZ-Z

Hours: 21

Topics:

Day 1

- Identifying Entry Points on AWS
- Security Considerations: Web Application Environments
- Application Security
- Securing Networking Communications – Part 1

Day 2

- Data Security
- Security Considerations: Hybrid Environments
- Monitoring and Collecting Logs on AWS
- Processing Logs on AWS
- Securing Networking Communications – Part 2
- Out-Of-Region Protection

Day 3

- Account Management on AWS
- Security Considerations: Serverless Environments
- Secrets Management on AWS
- Automating Security on AWS
- Threat Detection and Sensitive Data Monitoring