Exam Readiness: AWS Certified Security - Specialty

COURSE OVERVIEW

Course Modality
Classroom (virtual or in person)

Course Time
4 Hours

Course Level
Intermediate

Course Language
English

The AWS Certified Security Specialty exam validates technical skills and experience in securing and hardening workloads and architectures on the AWS platform. Attendees with two or more years of hands-on experience designing and deploying cloud architecture on AWS should join this half-day, course to learn how to prepare and succeed in the exam. We will help you prepare for the exam by exploring the exam's topic areas and mapping them to specific areas to study. We will review sample exam questions in each topic area, teaching you how to interpret the concepts being tested so that you can better eliminate incorrect responses.

Prerequisites:

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

- ✓ Minimum of five years of IT security experience, designing and implementing a security solution
- ✓ At least two years of hands-on experience securing AWS workloads, and security controls for workloads on AWS

Intended Audience:

This course is intended for:

- ✓ Individuals who perform a security role

Skill Covered:

In this course, you will learn how to:

- ✓ Navigate the logistics of the examination process
- ✓ Understand the exam structure and question types
- ✓ Identify how questions relate to AWS security best practices
- ✓ Interpret the concepts being tested by an exam question
- ✓ Allocate your time spent studying for the AWS Certified Security Specialty exam

COURSE CURRICULUM

Module 1:

Incident Response

- ✓ Given an AWS abuse notice, evaluate the suspected compromised instance or exposed access keys.
- ✓ Verify that the Incident Response plan includes relevant AWS services.
- ✓ Evaluate the configuration of automated alerting and execute possible remediation of security-related incidents and emerging issues.

Module 2:

Logging and Monitoring

- ✓ Design and implement security monitoring and alerting.
- ✓ Troubleshoot security monitoring and alerting.
- ✓ Design and implement a logging solution.
- ✓ Troubleshoot logging solutions.

Module 3:

Infrastructure Security

- ✓ Design edge security on AWS.
- ✓ Design and implement a secure network infrastructure.
- ✓ Troubleshoot a secure network infrastructure.
- ✓ Design and implement host-based security.

Module 4 :

Identity and Access Management

- ✓ Design and implement scalable authorization and authentication system to access AWS resources.
- ✓ Troubleshoot an authorization and authentication system to access AWS resources.

Module 5:

Data Protection

- ✓ Design and implement key management and use.
- ✓ Troubleshoot key management.
- ✓ Design and implement a data encryption a solution for data at rest and data n transit.

RECOMMENDED EXAMS

AWS Certified Security - Specialty

The AWS Certified Security – Specialty is intended for individuals who perform a security role with at least two years of hands-on experience securing AWS workloads.