AWS Certified Security – Specialty (SCS-C02)

Level: Specialty
Duration: 50–60 Hours

Course Overview

The **AWS Certified Security – Specialty** course is designed for individuals who perform security roles and want to demonstrate expertise in securing AWS environments. This course covers topics such as **data protection**, **incident response**, **identity and access management**, **logging and monitoring**, and **infrastructure security**, preparing learners for the **SCS-C02 certification**.

Course Objectives

- Design and implement security controls in AWS
- Manage identity and access using IAM and AWS SSO
- Monitor, log, and respond to security incidents
- Protect data in transit and at rest
- Prepare for the AWS Security – Specialty certification exam

---

Course Outline

Module 1: Introduction and Certification Overview

- Overview of the SCS-C02 exam structure and domains
- Key AWS security services
- Shared Responsibility Model
- Compliance and governance in AWS

Module 2: Incident Response

- Preparing for incident response
- Using AWS CloudTrail and Amazon GuardDuty

- Responding to security breaches and alerts
- Automating incident responses with AWS Lambda

Module 3: Logging and Monitoring

- Monitoring AWS environments with CloudWatch
- Analyzing activity with AWS CloudTrail and AWS Config
- Centralizing logs with Amazon S3 and Amazon Athena
- AWS Security Hub and Amazon Detective for investigation

Module 4: Identity and Access Management

- Managing permissions with IAM users, groups, roles, and policies
- AWS Organizations and Service Control Policies (SCPs)
- Using AWS SSO and federated access
- Fine-grained access with resource-based and identity-based policies

---

Module 5: Infrastructure Security

- Network segmentation and isolation with VPC
- Security groups and Network ACLs
- Protecting endpoints using AWS WAF, AWS Shield, and AWS Firewall Manager
- Patch management and security baselines with Systems Manager

---

Module 6: Data Protection and Encryption

- Encryption at rest using AWS KMS and CloudHSM
- Encryption in transit using TLS and AWS Certificate Manager
- S3 bucket policies and block public access settings
- Managing keys, rotation, and access control

Module 7: Security Automation and Best Practices

- Automating compliance checks with AWS Config rules
- Detecting misconfigurations using AWS Trusted Advisor
- Security automation with CloudFormation and Lambda

- Security architecture best practices and design

Module 8: Exam Preparation and Practice

- Practice questions by domain
- Scenario-based hands-on exercises
- Real-world use cases and case studies
- Final mock test and review session

Target Audience

- Security engineers, architects, and analysts
- IT professionals responsible for securing AWS environments
- Candidates preparing for the **AWS Security Specialty** certification exam

---

Prerequisites

- Minimum of 2 years of hands-on AWS experience (recommended)
- Strong understanding of security concepts, protocols, and AWS services