AWS Certified Security Specialty (SCS-C01)

Introduction

The AWS Certified Security - Specialty (SCS-C01) examination is intended for individuals who perform a security role. This exam validates an examinee's ability to effectively demonstrate knowledge about securing the AWS platform.

It validates an examinee's ability to demonstrate:

- An understanding of specialized data classifications and AWS data protection mechanisms.
- An understanding of data encryption methods and AWS mechanisms to implement them.
- An understanding of secure Internet protocols and AWS mechanisms to implement them.
- Working knowledge of AWS security services and features of services to provide a secure production environment.
- Competency gained from two or more years of production deployment experience using AWS security services and features.
- The ability to make tradeoff decisions with regard to cost, security, and deployment complexity is given a set of application requirements.
- An understanding of security operations and risks.

Course Objective

This course teaches you about core aspects such as:

- Understanding of specialized data classifications and AWS data protection mechanisms
- Deep-understanding of data encryption methods and mechanisms to implement them
- Different ways of securing Internet protocols with AWS
- Hands-on experience on AWS security services and features of services to deliver a secure production environment
- Ability to make well-calculated and quick decisions with regard to cost, security, and deployment complexities

Course Outline

Domain 1: Incident Response

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

Domain 2: Logging and Monitoring

2.1 Design and implement security monitoring and alerting.
2.2 Troubleshoot security monitoring and alerting.
2.3 Design and implement a logging solution.
2.4 Troubleshoot logging solutions.

Domain 3: Infrastructure Security

3.1 Design edge security on AWS.
3.2 Design and implement a secure network infrastructure.

3.3 Troubleshoot a secure network infrastructure.
3.4 Design and implement host-based security.

Domain 4: Identity and Access Management

4.1 Design and implement a scalable authorization and authentication system to access AWS resources.
4.2 Troubleshoot an authorization and authentication system to access AWS resources.

Domain 5: Data Protection

5.1 Design and implement key management and use.
5.2 Troubleshoot key management.
5.3 Design and implement a data encryption solution for data at rest and data in transit.

Prerequisites

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

Target Audience

- Security engineers
- Security architects

Duration

- 24 Hours Training Course