TechyEdz Solutions

A Blended Learning Approach

AWS Security Specialty

☎ 9032803832

☎ 9032803832

✉ contact@techyedz.com

🌐 www.techyedz.com

AWS Certified Security – Specialty (SCS-C01)

Course Overview:

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. This course is specially designed for the aspirants who intend to give the AWS Certified Security Specialty certification and as well for those who want to master the AWS Security as well.

Throughout the course, we look into various Real World scenario and look into why do website gets hacked, what could have been done to prevent it and learn the best practices related to Security for your AWS environment.

What you will learn:

- 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.
- A 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 given a set of application requirements.
- An understanding of security operations and risks.

Course Outline:

Cloud Security Introduction

- Cloud Security fundamentals
- AWS security model
- Shared Responsibility
- Exam Outline

Incident Response

- Given an AWS abuse notice, evaluate the suspected compromised instance or exposed access keys.
- Preparation stages for incident response
- Mitigation steps to perform Incident response steps
- Verify that the Incident Response plan includes relevant AWS services.
- Dealing with exposed access keys
- Evaluated suspected compromised EC2 Instances
- Evaluate the configuration of automated alerting, and execute possible remediation of security-related incidents and emerging issues.
- AWS Guard duty
- Penetration testing

Logging and Monitoring (VPC)

- Design and implement security monitoring and alerting.
- Design and implement a logging solution.
- Continuous Security Monitoring
- Introduction to Vulnerability Assessment
- AWS Inspector
- AWS Inspector Assessment targets
- AWS EC2 systems manager
- AWS Config
- Understanding CloudWatch

- VPC Flow Logs
- CloudWatch Events
- AWS Cloud Trail
- AWS Macie
- AWS Detective
- AWS Security Hub
- S3 Event notifications
- Trusted advisor recommendations
- Troubleshoot security monitoring and alerting.
- Troubleshoot logging solutions.

Infrastructure Security

- Design edge security on AWS.
- Design and implement a secure network infrastructure.
- AWS Organizations
- Managing OUs
- CloudFront
- AWS CloudFront Custom SSL
- Firewalls
- Security groups
- Network ACLs
- IPS/IDS concepts in cloud
- AWS Web Application Firewall (WAF)
- AWS Shield concepts
- DDoS Mitigation
- Network Segmentation
- Bastion Hosts
- Virtual Private Cloud (VPC)
- VPC Endpoints
- EC2 Tenancy

- Compliance Frameworks
- AWS lambda fundamentals
- AWS Simple Email Service
- AWS Route53 DNS
- Troubleshoot a secure network infrastructure
- Design and implement host-based security

Identity and Access Management

- Design and implement a scalable authorization and authentication system to access AWS resources.
- Understand the Principle of Least Privilege
- IAM Policies
- IAM JSON Policy Elements
- IAM Roles
- IAM Permission boundaries
- Evaluating effective permissions
- Understanding Delegation
- Cross account policies & roles
- Understanding Federation
- AWS Directory services
- AWS Organizations
- Single Sign-On
- SAML Overview Concepts
- S3 Security
- Cross Account S3 access
- S3 Versioning
- S3 MFA delete
- AWS License manager
- Troubleshoot an authorization and authentication system to access AWS resources.

Data Protection

- Design and implement key management and use
- Cryptography fundamentals
- Cryptography fundamentals
- Cloud Hardware Security Module (HSM)
- AWS Key Management Service (KMS)
- Envelope Encryption
- KMS Authentication and Access Control
- CloudTrail and Encryption
- EBS Architecture and Secure Data Wiping
- S3 Encryption
- AWS Certificate Manager
- ELB- ALB and NLB
- Docker and container security fundamentals
- AWS Glacier
- Troubleshoot key management.
- Design and implement a data encryption solution for data at rest and data in transit.

Prerequisites:

- A minimum of 5 years of IT security experience, designing and implementing security solutions
- At least 2 years of hands-on experience securing AWS workloads
- Security controls for workloads on AWS
- Basics of AWS
- AWS Solutions Architect Associate or Equivalent Knowledge

Who Can Attend:

- Those interested in gaining the AWS Security Specialty Certification
- Those who wants to gain deep security insights related to AWS

Number of Hours: 40hrs

Certification: AWS Certified Security – Specialty (SCS-C01)

Key Features:

- One to One Training
- Online Training
- Fastrack & Normal Track
- Resume Modification
- Mock Interviews
- Video Tutorials
- Materials
- Real Time Projects
- Virtual Live Experience
- Preparing for Certification