INFOSECTRAIN

AWS CERTIFIED SECURITY SPECIALTY (SCS-C02) CERTIFICATION TRAINING COURSE

KEY FEATURES

- 30 Hrs of Instructor-led Training
- Blended Learning Delivery Model
- Certified Trainer
- Training Certificate

OVERVIEW

The AWS Certified Security Specialty certification training program from InfosecTrain is specifically designed to provide you with a comprehensive understanding of AWS Security Architecture. You will gain the skills needed to design, deploy, and manage security infrastructure on the AWS Cloud Platform. This knowledge will enable you to effectively secure your organization's AWS infrastructure and protect it against cyber threats. By completing this course, you will be well-prepared to confidently take the AWS Certified Security Specialty certification exam.

Along with the right kind of theoretical knowledge to achieve the certification, you will also receive hands-on experience on certain specific services during this AWS Security training.

Why AWS Certified Security Specialty (SCS-C02) Certification Training with InfosecTrain?

InfosecTrain is a leading IT security training and consulting organization offering best-in-class yet cost-effective customized training programs to enterprises and individuals across the globe. We offer role-specific certification training programs and prepare professionals for the future. Our AWS Certified Security Speciality training is designed to equip you with comprehensive knowledge of the entire AWS security architecture.

Here's what you get when you choose InfosecTrain as your learning partner:

- **Flexible Schedule:** Training sessions to match your schedule and accommodate your needs.
- **Post Training Support with No Expiry Date:** Ongoing assistance and support until the learners achieve their certification goals.
- **Recorded Sessions:** Access to LMS and recorded sessions for post training reference.
- **Customized Training:** A training program that caters to your specific learning needs.
- **Knowledge Sharing Community:** Collaborative group discussions to facilitate knowledge sharing and learning.
- **Certificate:** Each candidate receives a certificate of participation as a testament to their accomplishment.

INFOSECTRAIN

Target Audience

- Candidates with an understanding of IT security and Cybersecurity concepts
- Those who are working in cloud computing and security domains looking to specialize in AWS Security Architecture
- Those who completed the AWS Associate level certifications and want to specialize in security.
- Those who want to build their career in AWS Security

Pre-Requisite

- IT/Cyber Security Concepts
- Knowledge Mapping to AWS Associate level certifications (Certification not mandatory)
- Virtualization concepts
- Basic understanding of networking and OS concepts
- The ideal applicant should have 3-5 years of expertise in designing and implementing security solutions. Furthermore, the ideal applicant should have at least 2 years of hands-on experience securing AWS workloads.

Exam Information

Exam Code	**SCS-C02**
Exam Format	Multiple Choice, Multiple Response
Number of Questions	65
Exam Duration	170 minutes
Passing Score	750/1000
Language	English, French, German, Italian, Japanese, Korean, Portuguese, Simplified Chinese, and Spanish.

Why Infosec Train?

INFOSECTRAIN

- Certified & Experienced Instructor
- Flexible Schedule
- Access to recorded sessions
- Post Training Support
- Tailor Made Training

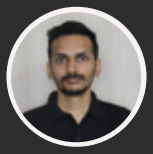
Our Expert Instructors

Trained over 1000+ students globally including Fortune 500 companies and recognized as a Microsoft Certified Trainer. Performing as an Enterprise Cloud Security Architect & Adoption Strategist, Auditor & Cloud Design Architect for over 10 years and served over 50+ enterprises worldwide.

KRISH

17+ Years Of Experience

SME, Cloud Security | Cloud Audit | CCSP | CCSK | AWS CS-S | AWS CAN-S | AWS CSA-P | AWS CDE-P | MCT | CCAK | Azure Security | Azure Adv. Architect | CEH | RHCE



An experienced Information Security Consultant and Trainer. Proven expertise in deploying, migrating, auditing and securing various public cloud platforms including Amazon Web Services (AWS) & Microsoft Azure.

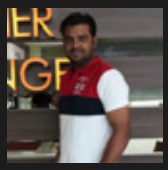
AMIT

Information Security | Cloud Security | Cloud Audit | Consultant and Trainer

HAPPY LEARNERS FROM THE WORLD

Naveen
India

I want to take this opportunity to thank Our Mentor, who has instrumental in getting me certified. This has been achieved by me with his extraordinary skills in mentoring and his guidance-one of the top qualified Trainers for the most challenging certifications with success gauranteed.



Shailesh
India

I want to express my deepest gratitiude to trainer, who helped me to pass my exam. The Trainer went the extra mile to assist me, and i have gained a significant benefit because of his knowledge and skills in Information Security. Infosectrain, you are a pioneer in the community and highly respected by everyone.

Gunjan Kumar
India

I would like to nominate Infosectrain Trainer to everyone willing to make their career in the information security domain. One of the best Trainer i have came across

DOMAIN WISE AGENDA

AWS CERTIFIED SECURITY - SPECIALTY (SCS-C02) Exam Domains

DOMAIN 1
14%

Threat Detection and Incident Response

DOMAIN 2
18%

Security Logging and Monitoring

DOMAIN 3
20%

Infrastructure Security

DOMAIN 4
16%

Identity and Access Management

DOMAIN 5
18%

Data Protection

DOMAIN 6
14%

Management and Security Governance

COURSE CONTENT

Domain 1: Threat Detection and Incident Response

Design and implement an incident response plan

- Incident Response Strategy
- Roles and responsibilities in IR plan specific to cloud incidents.
- Use case 1: Credentials compromise.
- Use case 2: Compromised EC2 Instances
- Playbooks and Runbooks for IR
- AWS Specific services helpful in Incident Response
- Third-party integration concepts
- Centralize security finding with security hub

Detect security threats and anomalies by using AWS services

- Threat detection services specific to AWS
- Visualizing and Detecting anomalies and correlation techniques
- Evaluate finding from security services
- Performing queries for validating security events
- Create metrics filters and dashboards to detect Anomalous activity

Respond to compromised resources and workloads

- AWS Security IR Guide
- Automating remediation by using AWS services
- Compromised resource management.
- Investigating and analyzing to conduct Root cause and log analysis.
- Capturing relevant forensics data from a compromised resource
- Protecting and preserving forensic artifacts
- Post-incident recovery

Domain 2: Security Logging and Monitoring

- Design and Implement monitoring and alerting to address security events
- Key AWS services for monitoring and alerting
- Monitoring metrics and baselines
- Analyzing environments and workloads to determine monitoring requirements according to business and security requirements
- Setting up tools and scripts to perform regular audits

Troubleshoot security monitoring and alerting

- Configuring of monitoring services and collecting event data
- Application monitoring, alerting, and visibility challenges

Design and implement a logging solution

- Key logging services and attributes
- Log destinations, Ingestion points and lifecycle management
- Logging specific to services and applications

Troubleshoot logging solutions

- AWS services that provide data sources and logging capabilities
- Access permissions that are necessary for logging
- Identifying misconfigurations and remediations specific to logging
- Reasons for missing logs and performing remediation steps

Design a log analysis solution

- Services and tools to analyze captured logs
- Identifying patterns in logs to indicate anomalies and known threats
- Log analysis features for AWS services
- Log format and components
- Normalizing, parsing, and correlating logs

Domain 3: Infrastructure Security

Design and implement security controls for edge services

- Define edge security strategies and security features
- Select proper edge services based on anticipated threats and attacks and define proper Protection mechanisms based on that
- Define layered Defense (Defense in Depth) mechanisms
- Applying restrictions based on different criteria
- Enable logging and monitoring across edge services to indicate attacks

Design and implement network security controls

- VPC security mechanisms including Security Groups, NACLs, and Network firewall
- Traffic Mirroring and VPC Flow Logs
- VPC Security mechanisms and implement network segmentation based on security requirements
- Network traffic management and segmentation
- Inter-VPC connectivity, Traffic isolation, and VPN concepts and deployment
- Peering and Transit Gateway
- AWS Point to Site and Site to Site VPN, Direct Connect
- Continuous optimization by identifying and removing unnecessary network access

Design and implement security controls for compute workloads

- Provisioning and maintenance of EC2 instances
- Create hardened images and backups
- Applying instance and service roles for defining permissions
- Host-based security mechanisms

- Vulnerability assessment using AWS Inspector
- Passing secrets and credentials security to computing workloads

Troubleshoot network security

Identifying, interpreting, and prioritizing network connectivity and analyzing reachability

Analyse log sources to identify problems

Network traffic sampling using traffic mirroring

Domain 4: Identity and Access Management

Design, implement and troubleshoot authentication for AWS resources

- Identity and Access Management
- Establish identity through an authentication system based on requirements.
- Managed Identities, Identity federation
- AWS Identity center, IAM and Cognito
- MFA, Conditional access, STS
- Troubleshoot authentication issues

Design, implement and troubleshoot authorization for AWS resources

- IAM policies and types
- Policy structure and troubleshooting
- Troubleshoot authorization issues
- ABAC and RBAC strategies
- Principle of least privilege and Separation of duties
- Investigate unintended permissions, authorization, or privileges

Domain 5: Data Protection

Design and implement controls that provide confidentiality and integrity for data in transit

- Design secure connectivity between AWS and on-premises networks
- Design mechanisms to require encryption when connecting to resources.
- Requiring DIT encryption for AWS API calls.
- Design mechanisms to forward traffic over secure connections.
- Designing cross-region networking

Design and implement controls that provide confidentiality and integrity for data at rest

- Encryption and integrity concepts
- Resource policies
- Configure services to activate encryption for data at rest and to protect data integrity by preventing Modifications.
- Cloud HSM and KMS

Design and implement controls to manage the data lifecycle at rest

- Lifecycle policies and configurations
- Automated life cycle management
- Establishing schedules and retention for AWS backup across AWS services.

Design and implement controls to protect credentials, secrets, and cryptographic key materials

- Designing management and rotation of secrets for workloads using a secret manager
- Designing KMS key policies to limit key usage to authorized users.
- Establishing mechanisms to import and remove customer-provider key material.

Domain 6: Management and Security Governance

Design a strategy to centrally deploy and manage AWS accounts

- Multi account strategies using AWS organization and Control tower
- SCPs and Policy multi-account policy enforcement
- Centralized management of security services and aggregation of findings
- Securing root account access

Implement a secure and consistent deployment strategy for cloud resources

- Deployment best practices with Infrastructure as a code
- Tagging and metadata
- Configure and deploy portfolios of approved AWS services.
- Securely sharing resources across AWS accounts
- Visibility and control over AWS infrastructure

Evaluate compliance of AWS resources

- Data classification by using AWS services
- Define config rules for detection of non-compliant AWS resources.
- Collecting and organizing evidence by using Security Hub and AWS audit manager

Identify security gaps through architectural reviews and cost analysis

- AWS cost and usage anomaly identification
- Strategies to reduce attack surfaces
- AWS well-architected framework to identify security gaps

INFOSECTRAIN

Course **Benefits**

$120,000 - $180,000 Cloud Security Architect

$100,000 - $150,000 Cloud Security Engineer

$100,000 - $150,000 Cloud Systems Administrator

$90,000 - $130,000 Cloud Network Engineer

HIRING COMPANIES

IBM

accenture

aws

ORACLE

Source: Indeed, Glassdoor


INFOSECTRAIN