

AWS

AWS Certified Security – Specialty (Security Engineering on AWS) Preparation Training

Delivered from Hacky Security's own curriculum, by instructors who also work our security operations centre. Classroom, online live, or at your office.

INTERMEDIATE

24 HOURS

3 DAYS

AWS SECURITY

At a glance

COURSE	AWS Certified Security – Specialty (Security Engineering on AWS)	WHAT IS INCLUDED
TRACK	AWS	✓ Instructor-led delivery by practitioners who also work our SOC
DOMAIN	Cyber Security	✓ Hands-on lab access for the duration of the course
LEVEL	Intermediate	✓ Course materials and lab guides
DURATION	24 hours (about 3 days)	✓ Hacky Security certificate of completion
DELIVERY	Classroom · Online live · On-site at your office	✓ Post-course support by email
LANGUAGE	English	
CLASS SIZE	Small cohorts — everyone gets lab time	

Who this is for

This is an intermediate course. It suits people already working in or moving into Cyber Security who want structured, hands-on preparation rather than a video library. If you are unsure whether the level fits your team, send us the job titles and we will tell you honestly — including if a different course would serve you better.

Course outline

About this course map

Six domains, mapped one-for-one to the AWS Certified Security – Specialty exam guide and taught in the same order, so nothing on the exam is left uncovered.

SCS-C02 is no longer current. AWS's own exam guide appendix records that SCS-C02 retired on 1 December 2025 and SCS-C03 launched on 2 December 2025, and the AWS exam guide index now lists SCS-C03 as the only version of this certification. This map covers SCS-C03. If you prepared against SCS-C02, the change is worth understanding rather than ignoring: the old Threat Detection and Incident Response domain and the old Security Logging and Monitoring domain were dissolved and rebuilt as Detection and as Incident Response, Management and Security Governance was renamed Security Foundations and Governance, Identity and Access Management gained four points of weighting, and Infrastructure Security lost two. Content on generative AI protections, inter-resource encryption in transit and data masking was added. Each domain below carries its published weighting, and we give it lab and classroom time in proportion.

This is a specialty exam, and the questions show it. They are long scenarios with four plausible answers, and the distractors are usually things that would work but are the wrong control, the wrong scope, or the wrong service for the constraint stated in the question. The teaching is built for that — you implement a control, then are told what the auditor or the incident found, and have to say what you would change.

Domain 01 — Detection

Knowing what happened in an account before anyone tells you. 16% of the scored exam, across three task statements.

- Analysing a workload to work out what actually needs monitoring, rather than enabling everything and drowning
- Workload monitoring strategy, resource health checks, and aggregating security and monitoring events across accounts
- Metrics, alerts and dashboards built on Amazon GuardDuty, AWS Security Hub, Amazon Macie and Amazon Security Lake
- Automated assessment and investigation using AWS Config conformance packs and AWS Systems Manager State Manager
- Choosing log sources against requirements, and configuring logging for AWS services and applications
- Organisation-wide AWS CloudTrail trails, dedicated Amazon CloudWatch logging accounts, and the CloudWatch Logs agent
- Log storage and security data lakes with Amazon Security Lake, and integrating third-party security tooling
- Analysing logs with CloudWatch Logs Insights, Amazon Athena and Security Hub findings, and normalising and correlating them with Amazon OpenSearch Service, AWS Lambda and Amazon Managed Grafana
- Network log sources chosen against the design and the threat: VPC Flow Logs, transit gateway flow logs and Amazon Route 53 Resolver logs
- Troubleshooting the monitoring pipeline itself — missing logs, broken agents, and permissions that silently drop events

Domain 02 — Incident Response

What you do in the hour after detection, and everything you had to arrange beforehand to make it possible. 14% of the scored exam, across two task statements.

- Designing response plans and runbooks, and holding them somewhere usable under pressure
- Preparing accounts for incidents: provisioned access, deployed tooling, minimised blast radius and AWS Shield Advanced protections
- Testing and validating the plan with AWS Fault Injection Service and AWS Resilience Hub before an incident does it for you
- Automated remediation with AWS Systems Manager, AWS Step Functions, Lambda and Amazon Application Recovery Controller
- Automated forensic collection for Amazon EC2, and capturing system and application logs as forensic artifacts
- Searching and correlating logs across applications and services to establish what an event actually touched
- Validating findings from AWS security services to size the scope and impact rather than trusting a severity label
- Containing and eradicating threats, applying network containment, and recovering resources from backup
- Root cause analysis, including using Amazon Detective to reconstruct the path

Domain 03 — Infrastructure Security

Securing the edge, the compute and the network the workload actually runs on. 18% of the scored exam, across three task statements.

- Selecting an edge security strategy against the threats you expect, rather than buying every edge service
- Edge protection with AWS WAF, AWS Shield Advanced, Amazon CloudFront headers, Amazon S3 cross-origin resource sharing and AWS IoT policies, including defence against the OWASP Top 10
- Edge rules driven by requirement: geography and geolocation, rate limiting, client fingerprinting
- Integrating AWS edge services with third-party tooling, including ingesting data in Open Cybersecurity Schema Framework format
- Hardened Amazon EC2 AMIs and container images built with EC2 Image Builder and Systems Manager, with controls embedded rather than applied later
- Instance profiles, service roles and execution roles as the authorisation model for compute
- Vulnerability scanning with Amazon Inspector across instances, container images and Lambda functions, and runtime monitoring with GuardDuty
- Patching at scale with Systems Manager Patch Manager, and continuous validation that patching actually happened
- Secure administrative access with Systems Manager Session Manager and EC2 Instance Connect, instead of open management ports
- Pipeline-stage vulnerability discovery with Amazon CodeGuru Security and Amazon Q Developer, and guardrails for generative AI applications against the GenAI OWASP Top 10 for LLM Applications
- Network controls with security groups, network ACLs and AWS Network Firewall, and troubleshooting when traffic is blocked by something other than what you are looking at
- Hybrid and multi-cloud connectivity with AWS Site-to-Site VPN, AWS Direct Connect and MACsec, and workload access with AWS Verified Access
- Segmentation for north-south and east-west traffic, isolated subnets, and finding unnecessary access with Network Access Analyzer

Domain 04 — Identity and Access Management

The largest domain, and the one where most real AWS incidents actually begin. 20% of the scored exam, across two task statements.

- Identity solutions for human, application and system authentication using AWS IAM Identity Center, Amazon Cognito and external identity providers
- Multi-factor authentication, and where it is a requirement rather than a recommendation
- Issuing temporary credentials with AWS STS and Amazon S3 presigned URLs, and designing away long-lived keys
- Troubleshooting authentication with CloudTrail, IAM Identity Center permission sets, Cognito and AWS Directory Service
- Authorisation controls including Amazon Verified Permissions, IAM Roles Anywhere, IAM paths, resource policies for cross-account access and role trust policies
- Attribute-based and role-based access control, including granting access from tags and attributes
- Writing and reading IAM policies to least privilege, with permission boundaries and session policies
- Diagnosing authorisation failures with the IAM Policy Simulator and IAM Access Analyzer, and knowing which of the several policy types denied the call
- Finding and correcting unintended permissions granted to a principal, service or resource

Domain 05 — Data Protection

Encryption, key custody and retention, treated as design decisions rather than checkboxes. 18% of the scored exam, across three task statements.

- Requiring encryption on connection through Elastic Load Balancing security policies and enforced TLS configuration
- Private access paths with AWS PrivateLink, VPC endpoints, AWS Client VPN and AWS Verified Access
- Inter-resource encryption in transit, including inter-node encryption for Amazon EMR, Amazon EKS and Amazon SageMaker AI, and Nitro encryption
- Encryption at rest: choosing between AWS KMS and AWS CloudHSM, and between client-side and server-side encryption, against a stated requirement
- Data integrity controls with S3 Object Lock, S3 Glacier Vault Lock, versioning, digital code signing and file validation
- Lifecycle and retention automation with S3 Lifecycle policies, Amazon EFS lifecycle policies and Amazon FSx for Lustre backup policies
- Replication and backup with AWS Backup, Amazon Data Lifecycle Manager and AWS DataSync, designed with ransomware in mind
- Credential and secret rotation with AWS Secrets Manager
- Imported key material and external key stores, and how they differ from AWS-generated keys in control and in obligation
- Masking sensitive data with CloudWatch Logs data protection policies and Amazon SNS message data protection
- Managing customer managed KMS keys and AWS Private Certificate Authority across one Region or several

Domain 06 — Security Foundations and Governance

Making the whole estate behave consistently, which is what a security specialist is actually hired for. 14% of the scored exam, across three task statements.

- Multi-account design with AWS Organizations, and AWS Control Tower deployed into new and existing environments
- Organisation policies that constrain permissions: service control policies, resource control policies, AI service opt-out policies and declarative policies
- Centralising security services through delegated administrator accounts rather than configuring each account by hand
- Root user management: centralised root access for member accounts, MFA, and break-glass procedures that are documented and tested
- Infrastructure as code for consistent, repeatable deployment, with CloudFormation StackSets, CloudFormation Guard and cfn-lint
- Tagging strategy for grouping resources by department, cost centre or environment, and the controls that depend on it
- Central enforcement of policy and configuration with AWS Firewall Manager
- Secure resource sharing across accounts with AWS Resource Access Manager and AWS Service Catalog
- Detecting and remediating non-compliant resources with AWS Config and Security Hub, with notification that reaches someone
- Evidence collection for audit with AWS Audit Manager and AWS Artifact, and architecture review with the AWS Well-Architected Tool

Who should take this

Cloud security engineers and architects, security operations staff who now own AWS accounts, DevOps and platform engineers responsible for guardrails, and consultants who audit or remediate AWS estates.

AWS recommends around five years of IT security experience designing and implementing security solutions, and two or more years of hands-on experience securing AWS workloads. There are no formal prerequisites and no experience audit — you can book it whenever you like — but this is a specialty exam and it assumes real operational history.

You will need to be comfortable in the AWS console and on a command line, able to read an IAM policy without help, and familiar with VPC networking, encryption concepts and how applications get deployed. An associate-level AWS certification is useful background but is not required.

The exam

The AWS Certified Security – Specialty is set and awarded by AWS, and delivered at Pearson VUE test centres or by online proctoring. The current version is SCS-C03.

- 65 questions, of which 50 are scored and 15 are unscored
- 170 minutes
- A scaled score of 750 out of 1000 is required to pass
- Multiple choice and multiple response, plus ordering and matching item types introduced in SCS-C03
- Scored compensatorily across the whole exam — there is no per-domain pass mark
- The exam fee is 300 USD

The exam fee is paid separately to AWS. We can arrange the booking on your behalf, and you choose your own date. Hacky Security is not an AWS Training Partner, and this course is taught from our own material rather than official AWS courseware.

How we deliver it

Three days, classroom or online live, or at your office for a private group. Roughly half the time is hands-on in a live multi-account AWS organisation we provide, so you are configuring the detection, the guardrails and the key policies rather than watching slides about them.

Domain checkpoints each day, and a full-length 65-question mock under exam conditions on the final afternoon, including the ordering and matching item types, followed by a walkthrough of why the nearly-right answer was wrong — which is the skill this exam is really testing.

Mapped to the AWS Certified Security – Specialty exam guide, SCS-C03. We track the AWS exam guide index and reissue this map when it changes. Taught from Hacky Security's own curriculum by instructors who secure AWS estates for a living.

Sitting the official exam

Exam voucher sold separately. We buy it from the certification body on your behalf and send you the code — you book your own exam date. This course is Hacky Security's own preparation training. The certification itself is awarded by the certification body, not by us.

Investment

FROM

₹66,500

per person

INR	₹66,500 per person
USD	\$799 per person
GBP	£629 per person
AED	AED 2,899 per person

Group, corporate and repeat-cohort pricing on request. Prices are reviewed quarterly and exclude the exam voucher.

Book this course

Tell us how many people, where, and when — we will come back with dates and a quote within one working day.

+91-8091900310 • info@hackysecurity.com

<https://hackysecurity.com/courses/hacky-aws-certified-security-specialty-training/>

CHANDIGARH • SHIMLA • DELHI • DUBAI • LONDON

Independent preparation training delivered from Hacky Security's own curriculum. Hacky Security Private Limited is not affiliated with or endorsed by the certification body named in this document. Certification names and codes are the trademarks of their respective owners and are used only to describe what this course prepares you for. Prices, durations and outlines are indicative and may change; the quotation we send you is the binding one. Issued 12 September 2026.