INFOSEC Skills
LIVE BOOT CAMPS

**Get live, expert instruction from anywhere.**

# AWS Certified Security – Specialty Boot Camp

The Security Engineering on AWS course is designed to help you better understand how to interact and build with Amazon Web Services (AWS) in a secure way with hands-on exercises to help you learn by doing.

## Course description

This 3-day Boot Camp is focused on teaching you specialized applications in the areas of AWS incident response best practices, event monitoring AWS services, common attacks, threats, exploits, and credentialing mechanisms and more.

This boot camp not only teaches you the knowledge and skills of the security engineering, it also prepares you to successfully pass the challenging AWS Certified Security – Specialty exam.

This course offers enrollment with a voucher. The voucher is pre-paid access to sit for the certifying exam upon eligibility.

## Who should attend

» Security engineers
» Security architects
» Cloud architects
» Cloud operators

## Boot camp at a glance

### What you'll learn

- ✓ Understanding of AWS Cloud Security based on CIA triad.
- ✓ Manage and provision accounts on AWS.
- ✓ Identify how to investigate threats and mitigate using AWS services.

### Delivery methods

- ✓ Online
- ✓ In person
- ✓ Team onsite

### Training duration

- ✓ Immediate access to Infosec Skills
- ✓ 3-day boot camp
- ✓ 90-day extended access to all boot camp materials

## The hands-on cybersecurity training platform that moves as fast as you do

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to days of live training from an experienced pro, you'll get unlimited access to hundreds of additional hands-on cybersecurity courses and cyber ranges to help you advance your skills before, during and after your boot camp. Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, or get a head start on your next certification goal.

### Start training immediately

Prepare for your boot camp with immediate access to the Infosec Skills on-demand training library.

### Learn by doing in the cyber range

Put what you've learned into practice with 100s of browser-based labs and hands-on projects.

### Get unlimited custom practice exams

Uncover knowledge gaps with unlimited practice exams attempts and skill assessments.

### 700+ IT and security courses

Earn CPEs and build new skills with hundreds of additional training courses.

# What's included

- Three days of expert, live AWS instruction
- Exam Pass Guarantee
- Exam voucher
- Unlimited practice exam attempts
- 100% Satisfaction Guarantee
- Free 90-day Infosec Skills subscription (access to 1,400+ additional courses and lab)
- 90-day extended access to Boot Camp components, including class recordings
- Knowledge Transfer Guarantee

## Prerequisites

None, but prior to enrolling in Infosec's AWS Certified Security – Specialty Boot Camp, it is recommended that you have completed the AWS Security Essentials (Classroom training) or AWS Security Fundamentals (Second Edition) (digital) and Architecting on AWS (Classroom Training), and possess a working knowledge of IT security practices, infrastructure concepts, and familiarity with the AWS Cloud.

## Exam objectives

This boot camp prepares you to pass AWS Certified Security – Specialty (SCS-C02) exam, which covers 6 domain areas designed to ensure relevancy across all disciplines of information security.

- Domain 1: Threat Detection and Incident Response
- Domain 2: Security Logging and Monitoring
- Domain 3: Infrastructure Security
- Domain 4: Identity and Access Management
- Domain 5: Data Protection
- Domain 6: Management and Security Governance

## Learn from experts

We don't just have great instructors, our instructors have years of industry experience and are recognized as experts. Over the past 15 years, we've helped tens of thousands of students get certified and advance their careers.

## Skill up and get certified, guaranteed

### Exam Pass Guarantee

If you don't pass your exam on the first attempt, get a second attempt for free. Includes the ability to re-sit the course for free for up to one year.

### 100% Satisfaction Guarantee

If you're not 100% satisfied with your training at the end of the first day, you may withdraw and enroll in a different online or in-person course.

### Knowledge Transfer Guarantee

If an employee leaves within three months of obtaining certification, Infosec will train a different employee for free for up to one year.

# Security Engineering on AWS details

Our instructors give you 100% of their time and dedication to ensure that your time is well spent. You receive an immersive experience with no distractions! The typical daily schedule is:

| | Day 1 | Day 2 | Day 3 |
|---|---|---|---|
| Morning session | Course Introduction<br>Intro to (SCS-C02)<br>Domain 1: Threat Detection and Incident Response | Domain 3: Infrastructure Security<br>Domain 4: Identity and Access Management | Domain 6: Management and Security Governance |
| Afternoon session | Domain 2: Security Logging and Monitoring | Domain 5: Data Protection | Recap & Review<br>Exam Tips & Practice Exam |

*Schedule may vary from class to class*

## Before your boot camp

Start learning now. You'll get immediate access to all the content in Infosec Skills the moment you enroll. Prepare for your live boot camp, uncover your knowledge gaps and maximize your training experience.

## During your boot camp

### Threat Detection and Incident Response

- Credential Security: Implementing strategies for invalidating and rotating credentials in response to breaches, using tools like AWS Identity and Access Management (IAM) and AWS Secrets Manager.
- Resource Isolation: Isolating AWS resources to contain potential security threats.
- Incident Response Planning: Creating playbooks and runbooks for effectively responding to security incidents.
- Security Service Deployment: Deploying security services such as AWS Security Hub, Amazon Macie, Amazon GuardDuty, Amazon Inspector, AWS Config, Amazon Detective, and AWS Identity and Access Management Access Analyzer.
- Integration Configuration: Setting up integrations with both native AWS services and third-party services, for instance, through Amazon EventBridge and the AWS Security Finding Format (ASFF).
- Security Findings Evaluation: Assessing security findings from services like GuardDuty, Security Hub, Macie, AWS Config, and IAM Access Analyzer.
- Threat Correlation: Using Detective to search and correlate security threats across various AWS services.
- Security Event Validation: Conducting queries with Amazon Athena to validate security events.
- Anomaly Detection: Creating metric filters and dashboards in Amazon CloudWatch to detect abnormal activity.
- Automated Remediation: Employing AWS services like Lambda, Step Functions, EventBridge, AWS Systems Manager runbooks, Security Hub, and AWS Config for automated remediation of security issues.
- Resource Compromise Response: Responding to compromised resources, such as isolating Amazon EC2 instances.
- Root Cause Analysis: Investigating and analyzing

incidents to determine the root causes, often using Detective.

- Forensics Data Capture: Capturing relevant forensics data from compromised resources, like Amazon Elastic Block Store (EBS) volume snapshots and memory dumps.
- Log Querying: Querying logs in Amazon S3 to gather contextual information related to security events, frequently with Athena.
- Forensic Artifact Protection: Protecting and preserving forensic artifacts through methods like S3 Object Lock, isolated forensic accounts, S3 Lifecycle, and S3 replication.
- Incident Preparation and Recovery: Preparing services for incidents and orchestrating service recovery after incidents occur.

## Security Logging and Monitoring

- Identifying Monitoring Needs: Analyzing architectures and workloads to determine security monitoring requirements and data sources.
- Designing Monitoring: Creating environment and workload monitoring solutions based on business and security needs.
- Automation and Alerting: Implementing automated tools and scripts for regular audits and setting up alert-generating metrics and thresholds.
- Configuration Analysis: Analyzing service functionality, permissions, and resource configurations, especially after events lacking visibility or alerting.
- Log Management: Evaluating and configuring logging services for alignment with security requirements, including log ingestion, storage, and lifecycle management.
- Access Permissions: Identifying and remediating missing access permissions for logging and misconfigurations.
- Log Analysis: Analyzing log patterns to detect anomalies and known threats, along with log normalization, parsing, and correlation.

## Infrastructure Security

- Edge Security: Defining security strategies for common scenarios and selecting edge services and protections based on threats and vulnerabilities.
- Network Segmentation: Implementing network segmentation, controls, and data flow management.
- Telemetry Monitoring: Determining telemetry sources for monitoring and addressing redundancy and security workload requirements.
- Access Management: Managing network access, configurations, and hardening, including vulnerability scanning, patching, and host-based security mechanisms.
- Problem Resolution: Analyzing connectivity issues and logs to identify and resolve network problems.

## Identity and Access Management

- Identity Establishment: Establishing identity using authentication systems, enabling multi-factor authentication, and using AWS STS for temporary credentials.
- Access Control: Implementing attribute-based access control, role-based access control, and applying the principle of least privilege.
- Error Analysis: Analyzing access or authorization errors, investigating unintended permissions, and unauthorized access.

## Security Services and Features

- Resource Policies: Designing resource policies for authorized user access and preventing unauthorized public access.
- Data Protection: Configuring data encryption at rest, mechanisms for data integrity protection, and encryption with AWS CloudHSM.
- Lifecycle Management: Designing data retention and automatic lifecycle management

mechanisms.

- Secrets Management: Managing and rotating secrets, and configuring KMS key policies.

### Management and Security Governance

- AWS Organizations: Deploying and configuring AWS Organizations, AWS Control Tower, and Service Control Policies (SCPs) for policy enforcement.
- Centralized Management: Managing security services centrally, securing AWS account root user credentials, and using CloudFormation for secure resource deployment.
- Resource Organization: Organizing AWS resources for management and deploying Firewall Manager for policy enforcement.
- Resource Sharing: Securely sharing resources across AWS accounts using AWS Resource Access Manager, identifying sensitive data with Macie.
- Compliance and Monitoring: Creating AWS Config rules, collecting and organizing evidence with Security Hub and AWS Audit Manager.
- Resource Optimization: Identifying resource anomalies, unused resources, and security gaps with the AWS Well-Architected Tool.

## After your boot camp

Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, get a head start on your next certification goal or start earning CPEs.

## About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at infosecinstitute.com.