AWS Certified Security - Specialty (SCS-C01) Exam Prep

AWS SCS-C01 Security Specialty. IAM, KMS, CloudTrail, and AWS security best practices.

IT Certifications Instructor: Brian Taylor • 5 sections • 44 lessons • 13.75h total

View this course online Browse all courses

About this course

This course prepares you for the AWS Certified Security Specialty (SCS-C01) exam. We cover IAM, KMS, CloudTrail, GuardDuty, and security best practices on AWS.

You will learn through hands-on labs, real security scenarios, and practice exams. The course includes video lessons and downloadable study materials.

Course curriculum

Section 1: Exam Overview & Core Security Foundations

- Understanding the SCS-C01 Exam Blueprint (12m)
  We'll break down the exam domains, question formats, and scoring so you know exactly what to expect on test day.
- Setting Up Your AWS Exam Environment (8m)
  A step-by-step guide to configuring your AWS account for security labs, including setting up a secure admin user.
- Shared Responsibility Model Deep Dive (15m)
  Learn the boundaries of AWS vs. customer responsibility with real examples for EC2, RDS, and Lambda.
- AWS Global Infrastructure & Security Regions (10m)
  Understand how region selection impacts security, compliance, and data residency for your architecture.
- Introduction to AWS Security Hub & Security Standards (18m)
  See how Security Hub aggregates findings and helps you measure compliance against CIS benchmarks.
- Key Security Concepts: Least Privilege & Defense in Depth (14m)
  We'll apply these core principles to AWS services with practical policy examples you can use.
- Exploring AWS Artifact for Compliance Reports (9m)
  Learn how to access audit reports and compliance documentation to support your security assessments.

Section 2: Identity & Access Management (IAM)

- IAM Users, Groups, and Roles: The Core Concepts (22m)
  A practical breakdown of when to use each identity type with examples for multi-account setups.
- Writing Effective IAM Policies: Syntax & Best Practices (28m)
  We'll build and test policies, covering explicit denies, condition keys, and avoiding common policy mistakes.
- AssumeRole: Cross-Account & Service-to-Service Access (25m)
  Walk through STS workflows and how to securely delegate access across your AWS environment.
- Securing Root Account & Implementing MFA (11m)
  Critical steps to lock down the root user and enforce multi-factor authentication for all privileged accounts.
- IAM Roles for EC2: Instance Profiles Explained (16m)
  Learn how to assign roles to EC2 instances securely, avoiding the need for long-term credentials.
- Identity-Based vs. Resource-Based Policies (19m)
  We'll compare policy types and show you how they interact, especially for S3 buckets and SQS queues.

- Using IAM Access Analyzer to Find Shared Resources (13m)
  A practical guide to using Access Analyzer to identify resources shared with external entities.
- Troubleshooting Common IAM Access Denied Errors (20m)
  A problem-solving session on diagnosing and fixing IAM permission issues in real scenarios.
- Advanced Role Session Tags & Attribute-Based Access (24m)
  Explore how to use session tags and ABAC to dynamically grant permissions based on user attributes.

Section 3: Data Protection & Encryption

- AWS KMS: Customer-Managed vs. AWS-Managed Keys (21m)
  Understand key policies, rotation, and when to use CMKs for enhanced control over your data.
- Encrypting Data at Rest: S3, EBS, and RDS (26m)
  Step-by-step walkthroughs of enabling encryption on storage services and managing the encryption keys.
- Server-Side vs. Client-Side Encryption for S3 (17m)
  We'll compare encryption methods and show you how to implement client-side encryption with KMS.
- Envelope Encryption & How KMS Works Under the Hood (19m)
  A look at the cryptographic process to help you understand KMS API calls and data key handling.
- AWS Secrets Manager vs. Parameter Store: Which to Choose? (15m)
  A practical comparison for storing secrets, including rotation, cost, and integration with Lambda.
- Securing Data in Transit: TLS and SSL on AWS (14m)
  Learn about certificate management with ACM and enforcing TLS on ELB and API Gateway.
- Macie: Discovering and Protecting Sensitive Data (12m)
  See how Macie uses machine learning to find PII and other sensitive data in S3.
- Backup and Recovery Strategies for Security (23m)
  Design resilient backup plans using AWS Backup and understand cross-region replication for DR.

Section 4: Network Security & Threat Detection

- VPC Security: NACLs vs. Security Groups (27m)
  We'll dissect the differences with packet-level examples to master stateless vs. stateful filtering.
- Designing a Secure VPC with Public and Private Subnets (30m)
  A real case study analysis of a 3-tier architecture, focusing on routing and NAT gateways.
- Web Application Firewall (WAF): Rules & Rule Groups (24m)
  Build WAF rules to mitigate common web exploits like SQL injection and cross-site scripting.
- AWS Shield Advanced: DDoS Protection Explained (13m)
  Understand what Shield Advanced offers, including cost protection and integration with WAF.
- GuardDuty: Threat Detection and Finding Analysis (22m)
  We'll configure GuardDuty and walk through analyzing a sample finding to determine the threat.
- Network Firewall: Centralized Traffic Inspection (25m)
  Deploy and configure AWS Network Firewall for advanced traffic filtering in your VPC.
- VPC Flow Logs: Capturing and Analyzing Network Traffic (18m)
  Learn how to enable flow logs and query them in Athena to investigate security incidents.
- PrivateLink & VPC Endpoints: Secure Service Access (20m)
  Keep traffic off the public internet by using VPC endpoints for AWS services.

- AWS Certificate Manager: Managing SSL/TLS Certificates (11m)
  A quick guide to requesting, deploying, and renewing certificates for your applications.
- Configuring AWS WAF with Rate-Based Rules (16m)
  A practical session on protecting your applications from brute-force attacks and traffic spikes.

Section 5: Incident Response & Secure Operations

- Incident Response Lifecycle on AWS (14m)
  We'll map the standard IR phases (Preparation, Detection, Containment, etc.) to AWS services.
- Using CloudTrail for Security Auditing & Forensics (29m)
  Learn to query event history, log to S3, and use CloudTrail Insights for anomaly detection.
- Automating Incident Response with Lambda & EventBridge (32m)
  Build a serverless function to automatically remediate a security finding, like a public S3 bucket.
- AWS Config: Configuration Management & Compliance (26m)
  Set up Config rules to continuously monitor your resource configurations for compliance drift.
- Forensic Analysis: Isolating and Snapshotting an EC2 Instance (21m)
  A step-by-step guide to preserving evidence from a compromised instance without impacting the attacker.
- Systems Manager Session Manager: Secure Instance Access (15m)
  Eliminate bastion hosts and SSH keys by using Session Manager for secure EC2 access.
- Patch Management with Systems Manager Patch Manager (19m)
  Create patch groups and maintenance windows to keep your fleet secure and up-to-date.
- Amazon Inspector: Vulnerability Scanning for EC2 & ECR (17m)
  Run vulnerability assessments on your instances and container images to find CVEs.
- GuardDuty + EventBridge: Building Custom Response Workflows (23m)
  A deeper dive into creating automated playbooks triggered by GuardDuty findings.
- Final Review: Tying All Domains Together (12m)
  A comprehensive review of key concepts from all domains with tips for exam day strategy.