Security Engineering on AWS

AWS Classroom Training

Course description

Security Engineering on AWS is a three-day, instructor-led classroom course that teaches security practitioners to secure Amazon Web Services (AWS) workloads across the six AWS security domains: identity and access management, infrastructure security, data protection, threat detection, incident response, and governance. Learners work through hands-on labs, instructor demonstrations, and knowledge checks that build from foundational identity and network controls to organization-wide detection, response, and governance. The course also covers protections for generative AI applications and the secure use of GenAI productivity tools.

Course level: Intermediate (200), with advanced (300) depth in identity and data protection

Duration: 3 days

Activities

This course includes presentations, hands-on labs, demonstrations, group exercises, and knowledge checks.

Course objectives

In this course, you learn to do the following:

Design and troubleshoot authentication and authorization strategies using least-privilege principles, attribute-based and role-based access control, and centralized identity.

Architect and troubleshoot infrastructure security controls for network edge services, compute workloads, and network segmentation.

Implement data-protection controls for data in transit and at rest, including key management, secrets rotation, and data masking.

Design monitoring, alerting, and logging solutions to detect anomalous activity across an AWS account or organization.

Develop and execute an incident response plan, including forensic artifact capture, containment, eradication, recovery, and root-cause analysis.

Govern an AWS environment at scale using AWS Organizations, AWS Control Tower, and compliance services.

Apply protections for generative AI applications and secure the use of GenAI productivity tools.

Intended audience

This course is intended for:

- Security engineers
- Cloud security architects
- Security operations engineers
- DevSecOps engineers
- Security-focused solutions architects
- IT professionals responsible for securing AWS workloads

Prerequisites

We recommend that attendees of this course have:

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

- Completed AWS Security Essentials (classroom) or AWS Security Fundamentals (digital)
- Completed AWS Cloud Practitioner Essentials, or equivalent cloud fundamentals
- Working knowledge of networking concepts (TCP/IP, DNS, and firewalls)
- Familiarity with the AWS Management Console and the AWS Command Line Interface (AWS CLI)

Course outline

Day 1

Module 1: Security Overview and Shared Responsibility

- Describe the AWS Shared Responsibility Model and how it shifts by service type.
- Explain defense-in-depth layering across identity, edge, network, compute, and data.
- Orient to the six AWS security domains and the course build, operate, and govern flow.

Module 2: Identity and Access Management - Authentication

- Design identity solutions for human, application, and system authentication with AWS IAM Identity Center, Amazon Cognito, and federation.
- Configure temporary credentials using AWS STS and IAM Roles Anywhere.
- Apply multi-factor authentication (MFA) strategies, including mandatory root MFA and phishing-resistant factors.
- Troubleshoot federated authentication failures using AWS CloudTrail.
- Hands-on lab 1: Federated access with IAM and multi-factor authentication.

Module 3: Identity and Access Management - Authorization

- Design least-privilege authorization with IAM policies, permission boundaries, and Amazon Verified Permissions.
- Analyze authorization failures using IAM Policy Simulator and IAM Access Analyzer.
- Remediate unintended permissions and the confused-deputy problem.
- Hands-on lab 2: Least-privilege with ABAC and IAM Access Analyzer.

Module 4: Infrastructure Security - Network Edge

- Select edge security strategies based on anticipated threats.
- Implement layered edge protection with AWS WAF, AWS Shield, and Amazon CloudFront.
- Configure AWS WAF web ACLs, managed rule groups, and rate-based rules.
- Filter outbound DNS with Amazon Route 53 Resolver DNS Firewall.

Day 2

Module 5: Infrastructure Security - Compute Workloads

- Harden compute workloads with appropriate roles, EC2 Image Builder, and AWS Systems Manager.
- Implement vulnerability management with Amazon Inspector (including code security) and Amazon GuardDuty.

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

- Configure secure administrative access without bastions or SSH keys using AWS Systems Manager Session Manager.
- Apply generative AI application protections (OWASP Top 10 for LLM Applications) and secure GenAI productivity tools.

Module 6: Infrastructure Security - Network Security Controls

- Design network segmentation with security groups, network ACLs, and AWS Network Firewall.
- Implement zero-trust application access with AWS Verified Access and Amazon VPC Lattice.
- Identify unintended network reachability with Network Access Analyzer.
- Secure hybrid connectivity with AWS Site-to-Site VPN and AWS Direct Connect (MACsec).
- Hands-on lab 3: Network security controls with AWS WAF and AWS Network Firewall segmentation.

Module 7: Data Protection - Data in Transit

- Enforce encryption for resource connections with ELB security policies and mutual TLS.
- Manage TLS certificates with AWS Certificate Manager (ACM).
- Configure private access with AWS PrivateLink and VPC endpoints.
- Configure inter-resource encryption in transit.

Module 8: Data Protection - Data at Rest

- Design encryption at rest with AWS KMS and AWS CloudHSM, including the three-layer KMS authorization model.
- Apply an end-to-end reference architecture for cross-account envelope encryption on Amazon S3.
- Configure data integrity and lifecycle controls with Amazon S3 Object Lock and S3 Glacier Vault Lock.
- Configure ransomware-resilient backup with AWS Backup and multi-party approval.
- Detect sensitive data at rest with Amazon Macie.
- Hands-on lab 4: S3 data security with SSE-KMS, bucket-policy enforcement, replication, and Macie.

Module 9: Data Protection - Secrets, Credentials, and Key Materials

- Manage secrets rotation with AWS Secrets Manager, including RDS-managed credentials.
- Manage imported versus AWS-generated key material and external key stores.
- Implement data masking with Amazon CloudWatch Logs and Amazon SNS data protection.
- Implement multi-Region key and certificate management with AWS Private CA.
- Hands-on lab 5: Multi-Region AWS KMS rotation, Secrets Manager, and data masking.

Day 3

Module 10: Detection - Logging Solutions

- Identify log sources based on requirements, including AWS CloudTrail, VPC Flow Logs, and network logs.
- Configure centralized log ingestion into a dedicated logging account and Amazon Security Lake.

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

- Analyze and correlate logs with CloudWatch Logs Insights, Amazon Athena, and Amazon OpenSearch Service.

Module 11: Detection - Monitoring and Alerting

- Configure workload monitoring and event aggregation across a multi-account organization.
- Aggregate findings with AWS Security Hub, Security Hub CSPM, Amazon GuardDuty, and Amazon Macie.
- Create metrics, alerts, and dashboards with Amazon CloudWatch and AWS Config to detect anomalous activity.
- Hands-on lab 6: Detection pipeline routing findings to alerts with Amazon EventBridge and Amazon SNS.

Module 12: Detection - Troubleshooting Monitoring and Logging

- Diagnose functionality, permissions, and configuration issues in logging pipelines.
- Remediate common misconfigurations that cause missing logs.
- Hands-on lab 7: Centralized logging pipeline and fixing broken logging.

Module 13: Incident Response

- Design incident response plans, runbooks, and break-glass access.
- Configure services for incident readiness, including AWS Security Incident Response and AWS Shield Advanced.
- Test incident response effectiveness with security simulations (game days) and GuardDuty event simulation.
- Capture forensic artifacts from a compromised resource.
- Validate findings to assess scope and impact.
- Apply containment, eradication, and recovery procedures.
- Perform root-cause analysis with Amazon Detective.
- Automate the initial incident response with Amazon EventBridge and AWS Lambda.
- Instructor demonstration: Breach response with Amazon Detective.
- Hands-on lab 8: Incident response - capture, isolate, remediate, and automate.

Module 14: Governance at Scale

- Design multi-account governance with AWS Organizations and AWS Control Tower.
- Enforce policy at scale with service control policies (SCPs) and resource control policies (RCPs).
- Evaluate compliance at scale with AWS Config, AWS Firewall Manager, and the AWS Well-Architected Tool.

Course wrap-up

- Course summary
- Next steps and additional resources

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.