

Cloud Security

Duration: 10 Days | 4 Hours per Day | Total: 40 Hours | Level: Intermediate

Course Overview

This course provides a comprehensive understanding of cloud security principles, architecture, identity and access management, network protection, data security, threat detection, incident response, and compliance. The course uses AWS as the primary platform for hands-on demonstrations and practical exercises, while introducing security concepts applicable across cloud environments.

Learning Outcomes

By the end of this course, participants will be able to:

1. Explain cloud security principles and the shared responsibility model.
2. Implement identity, access, network, and data protection controls.
3. Secure cloud workloads and identify common vulnerabilities.
4. Configure cloud logging, monitoring, and threat detection.
5. Assess cloud security posture and recommend remediation actions.
6. Apply incident response, governance, risk, and compliance practices.
7. Incorporate security controls into development and deployment pipelines.
8. Design a secure cloud architecture using industry best practices.

Target audience: Cloud administrators, infrastructure engineers, security analysts, cloud architects, DevOps engineers, IT operations teams, and professionals transitioning into cloud security.

Prerequisites: Basic understanding of cloud computing, networking, operating systems, and IT security concepts. Prior AWS experience is helpful but not mandatory.

Detailed Course Curriculum

Day 1: Cloud Security Fundamentals

- Cloud security principles, threats, and challenges
- Cloud service models: IaaS, PaaS, and SaaS
- Shared Responsibility Model
- Cloud security architecture and defense-in-depth

- Cloud threat landscape: misconfiguration, account compromise, and data breaches

Day 2: Identity and Access Management (IAM)

- Authentication, authorization, and identity federation
- Least privilege and role-based access control
- Multi-factor authentication and password policies
- IAM users, groups, roles, and policies
- Privileged access management and access reviews

Lab : Configure IAM roles, policies in AWS

Day 3: Cloud Network Security

- VPCs, subnets, routing, and network segmentation
- Security groups and network ACLs
- Firewalls, VPNs, and private connectivity
- Web Application Firewall (WAF) and DDoS protection
- Zero Trust principles and secure remote access

Lab : Design a segmented VPC with controlled network access

Day 4: Data Security and Encryption

- Data classification, privacy, and lifecycle management
- Encryption at rest and in transit
- Key management, rotation, and access controls
- Secrets management and credential protection
- Data loss prevention, backup, and recovery security

Lab : Secure S3 data using encryption, bucket policies, and AWS KMS

Day 5: Compute and Workload Security

- Secure configuration of cloud virtual machines
- Operating system hardening and patch management
- Container and Kubernetes security fundamentals
- Serverless security and workload isolation

- Vulnerability management

Day 6: Security Monitoring and Threat Detection

- Cloud logging, audit trails, and centralized monitoring
- Security event monitoring and alerting
- AWS CloudTrail, CloudWatch, GuardDuty, and Security Hub
- Detection of suspicious activity and anomalous access

Lab : Enable audit logging and investigate simulated security findings

Day 7: Vulnerability Management and Security Posture

- Cloud vulnerability assessment and risk prioritization
- Configuration baselines and security benchmarks
- Cloud Security Posture Management (CSPM)
- Misconfiguration detection and remediation
- Security assessments and penetration-testing considerations

Lab : Assess cloud resource configurations and remediate common findings

Day 8: Incident Response and Business Continuity

- Cloud incident response lifecycle
- Incident triage, containment, eradication, and recovery
- Compromised credentials and data exposure scenarios
- Forensics, evidence preservation, and audit trails
- Backup security, disaster recovery, and resilience

Lab : Respond to a simulated compromised instance

Day 9: Governance, Risk and Compliance

- Cloud security governance and risk management
- ISO 27001, NIST Cybersecurity Framework, CIS Benchmarks
- PCI DSS, GDPR, and audit readiness
- Policy-as-code and infrastructure-as-code security

Day 10: Advanced Cloud Security and Capstone

- Secure cloud architecture and threat modeling

- Cross-account security and centralized governance
- Multi-account logging and security operations
- Security automation and remediation workflows
- Capstone: Design and assess a secure cloud environment