CA304: Cloud Security

29 Instructional Hours 47 CPEs 18 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

INTERMEDIATE

This course provides a comprehensive and practical introduction to cloud security, focusing on how modern cloud environments are designed, deployed, and protected. It explores core cloud computing concepts, service and deployment models, and the shared responsibility framework, while diving deeply into real-world implementations using platforms such as AWS and Azure. Learners gain hands-on exposure to identity and access management, cloud networking, secure SaaS architecture, serverless computing, data protection, and security operations. The course emphasizes a practical, lab-driven approach, enabling participants to build, secure, monitor, and assess cloud infrastructures while understanding real-world vulnerabilities, attack surfaces, and defensive strategies.

You Will Be Able To

- Explain cloud computing models, architectures, and the shared responsibility model
- Configure and secure cloud environments using IAM, networking, and storage controls
- Design and analyze secure SaaS and serverless architectures
- Detect, monitor, and respond to cloud-based threats using native security tools
- Perform basic cloud penetration testing and identify common misconfigurations
- Implement security best practices across AWS, Azure, and containerized environments

Who Should Attend

This course is designed for students, IT professionals, and cybersecurity practitioners seeking to understand and secure cloud environments. It is particularly suitable for individuals pursuing roles in cybersecurity, cloud engineering, DevOps, or system administration. A basic understanding of networking and computing concepts is recommended, as the course builds progressively from foundational cloud principles to advanced security practices and real-world implementations.

Relevant Combat Roles

- Cloud Security Engineer
- Security Operations Analyst (SOC Analyst)
- Cloud / DevOps Engineer
- Penetration Tester (Cloud Specialist)
- Threat Detection and Incident Response Analyst

Topics Covered

Cloud Foundations & Architecture: Cloud computing models (IaaS, PaaS, SaaS, FaaS), SaaS architecture design, multi-tenancy, and secure cloud architecture principles

Identity, Access & Security Models: IAM (users, roles, policies, least privilege), shared responsibility model, and core cloud security principles

Core AWS Services & Infrastructure: AWS IAM, EC2, S3, VPC, Organizations, along with cloud networking (VPCs, subnets, routing, gateways)

Serverless & Infrastructure as Code: AWS Lambda, API Gateway, Terraform, and AWS SAM for scalable and automated deployments

Data Protection & Observability: Data storage (S3), encryption (KMS), secrets management (Secrets Manager), monitoring (CloudWatch), logging, metrics, and tracing

Security Operations & Advanced Topics: CloudTrail, GuardDuty, threat detection, penetration testing, container security (Docker, Kubernetes), and Azure fundamentals & security controls

Labs

Deploy and secure a cloud environment
(Create a VPC with public/private subnets, configure EC2 instances, implement secure access controls, bastion host, security groups)

Implement IAM security
(Create users, groups, and policies, apply least privilege, and test access control scenarios)

Build a serverless API
(Deploy a Lambda-backed API using API Gateway and store data securely in S3 using IAM roles and Secrets Manager)

Monitor and investigate activity
(Configure CloudTrail and CloudWatch, analyze logs, and detect suspicious actions within a cloud environment)