Cloud Security Training – 15 Module Curriculum

Industry-aligned, hands-on cloud security curriculum suitable for corporate, academic, and professional training programs.

Module 1: Cloud & Security Foundations

- Cloud service models and deployment types
- Shared Responsibility Model
- Cloud threat landscape and kill chain
- Common cloud breaches overview

Module 2: Cloud Lab Setup & Sandbox

- AWS / Azure / GCP free tier setup
- Secure account baseline
- Logging and budget alerts

Module 3: Cloud Architecture & Threat Modeling

- Reference architectures
- Trust boundaries
- STRIDE and attack path analysis

Module 4: Identity & Access Management (IAM)

- Users, roles, policies
- Least privilege
- IAM misconfig exploitation

Module 5: Advanced IAM & Federation

- SSO, SAML, OAuth, OIDC
- Workload identity
- Token abuse scenarios

Module 6: Cloud Networking Security – Core

- VPC/VNet design
- Security groups and NACLs
- Segmentation strategies

Module 7: Cloud Networking Security – Advanced

- DNS security
- Egress filtering
- Metadata service attacks

Module 8: Data Protection & Key Management

- Encryption models
- KMS and HSM basics
- Key rotation and misuse

Module 9: Storage & Compute Security

- Bucket exposure risks
- VM hardening
- Patch and image management

Module 10: Container Security

- Container threats
- Image scanning
- Registry hardening

Module 11: Kubernetes Security

- RBAC
- Pod security standards
- Kubernetes privilege escalation

Module 12: Serverless & Managed Services Security

- Function security
- API Gateway protection
- Event abuse risks

Module 13: Logging, Detection & Incident Response

- Centralized logging
- MITRE ATT&CK; for Cloud
- Cloud IR playbooks

Module 14: CSPM, IaC & CI/CD Security

- CSPM and CNAPP
- IaC scanning
- Supply chain attacks

Module 15: Governance, Zero Trust & Capstone

- Compliance basics
- Zero Trust for cloud
- Capstone project: Cloud security monitoring stack