Module 4 — Cloud & Application Security

Course Outline

Cloud Security Fundamentals

- Cloud service and deployment models (IaaS, PaaS, SaaS; public/private/hybrid).
- Shared responsibility model and cloud threat landscape.
- Identity and access management (IAM) basics for cloud providers.

Secure Cloud Architecture & Hardening

- Designing secure cloud architectures (network segmentation, VPCs, subnets).
- Secure configuration and hardening of cloud resources.
- Encryption for data at rest and in transit in cloud environments.

Secure Software Development (DevSecOps)

- Secure SDLC principles and integrating security into CI/CD.
- Static and dynamic application security testing (SAST/DAST).
- Infrastructure as Code (IaC) security and policy-as-code (e.g., Terraform, CloudFormation, Sentinel, OPA).

Application Threat Modeling & OWASP

- Threat modeling techniques (STRIDE, DREAD).
- OWASP Top 10 and secure coding practices for web and mobile apps.
- Input validation, authentication/authorization, session management best practices.

API, Container & Microservices Security

- Securing RESTful and GraphQL APIs (rate-limiting, auth, scopes).
- Container security lifecycle (image scanning, runtime protection, Kubernetes hardening).
- Service mesh security controls and observability.

Cloud Monitoring, Detection & Incident Handling

- Using cloud-native logging/monitoring (CloudWatch, Stackdriver, Azure Monitor) and SIEM integration.
- Threat detection patterns for cloud workloads and applications.
- Automated response playbooks and containment strategies for cloud incidents.

Compliance, Governance & Risk in the Cloud

- Mapping cloud controls to standards (ISO 27001, NIST, PCI-DSS, GDPR).

- Cloud governance, tagging, cost controls and auditability.
- Vendor risk management and third-party assessment considerations.

Expected Learning Outcomes

- Design and harden cloud architectures to reduce attack surface.
- Integrate security into development pipelines (DevSecOps) using SAST/DAST and IaC scanning.
- Identify and remediate common application vulnerabilities per OWASP guidance.
- Secure APIs, containers, and microservices across their lifecycle.
- Implement monitoring and incident handling strategies tailored for cloud environments.
- Align cloud deployments with compliance and governance frameworks.