COURSE SYLLABUS

Cloud Security Architecture & Hardening: Build It Secure, Keep It Secure Course

Two days live on cloud security architecture and operations, anchored to real recent breaches including the 2024 Snowflake tenant compromise and Storm-0558.

> Group classes (Live Online) and onsite training are available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/cloud-security-architecture-and-hardening



support@graduateschool.edu •
(888) 744-4723

Course Outline

Module 1

- Draw the Boundary: Cloud Security Architecture Foundations
- Service and deployment models
- Security design principles
- Assets, resources and trust boundaries
- Shared responsibility
- Control ownership versus inherited capability
- Common attack surfaces
- Defense in depth
- CNAPP as the umbrella over CSPM, CWPP and CIEM

Module 2

- Identity Is the Control Plane: IAM Architecture
- Identities, roles, permissions and entitlements
- Human versus workload identity
- Least privilege
- Role-based and attribute-based access
- Privileged access and administrative separation
- Stronger authentication including legacy non-SSO paths
- Entitlement management
- Case studies on the 2024 Snowflake tenant breach and the Storm-0558 signing-key compromise

Module 3

- Trust No Network: Cloud Network Security Architecture
- Security zones and trust boundaries

- Virtual networks, subnets, routing and gateways
- Segmentation and microsegmentation
- Inbound and outbound control
- Security groups and filtering
- Protecting management interfaces
- Zero Trust per NIST SP 800-207 and 800-207A
- Service mesh proxy architecture per SP 800-233

Module 4

- Protect the Data: Cloud Data Security & Cryptography
- Classification
- Protection at rest, in transit and in processing per NIST IR 8505
- Encryption across storage, databases and applications
- Key lifecycle management
- Organization-managed versus provider-managed keys, BYOK and HYOK
- Secrets, tokens, certificates and API keys
- Minimization, retention and secure deletion
- Post-quantum cryptography migration
- FIPS 140-3 and SP 800-57 for federal environments

Module 5

- Harden the Foundation: Secure Cloud Configuration
- Baselines using NIST guidance, the CSA Cloud Controls Matrix and CIS Benchmarks
- Insecure defaults and unnecessary services
- Hardening management planes
- Restricting public exposure
- Least functionality
- Configuration drift detection
- Managing approved exceptions
- The FedRAMP 20x model for federal environments

Module 6

- Lock Down the Workload: Compute, Containers & Serverless
- Hardening instances and operating systems
- Protecting images, templates and deployment artifacts
- Container isolation and runtime security
- Protecting registries against malicious and typosquatted images
- Serverless security and emerging abuse patterns
- Reducing workload privilege
- The NIST SP 800-204 series for cloud-native architectures

Module 7

- Secure the Front Door: Applications, APIs & Services
- Application attack surfaces
- Application-to-application communication
- API authentication and authorization per NIST SP 800-228 Update 1

- Secure API gateways
- Service identity and service-to-service trust
- Protecting secrets without relying on environment variables
- Secure development per SP 800-218 and 800-218A

Module 8

- See Everything: Logging, Monitoring & Detection
- Identifying security-relevant logs and telemetry
- Enabling logging across identity, network, workload and administrative activity
- Centralization and retention
- Protecting logs from alteration
- Alerting on suspicious administrative activity
- Detecting drift
- Supporting investigation
- CISA SCuBA baselines as a mandated example

Module 9

- Assume Something Breaks: Resilience, Recovery & Incident Readiness
- Designing for availability
- Single points of failure and critical dependencies
- Redundancy and fault tolerance
- Protecting backups
- Recovery objectives and restoration priorities
- Preparing for compromised identities, workloads and accounts including a compromised trust anchor
- NIST SP 1800-35

Module 10

- Architect, Harden, Defend: Cloud Security Workshop
- Review a fictional architecture, identify trust boundaries and insecure exposure, evaluate identity and privileged access risk against a real recent breach, assess segmentation, data protection and key management including post-quantum timing, then build and defend a prioritized hardening plan