SYLLABUS

CYBER SECURITY · COURSE HANDOUT 2026

CLOUD SECURITY

. ENCRYPTION . KEY MANA
NETWORK SECURITY . LOGG
. AZURE . GCP COMPLIANCE

DURATION	LEVEL	MODULES	MODE
50 Hours	**Intermediate to Advanced**	**8**	**Classroom · Online · Hybrid**

01 COURSE OVERVIEW

A cloud security course covering identity, data protection, monitoring and compliance across three platforms. The course works through the shared responsibility model in practice: least-privilege IAM, network boundaries, encryption and key management, logging and detection, workload protection, and compliance evidence.

Configuration exercises run on AWS, Azure and Google Cloud free tiers, ending in a security audit of a deployed environment.

WHO IT IS FOR

- Cloud and DevOps engineers
- Security architects and analysts
- Compliance and audit staff
- System administrators moving to cloud

PREREQUISITES

Working knowledge of at least one cloud platform and basic networking.

02 LEARNING OUTCOMES

01 Apply the shared responsibility model to a workload.

02 Design least-privilege identity and access policies.

03 Protect data at rest and in transit with managed keys.

04 Secure cloud networks with segmentation and private access.

05 Enable logging, detection and alerting across accounts.

06 Harden compute, container and serverless workloads.

07 Produce audit evidence against a compliance framework.

03 MODULE STRUCTURE

8 MODULES

01 CLOUD SECURITY FOUNDATIONS

- Shared responsibility
- Attack surface
- Guardrails and policy
- Threat model
- Landing zones

02 IDENTITY AND ACCESS

- IAM users, roles and policies
- Federation and SSO
- Privileged access
- Least privilege
- MFA
- Access reviews

LAB

POLICY HARDENING

03 DATA PROTECTION

- Encryption at rest
- KMS and Key Vault
- Backup and retention
- Encryption in transit
- Secrets management

LAB

KEY ROTATION

04 NETWORK SECURITY

- VPC and VNet design
- Private endpoints
- DDoS protection
- Security groups
- WAF
- Egress control

05 LOGGING AND DETECTION

- CloudTrail
- Cloud Logging
- GuardDuty and Defender
- Azure Monitor
- SIEM integration
- Alerting

LAB

DETECTION PIPELINE

06 WORKLOAD SECURITY

- Instance hardening
- Container security
- Serverless permissions
- Image scanning
- Patch automation

07 POSTURE AND COMPLIANCE

- CSPM tools
- Benchmarks
- ISO 27001
- SOC 2
- PCI DSS
- Evidence collection

TOOLS

PROWLER · SCOUTSUITE

08 INCIDENT RESPONSE IN CLOUD

- Account compromise
- Key leakage
- Forensic snapshots
- Containment automation
- Recovery

PROJECT

CLOUD SECURITY AUDIT REPORT

04 ASSESSMENT & CERTIFICATION

Module assignments and labs	**25%**
Mini projects	**20%**
Internal assessments	**15%**
Final project and review	**40%**

CERTIFICATION

Learners who complete all modules, submit the final project and clear the review receive a course completion certificate from Kaizen Infinities Private Limited. Project work is documented for the learner's portfolio, and interview preparation is included in the closing sessions.

05 CAREER OUTCOMES

ROLES THIS PROGRAMME PREPARES FOR

CLOUD SECURITY ENGINEER · CLOUD SECURITY ANALYST · DEVSECOPS ENGINEER · SECURITY ARCHITECT · COMPLIANCE ENGINEER

CALL US
+91 73051 33996

EMAIL US
apply@kaizeninfinities.com

VISIT OUR WEBSITE
www.kaizeninfinities.com