BOOST
THE LEADING TRAINING PROVIDER

Information Technology

Cloud Security Engineer Course

Course Introduction

The **Cloud Security Engineer Course** is a hands-on program designed to provide cybersecurity professionals with the tools, frameworks, and technical expertise needed to design and secure cloud environments. As organizations shift to hybrid and multi-cloud infrastructures, understanding cloud-specific risks, shared responsibility models, and security architectures is critical. This course equips learners to confidently assess cloud vulnerabilities, implement strong security controls, and ensure compliance across major cloud platforms such as AWS, Microsoft Azure, and Google Cloud.

Participants will gain in-depth exposure to identity and access management, cloud architecture best practices, data protection, incident response, and compliance within cloud ecosystems—all through practical labs and real-world scenarios.

Target Audience

- Cloud Security Engineers
- Cloud Architects and Solution Designers
- IT Security Professionals and Analysts
- DevSecOps and Infrastructure Engineers
- Network Security Engineers
- Professionals transitioning to cloud-based roles

Learning Objectives

- Understand cloud computing concepts, deployment models, and the shared responsibility model
- Design secure cloud architectures for IaaS, PaaS, and SaaS environments
- Implement robust identity and access management strategies in the cloud

- Secure cloud storage, databases, and workloads against internal and external threats
- Detect, respond to, and recover from cloud-specific incidents and breaches
- Apply compliance and governance best practices across multi-cloud environments
- Utilize security tools and dashboards native to AWS, Azure, and GCP

Course Outline

- **DAY 01**

  Cloud Fundamentals and Architecture Security

  - Cloud service and deployment models (IaaS, PaaS, SaaS, Public, Private, Hybrid)
  - Shared responsibility model across platforms
  - Understanding cloud attack surfaces and threats
  - Cloud reference architectures
  - Secure cloud design principles

- **Day 02**

  Identity, Access, and Infrastructure Security

  - Identity and Access Management (IAM) fundamentals
  - Role-based access control (RBAC) and policy enforcement
  - Network segmentation and security groups
  - Hardening virtual machines and containers
  - Secure CI/CD pipelines and DevSecOps integration

- **Day 03**

  Cloud Data Security and Application Security

  - Data lifecycle in the cloud and encryption mechanisms
  - Key Management Services (KMS) across cloud providers
  - Cloud database security best practices
  - API security and web application firewalls (WAFs)
  - Secure software development in the cloud

- **Day 04**

  Cloud Threat Detection, Response, and Incident Handling

  - Monitoring and logging cloud activities (CloudTrail, CloudWatch, Azure Monitor)
  - Security Information and Event Management (SIEM) integration
  - Cloud incident response planning and playbooks
  - Common cloud attacks and containment techniques
  - Recovery and business continuity in the cloud

- **Day 05**

  Compliance, Risk Management, and Hands-On Labs

  - Compliance standards (ISO 27017/27018, CSA, NIST, GDPR, HIPAA)
  - Cloud Governance, Risk, and Compliance (GRC)
  - Third-party and vendor risk in cloud environments
  - Hands-on labs: Secure configuration, access policies, and encryption setup

Confirmed Sessions

FROM	TO	DURATION	FEES	LOCATION
July 14, 2025	July 18, 2025	5 days	4250.00 $	UAE - Dubai
Dec. 7, 2025	Dec. 11, 2025	5 days	4250.00 $	KSA - Riyadh