# Google Cloud Security Engineer Course

**Course Duration: 40 Hours** **Course code: GCSE**

## 1. Course Overview

This course provides a comprehensive understanding of security practices and tools in Google Cloud Platform (GCP). It focuses on designing, implementing, and managing secure infrastructure, protecting data, managing identities, and ensuring compliance using Google Cloud security services.

## 2. What you'll learn?

**By the end of the course, you will be able to:**

- Understand Google Cloud security architecture and shared responsibility model
- Implement Identity and Access Management (IAM) policies
- Secure networks, workloads, and applications in GCP
- Protect sensitive data using encryption and key management
- Monitor, detect, and respond to security threats
- Ensure compliance and governance using GCP tools
- Implement best practices for cloud security

## 3. Target Audience

**This course is ideal for:**

- Cloud Security Engineers
- GCP Administrators and Architects
- DevOps Engineers
- Cybersecurity Professionals
- IT Professionals transitioning to cloud security

## 4. Pre-Requisites

Before taking this course, you should have:

- Basic knowledge of cloud computing concepts
- Familiarity with Google Cloud Platform
- Understanding of networking and security fundamentals
- Experience with Linux command line (recommended)

## 5. Course content

Module 1: Course Introduction

- Course overview and objectives
- Introduction to Google Cloud security
- Cloud security fundamentals

Module 2: Google Cloud Security Fundamentals

- Shared responsibility model
- Defense-in-depth strategy
- Security best practices in GCP
- Global infrastructure security

Module 3: Identity and Access Management (IAM)

- IAM roles and permissions
- Service accounts and policies
- IAM best practices
- Organization policies

Module 4: Resource Hierarchy and Access Control

- Organization, folders, and projects
- Policy inheritance
- Access control strategies
- Least privilege principle

Module 5: Network Security in GCP

- Virtual Private Cloud (VPC) security
- Firewall rules and policies
- Private Google Access
- VPC Service Controls

Module 6: Securing Compute Resources

- Securing Compute Engine instances
- Shielded VMs
- OS Login and metadata security
- Patch management

Module 7: Securing Kubernetes and Containers

- Google Kubernetes Engine (GKE) security
- Workload Identity
- Binary Authorization
- Container security best practices

Module 8: Data Protection and Encryption

- Encryption at rest and in transit
- Customer-managed encryption keys (CMEK)
- Cloud Key Management Service (KMS)
- Secrets management

Module 9: Security Monitoring and Logging

- Cloud Logging and Monitoring
- Cloud Audit Logs
- Security Command Center (SCC)
- Threat detection and alerting

Module 10: Identity-Aware Proxy and Access Security

- Identity-Aware Proxy (IAP)
- Context-aware access
- Secure remote access
- Zero Trust model

Module 11: Application Security in GCP

- Securing APIs and endpoints
- Web security best practices
- Cloud Armor (DDoS protection)
- API Gateway security

Module 12: Incident Response and Threat Management

- Incident response lifecycle
- Threat detection and mitigation
- Forensics and investigation
- Automated response strategies

Module 13: Compliance and Governance

- Regulatory compliance (ISO, GDPR, etc.)
- Security policies and governance
- Risk management
- Audit readiness

Module 14: DevSecOps and Automation

- Security in CI/CD pipelines
- Infrastructure as Code (IaC) security
- Policy automation

- Continuous security validation

Module 15: Best Practices and Security Optimization

- Cost vs security balance
- Performance and security trade-offs
- Real-world security architectures
- Common misconfigurations and fixes

Module 16: Final Project / Case Study

- Secure GCP environment setup
- End-to-end security implementation
- Real-world scenario execution
- Evaluation and feedback