Google Cloud Security Engineer Advance

Course Duration: 72 Hours **Course code: GCSEA**

1. Course Overview

During this Seven-day advanced course, learners focus on designing, implementing, and managing secure infrastructure on Google Cloud Platform (GCP). The course covers advanced security practices including identity and access management, network security, data protection, threat detection, and compliance. Learners will gain hands-on experience with tools like Cloud IAM, Security Command Center, VPC Service Controls, Cloud Armor, and Chronicle to secure cloud environments against modern threats.

2. What you'll learn?

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

- Design secure Google Cloud architectures using best practices
- Implement advanced IAM policies and access controls
- Secure networks using VPC, firewalls, and private connectivity
- Protect sensitive data using encryption and key management services
- Configure Security Command Center for threat detection
- Implement VPC Service Controls for data exfiltration prevention
- Use Cloud Armor for application security and DDoS protection
- Monitor, log, and respond to security incidents
- Ensure compliance with security standards and frameworks
- Automate security operations using GCP tools

3. Target Audience

Cloud security engineers, security analysts, DevSecOps engineers, system administrators, cloud architects, and professionals preparing for Google Cloud

Security certifications.

4. Pre-Requisites

Before taking this course, you should have:

- Basic understanding of Google Cloud Platform
- Knowledge of networking concepts (VPC, subnets, firewalls)
- Familiarity with Linux systems and cloud environments
- Understanding of security fundamentals (encryption, IAM, etc.)

5. Course content

Module 1: Course Introduction

- Introduction and course logistics
- Course objectives and roadmap
- Overview of cloud security principles

Module 2: Google Cloud Security Fundamentals Review

- Shared responsibility model
- GCP resource hierarchy and security
- Security best practices overview
- Identity fundamentals

Module 3: Advanced Identity and Access Management (IAM)

- IAM roles and policies deep dive
- Custom roles and least privilege design
- Service accounts and workload identity
- Organization policies and access boundaries

Module 4: Network Security in GCP

- VPC design for security

- Firewall rules and hierarchical firewall policies
- Private Google Access and Private Service Connect
- Secure hybrid connectivity (VPN, Interconnect)

Module 5: Data Protection and Encryption

- Encryption at rest and in transit
- Cloud Key Management Service (KMS)
- Customer-managed and customer-supplied encryption keys
- Secret Manager implementation

Module 6: Application Security and Web Protection

- Securing applications in GCP
- Cloud Armor (WAF and DDoS protection)
- Identity-Aware Proxy (IAP)
- Secure API management

Module 7: VPC Service Controls and Data Exfiltration Prevention

- Introduction to VPC Service Controls
- Service perimeters design
- Access levels and policies
- Real-world implementation scenarios

Module 8: Security Command Center (SCC)

- Overview of SCC
- Asset inventory and vulnerability scanning
- Threat detection and risk analysis
- Security health monitoring

Module 9: Logging, Monitoring, and Incident Response

- Cloud Logging and Cloud Monitoring

- Security event analysis
- Alerting and incident response strategies
- Forensics basics

Module 10: Threat Detection and Intelligence

- Introduction to Chronicle (SIEM)
- Threat intelligence integration
- Detecting anomalies and threats
- Security analytics

Module 11: DevSecOps and Security Automation

- Integrating security into CI/CD pipelines
- Using Cloud Build securely
- Infrastructure as Code (IaC) security
- Policy automation and validation

Module 12: Compliance and Governance

- Compliance frameworks (ISO, GDPR, etc.)
- Risk management strategies
- Auditing and reporting
- Governance best practices

Module 13: Advanced Security Architectures

- Zero Trust architecture in GCP
- Multi-layered security design
- Secure multi-cloud strategies
- High availability and disaster recovery security

Module 14: Security Best Practices and Optimization

- Cost vs security optimization

- Security benchmarking
- Common misconfigurations and fixes
- Continuous security improvement

Module 15: Capstone Project and Real-World Scenarios

- End-to-end secure architecture design
- Hands-on implementation project
- Incident response simulation
- Course summary and certification guidance