Google Cloud Cyber Security Engineer Course

Course Duration: 80 Hours **Course code: GCCSE**

1. Course Overview

This eight-day course focuses on securing cloud infrastructure, applications, and data on Google Cloud Platform (GCP). It provides hands-on experience with security tools and services such as IAM, VPC Service Controls, Cloud Armor, Security Command Center, and Chronicle. Learners will gain the skills required to design, implement, and manage secure cloud environments while ensuring compliance and protection against modern cyber threats.

2. What you'll learn?

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

- Understand cloud security principles and shared responsibility model
- Implement identity and access management (IAM) in GCP
- Secure networks, applications, and data in cloud environments
- Detect, monitor, and respond to security threats
- Use GCP security tools like Security Command Center and Cloud Armor
- Implement encryption and key management
- Ensure compliance and governance in cloud environments
- Perform security assessments and vulnerability management

3. Target Audience

- Cybersecurity professionals
- Cloud security engineers and architects
- DevSecOps engineers
- IT administrators managing cloud environments

4. Pre-Requisites

Before taking this course, you should have:

- Basic knowledge of cloud computing concepts
- Understanding of networking fundamentals
- Familiarity with Linux and system administration
- Basic understanding of cybersecurity concepts

5. Course content

Module 1: Course Introduction

- Introduction and course logistics
- Overview of cloud security in GCP
- Course objectives and lab setup

Module 2: Cloud Security Fundamentals

- Security in cloud computing
- Shared responsibility model
- Threat landscape and attack vectors
- Security best practices

Module 3: Identity and Access Management (IAM)

- IAM roles and permissions
- Service accounts and authentication
- Managing identities securely
- Implementing least privilege access

Module 4: Network Security in GCP

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

Module 5: Data Security and Encryption

- Data protection strategies
- Encryption at rest and in transit
- Cloud Key Management Service (KMS)
- Secrets management

Module 6: Application Security

- Securing cloud-native applications
- Identity-aware proxy (IAP)
- API security practices
- Protecting web applications with Cloud Armor

Module 7: Security Monitoring and Logging

- Cloud Logging and Monitoring
- Security Command Center overview
- Detecting threats and anomalies
- Setting up alerts and dashboards

Module 8: Threat Detection and Incident Response

- Identifying security incidents
- Using Chronicle for threat intelligence
- Incident response lifecycle
- Automating responses

Module 9: Vulnerability Management

- Vulnerability scanning tools
- Managing and patching vulnerabilities
- Container and VM security scanning
- Risk assessment

Module 10: Compliance and Governance

- Security policies and frameworks
- Compliance standards (ISO, GDPR, etc.)
- Auditing and reporting
- Governance best practices

Module 11: DevSecOps and Automation

- Integrating security into CI/CD pipelines
- Automating security checks
- Infrastructure as Code (IaC) security
- Continuous security monitoring

Module 12: Securing Containers and Kubernetes

- Security in GKE (Google Kubernetes Engine)
- Container image security
- Runtime protection
- Access control in Kubernetes

Module 13: Backup, Recovery, and Resilience

- Backup strategies in GCP
- Disaster recovery planning
- High availability and fault tolerance
- Business continuity planning

Module 14: Advanced Security Tools and Best Practices

- Advanced threat protection tools
- Security automation frameworks
- Zero Trust architecture
- Security optimization techniques

Module 15: Capstone Project and Real-World Scenarios

- Designing a secure GCP environment
- Implementing security controls
- Monitoring and responding to threats
- Final project and assessment

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com