Google Cloud DevSecOps Engineer Course

Course Duration: 40 Hours **Course code: GCDE**

1. Course Overview

This course focuses on integrating security practices into DevOps workflows on Google Cloud Platform (GCP). It equips learners with the skills to build secure CI/CD pipelines, implement automated security controls, and manage risks across the software development lifecycle (SDLC). The course emphasizes DevSecOps principles, cloud security, compliance, and continuous monitoring.

2. What you'll learn?

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

- Understand DevSecOps principles and secure SDLC practices
- Implement security in CI/CD pipelines using Google Cloud tools
- Manage identity, access, and secrets securely
- Perform vulnerability assessment and threat detection
- Secure containerized and Kubernetes-based applications
- Automate security testing and compliance checks
- Monitor, log, and respond to security incidents
- Apply governance, risk, and compliance (GRC) frameworks

3. Target Audience

- DevOps Engineers
- Security Engineers
- Cloud Engineers and Architects
- Site Reliability Engineers (SREs)
- Developers working with CI/CD pipelines

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

4. Pre-Requisites

Before taking this course, you should have:

- Basic understanding of Google Cloud Platform (GCP)
- Knowledge of DevOps practices and CI/CD
- Familiarity with Linux and networking
- Basic understanding of security concepts

5. Course content

Module 1: Course Introduction

- Course overview and objectives
- Introduction to DevSecOps
- Importance of security in DevOps

Module 2: DevSecOps Fundamentals

- DevSecOps lifecycle
- Secure software development lifecycle (SDLC)
- Shift-left security approach
- DevSecOps culture and practices

Module 3: Google Cloud Security Overview

- Shared responsibility model
- Security architecture in GCP
- Security best practices
- Identity and access fundamentals

Module 4: Identity and Access Management (IAM)

- IAM roles and permissions
- Service accounts and authentication
- Principle of least privilege
- Access control strategies

Module 5: Secure CI/CD Pipelines

- Introduction to Cloud Build and Cloud Deploy
- Integrating security into CI/CD
- Automated testing and validation
- Secure artifact management

Module 6: Secrets Management and Data Protection

- Managing secrets with Secret Manager
- Data encryption (at rest and in transit)
- Key Management Service (KMS)
- Secure configuration practices

Module 7: Container Security

- Securing Docker containers
- Container vulnerability scanning
- Image hardening
- Secure container registries

Module 8: Kubernetes Security (GKE)

- Securing Kubernetes clusters
- Role-based access control (RBAC)
- Network policies
- Workload security

Module 9: Application Security Testing

- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Dependency scanning
- Integrating testing into pipelines

Module 10: Monitoring, Logging, and Threat Detection

- Cloud Monitoring and Logging
- Security Command Center (SCC)
- Threat detection and alerting
- Incident response strategies

Module 11: Compliance and Governance

- Compliance frameworks (ISO, GDPR, etc.)
- Policy enforcement
- Auditing and reporting
- Governance best practices

Module 12: Infrastructure Security

- Securing VPC and networking
- Firewall rules and segmentation
- Identity-Aware Proxy (IAP)
- Zero Trust architecture

Module 13: Automation and Security Orchestration

- Automating security tasks
- Event-driven security workflows
- Integration with APIs
- Security orchestration tools

Module 14: Risk Management and Incident Response

- Risk assessment techniques
- Incident response lifecycle
- Root cause analysis
- Post-incident review

Module 15: Real-World Use Cases and Capstone Project

- Implementing secure DevOps pipelines
- Enterprise security scenarios
- Best practices and architecture design
- Final project and evaluation

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