Day 1: Introduction to DevSecOps and GCP Security Foundation

1.1 Introduction to DevSecOps

- What is DevSecOps?
- The DevSecOps lifecycle: Integrating security from development to production.
- Benefits of shifting security left.
- Overview of GCP services relevant to DevSecOps.

1.2 GCP Security Services Overview

- Key GCP security services: IAM, Cloud Security Command Center, Cloud Armor, KMS.
- Introduction to Google Cloud Operations (formerly Stackdriver) for monitoring and logging.
- GitHub - Authentications and Security needs
- Keeping Passwords off the code
- Handling Secrets with Secret Managers

1.3 IAM (Identity and Access Management) in GCP

- Overview of GCP IAM: Managing access to resources.
- Best practices for role-based access control (RBAC).
- Service accounts and least privilege.
- Access controls based on ACLs for storage like BQ, GCS, Cloud SQL etc.
- Provide fine grained permissions on service accounts/group users

1.4 Hands-on Lab: IAM and Service Account Setup

- Setting up users, roles, and permissions.
- Managing service accounts for secure automated deployments.

Outcome:

Participants will gain an understanding of DevSecOps, GCP's core security services, and practical knowledge of IAM for access management.

Day 2: Securing GCP Infrastructure and Network

2.1 Securing GCP Network Architecture

- Configuring Virtual Private Cloud (VPC) and subnets.
- Implementing firewalls, private networks, and routing.
- Best practices for securing external and internal traffic.

- Details on DNS and subnets

2.2 Encryption and Storage Security on GCP

- Encryption at rest and in transit.
- Managing encryption keys with Cloud Key Management Service (KMS).
- Securing Cloud Storage, BigQuery, and other data services.
- CMEK, CSEK encryption types and handling PII data
- Best practices for encryption of data in transition

Eg – a. Downstream system fetching data from GCP BQ using service account

b. Sending file via sftp from GCS to Other server/cloud

2.3 Hands-on Lab: Securing a GCP Network

- Creating a VPC, setting up firewall rules, and securing internal communications.
- Implementing encryption at rest for Cloud Storage.

Outcome:

Participants will understand how to secure GCP's network infrastructure, including firewalls, encryption, and private networks, with hands-on experience in securing a VPC.

Day 3: DevSecOps CI/CD Pipeline on GCP

3.1 Building Secure CI/CD Pipelines

- Overview of CI/CD on GCP using Cloud Build.
- Incorporating security checks in CI/CD pipelines.
- Static analysis and vulnerability scanning (e.g., using SonarQube).
- Basics concepts of CICD and use case
- Considering Github as a repository how to setup a CICD pipeline in GCP (With code authentication and approvals)

3.2 Container Security with Google Kubernetes Engine (GKE)

- Building secure container images.
- Using Container Registry for vulnerability scanning.

- Best practices for container security and management in GKE.

3.3 Hands-on Lab: Secure CI/CD Pipeline Setup

- Build a CI/CD pipeline in Cloud Build.
- Integrate security checks and vulnerability scans.
- Deploy a secure application to GKE with vulnerability scans.

Outcome:

By the end of Day 3, participants will know how to build secure CI/CD pipelines with integrated security checks and will have hands-on experience deploying secure applications on GKE.

Day 4: Advanced Security in GCP

4.1 Securing Kubernetes Workloads in GKE

- Role-Based Access Control (RBAC) in GKE.
- Implementing Network Policies to secure pod communications.
- Using Workload Identity for secure interaction between services.
- Load balancing in GKE for VMs
- Performance tuning of VMs

4.2 Infrastructure as Code (IaC) Security

- Using Terraform and Google Deployment Manager to manage secure infrastructure.
- Best practices for securing IaC (e.g., version control, audit trails).
- Continuous compliance and security guardrails in IaC.
- Basics of terraform

4.3 Hands-on Lab: Secure Kubernetes Workloads

- Configuring RBAC for a Kubernetes cluster.
- Implementing network policies to restrict pod communications.

Outcome:

Participants will be able to secure Kubernetes workloads on GKE and understand how to secure infrastructure as code using Terraform or Google Deployment Manager.

Day 5: Monitoring, Incident Response, and Compliance in GCP

5.1 Monitoring and Logging for Security

- Centralized logging and monitoring with Google Cloud Operations (formerly Stackdriver).
- Setting up alerts for security incidents.
- Automated responses to security threats.
- Log router usage in monitoring
- Effective logging mechanism for Users and Service Accounts
- Monitoring based on the Query size per user/SA
- How to effectively use Cloud to save cost and better efficiency of resources.

5.2 Incident Response and Auditing

- Using Security Command Center for threat detection and remediation.
- Incident response best practices on GCP.
- Audit logging and compliance for ISO, PCI DSS, HIPAA.

5.3 Hands-on Lab: Security Monitoring and Incident Response

- Setting up Cloud Operations for logging and monitoring.
- Using Security Command Center for automated security alerts and responses.