Google Cloud DevSecOps Engineer

Course Overview

A DevSecOps develops, implements, and monitors their organization's security infrastructure to protect sensitive information. This learning path guides you through a curated collection of concepts and labs that provide you with real-world, hands-on experience using Google Cloud technologies essential to the DevSecOps Engineer role.

Duration: 05 days / 40 hours

Level: Professional

Prerequisites: There is no prerequisite for this learning path. Basic knowledge of Linux and Network administration is helpful but not mandatory.

Course Outcome: Learner will be prepared to work as a DevSecOps Engineer on Google Cloud Platform

Table of Content

Google Cloud Fundamentals: Core Infrastructure

- Introducing Google Cloud
- Resources and Access in the Cloud
- Virtual Machines and Networks in the Cloud
- Storage in the Cloud
- Containers in the Cloud
- Applications in the Cloud
- Prompt Engineering

Architecting with Google Kubernetes Engine: Foundations

- Introduction to Containers and Kubernetes
- Kubernetes Architecture

Architecting with Google Kubernetes Engine: Workloads

- Workloads: Deployments and Jobs
- Google Kubernetes Engine Networking
- Persistent Data and Storage

Architecting with Google Kubernetes Engine: Production

- Access Control and Security in Kubernetes and Google Kubernetes Engine
- Google Kubernetes Engine Logging and Monitoring
- Using Google Cloud Managed Storage Services with Google Kubernetes Engine

- Using CI/CD with Google Kubernetes Engine

Managing Security in Google Cloud

- Foundations of Google Cloud Security
- Securing Access to Google Cloud
- Identity and Access Management (IAM)
- Configuring Virtual Private Cloud for Isolation and Security

Security Best Practices in Google Cloud

- Welcome to Security Best Practices in Google Cloud
- Securing Compute Engine: Techniques and Best Practices
- Securing Cloud Data: Techniques and Best Practices
- Application Security: Techniques and Best Practices
- Securing Google Kubernetes Engine: Techniques and Best Practices

Mitigating Security Vulnerabilities on Google Cloud

- Protecting against Distributed Denial of Service Attacks (DDoS)
- Content-Related Vulnerabilities: Techniques and Best Practices
- Monitoring, Logging, Auditing and Scanning

Getting Started with Terraform for Google Cloud

- Introduction to Terraform for Google Cloud
- Terms and Concepts
- Writing Infrastructure Code for Google Cloud
- Organizing and Reusing Configuration with Terraform Modules
- Introduction to Terraform State