Google Cloud Security Engineer Advance

Course Overview

A Security Engineer 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 Security Engineer role.

Duration: 09 days / 72 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 can take **Google Cloud Certified Professional Cloud Security Engineer** exam

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

Networking in Google Cloud: Fundamentals

- Welcome to Networking in Google Cloud
- VPC Networking Fundamentals
- Sharing VPC Networks
- Network Monitoring and Logging

Networking in Google Cloud: Routing and Addressing

- Welcome to Networking in Google Cloud
- Network Routing and Addressing in Google Cloud
- Private Connection Options

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

Security Practices with Google Security Operations SIEM

- Foundations of Chronicle
- Collecting and Parsing Data
- Access Management
- Building Rules to Find Threats
- Investigating Threats
- Responding to Threats

SOAR Fundamentals

- Intro and Architecture
- Chronicle SOAR Fundamentals
- Platform Overview
- Case Management
- User and Environment Management
- Integrations: Connectors and Ontology
- Playbooks Views
- Settings
- Dashboards Reports
- IDE
- Collaborator
- Incident Manager

Secure Software Delivery

- Gating Deployments with Binary Authorization
- Secure Builds with Cloud Build
- Securing Container Builds

Google Cloud Security for the Public Sector

- Cloud-first, Zero Trust Cybersecurity with Google Cloud
- BeyondCorp and reCAPTCHA
- CyberSecurity with Chronicle, CrowdStrike, and Palo Alto Networks