GCPManSec

Managing Security in Google Cloud

college@sela.co.il 03-6176666

Managing Security in Google Cloud

GCPManSec - Version: 1

5 days Course

Description:

This self-paced training course gives participants broad study of security controls and techniques on Google Cloud. Through recorded lectures, demonstrations, and hands-on labs, participants explore and deploy the components of a secure Google Cloud solution, including Cloud Identity, Resource Manager, Cloud IAM, Virtual Private Cloud firewalls, Cloud Load Balancing, Cloud Peering, Cloud Interconnect, and VPC Service Controls.

This is the first course of the Security in Google Cloud series. After completing this course, enroll in the Security Best Practices in Google Cloud course.

Intended audience:

[Cloud] information security analysts, architects, and engineers. Information security/cybersecurity specialists. Cloud infrastructure architects. Also intended for Google and partner field personnel who work with customers in those job roles. Also useful for cloud application developers.

Prerequisites:

Prior completion of Google Cloud Fundamentals: Core Infrastructure or equivalent experience. Prior completion of Networking in Google Cloud or equivalent experience. Knowledge of foundational concepts in information security: Fundamental concepts: vulnerability, threat, attack surface confidentiality, integrity, availability, Common threat

types and their mitigation strategies, Public-key cryptography, Public and private key pairs, Certificates Cipher types, Key width Certificate authorities, Transport Layer Security/Secure Sockets, Layer encrypted communication Public key infrastructures Security policy. Basic proficiency with command-line tools and Linux operating system environments. Systems Operations experience, including deploying and managing applications, either on-premises or in a public cloud environment. Reading comprehension of code in Python or JavaScript.

Objectives:

Understand the Google approach to security
Manage administrative identities using Cloud Identity
Implement IP traffic controls using VPC firewalls and Google Cloud Armor

Topics:

º Welcome to Managing Security in Google Cloud

Foundations of Google Cloud Security

- Module overview
- Google Cloud's approach to security
- VPC network security and monitoring
- The shared security responsibility model
- Threats mitigated by Google and Google Cloud
- Access transparency
- Module review3

Securing Access to Google Cloud

- Module overview
- Cloud Identity
- Google Cloud Directory Sync
- Managed Microsoft AD
- Google authentication versus SAML-based SSO
- Identity Platform
- Authentication best practices
- Demo Intro: Defining Users with Cloud Identity Console
- Lab Demo: Defining Users with Cloud Identity Console3
- Module review

Identity and Access Management (IAM)

- Module overview
- Resource Manager
- IAM roles
- Service accounts
- IAM & Organization policies
- Workload Identity Federation
- Policy Intelligence
- IAM best practices
- Lab Intro: Configuring IAM
- Getting Started with Google Cloud and Qwiklabs
- Module review

Configuring Virtual Private Cloud for Isolation and Security

- Module overview44s
- VPC firewall rules5m
- VPC firewall defaults6m

- VPC firewall best practices5m
- Lab Intro: Configuring VPC Firewalls22s
- Load balancing and SSL policies2m
- VPC peering
- Connecting to Google Cloud
- Cloud Interconnect
- VPC Service Controls
- Demo - VPC Service Controls
- Private Google API access
- Access Context Manager
- VPC Flow Logs1m
- Lab Intro: Configuring and Using VPC Flow Logs in Cloud Logging
- Cloud IDS
- Lab Intro: Getting Started with Cloud IDS
- Module review