
Security in Google Cloud Platform

Duration: 2 Days Course Code: GO5977

Overview:

This course gives participants broad study of security controls and techniques on Google Cloud. Through lectures, demonstrations, and hands-on labs, participants explore and deploy the components of a secure GCP solution. Participants also learn mitigation techniques for attacks at many points in a GCP-based infrastructure, including Distributed Denial-of-Service attacks, phishing attacks, and threats involving content classification and use.

Target Audience:

This class is intended for the following job roles:

- ? Cloud information security analysts, architects, and engineers
 - ? Information security/cybersecurity specialists
 - ? Cloud infrastructure architects
 - ? Developers of cloud applications
-

Objectives:

- | | |
|--|---|
| ■ This course teaches participants the following skills: | ■ ? Implementing Identity Aware Proxy |
| ■ ? Understanding the Google approach to security | ■ ? Analyzing changes to the configuration or metadata of resources with GCP audit logs |
| ■ ? Managing administrative identities using Cloud Identity. | ■ ? Scanning for and redact sensitive data with the Data Loss Prevention API |
| ■ ? Implementing least privilege administrative access using Google Cloud Resource Manager, Cloud IAM. | ■ ? Scanning a GCP deployment with Forseti |
| ■ ? Implementing IP traffic controls using VPC firewalls and Cloud Armor | ■ ? Remediating important types of vulnerabilities, especially in public access to data and VMs |
-

Prerequisites:

To get the most out of this course, participants should have:

? Prior completion of Google Cloud Platform Fundamentals: Core Infrastructure or equivalent experience

? Prior completion of Networking in Google Cloud Platform 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
-

Content:

Module 1 Foundations of GCP Security	PART II: SECURITY BEST PRACTICES ON GOOGLE CLOUD	? Lab: Using Cloud Security Scanner to find vulnerabilities in an App Engine application
? Understand the GCP shared security responsibility model	Module 5 Securing Compute Engine: techniques and best practices	? Identity Aware Proxy
? Understand Google Cloud's approach to security	? Compute Engine service accounts, default and customer-defined	? Lab: Configuring Identity Aware Proxy to protect a project
? Understand the kinds of threats mitigated by Google and by GCP	? IAM roles for VMs	Module 8 Securing Kubernetes: techniques and best practices
? Define and Understand Access Transparency and Access Approval (beta)	? API scopes for VMs	? Authorization
Module 2 Cloud Identity	? Managing SSH keys for Linux VMs	? Securing Workloads
? Cloud Identity	? Managing RDP logins for Windows VMs	? Securing Clusters
? Syncing with Microsoft Active Directory using Google Cloud Directory Sync	? Organization policy controls: trusted images, public IP address, disabling serial port	? Logging and Monitoring
? Using Managed Service for Microsoft Active Directory (beta)	? Encrypting VM images with customer-managed encryption keys and with customer-supplied encryption keys	PART III: MITIGATING VULNERABILITIES IN GOOGLE CLOUD
? Choosing between Google authentication and SAML-based SSO	? Finding and remediating public access to VMs	Module 9 Protecting against Distributed Denial of Service Attacks
? Best practices, including DNS configuration, super admin accounts	? Best practices, including using hardened custom images, custom service accounts (not the default service account),	? How DDoS attacks work
? Lab: Defining Users with Cloud Identity Console	tailored API scopes, and the use of application default credentials instead of user-managed keys	? Mitigations: GCLB, Cloud CDN, autoscaling, VPC ingress and egress firewalls, Cloud Armor (including its rules language)
Module 3 Identity, Access, and Key Management	? Lab: Configuring, using, and auditing VM service accounts and scopes	? Types of complementary partner products
? GCP Resource Manager: projects, folders, and organizations	? Encrypting VM disks with customer-supplied encryption keys	? Lab: Configuring GCLB, CDN, traffic blacklisting with Cloud Armor
? GCP IAM roles, including custom roles	? Lab: Encrypting disks with customer-supplied encryption keys	Module 10 Protecting against content-related vulnerabilities
? GCP IAM policies, including organization policies	? Using Shielded VMs to maintain the integrity of virtual machines	? Threat: Ransomware
? GCP IAM Labels		? Mitigations: Backups, IAM, Data Loss Prevention API
		? Threats: Data misuse, privacy violations, sensitive/restricted/unacceptable content

? GCP IAM Recommender	Module 6 Securing cloud data: techniques and best practices	? Threat: Identity and Oauth phishing
? GCP IAM Troubleshooter		
? GCP IAM Audit Logs	? Cloud Storage and IAM permissions	? Mitigations: Classifying content using Cloud ML APIs; scanning and redacting data using Data Loss Prevention API
? Best practices, including separation of duties and least privilege, the use of Google groups in policies, and avoiding the use of primitive roles	? Cloud Storage and ACLs	? Lab: Redacting Sensitive Data with Data Loss Prevention API
? Labs: Configuring Cloud IAM, including custom roles and organization policies	? Auditing cloud data, including finding and remediating publicly accessible data	Module 11 Monitoring, Logging, Auditing, and Scanning
Module 4 Configuring Google Virtual Private Cloud for Isolation and Security	? Signed Cloud Storage URLs	? Security Command Center
? Configuring VPC firewalls (both ingress and egress rules)	? Signed policy documents	? Stackdriver monitoring and logging
? Load balancing and SSL policies	? Encrypting Cloud Storage objects with customer-managed encryption keys and with customer-supplied encryption keys	? Lab: Installing Stackdriver agents
? Private Google API access	? Best practices, including deleting archived versions of objects after key rotation	? Lab: Configuring and using Stackdriver monitoring and logging
? SSL proxy use	? Lab: Using customer-supplied encryption keys with Cloud Storage	? VPC flow logs
? Best practices for VPC networks, including peering and shared VPC use, correct use of subnetworks	? Lab: Using customer-managed encryption keys with Cloud Storage and Cloud KMS	? Lab: Viewing and using VPC flow logs in Stackdriver
? Best security practices for VPNs	? BigQuery authorized views	? Cloud audit logging
? Security considerations for interconnect and peering options	? BigQuery IAM roles	? Lab: Configuring and viewing audit logs in Stackdriver
? Available security products from partners	? Best practices, including preferring IAM permissions over ACLs	? Deploying and Using Forseti
? Defining a service perimeter, including perimeter bridges	? Lab: Creating a BigQuery authorized view	? Lab: Inventorying a Deployment with Forseti Inventory (demo)
? Setting up private connectivity to Google APIs and services	Module 7 Securing Applications: techniques and best practices	? Lab: Scanning a Deployment with Forseti Scanner (demo)
? Lab: Configuring VPC firewalls	? Types of application security vulnerabilities	
	? DoS protections in App Engine and Cloud Functions	
	? Cloud Security Scanner	

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/