



Security in Google Cloud

Duration: 2 Days **Course Code: GO5977** **Delivery Method: Virtual Learning**

Overview:

Through lectures, demonstrations and hands-on labs, participants explore and implement the components of a safe GCP solution. Participants also learn attack mitigation techniques at many points in a GCP-based infrastructure, including distributed denial of service attacks, phishing attacks, and threats related to content classification and use.

Virtual Learning:

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Target Audience:

This class is intended for the following: Cloud Information Security Analysts, Architects and Engineers
Information Security and Cybersecurity Specialists
Cloud Infrastructure Architects
Cloud Application Developers

Objectives:

- This course teaches participants the following skills:
 - Understanding of Google's approach to security
 - Administrative identity management through Cloud Identity.
 - Implementation of administrative access with minimum privileges using Google Cloud Resource Manager, Cloud IAM.
 - Implementation of IP traffic controls using VPC firewalls and Cloud Armor
 - Identity Aware Proxy Implementation
 - Analysis of configuration changes or resource metadata with GC audit trails
 - Scanning and writing sensitive data with the Data Loss Prevention API
 - Scanning a GC implementation with Forseti
 - Remediate important types of vulnerabilities, especially in public access to data and virtual machines.
-

Prerequisites:

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

- Previous completion of Google Cloud fundamentals: Basic infrastructure or equivalent experience
 - Previous completion of Networking on the Google Cloud or equivalent experience
 - Knowledge of the fundamental concepts of information security: Fundamental concepts: vulnerability, threat, attack surface, confidentiality, integrity, availability
 - Types of common threats and their mitigation strategies, Public Key Cryptography, Public and Private Key Pairs, Certificates, Encryption Types,
 - Key Width, Certification Authorities. Transport Layer Security/Secure Sockets Transport Layer Encryption Communication, Public Key Infrastructures.
 - Security policy: Basic command line tools and Linux operating
-

system environments.

- Experience in system operations, including application deployment and management, either on-premise or in a public cloud environment, understanding of reading code in Python or JavaScript.
-

Content:

PART I: Security Management in the Google Cloud	Best security practices for VPNs	Signed Cloud Storage URLs
Module 1: Fundamentals of GC Safety	Security considerations for interconnection and peering options	Signed policy documents
Google Cloud security approach	Security products available from partners	Encrypting Cloud Storage Objects with Customer-Managed and Customer-Supplied Encryption Keys
The shared responsibility model for security	Module 5: Monitoring, Logging, Auditing and Scanning	Best practices, including deleting archived versions of objects after keystrokes
Threats mitigated by Google and GC	Stacker monitoring and logging	Authorized views of BigQuery
■ Transparency in access	VPC flow records	BigQuery IAM features
Module 2: Identity in the Cloud	Cloud Audit Log	■ Best practices, including preference of IAM permits over ACLs
Identity in the cloud	Deploying and Using Forseti	Module 8: Protection against distributed denial of service attacks: techniques and best practices
Synchronization with Microsoft Active Directory	PART II: Vulnerability Mitigation in the Google Cloud	How DDoS attacks work
Choice between Google and SAML-based SSO authentication	Module 6: Engine protection for computing: techniques and best practices	Mitigation: GCLB, Cloud CDN, Auto Scaling, VPC Input/Output Firewalls, Cloud Armor
GCP best practices	■ Calculate default and customer-defined engine service accounts	■ Types of complementary partner products
Module 3: Identity and Access Management	RIO functions for virtual machines	Module 9: Application Security: Techniques and Best Practices
GCP Resource Manager: projects, folders and organizations	Virtual Machine API Scopes	Types of application security vulnerabilities
GCP IAM features, including custom features	SSH key management for Linux virtual machines	DoS protections in App Engine and Cloud features
GCP IAM policies, including organizational policies	Managing RDP Logins for Windows Virtual Machines	Cloud Security Scanner
GCP IAM Best Practices	Organizational policy controls: trusted images, public IP address, serial port deactivation	Threat: Phishing and Oauth phishing
Module 4: Configuring the Google Virtual Private Cloud for Privacy and Security	Encryption of VM images with customer-managed and customer-supplied encryption keys	■ Identity Recognition Proxy
VPC firewall configuration (entry and exit rules)	Find and remedy public access to virtual machines	Module 10: Content-Related Vulnerabilities: Techniques and Best Practices
Load balancing and SSL policies		Threat: Ransomware
Private access to the Google API		Mitigation: backup API, IAM, data loss prevention

Use of SSL proxy

Best practices for structuring VPC networks

- WV best practices
- Encryption of VM discs with encryption keys provided by the customer

Module 7: Data Protection in the Cloud: Techniques and Best Practices

Cloud storage and AMI permissions

Cloud storage and ACLs

Cloud data auditing, including search and repair of publicly accessible data

Threats: Data misuse, privacy violations, confidential/restricted/unacceptable content

Mitigation: Content classification using Cloud ML APIs; data analysis and writing using Data Loss Prevention APIs

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK