# Security in Google Cloud

## Duration: 2 Days  Course Code: GO5977

### 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.

### 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

Module 1: Fundamentals of GC Safety

Google Cloud security approach

The shared responsibility model for security

Threats mitigated by Google and GC

- Transparency in access

Module 2: Identity in the Cloud

Identity in the cloud

Synchronization with Microsoft Active Directory

Choice between Google and SAML-based SSO authentication

GCP best practices

Module 3: Identity and Access Management

GCP Resource Manager: projects, folders and organizations

GCP IAM features, including custom features

GCP IAM policies, including organizational policies

GCP IAM Best Practices

Module 4: Configuring the Google Virtual Private Cloud for Privacy and Security

VPC firewall configuration (entry and exit rules)

Load balancing and SSL policies

Private access to the Google API

Best security practices for VPNs

Security considerations for interconnection and peering options

Security products available from partners

Module 5: Monitoring, Logging, Auditing and Scanning

Stacker monitoring and logging

VPC flow records

Cloud Audit Log

Deploying and Using Forseti

PART II: Vulnerability Mitigation in the Google Cloud

Module 6: Engine protection for computing: techniques and best practices

- Calculate default and customer-defined engine service accounts

RIO functions for virtual machines

Virtual Machine API Scopes

SSH key management for Linux virtual machines

Managing RDP Logins for Windows Virtual Machines

Organizational policy controls: trusted images, public IP address, serial port deactivation

Encryption of VM images with customer-managed and customer-supplied encryption keys

Find and remedy public access to virtual machines

Signed Cloud Storage URLs

Signed policy documents

Encrypting Cloud Storage Objects with Customer-Managed and Customer-Supplied Encryption Keys

Best practices, including deleting archived versions of objects after keystrokes

Authorized views of BigQuery

BigQuery IAM features

- Best practices, including preference of IAM permits over ACLs

Module 8: Protection against distributed denial of service attacks: techniques and best practices

How DDoS attacks work

Mitigation: GCLB, Cloud CDN, Auto Scaling, VPC Input/Output Firewalls, Cloud Armor

- Types of complementary partner products

Module 9: Application Security: Techniques and Best Practices

Types of application security vulnerabilities

DoS protections in App Engine and Cloud features

Cloud Security Scanner

Threat: Phishing and Oauth phishing

- Identity Recognition Proxy

Module 10: Content-Related Vulnerabilities: Techniques and Best Practices

Threat: Ransomware

Mitigation: backup API, IAM, data loss prevention

| | | |
|---|---|---|
| Use of SSL proxy<br><br>Best practices for structuring VPC networks | ■ WV best practices<br>■ Encryption of VM discs with encryption keys provided by the customer<br><br>Module 7: Data Protection in the Cloud: Techniques and Best Practices<br><br>Cloud storage and AMI permissions<br><br>Cloud storage and ACLs<br><br>Cloud data auditing, including search and repair of publicly accessible data | Threats: Data misuse, privacy violations, confidential/restricted/unacceptable content<br><br>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