Security in Google Cloud

Duration: 2 Days   Course Code: GO5977   Delivery Method: Company Event

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.

Company Events:

These events can be delivered exclusively for your company at one of our training centres or at your own location, specifically for your delegates and your needs. The Company Events can be tailored or standard course deliveries.

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:

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

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: