Security in the Google Cloud Platform Training

Duration: **3 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Overview

This course gives participants a broad study of security controls and techniques on Google Cloud Platform.

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.

Who Should Attend?

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

Prerequisites

In addition to the following classes, Students should possess Knowledge of foundational concepts in information security:

- Fundamental concepts including vulnerability, threat, attack surface, confidentiality, integrity, availability
- Common threat types and their mitigation strategies
- Public-key cryptography
- Public and private key pairs
- 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

Security in the Google Cloud Platform Training

Duration: **3 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

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