Security in Google Cloud Training

Duration: **3 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Overview

The Security in Google Cloud course provides a broad introduction to the security controls, technologies, and techniques used to protect Google Cloud environments.

Through recorded lectures, demonstrations, and hands-on labs, participants will explore the key components involved in designing and deploying a secure Google Cloud solution. The course covers technologies including Cloud Identity, Resource Manager, Identity and Access Management (IAM), Virtual Private Cloud (VPC) firewalls, Cloud Load Balancing, Direct Peering, Carrier Peering, Cloud Interconnect, and VPC Service Controls.

The program covers a wide range of security areas, from identity and access management and network protection to securing Compute Engine, cloud data, applications, and Google Kubernetes Engine environments. Participants will also explore DDoS protection, sensitive data security, monitoring, logging, auditing, and security scanning.

Products and Technologies

Google technologies:

Cloud Identity, Resource Manager, IAM, HSM, Secret Manager, Google Kubernetes Engine, Managed Service for Microsoft Active Directory, Cloud Interconnect, Cloud Storage, Web Security Scanner, Identity-Aware Proxy, VPC Service Controls, Google Cloud's operations suite (formerly Stackdriver), Google Cloud Armor, Compute Engine, and Cloud Data Loss Prevention API.

Third-party technologies:

Forseti Inventory and Forseti Scanner.

Prerequisites

Participants are expected to have:

- Completed Google Cloud Fundamentals: Core Infrastructure or have equivalent experience
- Completed Networking in Google Cloud or have equivalent experience
- A basic understanding of Kubernetes terminology, preferred but not required
- Knowledge of foundational information security concepts through practical experience or training such as SANS SEC301: Introduction to Cyber Security
- Basic proficiency with command-line tools and Linux operating system environments
- Systems Operations experience involving the deployment and management of applications in on-premises or public cloud environments
- The ability to read and understand Python or JavaScript code

Security in Google Cloud Training

Duration: **3 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Who Should Attend

This course is particularly relevant for:

- Cloud information security analysts, architects, and engineers
- Information security and cybersecurity specialists
- Cloud infrastructure architects

What You Will Learn

By the end of the course, participants should be able to:

- Explain Google's approach to security.
- Manage administrative identities with Cloud Identity.
- Apply least privilege administration through Resource Manager and IAM.
- Implement Identity-Aware Proxy.
- Control IP traffic using VPC firewalls and Google Cloud Armor.
- Remediate security vulnerabilities, particularly those involving public access to data and virtual machines.
- Scan and redact sensitive information with the Cloud Data Loss Prevention API.
- Analyze resource metadata configuration changes using audit logs.
- Scan Google Cloud deployments with Forseti and remediate important vulnerabilities, particularly those related to public access to data and VMs.

Outline

Module 1 – Foundations of Google Cloud Security

Topics

- Google Cloud's approach to security
- The Shared Security Responsibility Model
- Threats mitigated by Google and Google Cloud
- Access Transparency

Objectives

Participants will explore Google Cloud's approach to security and the shared security responsibility model. They will examine the types of threats mitigated by Google and Google Cloud and develop an understanding of Access Transparency.

Module 2 – Cloud Identity

Topics

- Cloud Identity
- Google Cloud Directory Sync
- Google Authentication versus SAML-based SSO

BILGINC IT Academy

info@bilginc.com

bilginc.com

- Authentication best practices

Objectives

Participants will learn the purpose and capabilities of Cloud Identity and explore how Directory Sync securely synchronizes users and permissions between an on-premises LDAP or AD server and the cloud.

The module also examines Google Cloud authentication methods, SSO configuration, and best practices for managing groups, permissions, domains, and administrators through Cloud Identity.

Module 3 – Identity and Access Management (IAM)

Topics

- Resource Manager
- IAM Roles
- IAM Policies
- IAM Recommender
- IAM Troubleshooter
- IAM Audit Logs
- IAM best practices

Objectives

Participants will examine Resource Manager concepts, including projects, folders, and organizations. They will learn how to implement IAM roles, including custom roles, and understand IAM and organization policies.

The module also addresses separation of duties, least privilege, the use of Google Groups in policies, avoiding basic roles, and the configuration of custom roles and organization policies.

Activity

- Lab: Configuring IAM

Module 4 – Configuring Virtual Private Cloud for Isolation and Security

Topics

- VPC Firewalls
- Load Balancing and SSL Policies
- Interconnect and Peering Policies
- Best practices for VPC Networks
- VPC Flow Logs

Objectives

Participants will explore best practices for configuring VPC firewall ingress and egress rules. They will examine load balancing, SSL policies, private Google API access, and SSL proxy usage.

The module also covers VPC network best practices, including peering, Shared VPC, subnetworks, VPN security, and security considerations for Interconnect and peering options. Participants will also explore

BILGINC IT Academy

info@bilginc.com

bilginc.com

partner security products, configure VPC firewalls, and examine how VPC Service Controls can help prevent data exfiltration.

Activities

- Lab: Configuring VPC Firewalls
- Lab: Configuring and Using VPC Flow Logs in Cloud Logging

Module 5 – Securing Compute Engine: Techniques and Best Practices

Topics

- Service Accounts, IAM Roles, and API Scopes
- Managing VM Logins
- Organization Policy Controls
- Compute Engine best practices
- Encrypting disks with CSEK

Objectives

Participants will learn about default and customer-defined Compute Engine service accounts, IAM roles and scopes for VMs, and how Shielded VMs help protect system and application integrity.

Activities

- Lab: Configuring, Using, and Auditing VM Service Accounts and Scopes
- Lab: Encrypting Disks with Customer-Supplied Encryption Keys

Module 6 – Securing Cloud Data: Techniques and Best Practices

Topics

- Cloud Storage IAM permissions and ACLs
- Auditing Cloud Data
- Signed URLs and Policy Documents
- Encryption with CMEK and CSEK
- Cloud HSM
- BigQuery IAM Roles and Authorized Views
- Storage best practices

Objectives

Participants will learn how permissions and roles can be used to protect cloud resources and how cloud data can be audited.

The module examines Signed URLs for providing access to Cloud Storage objects, Signed Policy Documents for controlling content placed in buckets, and data encryption using CMEK, CSEK, and Cloud HSM. Protecting BigQuery data with IAM roles and Authorized Views is also covered.

Activities

- Lab: Using Customer-Supplied Encryption Keys with Cloud Storage
- Lab: Using Customer-Managed Encryption Keys with Cloud Storage and Cloud KMS

BILGINC IT Academy

info@bilginc.com

bilginc.com

- Lab: Creating a BigQuery Authorized View

Module 7 – Application Security: Techniques and Best Practices

Topics

- Types of application security vulnerabilities
- Web Security Scanner
- Identity and OAuth phishing threats
- Identity-Aware Proxy
- Secret Manager

Objectives

Participants will review common application security vulnerabilities and examine DoS protections in App Engine and Cloud Functions.

They will explore the role of Web Security Scanner, threats associated with Identity and OAuth phishing, and how Identity-Aware Proxy can help mitigate risk. The module also covers the secure storage of application credentials and metadata with Secret Manager.

Activities

- Lab: Using Web Security Scanner to Find Vulnerabilities in an App Engine Application
- Lab: Configuring Identity-Aware Proxy to Protect a Project
- Lab: Configuring and Using Credentials with Secret Manager

Module 8 – Securing Google Kubernetes Engine: Techniques and Best Practices

Topics

- Introduction to Kubernetes/GKE
- Authentication and Authorization
- Hardening clusters
- Securing workloads
- Monitoring and Logging

Objectives

Participants will review the core components of a Kubernetes environment and examine authentication and authorization within Google Kubernetes Engine.

They will explore approaches for hardening Kubernetes clusters and workloads against attacks and become familiar with monitoring and logging options available in GKE.

Module 9 – Protecting Against Distributed Denial of Service Attacks (DDoS)

Topics

- How DDoS attacks work
- Google Cloud mitigations
- Types of complementary partner products

Security in Google Cloud Training

Duration: **3 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Objectives

Participants will learn how DDoS attacks operate and review common mitigation approaches, including Cloud Load Balancing, Cloud CDN, autoscaling, VPC ingress and egress firewalls, and Google Cloud Armor.

They will also explore complementary partner products and learn how Google Cloud Armor can be used to blocklist an IP address and restrict access to an HTTP load balancer.

Activity

- Lab: Configuring Traffic Blocklisting with Google Cloud Armor

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

Topics

- Ransomware threats
- Ransomware mitigations
- Data misuse, privacy violations, and sensitive content
- Content-related mitigations

Objectives

Participants will examine ransomware and mitigation approaches including backups, IAM, and the Cloud Data Loss Prevention API.

The module also covers content-related risks such as data misuse, privacy violations, and sensitive, restricted, or unacceptable content. Participants will review mitigation techniques including content classification with Cloud ML APIs and scanning and redacting data through the DLP API.

Activity

- Lab: Redacting Sensitive Data with the DLP API

Module 11 – Monitoring, Logging, Auditing, and Scanning

Topics

- Cloud Audit Logs
- Deploying and using Forseti

Objectives

Participants will explore Security Command Center, Cloud Monitoring, and Cloud Logging. They will learn how to install Monitoring and Logging Agents and configure and review Cloud Audit Logs.

The module also provides experience with deploying and using Forseti, inventorying a deployment through Forseti Inventory, and scanning a deployment using Forseti Scanner.

Activities

- Lab: Installing Cloud Logging and Monitoring Agents

Security in Google Cloud Training

Duration: **3 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

- Lab: Configuring and Using Cloud Logging and Monitoring
- Lab: Configuring and Viewing Cloud Audit Logs