Security in Google Cloud

Duration: 3 Days Course Code: GO5977 Delivery Method: Virtual Learning

Overview:

This training course gives you a broad study of security controls and techniques in Google Cloud.

Through lectures, demonstrations, and labs, you explore and deploy the components of a secure Google Cloud solution. You use services including Cloud Identity, Identity and Access Management (IAM), Cloud Load Balancing, Cloud IDS, Web Security Scanner, BeyondCorp Enterprise, and Cloud DNS.

Products:
Cloud Identity, Resource Manager, Identity and Access Management (IAM), Cloud HSM, Cloud 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, Cloud Data Loss Prevention API, Cloud Intrusion Detection System (IDS), Cloud DNS, Identity Platform, Policy Intelligence, Workload identity federation, Cloud IDS, BeyondCorp Enterprise, Certificate Authority Service

Updated July 2026

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:

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

Objectives:

- **After completing this course participants should be able to:**
- Identify the foundations of Google Cloud security.
- Manage administration identities with Google Cloud.
- Implement user administration with Identity and Access Management (IAM).
- Configure Virtual Private Clouds (VPCs) for isolation, security, and logging.
- Apply techniques and best practices for securely managing Compute Engine.
- Apply techniques and best practices for securely managing Google Cloud data.
- Apply techniques and best practices for securing Google Cloud applications.
- Apply techniques and best practices for securing Google Kubernetes Engine (GKE) resources.
- Manage protection against distributed denial-of-service attacks (DDoS).
- Manage content-related vulnerabilities.
- Implement Google Cloud monitoring, logging, auditing, and scanning solutions.

Prerequisites:

Attendees should meet the following prerequisites:

- Knowledge of foundational concepts in information security, through experience or online training such as SANS SEC301:

Testing and Certification

Recommended as preparation for the following exam:

- Google Professional Cloud Security Engineer

Introduction to Cyber Security.

- 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.
- Basic understanding of Kubernetes terminology (preferred but not required).
- Attendance of recommended courses.

Content:

Module 1: Foundations of Google Cloud Security

- Explain the shared security responsibility model of Google Cloud.
- Describe how Google Cloud approaches security.
- Recognize threats mitigated by Google and Google Cloud.
- Identify Google Cloud's commitments to regulatory compliance.

Module 2: Securing Access to Google Cloud

- Describe what Cloud Identity is and what it does.
- Explain how Google Cloud Directory Sync securely syncs users and permissions between your on-premises LDAP or AD server and the cloud.
- Explore and apply best practices for managing groups, permissions, domains, and administrators with Cloud Identity.

Module 3: Identity and Access Management (IAM)

- Identify IAM roles and permissions that can be used to organize resources in Google Cloud.
- Explain the management-related features of Google Cloud projects.
- Define IAM policies, including organization policies.
- Implement access control with IAM.
- Provide access to Google Cloud resources by using predefined and custom IAM roles.

Module 4: Configuring Virtual Private Cloud for Isolation and Security

- Describe the function of VPC networks.
- Recognize and implement best practices for configuring VPC firewalls (both ingress and egress rules).
- Secure projects with VPC Service Controls.
- Apply SSL policies to load balancers.
- Enable VPC flow logging, and then use Cloud Logging to access logs.
- Deploy Cloud IDS, and view threat details in the Google Cloud console.

Module 5: Securing Compute Engine: Techniques and Best Practices

- Create and manage service accounts for Compute Engine instances (default and customer-defined).
- Detail IAM roles and scopes for VMs.
- Explore and apply best practices for Compute Engine instances.
- Explain the function of the Organization Policy Service.

Module 6: Securing Cloud Data: Techniques and Best Practices

- Use IAM permissions and roles to secure cloud resources.
- Create and wrap encryption keys using the Compute Engine RSA public key certificate.
- Encrypt and attach persistent disks to Compute Engine instances.
- Manage keys and encrypted data by using Cloud Key Management Service (Cloud KMS) and Cloud HSM.
- Create BigQuery authorized views.
- Recognize and implement best practices for configuring storage options.

Module 7: Securing Applications: Techniques and Best Practices

- Recall various types of application security vulnerabilities.
- Detect vulnerabilities in App Engine applications by using Web Security Scanner.
- Secure Compute Engine Applications by using BeyondCorp Enterprise.
- Secure application credentials by using Secret Manager.
- Identify the threats of OAuth and Identity Phishing.

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

- Explain the differences between Kubernetes service accounts and Google service accounts.
- Recognize and implement best practices for securely configuring GKE.
- Explain logging and monitoring options in Google Kubernetes Engine.

Module 9: Protecting against Distributed Denial-of-Service Attacks (DDoS)

- Identify the four layers of DDoS Mitigation.
- Identify methods Google Cloud uses to mitigate the risk of DDoS for its customers.
- Use Google Cloud Armor to blocklist an IP address and restrict access to an HTTP Load Balancer.

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

- Discuss the threat of ransomware.
- Explain ransomware mitigations strategies (backups, IAM, Cloud Data Loss Prevention API).
- Highlight common threats to content (data misuse; privacy violations; sensitive, restricted, or unacceptable content).
- Identify solutions for threats to content (classification, scanning, and redacting).
- Detect and redact sensitive data by using the Cloud DLP API.

Module 11: Monitoring, Logging, Auditing, and Scanning

- Explain and use the Security Command Center.
- Apply Cloud Monitoring and Cloud Logging to a project.
- Apply Cloud Audit Logs to a project.
- Identify methods for automating security in Google Cloud environments.

Additional Information:

Official course book provided to participants

Further Information:

For More information, or to book your course, please call us on +1 (800) 268 7737

ilt.customerservice@globalknowledge.com

www.globalknowledge.com/en-ca/

Global Knowledge Network (Canada) Inc., 150 Knowledge Park Drive, Suite 130, Fredericton, NB, E3C 0N9