Training: Google Cloud

Security in Google Cloud

Google Cloud

TRANING TERMS

2026-06-30 | 3 days | Warszawa / Virtual Classroom

TRAINING GOALS:

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.

What you'll learn

- 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.

Audience

This course is primarily intended for:

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

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

CONSPECT:

- Foundations of Google Cloud Security
  - Topics
  - The approach of Google Cloud to security
  - The shared security responsibility model
  - Threats mitigated by Google and Google Cloud
  - Access transparency
  - Objectives
    - 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.
- Securing Access to Google Cloud
  - Topics
    - Cloud Identity
    - Google Cloud Directory Sync
    - Managed Microsoft AD
    - Google authentication versus SAML-based SSO
    - Identity Platform
    - Authentication best practices
  - Objectives
    - 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.

- Activities
    - Demo: Defining Users with Cloud Identity Console

- Identity and Access Management (IAM)
    - Topics
        - Resource Manager
        - IAM roles
        - Service accounts
        - IAM and Organization policies
        - Workload identity federation
        - Policy Intelligence
    - Objectives
        - 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.
    - Activities
        - Lab: Configuring IAM

- Configuring Virtual Private Cloud for Isolation and Security
    - Topics
        - VPC firewalls
        - Load balancing and SSL policies
        - Cloud Interconnect
        - VPC Network Peering
        - VPC Service Controls
        - Access Context Manager
        - VPC Flow Logs
        - Cloud IDS
    - Objectives
        - 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.
    - Activities
        - Lab: Configuring VPC Firewalls
        - Lab: Configuring and Using VPC Flow Logs in Cloud Logging
        - Demo: Securing Projects with VPC Service Controls
        - Lab: Getting Started with Cloud IDS
- Securing Compute Engine: Techniques and Best Practices
    - Topics
        - Service accounts, IAM roles, and API scopes
        - Managing VM logins
        - Organization policy controls
        - Shielded VMs and Confidential VMs
        - Certificate Authority Service
        - Compute Engine best practices
    - Objectives
        - 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.
    - Activities
        - Lab: Configuring, Using, and Auditing VM Service Accounts and Scopes
- Securing Cloud Data: Techniques and Best Practices
    - Topics
        - Cloud Storage IAM permissions and ACLs
        - Auditing cloud data
        - Signed URLs and policy documents
        - Encrypting with Customer-managed encryption keys (CMEK) and Customer-supplied encryption keys (CSEK)
        - Cloud HSM
        - BigQuery IAM roles and authorized views
        - Storage best practices
        - Storage best practices
    - Objectives
        - 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.
    - Activities
        - Lab: Using Customer-Supplied Encryption Keys with Cloud Storage
        - Lab: Using Customer-Managed Encryption Keys with Cloud Storage and Cloud KMS
        - Lab: Creating a BigQuery Authorized View
- Securing Applications: Techniques and Best Practices
    - Topics
        - Types of application security vulnerabilities
        - Web Security Scanner
        - Threat: Identity and OAuth phishing
        - Identity-Aware Proxy
        - Secret Manager
    - Objectives
        - 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.
    - Activities
        - Lab: Identify Application Vulnerabilities with Security Command Center
        - Lab: Securing Compute Engine Applications with BeyondCorp Enterprise
        - Lab: Configuring and Using Credentials with Secret Manager
- Securing Google Kubernetes Engine: Techniques and Best Practices
    - Topics
        - Types of application security vulnerabilities
        - Web Security Scanner
        - Threat: Identity and OAuth phishing
        - Identity-Aware Proxy
        - Secret Manager
    - Objectives
        - Explain the differences between Kubernetes service accounts and Google service accounts.

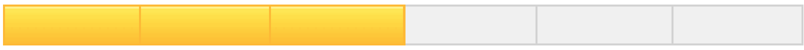
        - Recognize and implement best practices for securely configuring GKE.
        - Explain logging and monitoring options in Google Kubernetes Engine.
- Protecting against Distributed Denial-of-Service Attacks (DDoS)
    - Topics
        - How DDoS attacks work
        - Google Cloud mitigations
        - Types of complementary partner products
    - Objectives
        - 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
    - Activities
        - Lab: Configuring Traffic Blocklisting with Google Cloud Armor
- Content-Related Vulnerabilities: Techniques and Best Practices
    - Topics
        - Threat: Ransomware
        - Ransomware mitigations
        - Threats: data misuse, privacy violations, sensitive content
        - Content-related mitigation
        - Redacting Sensitive Data with the DLP API
    - Objectives
        - 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.
    - Activities
        - Lab: Redacting Sensitive Data with the DLP API
- Monitoring, Logging, Auditing, and Scanning
    - Topics
        - Security Command Center
        - Cloud Monitoring and Cloud Logging
        - Cloud Audit Logs
        - Cloud security automation

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

REQUIREMENTS:

- Prior completion of the Google Cloud Fundamentals: Core Infrastructure course or equivalent experience.
- Prior completion of the Networking in Google Cloud course or equivalent experience.
- Knowledge of foundational concepts in information security, through experience or online training such as SANS SEC301: 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).

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by Google Cloud (course completion).

This course is intended to help you prepare for the Professional Cloud Security Engineer certification exam. Google Cloud certification exams are offered at Kryterion test centers worldwide. More information about Professional Cloud Security Engineer exam https://cloud.google.com/learn/certification/cloud-security-engineer

TRAINER:

Authorized Google Cloud Trainer