Security in Google Cloud

Duration 3 day(s) (T-GCPSEC-I)

Official Training

Description

This training course gives you a broad study of security controls and techniques in Google Cloud. Through recorded lectures, demonstrations, and hands-on labs, you'll explore and deploy the components of a secure Google Cloud solution, including Cloud Identity, Resource Manager, Identity and Access Management (IAM), Virtual Private Cloud firewalls, Cloud Load Balancing, Direct Peering, Carrier Peering, Cloud Interconnect, and VPC Service Controls.

For each lab, Qwiklabs offers a free set of resources for a fixed amount of time and a clean environment with permissions.

Goals

- Understand Google's approach to security.
- Manage administration identities using Cloud Identity.
- Implement least privilege administration using Resource Manager and IAM.
- Implement Identity-Aware Proxy.
- Implement IP traffic controls using VPC firewalls and Google Cloud Armor.
- Remediate security vulnerabilities, especially public access to data and virtual machines.
- Scan for and redact sensitive data using the Cloud Data Loss Prevention API.
- Analyze changes to resource metadata configuration using audit logs.
- Scan a Google Cloud deployment with Forseti, to remediate important types of vulnerabilities, especially in public access to data and VMs.

Public

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

Prerequisites

- Prior completion of Google Cloud Fundamentals: Core Infrastructure or equivalent experience
- Prior completion of Networking in Google Cloud or equivalent experience
- Basic understanding of Kubernetes terminology (preferred but not required)
- Knowledge of foundational concepts in information security, through experience or through online training such as SANS's 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

Structure

To define

Program

- Foundations of Google Cloud Security
  - Understand the shared security responsibility model.
  - Understand the kinds of threats mitigated by Google and by Google Cloud.
  - Define and understand access transparency.
- Cloud Identity
  - Learn what Cloud Identity is and what it does.
  - Learn how Directory Sync securely syncs users and permissions between your on-prem LDAP or AD server and the cloud.
  - Understand the two ways Google Cloud handles authentication and how to set up SSO.
  - Explore best practices for managing groups, permissions, domains and admins with Cloud Identity.
- Identity and Access Management (IAM)
  - Understand Resource Manager: projects, folders, and organizations.
  - Learn how to implement IAM roles, including custom roles.
  - Understand IAM policies, including organization policies.
  - Understand best practices, including separation of duties and least privilege, the use of Google groups in policies, and avoiding the use of basic roles.
  - Learn how to configure IAM, including custom roles and organization policies.
- Configuring Virtual Private Cloud for Isolation and Security
  - Learn best practices for configuring VPC firewalls (both ingress and egress rules).
  - Understand load balancing and SSL policies.
  - Understand how to set up private Google API access.
  - Understand SSL proxy use.
  - Learn best practices for VPC networks, including peering and shared VPC use, and the correct use of subnetworks.
  - Learn best security practices for VPNs.
  - Understand security considerations for interconnect and peering options.
  - Become familiar with available security products from partners.
  - Learn to configure VPC firewalls.
  - Prevent data exfiltration with VPC Service Controls.
- Securing Compute Engine: Techniques and Best Practices
  - Learn about Compute Engine service accounts, default and customer-defined.
  - Understand IAM roles and scopes for VMs.
  - Understand how Shielded VMs help maintain your system and application integrity.
- Securing Cloud Data: Techniques and Best Practices
  - Use cloud permissions and roles to secure cloud resources.
  - Audit cloud data.
  - Use signed URLs to give access to objects in a Cloud Storage bucket.
  - Manage what can be placed in a Cloud Storage bucket using Signed Policy Document.
  - Encrypt cloud data using customer managed encryption keys (CMEK), customer supplied encryption keys (CSEK), and Cloud HSM.
  - Protecting data in BigQuery using IAM roles and authorized views.
- Application Security: Techniques and Best Practices
  - Recall various types of application security vulnerabilities.
  - Understand DoS protections in App Engine and Cloud Functions.
  - Understand the role of Web Security Scanner in mitigating risks.
  - Define and recall the threats posed by Identity and Oauth phishing.
  - Understand the role of Identity-Aware Proxy in mitigating risks.
  - Store application credentials and metadata securely using Secret Manager.
- Securing Google Kubernetes Engine: Techniques and Best Practices
  - Understand the basic components of a Kubernetes environment.
  - Understand how authentication and authorization works in Google Kubernetes Engine.
  - Recall how to harden Kubernetes Clusters against attacks.
  - Recall how to harden Kubernetes workloads against attacks.
  - Understand logging and monitoring options in Google Kubernetes Engine.
- Protecting against Distributed Denial of Service Attacks (DDoS)
  - Understand how DDoS attacks work.
  - Recall common mitigations: Cloud Load Balancing, Cloud CDN, autoscaling, VPC ingress and egress firewalls, Google Cloud Armor.
  - Recall the various types of complementary partner products available.
  - Use Google Cloud Armor to blocklist an IP address and restrict access to an HTTP load balancer.
- Content-Related Vulnerabilities: Techniques and Best Practices

- Discuss the threat of ransomware.
- Understand ransomware mitigations: Backups, IAM, Cloud Data Loss Prevention API.
- Understand threats to content: Data misuse, privacy violations, sensitive/restricted/ unacceptable content.
- Recall mitigations for threats to content: Classifying content using Cloud ML APIs; scanning and redacting data using the DLP API.

- Monitoring, Logging, Auditing, and Scanning
  - Understand and use Security Command Center.
  - Understand and use Cloud Monitoring and Cloud Logging.
  - Install the Monitoring and Logging Agents.
  - Understand Cloud Audit Logs.
  - Gain experience configuring and viewing Cloud Audit Logs.
  - Gain experience deploying and using Forseti.
  - Learn how to inventory a deployment with Forseti Inventory.
  - Learn how to scan a deployment with Forseti Scanner.