GC-SGC

SECURITY IN GOOGLE CLOUD

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
3 Days	Intermediate	Google Cloud	VILT & ILT	NA

INTRODUCTION

This three-day instructor-led course gives you a broad study of security controls and techniques in Google Cloud.

Through lectures, demonstrations, and hands-on labs, you'll explore and deploy the components of a secure Google Cloud solution, using services like Cloud Identity, Identity and Access Management (IAM), Cloud Load Balancing, Cloud IDS, Web Security Scanner, BeyondCorp Enterprise, Cloud DNS, and much more.

This course is a continuation of the Networking in Google Cloud Platform course and assumes hands-on experience with the technologies covered in that course.

AUDIENCE PROFILE

This course is intended for the following participants:

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

PREREQUISITES

- Completed Google Cloud Fundamentals: Core Infrastructure or equivalent experience.
- Completed Networking in Google Cloud Platform or equivalent experience.
- 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.
- Basic understanding of Kubernetes terminology (preferred but not required).

COURSE OBJECTIVES

This course teaches participants the following skills:

- 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.

COURSE CONTENT

Lesson 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

- Learn about Google Cloud's approach to security.
- Understand the shared security responsibility model.
- Understand the kinds of threats mitigated by Google and by Google Cloud.
- Define and understand access transparency.

Lesson 2: 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.
- Demo: Defining Users with Cloud Identity Console.

Objectives

- 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.

Lesson 3: Identity and Access Management (IAM)

Topics

- Resource Manager.
- IAM roles.
- Service accounts.
- IAM & Organisation policies.
- Workload Identity Federation.
- Policy Intelligence.

Objectives

- 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.

Activities

- Lab: Configuring IAM.

Lesson 4: Configuring Virtual Private Cloud for Isolation and Security

Topics

- VPC firewalls.
- Load balancing and SSL policies.
- Interconnect and Peering options.
- VPC Service Controls.
- Access Context Manager.
- VPC Flow Logs.
- Cloud IDS.

Objectives

- 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.

Activities

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

Lesson 5: Securing Compute Engine: Techniques and Best Practices

Topics

- Service accounts, IAM roles, and API scopes.
- Managing VM logins.
- Organisation policy controls.
- Shielded VMs and Confidential VMs.
- Certificate Authority Service.
- Compute Engine best practices.

Objectives

- 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.

Activities

- Lab: Configuring, Using, and Auditing VM Service Accounts and Scopes.

- Lab: Encrypting Disks with Customer-Supplied Encryption Keys.

Lesson 6: Securing Cloud Data: Techniques and Best Practices

Topics

- Cloud Storage IAM permissions, and ACLs.
- Auditing cloud data.
- Signed URLs and policy documents.
- Encrypting with CMEK and CSEK.
- Cloud HSM.
- BigQuery IAM roles and authorised views.
- Storage best practices.

Objectives

- 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.

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 Authorised View.

Lesson 7: 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.
- 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.

Activities

- Lab: Using Web Security Scanner to Find Vulnerabilities in an App Engine Application.
- Lab: Securing Compute Engine Applications with BeyondCorp Enterprise.
- Lab: Configuring and Using Credentials with Secret Manager.

Lesson 8: 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

- 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.

Lesson 9: Protecting Against Distributed Denial of Service Attacks (DDoS)

Topics

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

Objectives

- 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.

Activities

- Lab: Configuring Traffic Blocklisting with Google Cloud Armor.

Lesson 10: Content-Related Vulnerabilities: Techniques and Best Practice

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.
- 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.

Activities

- Lab: Redacting Sensitive Data with the DLP API.

Lesson 11: Monitoring, Logging, Auditing, and Scanning

Topics

- Security Command Centre.
- Cloud Monitoring and Cloud Logging.
- Cloud Audit Logs.
- Cloud security automation.

Objectives

- 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.

Activities

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

ASSOCIATED CERTIFICATIONS & EXAM

This exam prepares you for the Google Cloud Certified: Professional Cloud Security Engineer certification exam.