Contact:
Info@silverlake.sg
+65 - 65882456

Security in Google Cloud Platform

Course#:SE-GCP
Duration:2 Days
Price:0.00

Course Description

This course gives participants broad study of security controls and techniques on Google Cloud Platform. Through lectures, demonstrations, and hands-on labs, participants explore and deploy the components of a secure GCP solution. Participants also learn mitigation techniques for attacks at many points in a GCP-based infrastructure, including Distributed Denial-of-Service attacks, phishing attacks, and threats involving content classification and use.

Objectives

Audience

This class is intended for the following job roles:

Cloud information security analysts, architects, and engineers
Information security/cybersecurity specialists
Cloud infrastructure architects
Additionally, the course is intended for Google and partner field personnel who work with customers in those job roles. The course should also be useful to developers of cloud applications.

Prerequisites

Prior completion of Google Cloud Platform Fundamentals: Core Infrastructure or equivalent experience
Prior completion of Networking in Google Cloud Platformor equivalent experience

Content

Through lectures, demonstrations, and hands-on labs, participants explore and deploy the components of a secure GCP solution. Participants also learn mitigation techniques for attacks at many points in a GCP-based infrastructure, including Distributed Denial-of-Service attacks, phishing attacks, and threats involving content classification and use.

Module 1: Foundations of GCP Security

Google Clouds approach to security
The shared security responsibility model
Threats mitigated by Google and by GCP
Access Transparency

Module 2: Cloud Identity

Cloud Identity
Syncing with Microsoft Active Directory
Choosing between Google authentication and SAML-based SSO
GCP best practices

Module 3: Identity and Access Management

GCP Resource Manager: projects, folders, and organizations
GCP IAM roles, including custom roles
GCP IAM policies, including organization policies
GCP IAM best practices

Module 4: Configuring Google Virtual Private Cloud for Isolation and Security

Configuring VPC firewalls (both ingress and egress rules)
Load balancing and SSL policies
Private Google API access

SSL proxy use
Best practices for structuring VPC networks
Best security practices for VPNs
Security considerations for interconnect and peering options
Available security products from partners

Module 5: Monitoring, Logging, Auditing, and Scanning

Stackdriver monitoring and logging
VPC flow logs
Cloud audit logging
Deploying and Using Forseti

Module 6: Securing Compute Engine: techniques and best practices

Compute Engine service accounts, default and customer-defined
IAM roles for VMs
API scopes for VMs
Managing SSH keys for Linux VMs
Managing RDP logins for Windows VMs
Organization policy controls: trusted images, public IP address, disabling serial port
Encrypting VM images with customer-managed encryption keys and with customer-supplied encryption keys
Finding and remediating public access to VMs
VM best practices
Encrypting VM disks with customer-supplied encryption keys

Module 7: Securing cloud data: techniques and best practices

Cloud Storage and IAM permissions
Cloud Storage and ACLs
Auditing cloud data, including finding and remediating publicly accessible data

Signed Cloud Storage URLs
Signed policy documents
Encrypting Cloud Storage objects with customer-managed encryption keys and with customer-supplied encryption keys
Best practices, including deleting archived versions of objects after key rotation
BigQuery authorized views
BigQuery IAM roles
Best practices, including preferring IAM permissions over ACLs

Module 8: Protecting against Distributed Denial of Service Attacks: techniques and best practices

How DDoS attacks work
Mitigations: GCLB, Cloud CDN, autoscaling, VPC ingress and egress firewalls, Cloud Armor
Types of complementary partner products

Module 9: Application Security: techniques and best practices

Types of application security vulnerabilities
DoS protections in App Engine and Cloud Functions
Cloud Security Scanner
Threat: Identity and Oauth phishing
Identity Aware Proxy

Module 10: Content-related vulnerabilities: techniques and best practices

Threat: Ransomware
Mitigations: Backups, IAM, Data Loss Prevention API
Threats: Data misuse, privacy violations, sensitive/restricted/unacceptable content
Mitigations: Classifying content using Cloud ML APIs; scanning and redacting data using Data Loss Prevention API