Security in Google Cloud Platform (SGCP-3D)

ID GO-SGCP-3D **Duración** 3 días

Quién debería asistir

This class is intended for the following job roles:

- Cloud information security analysts, architects, and engineers
- Information security/cybersecurity specialists
- Cloud infrastructure architects
- Developers of cloud applications.

Este curso es parte de las siguientes Certificaciones

Google Cloud Certified Professional Cloud Security Engineer (PCSE)

Prerrequisitos

To get the most out of this course, participants should have:

- Prior completion of Google Cloud Fundamentals: Core Infrastructure (GCF-CI) or equivalent experience
- Prior completion of Networking in Google Cloud Platform (NGCP) or equivalent experience
- Knowledge of foundational concepts in information security:
  - Fundamental concepts:
    - vulnerability, threat, attack surface
    - confidentiality, integrity, availability
  - Common threat types and their mitigation strategies
  - Public-key cryptography
    - Public and private key pairs
    - Certificates
    - Cipher types
    - Key width
  - Certificate authorities
  - Transport Layer Security/Secure Sockets Layer encrypted communication
  - Public key infrastructures
  - Security policy
- 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

Objetivos del curso

This course teaches participants the following skills:

- Understanding the Google approach to security
- Managing administrative identities using Cloud Identity.
- Implementing least privilege administrative access using Google Cloud Resource Manager, Cloud IAM.
- Implementing IP traffic controls using VPC firewalls and Cloud Armor
- Implementing Identity Aware Proxy
- Analyzing changes to the configuration or metadata of resources with GCP audit logs
- Scanning for and redact sensitive data with the Data Loss Prevention API
- Scanning a GCP deployment with Forseti
- Remediating important types of vulnerabilities, especially in public access to data and VMs

Contenido del curso

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.

Esquema Detallado del Curso

PART I: MANAGING SECURITY IN GOOGLE CLOUD

Module 1 Foundations of GCP Security

- Understand the GCP shared security responsibility model
- Understand Google Cloud's approach to security
- Understand the kinds of threats mitigated by Google and by GCP
- Define and Understand Access Transparency and Access Approval (beta)

Module 2 Cloud Identity

- Cloud Identity
- Syncing with Microsoft Active Directory using Google Cloud Directory Sync
- Using Managed Service for Microsoft Active Directory (beta)
- Choosing between Google authentication and SAML-based SSO
- Best practices, including DNS configuration, super admin accounts
- Lab: Defining Users with Cloud Identity Console

Module 3 Identity, Access, and Key Management

- GCP Resource Manager: projects, folders, and organizations
- GCP IAM roles, including custom roles
- GCP IAM policies, including organization policies
- GCP IAM Labels
- GCP IAM Recommender
- GCP IAM Troubleshooter
- GCP IAM Audit Logs
- Best practices, including separation of duties and least privilege, the use of Google groups in policies, and avoiding the use of primitive roles
- Labs: Configuring Cloud IAM, including custom roles and organization policies

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 VPC networks, including peering and shared VPC use, correct use of subnetworks
- Best security practices for VPNs
- Security considerations for interconnect and peering options
- Available security products from partners
- Defining a service perimeter, including perimeter bridges
- Setting up private connectivity to Google APIs and services
- Lab: Configuring VPC firewalls

PART II: SECURITY BEST PRACTICES ON GOOGLE CLOUD

Module 5 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
- Best practices, including using hardened custom images, custom service accounts (not the default service account), tailored API scopes, and the use of application default credentials instead of user-managed keys
- Lab: Configuring, using, and auditing VM service accounts and scopes
- Encrypting VM disks with customer-supplied encryption keys
- Lab: Encrypting disks with customer-supplied encryption keys
- Using Shielded VMs to maintain the integrity of virtual machines

Module 6 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
- Lab: Using customer-supplied encryption keys with Cloud Storage
- Lab: Using customer-managed encryption keys with Cloud Storage and Cloud KMS
- BigQuery authorized views
- BigQuery IAM roles
- Best practices, including preferring IAM permissions over ACLs
- Lab: Creating a BigQuery authorized view

Module 7 Securing Applications: techniques and best practices

- Types of application security vulnerabilities
- DoS protections in App Engine and Cloud Functions
- Cloud Security Scanner
- Lab: Using Cloud Security Scanner to find

vulnerabilities in an App Engine application (demo)
- Identity Aware Proxy
- Lab: Configuring Identity Aware Proxy to protect a project

Module 8 Securing Kubernetes: techniques and best practices

- Authorization
- Securing Workloads
- Securing Clusters
- Logging and Monitoring

PART III: MITIGATING VULNERABILITIES IN GOOGLE CLOUD

Module 9 Protecting against Distributed Denial of Service Attacks

- How DDoS attacks work
- Mitigations: GCLB, Cloud CDN, autoscaling, VPC ingress and egress firewalls, Cloud Armor (including its rules language)
- Types of complementary partner products
- Lab: Configuring GCLB, CDN, traffic blacklisting with Cloud Armor

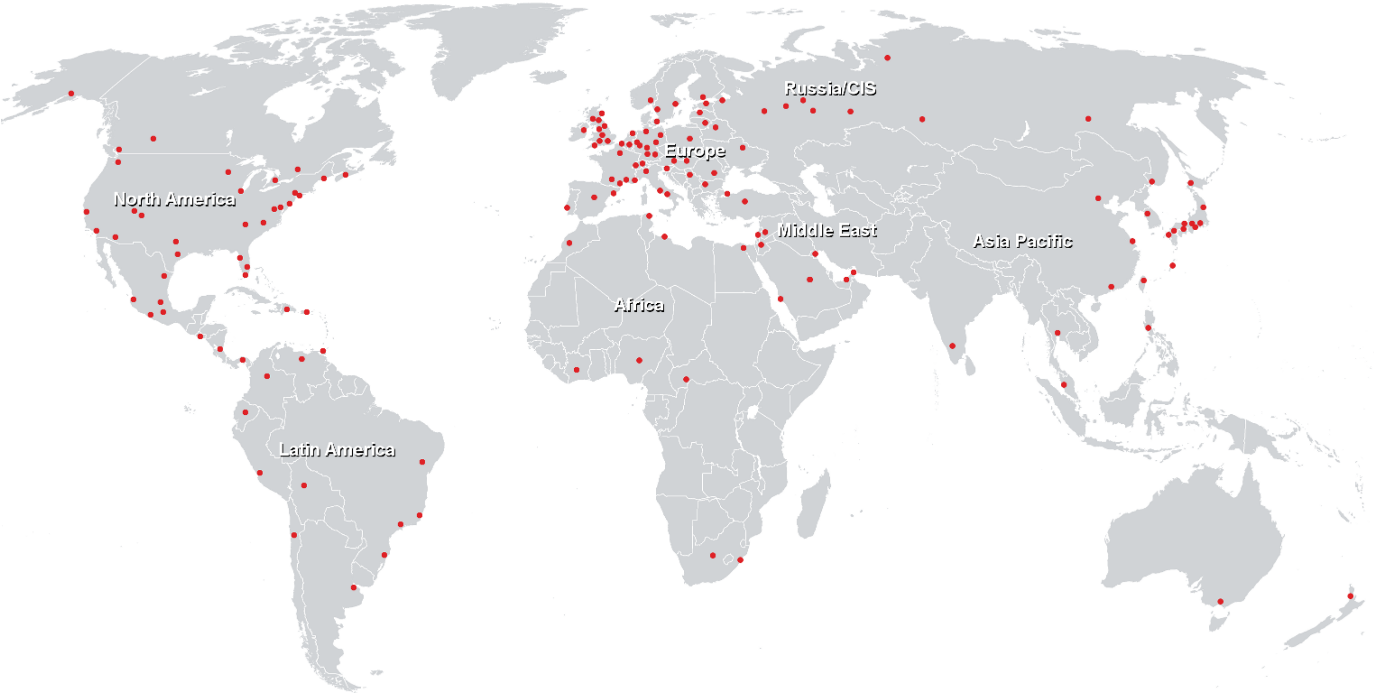
Module 10 Protecting against content-related vulnerabilities

- Threat: Ransomware
- Mitigations: Backups, IAM, Data Loss Prevention API
- Threats: Data misuse, privacy violations, sensitive/restricted/unacceptable content
- Threat: Identity and Oauth phishing
- Mitigations: Classifying content using Cloud ML APIs; scanning and redacting data using Data Loss Prevention API
- Lab: Redacting Sensitive Data with Data Loss Prevention API

Module 11 Monitoring, Logging, Auditing, and Scanning

- Security Command Center
- Stackdriver monitoring and logging
- Lab: Installing Stackdriver agents
- Lab: Configuring and using Stackdriver monitoring and logging
- VPC flow logs
- Lab: Viewing and using VPC flow logs in Stackdriver
- Cloud audit logging
- Lab: Configuring and viewing audit logs in Stackdriver
- Deploying and Using Forseti
- Lab: Inventorying a Deployment with Forseti Inventory (demo)
- Lab: Scanning a Deployment with Forseti Scanner

Centros de Entrenamiento Mundial


Russia/CIS
Europe
North America
Middle East
Asia Pacific
Africa
Latin America