Curso Security in Google Cloud

Calle de la Basílica, 19
28020 Madrid
(34) 915 53 61 62
www.cas-training.com

Nivel
Intermedio

Duración
21 horas

Modalidad
Aula Virtual

Learning
by doing

Curso
Oficial

Curso Security in Google Cloud

Dirigido a:

- Analistas, arquitectos e ingenieros de seguridad de la información en la nube.
- Especialistas en seguridad y ciberseguridad de la información.
- Arquitectos de infraestructura en la nube.

Objetivos:

- Comprender el enfoque de seguridad de Google.
- Administrar las identidades de administración mediante Cloud Identity.
- Implementar la administración de privilegios mínimos mediante Resource Manager e IAM.
- Implementar el Identity-Aware Proxy.
- Implementar controles de tráfico IP utilizando firewalls VPC y Google Cloud Armor.
- Corregir las vulnerabilidades de seguridad, especialmente el acceso público a datos y máquinas virtuales.
- Buscar y eliminar datos confidenciales con la API de prevención de pérdida de datos en la nube.
- Analizar los cambios en la configuración de los metadatos de los recursos mediante registros de auditoría.
- Escanear una implementación de Google Cloud con Forseti, para solucionar vulnerabilidades importantes, especialmente en el acceso público a los datos y VMs.

Requisitos:

- Haber completado el curso Google Cloud Fundamentals: Core Infrastructure o tener una experiencia equivalente.
- Haber completado el curso Networking in Google Cloud o tener una experiencia equivalente.
- Comprensión básica de la terminología de Kubernetes (preferido pero no obligatorio).
- Conocimiento de conceptos fundamentales en seguridad de la información, a través de la experiencia o mediante capacitación en línea, como "SANS's SEC301: Introduction to Cyber Security".
- Competencia básica con herramientas de línea de comandos y entornos de sistema operativo Linux.
- Experiencia en operaciones de sistemas, incluida la implementación y administración de aplicaciones, ya sea en las instalaciones o en un entorno de nube pública.
- Comprensión de lectura de código en Python o Javascript.

Material del curso:

Documentación oficial para el **curso Security in Google Cloud**.

Perfil del docente:

- Formador certificado por Google Cloud.
- Más de 5 años de experiencia profesional.
- Más de 4 años de experiencia docente.
- Profesional activo en empresas del sector IT.

Metodología:

- "Learning by doing" se centra en un contexto real y concreto, buscando un aprendizaje en equipo para la resolución de problemas en el sector empresarial.
- Aulas con grupos reducidos para que el profesional adquiera la mejor atención por parte de nuestros instructores profesionales.
- El programa de estudios como partners oficiales es confeccionado por nuestro equipo de formación y revisado por las marcas de referencia en el sector.
- La impartición de las clases podrá ser realizada tanto en modalidad Presencial como Virtual.

Contenidos:

Módulo 1: Foundations of Google Cloud Security

- Temas:
  - Google Cloud's Approach to Security
  - The Shared Security Responsibility Model
  - Threats Mitigated by Google and Google Cloud
  - Access Transparency
- Objetivos:
  - 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.

Módulo 2: Cloud Identity

- Temas:
  - Cloud Identity
  - Google Cloud Directory Sync
  - Google Authentication Versus SAML-based SSO
  - Authentication Best Practices
- Objetivos:
  - 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.

Módulo 3: Identity and Access Management (IAM)

- Temas:
  - Resource Manager
  - IAM Roles
  - IAM Policies
  - IAM Recommender
  - IAM Troubleshooter
  - IAM Audit Logs
  - IAM Best Practices
- Objetivos:
  - 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.

Módulo 4: Configuring Virtual Private Cloud for Isolation and Security

- Temas:
  - VPC Firewalls
  - Load Balancing and SSL Policies
  - Interconnect and Peering Policies
  - Best Practices for VPC Networks
  - VPC Flow Logs
  - 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.
- Objetivos:
  - 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.

Módulo 5: Securing Compute Engine: Techniques and Best Practices

- Temas:
  - Service Accounts, IAM Roles and API Scopes
  - Managing VM Logins
  - Organization Policy Controls
  - Compute Engine Best Practices
  - Encrypting Disks with CSEK
- Objetivos:
  - 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.

Módulo 6: Securing Cloud Data: Techniques and Best Practices

- Temas:
  - 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 Authorized Views
  - Storage Best Practices
- Objetivos:
  - 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.

Módulo 7: Application Security: Techniques and Best Practices

- Temas:
  - Types of Application Security Vulnerabilities
  - Web Security Scanner
  - Threat: Identity and Oauth Phishing
  - Identity-Aware Proxy
  - Secret Manager
- Objetivos:
  - 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.

Módulo 8: Securing Google Kubernetes Engine: Techniques and Best Practices

- Temas:
  - Introduction to Kubernetes/GKE
  - Authentication and Authorization
  - Hardening Your Clusters
  - Securing Your Workloads
  - Monitoring and Logging
- Objetivos:
  - 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.

Módulo 9: Protecting against Distributed Denial of Service Attacks (DDoS)

- Temas:
  - How DDoS Attacks Work
  - Google Cloud Mitigations
  - Types of Complementary Partner Products
- Objetivos:
  - 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.

Módulo 10: Content-Related Vulnerabilities: Techniques and Best Practices

- Temas:
  - Threat Ransomware
  - Ransomware Mitigations
  - Threats: Data Misuse, Privacy Violations, Sensitive Content
  - Content-Related Mitigations
- Objetivos:
  - 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.

Módulo 11: Monitoring, Logging, Auditing, and Scanning

- Temas:
  - Cloud Audit Logs
  - Deploying and Using Forseti
- Objetivos:
  - 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.

CAS TRAINING

UN ESPACIO PARA CRECER

cas-training.com

Curso Security in Google Cloud