Security in Google Cloud

Duración: 3 día (24 hrs)

Descripción general

Este curso proporciona un amplio análisis de los controles y técnicas de seguridad en Google Cloud. A través de clases, demostraciones y labs, explorará e implementará los componentes de una solución segura en Google Cloud. Utilizará servicios que incluyen Cloud Identity, Identity and Access Management (IAM), Cloud Load Balancing, Cloud IDS, Web Security Scanner, BeyondCorp Enterprise y Cloud DNS.

Objetivos

- Identificar los fundamentos de Google Cloud Security.
- Gestionar identidades de administración con Google Cloud.
- Implementar la administración de usuarios con Identity and Access Management (IAM).
- Configurar Virtual Private Clouds (VPC) para el aislamiento, la seguridad y el registro.
- Aplicar técnicas y mejores prácticas para gestionar de forma segura Compute Engine.
- Aplicar técnicas y mejores prácticas para gestionar de forma segura los datos de Google Cloud.
- Aplicar técnicas y mejores prácticas para asegurar aplicaciones en Google Cloud.
- Aplicar técnicas y mejores prácticas para asegurar los recursos de Google Kubernetes Engine (GKE).
- Gestionar la protección contra ataques de denegación de servicio distribuido (DDoS).
- Gestionar vulnerabilidades relacionadas con el contenido.
- Implementar soluciones de monitoreo, registro, auditoría y escaneo en Google Cloud.

Prerrequisitos del curso

- Google Cloud Fundamentals: Core Infrastructure
- Haber completado previamente el curso Networking in Google Cloud o tener experiencia equivalente.
- Tener conocimientos conceptuales fundamentales en seguridad de la información, ya sea por experiencia o mediante formación on-line como SANS SEC301: Introduction to Cyber Security.

- Tener competencia básica con herramientas de línea de comandos y entornos del sistema operativo Linux.
- Experiencia en operaciones de sistemas, incluida la implementación y gestión de aplicaciones, ya sea en entornos locales o en un entorno de cloud pública.
- Comprensión de lectura de código en Python o Javascript.
- Comprensión básica de la terminología de Kubernetes (preferiblemente, pero no esencial).

Dirigido a:

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

Esquema del curso

Fundamentos de la Seguridad en Google Cloud

- Explicar el modelo de responsabilidad compartida de seguridad de Google Cloud.
- Describir cómo aborda Google Cloud la seguridad.
- Reconocer amenazas mitigadas por Google y Google Cloud.
- Identificar los compromisos de Google Cloud con el cumplimiento normativo.

Seguridad en el Acceso a Google Cloud

- Describir qué es Cloud Identity y qué hace.
- Explicar cómo Cloud Directory Sync de Google Cloud sincroniza de forma segura usuarios y permisos entre su servidor LDAP o AD local y cloud.
- Explorar y aplicar las mejores prácticas para gestionar grupos, permisos, dominios y administradores con Cloud Identity.

Identity and Access Management (IAM)

- Identificar roles y permisos de IAM que se pueden utilizar para organizar recursos en Google Cloud.
- Explicar las características relacionadas con la gestión de proyectos de Google Cloud.
- Definir políticas de IAM, incluidas las políticas de la organización.
- Implementar el control de acceso con IAM.
- Proporcionar acceso a los recursos de Google Cloud mediante roles IAM predefinidos y personalizados.

Configuración de Virtual Private Cloud para Aislamiento y Seguridad

- Describir la función de las redes VPC.
- Reconocer e implementar las mejores prácticas para configurar firewalls de VPC (reglas de entrada y salida).
- Asegurar proyectos con VPC Service Controls.
- Aplicar políticas SSL a equilibradores de carga.
- Habilitar el registro de flujos de VPC y luego utilizar Cloud Logging para acceder a los registros.
- Implementar Cloud IDS y ver detalles de amenazas en la consola de Google Cloud.

Seguridad en Compute Engine: Técnicas y Recomendaciones

- Crear y gestionar cuentas de servicio para instancias de Compute Engine (predeterminadas y definidas por el cliente).
- Detallar roles y alcances de IAM para máquinas virtuales.
- Explorar y aplicar las mejores prácticas para las instancias de Compute Engine.
- Explicar la función del servicio de políticas de organización.

Seguridad en Datos de Cloud: Técnicas y Recomendaciones

- Utilizar permisos y roles de IAM para asegurar recursos en la nube.
- Crear y envolver claves de cifrado utilizando el certificado de clave pública RSA de Compute Engine.
- Cifrar y adjuntar discos persistentes a instancias de Compute Engine.
- Gestionar claves y datos cifrados mediante Cloud Key Management Service (Cloud KMS) y Cloud HSM.
- Crear vistas autorizadas de BigQuery.
- Reconocer e implementar las mejores prácticas para configurar opciones de almacenamiento.

Seguridad en Aplicaciones: Técnicas y Mejores Prácticas

- Recordar varios tipos de vulnerabilidades de seguridad de aplicaciones.
- Detectar vulnerabilidades en aplicaciones de App Engine mediante Web Security Scanner.
- Asegurar aplicaciones de Compute Engine mediante BeyondCorp Enterprise.
- Asegurar credenciales de aplicaciones mediante Secret Manager.
- Identificar las amenazas de OAuth y el phishing de identidad.

Seguridad en Google Kubernetes Engine: Técnicas y Mejores Prácticas

- Explicar las diferencias entre las cuentas de servicio de Kubernetes y las cuentas de servicio de Google.
- Reconocer e implementar las mejores prácticas para configurar de forma segura GKE.
- Explicar las opciones de registro y monitoreo en Google Kubernetes Engine.

Protección contra Ataques de Denegación de Servicio Distribuido (DDoS)

- Identificar las cuatro capas de mitigación de DDoS.
- Identificar los métodos que utiliza Google Cloud para mitigar el riesgo de DDoS para sus clientes.
- Utilizar Google Cloud Armor para bloquear una dirección IP y restringir el acceso a un equilibrador de carga HTTP.

Vulnerabilidades Relacionadas con el Contenido: Técnicas y Mejores Prácticas

- Discutir la amenaza del ransomware.
- Explicar estrategias de mitigación del ransomware (copias de seguridad, IAM, Cloud Data Loss Prevention API).
- Destacar amenazas comunes al contenido (uso indebido de datos; violaciones de privacidad; contenido sensible, restringido o inaceptable).
- Identificar soluciones para amenazas al contenido (clasificación, exploración y redacción).
- Detectar y redactar datos sensibles mediante el uso de la API de Cloud DLP.

Monitorización, Registro, Auditoría y Detección

- Explicar y utilizar el Security Command Center.
- Aplicar Cloud Monitoring y Cloud Logging a un proyecto.
- Aplicar Cloud Audit Logs a un proyecto.
- Identificar métodos para automatizar la seguridad en entornos de Google Cloud.