Seguridad en Google Cloud

Código: GOO-038

Propuesta de Valor: GOOGLE

Duración: 24 Horas

Este curso utiliza conferencias, demostraciones y laboratorios prácticos para enseñarle sobre una variedad de técnicas y controles de seguridad de Google Cloud. Explorará los componentes de Google Cloud e implementará una solución segura en la plataforma. También aprenderá a mitigar los ataques en varios puntos de una infraestructura basada en Google Cloud, incluidos los ataques distribuidos de denegación de servicio, los ataques de phishing y las amenazas que implican la clasificación y el uso de contenido.

AUDIENCIA

Esta clase está destinada a los siguientes puestos de trabajo:

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

PRE REQUISITOS

Para aprovechar al máximo este curso, los participantes deben tener:

- Finalización previa de Google Cloud Fundamentals: Core Infrastructure o experiencia equivalente.
- Finalización previa de Networking en Google Cloud o experiencia equivalente.

OBJETIVOS

Este curso les enseña a los participantes las siguientes habilidades:

- Implementación de acceso administrativo con privilegios mínimos mediante Google Resource Manager, Cloud IAM.
- Implementación de controles de tráfico de IP mediante firewalls VPC y Google Cloud Armor.

/

CERTIFICACIÓN DISPONIBLE

- Certificación emitida por COGNOS.

CONTENIDO

1. FUNDAMENTOS DE LA SEGURIDAD DE GCP

1.1. COMPRENDE EL MODELO DE RESPONSABILIDAD DE SEGURIDAD COMPARTIDA DE GCP
1.2. COMPRENDA EL ENFOQUE DE SEGURIDAD DE GOOGLE CLOUD
1.3. COMPRENDA LOS TIPOS DE AMENAZAS QUE MITIGAN GOOGLE Y GCP
1.4. DEFINIR Y COMPRENDER LA TRANSPARENCIA DE ACCESO Y LA APROBACIÓN DE ACCESO (BETA)

2. CLOUD IDENTITY

2.1. CLOUD IDENTITY
2.2. SINCRONIZACIÓN CON MICROSOFT ACTIVE DIRECTORY MEDIANTE GOOGLE CLOUD DIRECTORY SYNC
2.3. USO DE MANAGED SERVICE PARA MICROSOFT ACTIVE DIRECTORY (BETA)
2.4. ELEGIR ENTRE AUTENTICACIÓN DE GOOGLE Y SSO BASADO EN SAML
2.5. MEJORES PRÁCTICAS, INCLUIDA LA CONFIGURACIÓN DE DNS, CUENTAS DE SUPERADMINISTRADOR
2.6. LABORATORIO: DEFINICIÓN DE USUARIOS CON CLOUD IDENTITY CONSOLE

3. GESTIÓN DE IDENTIDADES, ACCESOS Y CLAVES

3.1. ADMINISTRADOR DE RECURSOS DE GCP: PROYECTOS, CARPETAS Y ORGANIZACIONES
3.2. FUNCIONES DE GCP IAM, INCLUIDAS LAS FUNCIONES PERSONALIZADAS
3.3. POLÍTICAS DE GCP IAM, INCLUIDAS LAS POLÍTICAS DE LA ORGANIZACIÓN
3.4. ETIQUETAS DE IAM DE GCP
3.5. RECOMENDADOR DE IAM DE GCP
3.6. SOLUCIONADOR DE PROBLEMAS DE GCP IAM
3.7. REGISTROS DE AUDITORÍA DE IAM DE GCP
3.8. PRÁCTICAS RECOMENDADAS, INCLUIDA LA SEPARACIÓN DE DEBERES Y PRIVILEGIOS MÍNIMOS, EL USO DE GRUPOS DE GOOGLE EN LAS POLÍTICAS Y EVITAR EL USO DE ROLES PRIMITIVOS
3.9. LABS: CONFIGURACIÓN DE CLOUD IAM, INCLUIDAS LAS FUNCIONES PERSONALIZADAS Y LAS POLÍTICAS DE LA ORGANIZACIÓN

4. CONFIGURACIÓN DE LA NUBE PRIVADA VIRTUAL DE GOOGLE PARA EL AISLAMIENTO Y LA SEGURIDAD

4.1. CONFIGURACIÓN DE FIREWALLS DE VPC (REGLAS DE ENTRADA Y SALIDA)
4.2. EQUILIBRIO DE CARGA Y POLÍTICAS SSL
4.3. ACCESO PRIVADO A LA API DE GOOGLE
4.4. USO DE PROXY SSL
4.5. MEJORES PRÁCTICAS PARA REDES DE VPC, INCLUIDO EL INTERCAMBIO DE TRÁFICO Y EL USO DE VPC COMPARTIDAS, EL USO CORRECTO DE SUBREDES
4.6. MEJORES PRÁCTICAS DE SEGURIDAD PARA VPN
4.7. CONSIDERACIONES DE SEGURIDAD PARA LAS OPCIONES DE INTERCONEXIÓN Y EMPAREJAMIENTO

4.8. PRODUCTOS DE SEGURIDAD DISPONIBLES DE SOCIOS
4.9. DEFINICIÓN DE UN PERÍMETRO DE SERVICIO, INCLUIDOS LOS PUENTES PERIMETRALES
4.10. CONFIGURAR LA CONECTIVIDAD PRIVADA A LAS API Y LOS SERVICIOS DE GOOGLE
4.11. LABORATORIO: CONFIGURACIÓN DE FIREWALLS DE VPC

5. PROTECCIÓN DE COMPUTE ENGINE: TÉCNICAS Y PRÁCTICAS RECOMENDADAS

5.1. CUENTAS DE SERVICIO DE COMPUTE ENGINE, PREDETERMINADAS Y DEFINIDAS POR EL CLIENTE
5.2. ROLES DE IAM PARA VM
5.3. ÁMBITOS DE API PARA MÁQUINAS VIRTUALES
5.4. GESTIÓN DE CLAVES SSH PARA MÁQUINAS VIRTUALES LINUX
5.5. GESTIÓN DE INICIOS DE SESIÓN RDP PARA MÁQUINAS VIRTUALES DE WINDOWS
5.6. CONTROLES DE LA POLÍTICA DE LA ORGANIZACIÓN: IMÁGENES CONFIABLES, DIRECCIÓN IP PÚBLICA, DESHABILITACIÓN DEL PUERTO SERIE
5.7. CIFRADO DE IMÁGENES DE VM CON CLAVES DE CIFRADO ADMINISTRADAS POR EL CLIENTE Y CON CLAVES DE CIFRADO PROPORCIONADAS POR EL CLIENTE
5.8. ENCONTRAR Y CORREGIR EL ACCESO PÚBLICO A LAS MÁQUINAS VIRTUALES
5.9. LABORATORIO: CONFIGURACIÓN, USO Y AUDITORÍA DE ALCANCES Y CUENTAS DE SERVICIO DE VM
5.10. CIFRADO DE DISCOS DE VM CON CLAVES DE CIFRADO PROPORCIONADAS POR EL CLIENTE
5.11. LABORATORIO: CIFRADO DE DISCOS CON CLAVES DE CIFRADO PROPORCIONADAS POR EL CLIENTE
5.12. USO DE MÁQUINAS VIRTUALES BLINDADAS PARA MANTENER LA INTEGRIDAD DE LAS MÁQUINAS VIRTUALES

6. REGISTRO Y ANÁLISIS AVANZADOS

6.1. PERMISOS DE CLOUD STORAGE E IAM
6.2. ALMACENAMIENTO EN LA NUBE Y ACL
6.3. AUDITORÍA DE DATOS EN LA NUBE, INCLUIDA LA BÚSQUEDA Y REPARACIÓN DE DATOS DE ACCESO PÚBLICO
6.4. URL DE CLOUD STORAGE FIRMADAS
6.5. DOCUMENTOS DE PÓLIZA FIRMADOS
6.6. CIFRAR OBJETOS DE CLOUD STORAGE CON CLAVES DE CIFRADO ADMINISTRADAS POR EL CLIENTE Y CON CLAVES DE CIFRADO PROPORCIONADAS POR EL CLIENTE
6.7. MEJORES PRÁCTICAS, INCLUIDA LA ELIMINACIÓN DE VERSIONES ARCHIVADAS DE OBJETOS DESPUÉS DE LA ROTACIÓN DE CLAVES
6.8. LABORATORIO: USO DE CLAVES DE CIFRADO PROPORCIONADAS POR EL CLIENTE CON CLOUD STORAGE
6.9. LABORATORIO: USO DE CLAVES DE CIFRADO ADMINISTRADAS POR EL CLIENTE CON CLOUD STORAGE Y CLOUD KMS
6.10. VISTAS AUTORIZADAS DE BIGQUERY
6.11. FUNCIONES DE BIGQUERY IAM
6.12. FUNCIONES DE BIGQUERY IAM
6.13. FUNCIONES DE BIGQUERY IAM
6.14. MEJORES PRÁCTICAS, INCLUIDA LA PREFERENCIA POR LOS PERMISOS DE IAM SOBRE LAS ACL
6.15. LABORATORIO: CREACIÓN DE UNA VISTA AUTORIZADA DE BIGQUERY

7. PROTECCIÓN DE APLICACIONES: TÉCNICAS Y MEJORES PRÁCTICAS

7.1. TIPOS DE VULNERABILIDADES DE SEGURIDAD DE APLICACIONES
7.2. PROTECCIONES DOS EN APP ENGINE Y CLOUD FUNCTIONS

7.3. ESCÁNER DE SEGURIDAD EN LA NUBE
7.4. LABORATORIO: USO DE CLOUD SECURITY SCANNER PARA ENCONTRAR VULNERABILIDADES EN UNA APLICACIÓN DE APP ENGINE
7.5. PROXY CON RECONOCIMIENTO DE IDENTIDAD
7.6. LABORATORIO: CONFIGURACIÓN DE IDENTITY AWARE PROXY PARA PROTEGER UN PROYECTO

8. PROTECCIÓN DE KUBERNETES: TÉCNICAS Y MEJORES PRÁCTICAS

8.1. AUTORIZACIÓN
8.2. ASEGURAR CARGAS DE TRABAJO
8.3. PROTECCIÓN DE CLÚSTERES
8.4. REGISTRO Y SEGUIMIENTO

9. PROTECCIÓN CONTRA ATAQUES DISTRIBUIDOS DE DENEGACIÓN DE SERVICIO

9.1. CÓMO FUNCIONAN LOS ATAQUES DDOS
9.2. MITIGACIONES: GCLB, CLOUD CDN, AJUSTE DE ESCALA AUTOMÁTICO, FIREWALLS DE ENTRADA Y SALIDA DE VPC, CLOUD ARMOR (INCLUIDO SU LENGUAJE DE REGLAS)
9.3. TIPOS DE PRODUCTOS DE SOCIOS COMPLEMENTARIOS
9.4. LABORATORIO: CONFIGURACIÓN DE GCLB, CDN, LISTAS NEGRAS DE TRÁFICO CON CLOUD ARMOR

10. PROTECCIÓN CONTRA VULNERABILIDADES RELACIONADAS CON EL CONTENIDO

10.1. AMENAZA: RANSOMWARE
10.2. MITIGACIONES: COPIAS DE SEGURIDAD, IAM, API DE PREVENCIÓN DE PÉRDIDA DE DATOS
10.3. AMENAZAS: USO INDEBIDO DE DATOS, VIOLACIONES DE LA PRIVACIDAD, CONTENIDO SENSIBLE / RESTRINGIDO / INACEPTABLE
10.4. AMENAZA: IDENTIDAD Y PHISHING DE OAUTH
10.5. MITIGACIONES: CLASIFICACIÓN DE CONTENIDO MEDIANTE LAS API DE CLOUD ML; ESCANEAR Y REDACTAR DATOS MEDIANTE LA API DE PREVENCIÓN DE PÉRDIDA DE DATOS
10.6. LABORATORIO: REDACCIÓN DE DATOS CONFIDENCIALES CON LA API DE PREVENCIÓN DE PÉRDIDA DE DATOS

11. SUPERVISIÓN, REGISTRO, AUDITORÍA Y ESCANEO

11.1. CENTRO DE COMANDO DE SEGURIDAD
11.2. SUPERVISIÓN Y REGISTRO DE STACKDRIVER
11.3. LABORATORIO: INSTALACIÓN DE AGENTES DE STACKDRIVER
11.4. LABORATORIO: CONFIGURACIÓN Y USO DE LA SUPERVISIÓN Y EL REGISTRO DE STACKDRIVER
11.5. REGISTROS DE FLUJO DE VPC
11.6. LABORATORIO: VISUALIZACIÓN Y USO DE REGISTROS DE FLUJO DE VPC EN STACKDRIVER
11.7. REGISTRO DE AUDITORÍA EN LA NUBE
11.8. LABORATORIO: CONFIGURACIÓN Y VISUALIZACIÓN DE REGISTROS DE AUDITORÍA EN STACKDRIVER
11.9. IMPLEMENTACIÓN Y USO DE FORSETI
11.10. LABORATORIO: INVENTARIO DE UNA IMPLEMENTACIÓN CON FORSETI INVENTORY (DEMOSTRACIÓN)
11.11. LABORATORIO: ESCANEO DE UNA IMPLEMENTACIÓN CON FORSETI SCANNER (DEMOSTRACIÓN)

BENEFICIOS

- Al finalizar el curso podrás comprender el enfoque de seguridad de Google. Administrar identidades administrativas mediante Cloud Identity.