[sfeir] Institute

Google Cloud | GCP300SEC

Security in Google Cloud

Approfondissez vos connaissances des contrôles et des techniques de sécurité dans Google Cloud

3jours / 21h

Objectifs pédagogiques

- Identifier les fondements de la sécurité Google Cloud.
- Gérer les identités d'administration avec Google Cloud.
- Implémenter l'administration des utilisateurs avec Identity and Access Management (IAM).
- Configurer des Virtual Private Clouds (VPC) pour l'isolation, la sécurité et la journalisation.
- Appliquer des techniques et des bonnes pratiques pour gérer en toute sécurité Compute Engine.
- Appliquer des techniques et des bonnes pratiques pour gérer en toute sécurité les données Google Cloud.
- Appliquer des techniques et des bonnes pratiques pour sécuriser les applications Google Cloud.
- Appliquer des techniques et des bonnes pratiques pour sécuriser les ressources Google Kubernetes Engine (GKE).
- Gérer la protection contre les attaques par déni de service distribué (DDoS).
- Gérer les vulnérabilités liées au contenu.
- Mettre en œuvre les solutions de surveillance, de journalisation, d'audit et d'analyse de Google Cloud

Public cible

- Analystes, architectes et ingénieurs en sécurité de l'information dans le cloud
- Spécialistes en sécurité de l'information/cybersécurité
- Architectes d'infrastructure cloud

Prérequis

Pour tirer le meilleur parti de ce cours, les participants doivent :

- Suivi le cours Google Cloud Fundamentals: Core Infrastructure ou avoir des connaissances équivalentes
- Suivi le cours Networking in Google Cloud ou avoir des connaissances équivalentes
- Connaître les concepts fondamentaux de la sécurité de l'information, par l'expérience ou par une formation en ligne telle que la formation de SANS SEC301: Introduction
- to Cyber Security
- Avoir des compétences de base avec les outils de ligne de commande et les environnements de système d'exploitation Linux.
- Avoir une expérience de l'exploitation des systèmes, y compris le déploiement et la gestion d'applications, sur site ou dans un environnement de cloud public.
- Compréhension de base de lecture de code en Python ou Javascript.
- Compréhension de base de la terminologie de Kubernetes (souhaité mais pas obligatoire).

Programme

Module 1: Les bases de la sécurité Google Cloud

Sujets

- L'approche de Google Cloud en matière de sécurité
- Le modèle de responsabilité partagée en matière de sécurité
- Menaces atténuées par Google et Google Cloud
- Accéder à la transparence

Objectifs

- Expliquer le modèle de responsabilité partagée en matière de sécurité de Google Cloud.

- Décrire l’approche de Google Cloud en matière de sécurité.
- Reconnaître les types de menaces atténuées par Google et par Google Cloud.
- Identifier les engagements de Google Cloud en matière de conformité réglementaire.

Module 2: Sécuriser l’accès à Google Cloud

Sujets

- Identité Cloud
- Synchronisation d’annuaire Google Cloud
- Microsoft AD géré
- Authentification Google par rapport à l’authentification unique basée sur SAML
- Plate-forme d’identité
- Meilleures pratiques d’authentification

Objectifs

- Décrire ce qu’est Cloud Identity et ce qu’il fait.
- Expliquer comment Google Cloud Directory Sync synchronise en toute sécurité les utilisateurs et les autorisations entre votre serveur LDAP ou AD sur site et le cloud.
- Explorer et appliquer les bonnes pratiques de gestion des groupes, des autorisations, des domaines et des administrateurs avec Cloud Identity.

Activités

- Démonstration : Définir des utilisateurs avec Cloud Identity Console

Module 3: Identity and Access Management (IAM)

Sujets

- Gestionnaire de ressources
- Rôles IAM
- Comptes de service
- Politiques IAM et d’Organization
- Fédération d’identité de charge de travail
- Intelligence politique

Objectifs

- Identifier les objets IAM pouvant être utilisés pour organiser les ressources dans Google Cloud.
- Expliquer les fonctionnalités liées à la gestion des projets Google Cloud.

- Définir les politiques IAM, y compris les politiques d'organisation.
- Mettre en œuvre le contrôle d'accès avec Cloud IAM.
- Fournir un accès aux ressources Google Cloud à l'aide de rôles IAM prédéfinis et personnalisés.

Activités

- Configuration d'IAM

Module 4: Configuration du cloud privé virtuel pour l'isolation et la sécurité

Sujets

- Pare-feu VPC
- Équilibrage de charge et politiques SSL
- Options d'interconnexion et d'appairage
- VPC Service Controls
- Access Context Manager
- VPC Flow Logs
- Cloud IDS

Objectifs

- Décrire la fonction des réseaux VPC.
- Reconnaître et mettre en œuvre les meilleures pratiques pour la configuration des pare-feu VPC (règles d'entrée et de sortie).
- Sécurisez les projets avec VPC Service Controls.
- Appliquer des politiques SSL aux équilibreurs de charge.
- Activez la journalisation de flux VPC, puis utilisez Cloud Logging pour accéder aux journaux.
- Déployer Cloud IDS et afficher les détails des menaces dans Cloud Console

Activités

- Lab: Configuration des pare-feu VPC
- Lab: Configurer et utiliser les journaux de flux VPC dans Cloud Logging
- Démonstration : Sécuriser des projets avec VPC Service Controls
- Lab: Premiers pas avec Cloud IDS

Module 5: Sécuriser Compute Engine : techniques et bonnes pratiques

Sujets

- Service accounts, rôles IAM et champs d'application d'API

- Gestion des connexions aux VM
- Contrôles de la politique de l'Organization
- Shielded VMs et Confidential VMs
- • Certificate Authority Service
- Bonnes pratiques de Compute Engine

Objectifs

- Créer et gérer des comptes de service pour les instances Compute Engine (par défaut et définis par le client).
- Détailler les rôles et les étendues IAM pour les machines virtuelles.
- Explorer et appliquer les bonnes pratiques pour les instances Compute Engine.
- Expliquer la fonction du service Règle d'administration.

Activités

- Lab : Configuration, utilisation et audit des comptes de service et des étendues de VM

Module 6: Securing Cloud Data: Techniques and Best Practices

Sujets

- Autorisations Cloud Storage IAM et LCA
- Audit des données cloud
- URL et documents de politique signés
- Chiffrement avec CMEK et CSEK
- HSM cloud
- Rôles BigQuery IAM et vues autorisées
- Meilleures pratiques de stockage

Objectifs

- Utiliser les autorisations et les rôles IAM pour sécuriser les ressources cloud.
- Créer et encapsuler des clés de chiffrement à l'aide du certificat de clé publique RSA de Google Compute Engine.
- Chiffrer les disques persistants et les associer aux instances Compute Engine.
- Gérer les clés et les données chiffrées à l'aide de Cloud Key Management Service (Cloud KMS) et Cloud HSM.
- Créer des vues BigQuery autorisées.
- Reconnaître et mettre en œuvre les meilleures pratiques de configuration des options de stockage.

Activités

- Lab : Utilisation des clés de chiffrement fournies par le client avec Cloud Storage
- Lab : Utiliser des clés de chiffrement gérées par le client avec Cloud Storage et Cloud KMS
- Lab : Créer une vue autorisée BigQuery

Module 7: Sécurisation des applications : techniques et bonnes pratiques

Sujets

- Types de vulnérabilités de sécurité des applications
- Web Security Scanner
- Menace : hameçonnage d'identité et Oauth
- Identity-Aware Proxy
- Secret Manager

Objectifs

- Rappel des différents types de vulnérabilités de sécurité des applications.
- Détecter les vulnérabilités dans les applications App Engine à l'aide de Web Security Scanner.
- Sécuriser les applications Compute Engine à l'aide de BeyondCorp Enterprise.
- Sécuriser les informations d'identification de l'application à l'aide de Secret Manager.
- Identifier les menaces d'OAuth et d'hameçonnage d'identité.

Activités

- Atelier : Utiliser Web Security Scanner pour rechercher des vulnérabilités dans une application App Engine
- Atelier : Sécuriser les applications Compute Engine avec BeyondCorp Enterprise
- Atelier : Configurer et utiliser des identifiants avec Secret Manager

Module 8: Sécuriser Google Kubernetes Engine : techniques et bonnes pratiques

Sujets

- Authentification et autorisation
- Durcissement de vos clusters
- Sécurisation de vos charges de travail
- Surveillance et journalisation

Objectifs

- Expliquer les différences entre les comptes de service Kubernetes et les comptes de service Google.
- Reconnaître et mettre en œuvre les bonnes pratiques pour configurer GKE en toute sécurité.
- Expliquer les options de journalisation et de surveillance dans Google Kubernetes Engine.

Module 9: Protection contre les attaques par déni de service distribué (DDoS)

Sujets

- Comment fonctionnent les attaques DDoS
- Atténuations Google Cloud
- Types de produits partenaires complémentaires

Objectifs

- Identifier les quatre couches de l'atténuation DDoS.
- Identifier les méthodes utilisées par Google Cloud pour atténuer le risque de DDoS pour ses clients.
- Utiliser Google Cloud Armor pour bloquer une adresse IP et restreindre l'accès à une adresse HTTP.
- Équilibreur de charge

Activités

- Lab : Configurer la liste de blocage du trafic avec Google Cloud Armor

Module 10: Vulnérabilités liées au contenu : techniques et bonnes pratiques

Sujets

- Menace : rançongiciel
- Atténuation des ransomwares
- Menaces : utilisation abusive des données, violation de la vie privée, contenu sensible
- Atténuation liée au contenu
- Masquer les données sensibles avec l'API DLP

Objectifs

- Discuter de la menace des ransomwares.
- Expliquer les stratégies d'atténuation des ransomwares (sauvegardes, IAM, API Cloud Data Loss Prevention).

- Mettre en évidence les menaces courantes pour le contenu (utilisation abusive des données, violations de la vie privée, contenu sensible/restreint/inacceptable).
- Identifier les solutions aux menaces sur le contenu (classification, analyse, rédaction).
- Détecter et masquer les données sensibles à l'aide de l'API Cloud DLP.

Activités

- Lab : Masquer les données sensibles avec l'API DLP

Module 11: Surveillance, journalisation, audit et analyse

Sujets

- Centre de commandement de la sécurité
- Surveillance dans le cloud et journalisation dans le cloud
- Journaux d'audit cloud
- Automatisation de la sécurité dans le cloud

Objectifs

- Expliquer et utiliser le Security Command Center.
- Appliquer Cloud Monitoring et Cloud Logging à un projet.
- Appliquer les journaux d'audit Cloud à un projet.
- Identifier les méthodes d'automatisation de la sécurité dans les environnements Google Cloud.

Activités

- Lab : Configurer et utiliser Cloud Monitoring et Cloud Logging
- Lab : Configurer et afficher les journaux d'audit Cloud