La sécurité avec Google Cloud

Durée 3 jour(s) (T-GCPSEC-I)

Formation officielle

Description

Cette formation apporte aux participants une vaste étude sur des contrôles et techniques de sécurité avec Google Cloud. Grâce à des cours, des démonstrations et des ateliers pratiques, les participants explorent et déploient les composants d'une solution Google Cloud sécurisée. Ils apprennent également des techniques de limitation des attaques visant de nombreux points d'une infrastructure basée sur Google Cloud, y compris des attaques par déni de service distribué, des attaques d'hameçonnage et des menaces impliquant l'utilisation et la classification du contenu.

Ressources pédagogiques

Qwiklabs (solution dédiée Google) pour chaque atelier vous offre un ensemble de ressources disponible gratuitement pendant une période donnée ainsi qu'un environnement vierge avec les autorisations requises.

Formation disponible en Présentiel / Distanciel / Hybride **

La formation à distance se déroule de préférence sur des jours consécutifs (contactez nous si besoin de décomposer en demies journées)

En inter-entreprises, l'outil de visio-conférence privilégié est Google Meet.

En intra-entreprises, on privilégie Google Meet mais Microsoft Teams, Zoom sont également proposés.

** Formation hybride : Parcours mêlant action de formation en présentiel, en distanciel, en asynchrone, en synchrone, autoformation dirigée et apprentissage coaché.

Objectifs

- Comprendre l'approche de Google concernant la sécurité.
- Gérer et administrer les identités avec Cloud Identity.
- Implémenter le principe du moindre privilège en utilisant Resource Manager et IAM.
- Implémenter Identity-Aware Proxy.
- Implémenter le contrôle de traffic IP en utilisant les pare-feux VPC et Google Cloud Armor.
- Remédier aux vulnérabilités, en particulier l'accès publique aux données et aux machines virtuelles.
- Scanner et masquer les données sensibles en utilisant Cloud Data Loss Prevention API.
- Analyser les changements des configurations des ressources en utilisant les journaux d'audit.
- Scanner un déploiement Google Cloud avec Forseti, remédier aux types de vulnérabilités les plus importants, en particulier concernant l'accès publique aux données et VMs.

Public

- Analystes, architectes et ingénieurs en sécurité de l'information [Cloud]
- Spécialistes en sécurité/cybersécurité de l'information
- Architectes d'infrastructure cloud.
- Avoir suivi le cours Google Cloud Fundamentals: Core Infrastructure ou avoir une expérience équivalente.
- Avoir suivi la formation Networking in Google Cloud ou avoir une expérience équivalente.
- Avoir suivi la formation SEC301: Introduction to Cyber Security ou avoir une expérience équivalente.

Prérequis

Aucun

Répartition

À définir

Evaluations des acquis

L'évaluation des acquis de la formation se fera en séance au travers d'ateliers, d'exercices et/ou de travaux pratiques. Dans le cas d'une formation officielle éditeur, veuillez nous consulter afin que nous vous fassions part des modalités d'évaluation.

A l'issue de la formation, vous sera transmis une évaluation à chaud de l'action de formation qui vous permettra de nous faire part de vos retours quant à votre expérience apprenant avec Zenika.

Ressources pédagogiques

Les ressources pédagogiques proviennent de productions des équipes Zenika et/ou de la documentation éditeur dans le cas d'une formation "Officielle". Les documents sont en français ou en anglais.

RQTH et ma formation Zenika

Si vous êtes sujet à un handicap, prenez contact avec nos équipes pour que nous puissions définir ensemble comment nous pourrons aménager la session afin que vous puissiez vivre une expérience en formation inchangée.

Programme

- Principes de base de la sécurité Google Cloud
  - Comprendre les principes du modèle de responsabilité partagé.
  - Comprendre le type de menaces mitigées par Google et Google Cloud.
  - Définir et comprendre Access Transparency.
- Cloud Identity
  - Apprendre ce qu'est Cloud Identity et son utilité.
  - Apprendre comment Directory Sync synchronise de façon sécurisée les utilisateurs et les permissions entre votre LDAP ou serveur AD et le Cloud.
  - Comprendre les deux manières dont Google Cloud gère l'authentification et mettre en place du SSO.
  - Explorer les bonnes pratiques pour gérer vos groupes, permissions, domaines et administrateurs avec Cloud Identity.
- Gestion de l'authentification et des accès
  - Comprendre Resource Manager: projets, dossiers et organisations.
  - Apprendre comment implémenter les rôles IAM, y compris les rôles personnalisés.
  - Comprendre les stratégies IAM, y compris les stratégies de niveau organisation.
  - Comprendre les bonnes pratiques, notamment la séparation des rôles et le principe de moindre privilège, l'utilisation des Google groups dans les stratégies et éviter l'utilisation des rôles basiques.
  - Apprendre comment configurer IAM, notamment les rôles personnalisés et les stratégies d'organisation.
- Configuration du cloud privé virtuel pour l'isolation et la sécurité
  - Apprendre les bonnes pratiques pour configurer les pare-feux VPC (à la fois les règles d'ingress et egress).
  - Comprendre la répartition de charge et les stratégies SSL.
  - Comprendre comment mettre en place l'accès privé au API Google.
  - Comprendre l'utilisation du proxy SSL.
  - Apprendre les bonnes pratiques des réseaux VPC, notamment le peering et l'utilisation des VPC partagés, ainsi que l'utilisation correcte des sous-réseaux.
  - Apprendre les bonnes pratiques de sécurité pour les VPNs.
  - Comprendre les problématiques de sécurité pour les options d'interconnexion et de peering.
  - Se familiariser avec les produits de sécurité des partenaires.
  - Apprendre à configurer les pare-feux VPC.
  - Prévenir l'exfiltration de données avec VPC Service Controls.
- Sécurisation de Compute Engine : techniques et bonnes pratiques
  - Découvrir les comptes de service Compute Engine, ceux par défaut et les personnalisés.
  - Comprendre les rôles IAM et les scopes pour les VMs.
  - Comprendre comment les Shielded VMs vous aide à maintenir l'intégrité du système et des applications.
- Sécurisation des données dans le cloud : techniques et bonnes pratiques
  - Utiliser les permissions Cloud et les rôles pour sécuriser vos ressources cloud.
  - Auditer les données cloud.
  - Utiliser des URLs signées pour donner accès aux objets dans un bucket Cloud Storage.
  - Gérer ce qui peut être déposé dans un bucket Cloud Storage en utilisant Signed Policy Document.
  - Chiffrer vos données cloud en utilisant des clés gérées par le client (CMEK), des clées fournies par le client (CSEK) et Cloud HSM.
  - Protéger vos données dans BigQuery en utilisant les rôles IAM et les vues autorisées.
- Sécurité des applications : Techniques et bonnes pratiques
  - Rappeler les différents types de vulnérabilités applicatives.
  - Comprendre les protections d'App Engine et Cloud Functions contre les dénis de services (DOS).
  - Comprendre le rôle de Web Security Scanner pour mitiger les risques.
  - Définir et rappeler les menaces liées au hammeçonnage d'identité et Oauth.
  - Comprendre le rôle de Identity-Aware Proxy pour mitiger les risques.
  - Stocker les informations d'authentification d'application et les méta-données de façon sécurisée en utilisant Secret Manager.
- Sécurisation de Google Kubernetes Engine : Techniques et bonnes pratiques
  - Comprendre les composants de base d'un environnement Kubernetes.
  - Comprendre comment l'authentication et les autorisations fonctionnent dans Google Kubernetes Engine.
  - Rappeler comment durcir les cluster Kubernetes contre les attaques.
  - Rappeler comment durcir les applications Kubernetes contre les attaques.
  - Comprendre les options de journalisation et de surveillance de Google Kubernetes Engine.
- Protection contre les attaques par déni de service distribué (DDoS)
  - Comprendre comment fonctionne les attaques de déni de service distribué (DDoS).
  - Rappeler les mitigations communes : Cloud Load Balancing, Cloud CDN, l'autoscaling, les pare-feux VPC et Google Cloud Armor.

    - Rappeler les différents types de produits complémentaires fournis par les partenaires.
    - Utiliser Google Cloud Armor pour bloquer une adresse IP et restreindre l'accès à un répartiteur de charge HTTP.
- Failles liées au contenu : techniques et bonnes pratiques
    - Discuter la menace des ransomware.
    - Comprendre les mitigations de ransomware : sauvegardes, IAM, Cloud Data Loss Prevention API.
    - Comprendre les menaces envers le contenu : mauvaise utilisation des données, violation de la vie privée, contenu sensible, restreint ou inacceptable.
    - Rappeler les mitigation des menaces de contenu : Classer les données en utilisant les APIs Cloud ML; scanner et expurger les données en utilisant l'API DLP.
- Surveillance, journalisation, audits et analyses
    - Comprendre et utiliser Security Command Center.
    - Comprendre et utiliser Cloud Monitoring et Cloud Logging.
    - Installer les agents de journalisation et de surveillance.
    - Comprendre les journaux d'audit cloud.
    - Configurer et consulter les journaux d'audit cloud.
    - Déployer et utiliser Forseti.
    - Apprendre comment inventorier un déploiement avec Forseti Inventory.
    - Apprendre comment scanner un déploiement avec Forseti Scanner.