Programme de Formation

La sécurité avec Google Cloud

Organisation

Durée en jours : 3 jour(s)
Durée en heures : 21 heures

Mode d'organisation : Mixte

Contenu pédagogique

Public visé

- Analystes, architectes et ingénieurs en sécurité de l'information [Cloud]
- Spécialistes en sécurité/cybersécurité de l'information
- Architectes d'infrastructure cloud.

Objectifs pédagogiques

- 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 IdentityAware Proxy.
- Implémenter le contrôle de traffic IP en utilisant les parefeux 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.

Prérequis

- 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.

Description

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.

Moyens et supports pédagogiques

Les ressources pédagogiques proviennent de **productions des équipes Zenika**, qui mettent à profit leur **expertise** et leur **expérience** dans le domaine de la formation professionnelle.

Ces ressources sont soigneusement élaborées pour répondre aux besoins spécifiques des apprenants et garantir une compréhension approfondie des sujets abordés.

Dans le cas d'une formation "Officielle", la documentation utilisée est issue directement des éditeurs, ce qui assure une conformité avec les standards et les meilleures pratiques du secteur.

Les documents sont disponibles en français ou en anglais, permettant ainsi une accessibilité maximale pour un public diversifié.

De plus, ces ressources incluent souvent des **études de cas,** des **exercices pratiques** et des **supports visuels** afin d'enrichir **l'expérience d'apprentissage** et de favoriser **l'engagement des participants**.

Modalités d'évaluation et de suivi

En amont de la formation, les stagiaires reçoivent un **questionnaire** permettant de mesurer leurs attentes, leurs compétences et leur niveau à l'entrée de la formation. Ce questionnaire est conçu pour recueillir des informations précieuses sur le parcours professionnel des participants, leurs motivations personnelles ainsi que les compétences spécifiques qu'ils souhaitent développer. Cela permet aux formateurs d'adapter le contenu de la formation en fonction des besoins identifiés.

Tout au long de la formation, la **progression** et l'atteinte des **objectifs pédagogiques** des stagiaires sont évaluées, au travers de :

- **travaux pratiques**, qui incluent des exercices concrets permettant d'appliquer les connaissances théoriques acquises dans un contexte réel.
- **échanges entre pairs**, favorisant une dynamique collaborative où les stagiaires peuvent partager leurs expériences et apprendre les uns des autres.
- **mises en situation concrètes**, simulant des scénarios professionnels afin d'évaluer la capacité des stagiaires à réagir et à s'adapter face à diverses situations.

Durant la dernière heure de la formation, un **questionnaire d'évaluation** ainsi qu'un **questionnaire à chaud de fin de formation** seront soumis à chaque stagiaire pour s'assurer de la bonne acquisition des compétences tout au long de la formation et de l'adéquation de ces acquis avec les attentes des stagiaires (émis en amont de la formation). Ce processus d'évaluation permet également aux formateurs d'obtenir un retour constructif sur le déroulement du programme et d'identifier les points à améliorer pour les prochaines sessions.

Dans le cas d'une **formation officielle éditeur**, n'hésitez pas à nous consulter afin que nous vous fassions part des modalités d'évaluation des acquis. Nous sommes également disponibles pour discuter des certifications possibles qui pourraient être délivrées à l'issue de cette formation, garantissant ainsi une reconnaissance officielle des compétences acquises par les participants.

Informations sur l'admission

L'inscription à nos formations est accessible **jusqu'à 15 jours ouvrés avant le début de la formation**.

Pour vous inscrire, il vous suffit de faire une demande via notre site Internet, où vous trouverez toutes les informations nécessaires sur les différentes formations proposées, les dates et les contenus.

Vous pouvez également nous contacter directement par mail à l'adresse suivante : training@zenika.com.

Notre équipe se fera un plaisir de répondre à toutes vos questions et de vous accompagner dans le processus d'inscription.

N'attendez plus pour développer vos compétences et rejoindre nos sessions enrichissantes !

Informations sur l'accessibilité

Besoin d'un coup de pouce pour adapter votre formation ? On s'en charge !

Chaque apprenant est unique. Que vous ayez besoin d'ajuster le rythme, le contenu, ou même les modalités d'apprentissage, nos équipes expertes sont là pour vous écouter et co-construire une solution sur-mesure.

Nous nous engageons à offrir à chacun une expérience de formation enrichissante, accessible et parfaitement adaptée à vos besoins. Besoin d'un aménagement spécifique ? Un petit tweak pédagogique ou technique ? Pas de souci, nous sommes prêts à relever ce genre de défis avec vous.

Contactez-nous, et ensemble, nous trouverons la meilleure solution pour répondre à vos attentes.