Sécurité dans Google Cloud

Durée: 3 Jours **Réf de cours: GO5977** **Méthodes d'apprentissage: Intra-entreprise & sur-mesure**

Résumé:

Ce cours de formation Google vous offre une étude approfondie des contrôles et des techniques de sécurité dans Google Cloud.
Le cours alterne entre présentations effectuées par le formateur, démonstrations et exercices pratiques, et permet d'explorer et de déployer les composants d'une solution Google Cloud sécurisée.
Vous utilisez des services tels que Cloud Identity, Identity and Access Management (IAM), Cloud Load Balancing, Cloud IDS, Web Security Scanner, BeyondCorp Enterprise et Cloud DNS.
Mise à jour : 16/02/2026

Formation intra-entreprise

Cette formation est délivrable en session intra-entreprise, dans vos locaux ou dans les nôtres. Son contenu peut être adapté sur-mesure pour répondre aux besoins de vos collaborateurs. Contactez votre conseiller formation Global Knowledge ou adressez votre demande à info@globalknowledge.fr.

Public visé:

Cette formation s'adresse aux : Analystes, architectes et ingénieurs en sécurité de l'information Spécialistes en sécurité de l'information / cybersécurité Architectes d'infrastructure cloud Développeurs sur Google Cloud

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Identifier les fondements de la sécurité de Google Cloud.
- Gérer les identités d'administration avec Google Cloud.
- Mettre en œuvre l'administration des utilisateurs avec Identity and Access Management (IAM).
- Configurer les Virtual Private Clouds (VPC) pour l'isolement, la sécurité et la journalisation.
- Appliquer les techniques et les meilleures pratiques pour gérer en toute sécurité Compute Engine.
- Appliquer les techniques et les meilleures pratiques pour gérer en toute sécurité les données de Google Cloud.
- Appliquer les techniques et les meilleures pratiques pour sécuriser les applications Google Cloud.
- Appliquer les techniques et les meilleures pratiques pour sécuriser les ressources de 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.

Pré-requis:

Avoir suivi les formations Google Cloud Platform suivantes ou avoir une expérience équivalente :

- Avoir suivi le cours Google Cloud Fondamentaux : Infrastructure essentielles (GP8324) ou posséder une expérience équivalente.
- Avoir suivi le cours Mise en réseau dans Google Cloud (GO5976) ou posséder une expérience équivalente.
- Connaissance des concepts fondamentaux de la sécurité de l'information, acquise par l'expérience ou via une formation en ligne telle que SANS SEC301: Introduction to Cyber Security.
- Maîtrise de base des outils en ligne de commande et des environnements de système d'exploitation Linux.

Test et certification

- Expérience en opérations système, y compris le déploiement et la gestion d'applications, que ce soit sur site ou dans un environnement de cloud public.
- Compréhension écrite de code en Python ou Javascript.
- Compréhension de base de la terminologie Kubernetes (préférable mais non obligatoire)

Contenu:

Fondamentaux de la sécurité de Google Cloud

- 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 menaces atténuées par Google et Google Cloud.
- Identifier les engagements de Google Cloud en matière de conformité réglementaire

Sécurisation de l'accès à Google Cloud

- 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 meilleures pratiques pour la gestion des groupes, des autorisations, des domaines et des administrateurs avec Cloud Identity
- Démonstration : Définition des utilisateurs avec la console Cloud Identity

Gestion des identités et des accès (IAM)

- Identifier les rôles et autorisations IAM qui peuvent être utilisés pour organiser les ressources dans Google Cloud.
- Expliquer les fonctionnalités de gestion des projets Google Cloud.
- Définir les politiques IAM, y compris les politiques d'organisation.
- Mettre en œuvre le contrôle d'accès avec IAM.
- Fournir l'accès aux ressources Google Cloud en utilisant des rôles IAM prédéfinis et personnalisés.
- Exercice pratique : Configuration d'IAM

Configuration du Google VPC (Virtual Private Cloud) pour l'isolation et la sécurité

- 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).
- Sécuriser les projets avec VPC Service Controls.
- Appliquer les politiques SSL aux équilibreurs de charge.
- Activer la journalisation des flux VPC, puis utiliser Cloud Logging pour accéder aux journaux.
- Déployer Cloud IDS et afficher les détails des menaces dans la console Google Cloud.
- Exercice pratique : Configuration des pare-feu VPC

Sécurisation de Compute Engine : techniques et meilleures pratiques

- Créer et gérer des comptes de service pour les instances Compute Engine (par défaut et définis par le client).
- Détailler les rôles et les portées IAM pour les VM.
- Explorer et appliquer les meilleures pratiques pour les instances Compute Engine.
- Expliquer la fonction du service de politique d'organisation.
- Exercice pratique : Configuration, utilisation et audit des comptes de service et des portées de VM

Sécurisation des données cloud : techniques et meilleures les pratiques

- Utiliser les autorisations et les rôles IAM pour sécuriser les ressources cloud.
- Créer et envelopper des clés de chiffrement à l'aide du certificat de clé publique RSA de Compute Engine.
- Chiffrer et attacher des disques persistants 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 autorisées BigQuery.
- Reconnaître et mettre en œuvre les meilleures pratiques pour la configuration des options de stockage.
- Exercice pratique : Utilisation des clés de chiffrement fournies par le client avec Cloud Storage
- Exercice pratique : Utilisation des clés de chiffrement gérées par le client avec Cloud Storage et Cloud KMS
- Exercice pratique : Création d'une vue autorisée BigQuery

Sécurisation des applications : techniques et meilleures pratiques

- Rappeler divers 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 identifiants d'application à l'aide de Secret Manager.
- Identifier les menaces de l'hameçonnage OAuth et d'identité.
- Exercice pratique : Identification des vulnérabilités des applications avec Security Command Center
- Exercice pratique : Sécurisation des

Protection contre les attaques déni de service distribué - Distributed Denial of Service (DDoS)

- Identifier les quatre couches de l'atténuation des DDoS.
- Identifier les méthodes que Google Cloud utilise pour atténuer le risque de DDoS pour ses clients.
- Utiliser Google Cloud Armor pour bloquer une adresse IP et restreindre l'accès à un équilibreur de charge HTTP.
- Exercice pratique: Configuration du blocage de trafic avec Google Cloud Armor

Vulnérabilités liées au contenu : techniques et meilleures pratiques

- Discuter de la menace des rançongiciels.
- Expliquer les stratégies d'atténuation des rançongiciels (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 ou inacceptable).
- Identifier des solutions pour les menaces liées au contenu (classification, analyse et rédaction).
- Détecter et rédiger des données sensibles à l'aide de l'API Cloud DLP.
- Exercice pratique : Rédaction de données sensibles avec l'API DLP

Surveillance, journalisation, audit et analyse

- 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 pour automatiser la sécurité dans les environnements Google Cloud.
- Exercice pratique : Configuration et utilisation de Cloud Monitoring et Cloud Logging
- Exercice pratique : Configuration et visualisation des journaux d'audit Cloud

- Exercice pratique : Configuration et utilisation des journaux de flux VPC dans Cloud Logging
- Démonstration: Sécurisation des projets avec VPC Service Controls
- Exercice pratique : Démarrage avec Cloud IDS

applications Compute Engine avec BeyondCorp Enterprise
- Exercice pratique : Configuration et utilisation des identifiants avec Secret Manager

Sécurisation de Google Kubernetes Engine : techniques et meilleures pratiques

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

Méthodes pédagogiques :

Supports de cours et labs officiels Google. Les participants réalisent un test d'évaluation des connaissances en amont et en aval de la formation pour valider les connaissances acquises pendant la formation.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement