Formation Google Cloud Platform - Sécurité

Contrôles et techniques de sécurité sur Google Cloud Platform

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

À travers des présentations, des démonstrations et des ateliers pratiques, les participants découvrent et déploient les composants d'une solution GCP sécurisée. Ils apprennent également des techniques d'atténuation des risques d'attaques pouvant survenir en de nombreux points d'une infrastructure basée sur GCP, telles que des attaques par déni de service distribué (DDoS) ou par hameçonnage, ou des menaces impliquant une classification et une utilisation de contenu.

Référence	GCP300SEC
Durée	3 jours (21h)
Tarif	à partir de 2 550 €HT

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 23 au 25 juin 2025

du 24 au 26 novembre 2025

VOIR TOUTES LES DATES

Objectifs

| Identifier l'approche Google en matière de sécurité
| Gérer des identités d'administration à l'aide de Cloud Identity
| Implémenter un accès administrateur avec un principe de moindre privilège à l'aide de Google Cloud Resource Manager et Cloud IAM
| Implémenter des contrôles de trafic IP à l'aide de pare-feu VPC et de Cloud Armor
| Implémenter la fonctionnalité Identity-Aware Proxy
| Analyser les modifications apportées à la configuration ou aux métadonnées des ressources à l'aide des journaux d'audit GCP
| Détecter des données sensibles et les masquer à l'aide de l'API Data Loss Prevention
| Analyser un déploiement GCP à l'aide de Forseti
| Résoudre les problèmes liés aux principaux types de faille, et plus particulièrement dans le cas d'un accès public aux données et aux machines virtuelles

Public

| Architectes, administrateurs et personnel SysOps / DevOps dans le cloud
| Toute personne utilisant Google Cloud Platform pour créer de nouvelles solutions ou pour intégrer des systèmes, des environnements d'application et une infrastructure existants à la plate-forme Google Cloud

Prérequis

| Avoir suivi la formation "Google Cloud Platform - Les fondamentaux de l'infrastructure" ou connaissances équivalentes
| Maîtrise des outils de ligne de commande et des environnements de système d'exploitation Linux
| Pour suivre cette formation dans des conditions optimales, nous vous recommandons de venir en formation avec un ordinateur portable

Programme de la formation

Principes de base liés à la sécurité GCP
| Approche de Google Cloud en matière de sécurité
| Modèle de responsabilité partagée en matière de sécurité
| Menaces dont les risques peuvent être atténués à l'aide de Google et GCP
| Access Transparency

Cloud Identity
| Cloud Identity

| Synchronisation avec Microsoft Active Directory
| Choisir entre une authentification Google et une authentification unique SAML
| Bonnes pratiques relatives à GCP

Gestion de l'authentification et des accès
| GCP Resource Manager : projets, dossiers et organisations
| Rôles IAM GCP, y compris les rôles personnalisés
| Règles IAM GCP, y compris les règles d'administration
| Bonnes pratiques relatives à IAM GCP

Configurer un cloud privé virtuel Google dans un objectif d'isolation et de sécurité
| Configurer des règles de pare-feu VPC d'entrée et de sortie
| Équilibrage de charge et règles SSL
| Accès privé à l'API Google
| Utilisation du proxy SSL
| Bonnes pratiques en matière de structuration de réseaux VPC
| Bonnes pratiques en matière de sécurité des réseaux VPN
| Considérations relatives à la sécurité pour les options d'interconnexion et d'appairage
| Produits de sécurité mis à disposition par nos partenaires

Surveillance, journalisation, audits et analyses
| Stackdriver Monitoring et Stackdriver Logging
| Journaux de flux VPC
| Cloud Audit Logging
| Déployer et utiliser Forseti

Techniques et bonnes pratiques en matière de sécurisation de Compute Engine
| Comptes de service Compute Engine par défaut et définis par le client
| Rôles IAM pour les machines virtuelles
| Champs d'application des API pour les machines virtuelles
| Gérer des clés SSH pour les machines virtuelles Linux
| Gérer les connexions RDP pour les machines virtuelles Windows
| Contrôles de règles d'administration : images de confiance, adresses IP publiques, désactivation du port de série
| Chiffrement des images de machines virtuelles à l'aide de clés de chiffrement gérées par le client, et de clés fournies par ce dernier
| Détecter et résoudre les problèmes d'accès public aux machines virtuelles
| Bonnes pratiques en matière de machines virtuelles
| Chiffrer des disques de machines virtuelles à l'aide de clés fournies par le client

Techniques et bonnes pratiques en matière de sécurisation des données sur le cloud
| Autorisations Cloud Storage et IAM
| Cloud Storage et LCA
| Créer des journaux d'audit relatifs aux données cloud comprenant la détection et la résolution de problèmes liés aux données accessibles au public
| URL Cloud Storage signées
| Documents réglementaires signés
| Chiffrer des objets Cloud Storage à l'aide de clés de chiffrement gérées par le client et de clés fournies par ce dernier
| Bonnes pratiques, telles que la suppression de versions archivées d'objets après rotation des clés
| Vues BigQuery autorisées
| Rôles IAM BigQuery
| Bonnes pratiques, telles que l'utilisation recommandée d'autorisations IAM plutôt que de LCA

Techniques et bonnes pratiques en matière de protection contre les attaques par déni de service distribué
| Fonctionnement des attaques DDoS
| Atténuation des risques : équilibrage de charge Google Cloud, Cloud CDN, autoscaling, règles de pare-feu d'entrée et de sortie VPC, Cloud Armor
| Types de produits partenaires supplémentaires

Techniques et bonnes pratiques en matière de sécurité des applications
| Types de failles de sécurité des applications
| Protections DoS dans App Engine et Cloud Functions
| Cloud Security Scanner
| Menace : hameçonnage des identités et Oauth
| Identity-Aware Proxy

HUB Formation - 14 avenue de l'Opéra - 75001 Paris
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

Techniques et bonnes pratiques en matière de failles liées au contenu
| Menace : rançongiciel
| Méthodes d'atténuation des risques : sauvegardes, IAM, API Data Loss Prevention
| Menaces : usage abusif des données, non-respect de la confidentialité, contenu sensible, limité ou non autorisé
| Méthodes d'atténuation des risques : classifier du contenu à l'aide des API Cloud ML, et analyser et masquer des données à l'aide de l'API Data Loss Prevention

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.