Security in Google Cloud Platform
Cours officiel, préparation aux examens de certification Google Cloud

Cours Pratique de 3 jours - 21h
Réf : GQD - Prix 2024 : 2 890€ HT

Avec cette formation, vous apprendrez à maîtriser les contrôles et techniques de sécurité sur Google Cloud Platform. Grâce à de nombreux travaux pratiques, vous explorerez et déploierez les composants d'une solution Google Cloud sécurisée. Vous découvrirez également les techniques d'atténuation des attaques à de nombreux points d'une infrastructure Google Cloud, y compris les attaques par déni de service distribué, les attaques de phishing et les menaces impliquant la classification et l'utilisation du contenu.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Comprendre l'approche de Google en matière de sécurité

Savoir effectuer la gestion des identités administratives à l'aide de Cloud Identity

Implémenter l'accès administratif au 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 des modifications Identity Aware Proxy Analyzing de la configuration ou des métadonnées des ressources

Sécuriser un environnement Kubernetes

Rechercher et expurger des données sensibles avec l'API Data Loss Prevention

Analyser un déploiement Google Cloud avec Forseti

Corriger d'importants types de vulnérabilités, surtout dans l'accès public aux données et aux machines virtuelles (VM)

MÉTHODES PÉDAGOGIQUES

Animation de la formation en français. Support de cours officiel en anglais.

CERTIFICATION

Nous vous recommandons de suivre cette formation si vous souhaitez préparer la certification "Google Cloud Professional Cloud Security Engineer".

PARTICIPANTS

Analystes, architectes et ingénieurs en sécurité de l'information, spécialistes en sécurité de l'information ou cybersécurité, architectes d'infrastructures clouds.

PRÉREQUIS

Avoir suivi "GCP Fundamentals: Core Infrastructure", "Networking in GCP" ou avoir une expérience équivalente. Bonnes connaissances des concepts fondamentaux de la sécurité de l'information, etc.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.
Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.
Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation…
À l'issue de chaque stage, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur.
Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

LE PROGRAMME

dernière mise à jour : 09/2021

1) Fondements de la sécurité GCP

- Comprendre le modèle de responsabilité partagée en matière de sécurité de GCP.
- Comprendre l'approche de Google Cloud en matière de sécurité.
- Comprendre les types de menaces atténuées par Google et par GCP.
- Définir et comprendre la transparence d'accès et l'approbation d'accès (bêta).

2) Cloud Identity

- Cloud Identity.

- Synchronisation avec Microsoft Active Directory à l'aide de Google Cloud Directory Sync.
- Utilisation du service géré pour Microsoft Active Directory (bêta).
- Choisir entre l'authentification Google et l'authentification unique basée sur SAML.
- Bonnes pratiques, y compris la configuration DNS et les comptes de super administrateur.

Travaux pratiques : Définir des utilisateurs avec Cloud Identity Console.

3) Identités, accès et gestion des clés

- Gestionnaire de ressources GCP : projets, dossiers et organisations.
- Rôles GCP IAM, y compris les rôles personnalisés.
- Stratégies IAM de GCP, y compris les stratégies d'organisation.
- Libellés GCP Now.
- Maintenant, GCP recommande.
- Outil de dépannage GCP IAM.
- Journaux d'audit GCP IAM.
- Bonnes pratiques, y compris la séparation des tâches et le moindre privilège, etc.

Travaux pratiques : Configuration de Cloud IAM, y compris les rôles personnalisés et les règles d'organisation.

4) Configurer un cloud privé virtuel de Google pour l'isolement et la sécurité

- Configuration des pare-feu VPC (règles d'entrée et de sortie).
- Équilibrage de charge et politiques SSL.
- Accès privé à l'API Google.
- Utilisation du proxy SSL.
- Bonnes pratiques pour les réseaux VPC, y compris l'appairage et l'utilisation de VPC partagés.
- Meilleures pratiques de sécurité pour les VPN.
- Considérations de sécurité pour les options d'interconnexion et d'appairage.
- Produits de sécurité disponibles auprès des partenaires.
- Définition d'un périmètre de service, y compris des ponts de périmètre.
- Configuration d'une connectivité privée aux API et services Google.

Travaux pratiques : Configuration des pare-feu VPC.

5) Sécurisation de Compute Engine : techniques et bonnes pratiques

- Comptes de service Compute Engine, par défaut et définis par le client.
- Rôles IAM pour les machines virtuelles.
- Champs d'application de l'API pour les machines virtuelles.
- Gestion des clés SSH pour les machines virtuelles Linux.
- Gestion des connexions RDP pour les machines virtuelles Windows.
- Contrôles de stratégie de l'organisation : images approuvées, adresse IP publique, désactivation du port série.
- Chiffrement des images de VM avec des clés de chiffrement gérées par le client et fournies par le client.
- Recherche et correction de l'accès public aux VM.
- Meilleures pratiques, notamment l'utilisation d'images personnalisées renforcées, comptes de service personnalisés...
- Chiffrement des disques de VM avec des clés de chiffrement fournies par le client.
- Utilisation de VM blindées pour maintenir l'intégrité des VM.

Travaux pratiques : Configurer, utiliser et auditer des comptes et des étendues de service de VM. Effectuer un chiffrement de disques avec des clés de chiffrement fournies par le client.

6) Sécurisation des données cloud : techniques et meilleures pratiques

- Cloud Storage et autorisations IAM.
- Cloud Storage et ACLs.
- Audit des données cloud, y compris la recherche et la correction des données accessibles publiquement.
- URL signées de Cloud Storage.

- Signed policy documents.
- Chiffrement des objets Cloud Storage avec des clés de chiffrement gérées et fournies par le client.
- Meilleures pratiques, y compris la suppression de versions archivées d'objets après rotation des clés.
- Vues autorisées par BigQuery.
- Rôles BigQuery IAM.
- Meilleures pratiques, notamment préférer les autorisations IAM aux ACL.

Travaux pratiques : Utiliser des clés de chiffrement fournies par le client avec Cloud Storage. Utiliser des clés de chiffrement gérées par le client avec Cloud Storage et Cloud KMS. Créer une vue autorisée BigQuery.

7) Sécurisation des applications : techniques et meilleures pratiques

- Types de vulnérabilités de sécurité des applications.
- Protections DoS dans App Engine et les Cloud Functions.
- Cloud Security Scanner.
- Identity Aware Proxy.

Travaux pratiques : Utiliser Cloud Security Scanner pour rechercher des vulnérabilités dans une application App Engine. Configurer Identity Aware Proxy pour protéger un projet.

8) Sécurisation Kubernetes : techniques et meilleures pratiques

- Autorisation.
- Sécurisation des charges de travail.
- Sécurisation des clusters.
- Journalisation et surveillance.

9) Protéger contre les attaques Distributed Denial of Service (DDoS)

- Fonctionnement des attaques DDoS.
- Atténuations : GCLB, Cloud CDN, autoscaling, pare-feu VPC ingress et egress , Cloud Armor.
- Types de produits partenaires complémentaires.

Travaux pratiques : Configurer GCLB, CDN, blacklister du trafic avec Cloud Armor.

10) Protéger contre les vulnérabilités liées au contenu

- Menace : ransomware.
- Atténuations : sauvegardes, IAM, Data Loss Prevention API.
- Menaces : utilisation abusive des données, violations de la vie privée, contenu sensible/restreint/inacceptable.
- Menace: phishing d'identité et Oauth.
- Atténuation : classification du contenu à l'aide des API Cloud ML.
- Numérisation et rédaction de données à l'aide de l'API Data Loss Prevention.

Travaux pratiques : Rédaction de données sensibles avec l'API Data Loss Prevention.

11) Surveillance, la journalisation, l'audit et le scanning

- Security Command Center.
- Surveillance et journalisation Stackdriver.
- Journaux de flux VPC.
- Journalisation d'audit cloud.
- Déploiement et utilisation de Forseti.

Travaux pratiques : Installer des agents Stackdriver. Configurer et utiliser la surveillance et la journalisation Stackdriver. Afficher et utiliser des journaux de flux VPC dans Stackdriver. Configurer et afficher des journaux d'audit dans Stackdriver, etc.

LES DATES

CLASSE À DISTANCE
2024 : 13 mai, 04 juin, 09 juil., 26 août, 03 sept., 01 oct., 19 nov., 17 déc.

PARIS
2024 : 04 juin, 09 juil., 26 août, 03 sept., 01 oct., 19 nov., 17 déc.