

Formation Google Cloud Platform GCP300SEC – Security in Google Cloud Platform

Durée de la formation : 3 jour(s) / 21 heure(s)

OBJECTIFS

A l'issue de la formation, l'apprenant sera capable de :

- Comprendre l'approche de Google en matière de sécurité
- Gestion des identités administratives à l'aide de Cloud Identity.
- Implémentation de l'accès administratif au moindre privilège à l'aide de Google Cloud Resource Manager, Cloud IAM.
- Implémentation de contrôles de trafic IP à l'aide de pare-feu VPC et de Cloud Armor
- Implémentation des modifications Identity Aware Proxy Analyzing de la configuration ou des métadonnées des ressources avec les journaux d'audit GCP
- Recherche et expurgation de données sensibles avec l'API Data Loss Prevention
- Analyse d'un déploiement GCP avec Forseti
- Correction d'importants types de vulnérabilités, en particulier dans l'accès public aux données et aux machines virtuelles

PREREQUIS

Avoir suivi la formation Google Cloud Platform Fundamentals : Core Infrastructure ou avoir une expérience équivalente

Avoir suivi la formation Networking in Google Cloud Platform ou avoir une expérience équivalente

Connaissance des concepts fondamentaux de la sécurité de l'information:

Concepts fondamentaux:

- vulnerability, threat, attack surface
- confidentiality, integrity, availability

Types de menaces courantes et leurs stratégies d'atténuation

- Public-key cryptography
- Public and private key pairs
- Certificates
- Cipher types
- Key width
- Certificate authorities
- Transport Layer Security/Secure Sockets Layer encrypted communication
- Public key infrastructures
- Security policy

Compétence de base avec les outils de ligne de commande et les environnements de système d'exploitation Linux

Expérience des opérations de systèmes, y compris le déploiement et la gestion d'applications, sur site ou dans un environnement de cloud public

Compréhension du code en Python ou JavaScript

Cette formation ne peut être financée que dans le cadre d'un projet d'entreprise (prise en charge entreprise ou OPCO). Les dossiers à financement personnel et CPF ne sont pas pris en compte.

Formation Google Cloud Platform GCP300SEC – Security in Google Cloud Platform

Durée de la formation : 3 jour(s) / 21 heure(s)

PUBLIC

Analystes, architectes et ingénieurs en sécurité de l'information
Spécialistes en sécurité de l'information / cybersécurité
Architectes d'infrastructure cloud

Formation Google Cloud Platform GCP300SEC – Security in Google Cloud Platform

Durée de la formation : 3 jour(s) / 21 heure(s)

PROGRAMME

PARTIE I : GÉRER LA SÉCURITÉ DANS GOOGLE CLOUD

Module 1: Fondations de la sécurité GCP

Comprendre le modèle de responsabilité partagée en matière de sécurité 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)

Module 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 (version bêta)

Choix entre l'authentification Google et l'authentification unique basée sur SAML

Meilleures pratiques, y compris la configuration DNS, les comptes de super administrateur

Lab: Définition d'utilisateurs avec Cloud Identity Console

Module 3: Gestion des identités, des accès et des clés

GCP Resource Manager: projets, dossiers et organisations

Rôles GCP IAM, y compris les rôles personnalisés

Stratégies GCP IAM, y compris les stratégies d'organisation

Labels GCP IAM

GCP IAM Recommender

Outil de dépannage GCP IAM

Journaux d'audit GCP IAM

Les meilleures pratiques, y compris la séparation des fonctions et le moindre privilège, l'utilisation de groupes Google dans les politiques et éviter l'utilisation des rôles primitifs

Lab: Configuration de Cloud IAM, y compris les rôles personnalisés et l'organisation de stratégies

Module 4: Configurer un Google Virtual Private Cloud pour l'isolement et 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

Meilleures pratiques pour les réseaux VPC, y compris l'homologation et le VPC partagé utilisation, utilisation correcte des sous-réseaux

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

Définir un périmètre de service, y compris des ponts de périmètre

Configuration de la connectivité privée aux API et services Google

Lab: Configuration des pare-feu VPC

PARTIE II : MEILLEURES PRATIQUES DE SÉCURITÉ SUR GOOGLE CLOUD

Module 5: Sécurisation de Compute Engine: techniques et meilleures pratiques

Comptes de service Compute Engine, par défaut et définis par le client

Rôles IAM pour les machines virtuelles

Scope d'APIs 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 machine virtuelle avec des clés de chiffrement gérées par le client et avec des clés de chiffrement fournies par le client

Recherche et correction de l'accès public aux machines virtuelles

Meilleures pratiques, notamment l'utilisation d'images personnalisées renforcées, comptes de service personnalisés (pas le

Formation Google Cloud Platform GCP300SEC – Security in Google Cloud Platform

Durée de la formation : 3 jour(s) / 21 heure(s)

compte de service par défaut), scope d'APIs personnalisés et l'utilisation des informations d'identification par défaut de l'application au lieu de clés gérées par l'utilisateur

Chiffrement des disques VM avec des clés de chiffrement fournies par le client

Utilisation de machines virtuelles blindées pour maintenir l'intégrité des machines virtuelles

Labs: Configuration, utilisation et audit des comptes et des étendues de service de machine virtuelle

Chiffrement de disques avec des clés de chiffrement fournies par le client

Module 6: Sécurisation des données cloud: techniques et meilleures les pratiques

Cloud Storage et autorisations IAM

Cloud Storage et ACLs

Audit des données cloud, y compris la recherche et la correction données accessibles publiquement

URL signées de Cloud Storage

Signed policy documents

Chiffrement des objets Cloud Storage avec des clés de chiffrement gérées par le client et avec des clés de chiffrement 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

Labs: Utilisation de clés de chiffrement fournies par le client avec Cloud Storage

Utilisation de clés de chiffrement gérées par le client avec Cloud Storage et Cloud KMS

Création d'une vue autorisée BigQuery

Module 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

Labs: Utilisation de Cloud Security Scanner pour rechercher des vulnérabilités dans une application App Engine

Configurer Identity Aware Proxy pour protéger un projet

Module 8: Sécuriser Kubernetes: techniques et meilleures pratiques

Autorisation

Sécurisation des charges de travail

Sécurisation des clusters

Journalisation et surveillance

PARTIE III : ATTÉNUER LES VULNÉRABILITÉS DANS GOOGLE CLOUD

Module 9: Protéger contre les attaques Distributed Denial of Service

Fonctionnement des attaques DDoS

Mitigations: GCLB, Cloud CDN, autoscaling, pare-feu VPC ingress et egress, Cloud Armor (y compris son langage de règles)

Types de produits partenaires complémentaires

Lab:

Configuration de GCLB, CDN, blacklister du trafic avec Cloud Armor

Module 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

Lab: Rédaction de données sensibles avec l'API Data Loss Prevention

Module 11: Monitoring, Logging, Auditing, et Scanning

Security Command Center

Surveillance et journalisation Stackdriver

Journaux de flux VPC

Journalisation d'audit cloud

Formation Google Cloud Platform GCP300SEC – Security in Google Cloud Platform

Durée de la formation : 3 jour(s) / 21 heure(s)

Déployer et utiliser Forseti

Labs: Installation d'agents Stackdriver

Configuration et utilisation de la surveillance et de la journalisation Stackdriver

Affichage et utilisation des journaux de flux VPC dans Stackdriver

Configuration et affichage des journaux d'audit dans Stackdriver

Inventorier un déploiement avec Forseti Inventory (démonstration)

Analyse d'un déploiement avec Forseti Scanner (démonstration)

Formation Google Cloud Platform GCP300SEC – Security in Google Cloud Platform

Durée de la formation : 3 jour(s) / 21 heure(s)

Prise en compte du handicap

Pour les personnes en situation de handicap, afin de nous permettre d'organiser le déroulement de la formation dans les meilleures conditions possibles, contactez-nous via notre formulaire de contact ou par mail (formation@access-it.fr) ou par téléphone (0320619506). Un entretien avec notre référente handicap pourra être programmé afin d'identifier les besoins et aménagements nécessaires.

Modalités et moyens Pédagogiques, techniques et d'encadrement mis en œuvre

Répartition théorie/pratique : 45%/55%. Cette formation se compose d'une alternance d'apports théoriques, de travaux pratiques s'articulant autour d'une application fil rouge, de démonstrations, de phases d'échanges entre participants et de synthèses de la part du formateur.

Formation accessible à distance de n'importe où et n'importe quand, via un ordinateur type PC disposant d'une connexion à Internet à haut débit (ADSL ou plus).

Pour assurer un démarrage dans les meilleures conditions au premier jour de la formation, notre service logistique se met systématiquement en relation, en amont, avec vous afin de réaliser un test de validation technique et de vous présenter l'environnement de formation.

Pendant toute la durée de la formation, le stagiaire dispose d'une assistance technique et pédagogique illimitée, par e-mail, avec un délai de prise en compte et de traitement qui n'excède pas 24h. En complément, le stagiaire peut planifier un rendez-vous pédagogique avec un formateur expert afin d'échanger sur des éléments de la formation.

La durée de la formation affichée sur cette page est une durée estimée qui peut varier en fonction du profil du stagiaire et de ses objectifs (notamment s'il souhaite valider sa formation par le passage d'un examen de certification).

Durant la formation, le formateur prévoit :

Des démonstrations organisées en modules et en séquences découpées le plus finement possible, en suivant le programme pédagogique détaillé sur cette page ;

Des énoncés et corrigés de travaux pratiques à réaliser tout au long de la formation ;

Des travaux pratiques sont proposés ; la plateforme prévoit l'environnement technique nécessaire à la réalisation de l'ensemble des travaux pratiques ;

Le formateur valide les connaissances acquises après chaque TP ;

Il est proposé un ou plusieurs livres numériques faisant office d'ouvrage(s) de référence sur le thème de la formation.

Validation et sanction de la formation

Une attestation mentionnant les objectifs, la nature et la durée de l'action et les résultats de l'évaluation des acquis de la formation sera remise au stagiaire à l'issue de sa formation par courrier électronique.

A la demande, il sera délivré un certificat de réalisation.

Type de formation

Professionalisante ayant pour objectif le perfectionnement, l'élargissement des compétences

Moyens permettant de suivre l'exécution de l'action

Le contrôle de la présence des stagiaires sera assuré par la vérification de l'assiduité des participants. Le stagiaire signera une feuille de présence par demi-journée de formation. Celle-ci sera également signée par le formateur.

Modalité d'évaluation des acquis

Durant la formation, le participant est amené à mettre en pratique les éléments du cours par la réalisation de travaux pratiques réalisés sur PC.

La validation des acquis du stagiaire est faite par le formateur à la fin de chaque atelier. Cette validation individuelle est possible du fait du faible nombre de participants par session de formation (6 personnes maximum).

À la fin de la formation, le stagiaire a donc atteint les objectifs fixés par la formation.

En complément, pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par l'éditeur en passant un examen de certification.

Access it étant centre d'examen ENI, les examens peuvent être réalisés sur demande à distance ou dans nos locaux de Villeneuve d'Ascq.

Les candidats à la certification doivent produire un travail personnel important en vue de se présenter au passage de l'examen, le seul suivi de la formation ne constitue pas un élément suffisant pour garantir un bon résultat et/ou l'obtention de la certification

Assistance Post-Formation

Toute personne ayant suivi une formation avec Access it bénéficie d'une assistance post-formation d'une durée de 1 mois. Ce nouveau service d'accompagnement permet aux stagiaires rencontrant des difficultés dans la mise en œuvre des connaissances acquises de solliciter l'aide de nos formateurs sur des aspects relatifs aux programmes de formation suivis. Pour en bénéficier, il suffit de se rendre sur la page contact de notre site web et de remplir le formulaire. Une réponse est apportée par mail ou par téléphone dans un délai de 48 heures.

Centre d'Examen

Notre centre de formation agréé Qualiopi bénéficie de l'agrément d'ENI et ICDL pour les certifications informatiques. C'est pour nos clients la garantie de pouvoir suivre des formations préparant à des certifications professionnelles.

Aide à l'orientation

Pour chacune des grandes thématiques couvertes par notre offre de formation, nous proposons via nos spécialistes un rendez-vous physique ou téléphonique qui via un diagnostic permettra aux personnes souhaitant être accompagnées dans le choix d'un programme ou dans la définition d'un parcours de formation une orientation vers les programmes les plus adaptés à leurs besoins et à leur niveau.

Aspects Pratiques

Dès leur inscription, les participants sont contactés par nos services qui s'assurent que les débits internet constatés sur le lieu depuis lequel ils souhaitent se former sont suffisants pour suivre la formation dans des conditions optimales.

À l'occasion de cet appel, nos experts s'assurent également qu'ils disposent du matériel nécessaire pour suivre la formation (PC Portable, webcam, Micro-casque..).

Avant le début de la formation, les participants reçoivent un lien leur permettant d'accéder à la classe virtuelle et leurs identifiants personnels de connexion. Un aide à l'utilisation de la solution de visioconférence utilisée leur est également proposée.

Le jour de la formation, ils se connectent à la classe virtuelle depuis leur navigateur internet. Ils voient et entendent le formateur ainsi que les autres participants et peuvent à tout moment communiquer avec eux.

Ils participent aux échanges et réalisent les ateliers dans les mêmes conditions que s'ils étaient en salle. Grâce à nos outils de prise en main à distance, les formateurs peuvent à tout moment prendre la main sur leurs postes pour les aider ou vérifier leurs TP.

Tout au long de la formation, les participants peuvent bénéficier de l'assistance immédiate de nos experts en composant le numéro qui leur a été communiqué avant la formation.

Des bilans intermédiaires ont lieu en présence des participants du formateur et du référent pédagogique d'Access it afin de vérifier l'état d'avancement de la session, les difficultés rencontrées et permettre d'éventuels actions correctives.

Bénéfices pour les participants

Se former depuis leur lieu de travail ou leur domicile,

Accéder sans se déplacer à la qualité d'une formation délivrée par un formateur consultant ayant une expérience probante sur le sujet animé.

Bénéficier à distance de la richesse d'une formation interentreprises : échanges avec le formateur et les autres participants, partages d'expériences, ateliers pratiques...

Pouvoir se former en toutes circonstances et notamment en cas d'imprévu.

Bénéfices pour l'entreprise

Optimiser ses budgets en limitant les frais de déplacement et d'hébergement.

Proposer à tous ses collaborateurs, quelle que soit leur situation géographique, des formations de qualité (en Inter comme en Intra).

Limites les temps de déplacement.

Proposer davantage de choix dans les formations à des collaborateurs peu mobiles.

Assurer la montée en compétences de ses collaborateurs quelles que soient les circonstances