Google Cloud Platform : La Sécurité sur GCP

DÉCOUVRIR LES CONTRÔLES ET TECHNIQUES DE SÉCURITÉ SUR GOOGLE CLOUD PLATFORM

Référence : GPCSEC
Durée : 3 jours (21h.)
Tarif : 2370 € HT
Contact : 01 43 34 90 94

Niveau : Avancé
Classe à distance : Possible
Version : v2026-0305 (05/03/2026)
Cours officiel : Google
Certification : Professional Cloud Security Engineer

Prochaines sessions :
- 01 juillet au 03 juillet
- 04 août au 06 août
- 05 octobre au 07 octobre

plus de dates sur https://www.plb.fr

Comme toute infrastructure de stockage, la Google Cloud Platform est susceptible de subir des attaques (DDoS, hameçonnage...) visant à compromettre son intégrité. Pour la préserver de telles menaces, différentes techniques d'atténuation des risques sont intégrées au processus d'exploitation et de maintenance de la GCP.

Cette **formation Google Cloud Platform - Sécurité sur GCP (SGCP)** présente aux participants une étude approfondie des contrôles et techniques de sécurité sur GCP en leur faisant découvrir et déployer les composants d'une solution Google Cloud Platform sécurisée.

Objectifs

Objectif opérationnel :

Savoir déployer les composants d'une solution Google Cloud Platform sécurisée.

Objectifs pédagogiques :

À l'issue de cette **formation Google Cloud Platform - Sécurité sur GCP (SGCP)** vous aurez acquis les connaissances et les compétences nécessaires pour :

- Comprendre 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

Ce stage en sécurité sur la Google Cloud Platform s'adresse aux analystes, architectes et ingénieurs dans le domaine de la sécurité des informations basées sur le Cloud, aux spécialistes des questions de sécurité et de cybersécurité des informations, aux architectes des infrastructures Cloud, et aux développeurs d'applications Cloud.

Pré-requis

Pour suivre ce cours, les stagiaires doivent avoir assisté à la formation Google Cloud Platform : Les Fondamentaux pour l'Infrastructure (GCPIF) ainsi qu'à la formation Google Cloud Platform : Mise en Réseau (GCPNET) , ou disposer d'une expérience équivalente.

Il leur est également nécessaire de connaître les concepts de base relatifs à la sécurité des informations, à savoir :

- Les concepts fondamentaux : les failles, les menaces et la surface d'attaque ; la confidentialité, l'intégrité et la disponibilité.
- Les types de menaces courants et les stratégies d'atténuation des risques
- La cryptographie à clé publique : les paires de clés publiques et privées, les certificats, les types

PLB – 3-5 rue Maurice Ravel – 92 300 Levallois-Perret – Tél. : 01 43 34 90 94 – www.plb.fr
SAS au capital de 100 000 € – RCS Nanterre B 421 694 779 – APE 6202A – Siret : 42169477900057
N° Déclaration d'activité : 119 211 300 92 – Cet enregistrement ne vaut pas agrément de l'État.

d'algorithmes de chiffrement et la longueur de clé
- Les autorités de certification
- Les communications chiffrées par Transport Layer Security et Secure Sockets Layer
- Les infrastructures à clé publique
- Les règles de sécurité

Par ailleurs, une maîtrise des principes de base des outils de ligne et des environnements du système d'exploitation Linux ainsi qu'une expérience dans le domaine de l'exploitation de systèmes, y compris en ce qui concerne le déploiement et la gestion d'applications sur site ou dans un environnement de cloud public, sont attendues.

Enfin, les participants doivent savoir lire du code rédigé en Python ou JavaScript !

Certification Professional Cloud Security Engineer

- Durée : 2 heures
- Langues : anglais, japonais
- Format de l'examen : 50 à 60 questions à choix et sélections multiples
- Expérience recommandée : au moins trois ans d'expérience dans le secteur, dont plus d'un an dans la conception et la gestion de solutions à l'aide de Google Cloud

Contenu du cours

Principes de bases liés à la sécurité dans Google Cloud Platform

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
Rôles IAM GCP, y compris les rôles personnalisés
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 les partenaires de Google

Surveillance, journalisation, audits et analyses

Stackdriver Monitoring et Stackdriver Logging
Journaux de flux VPC
Cloud Audit Logging
Déployer et utiliser Forseti

PLB – 3-5 rue Maurice Ravel – 92 300 Levallois-Perret – Tél. : 01 43 34 90 94 – www.plb.fr
SAS au capital de 100 000 € – RCS Nanterre B 421 694 779 – APE 6202A – Siret : 42169477900057
N° Déclaration d'activité : 119 211 300 92 – Cet enregistrement ne vaut pas agrément de l'État.

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 Google 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

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

Moyens pédagogiques et techniques

Les formations PLB sont conçues et animées par des experts en activité.
Les **cours pratiques** alternent **travaux pratiques** , concrets et progressifs construits sous forme de projet fil rouge, **et apports théoriques** (en moyenne 60% de travaux pratiques, 40% de théorie).

PLB – 3-5 rue Maurice Ravel – 92 300 Levallois-Perret – Tél. : 01 43 34 90 94 – www.plb.fr
SAS au capital de 100 000 € – RCS Nanterre B 421 694 779 – APE 6202A – Siret : 42169477900057
N° Déclaration d'activité : 119 211 300 92 – Cet enregistrement ne vaut pas agrément de l'État.

Les **séminaires** font alterner **études de cas et démonstrations** concrètes, issues de l'expérience terrain de nos formateurs, **et apports théoriques.**
Le support de cours et le cahier d'exercices incluant les corrigés sont fournis en français, au format PDF, et sont téléchargeables.
Chaque participant, en présentiel ou en classe virtuelle, accède aux travaux pratiques ou aux démonstrations via un poste de travail qui lui est dédié, configuré et équipé des logiciels et outils spécifiques présentés dans cette formation, dans leur dernière version.
Les cours et examens de certification officiels suivent les conditions de l'éditeur, du constructeur ou du certificateur. Ils sont susceptibles d'évoluer à tout moment.
La plupart des formations peuvent être suivies indifféremment en présentiel ou en classe à distance synchrone depuis votre entreprise ou votre domicile (voir les Modalités pédagogiques, techniques et de suivi spécifiques aux formations à distance).
Les salles sont équipées pour accueillir ces deux modalités: vidéoprojecteur, écran/tableau interactif, webcam et sonorisation, accès Internet très haut débit et espace documentaire partagé.
L'accès aux ressources pédagogiques, techniques et de suivi s'effectue via un espace personnel 100% digital.
Le service d'assistance technique est joignable par chat et téléphone avant et pendant la formation.
Nos bâtiments sont classés ERP 5. En cas de handicap, contactez-nous par téléphone ou via l'adresse accessibilite@plb.fr afin de mettre en place l'équipement et l'accompagnement adaptés.

Modalités de suivi et d'évaluation

Les pré-requis sont évalués **par QCM** avant l'entrée en formation.
Les participants réalisent, **en début et en fin de formation, une auto-évaluation** de leurs connaissances et compétences au regard des objectifs pédagogiques de la formation.
L'évaluation des acquis en cours de formation est réalisée au fur et à mesure **des études de cas et/ou Travaux Pratiques** (50% du temps minimum pour les cours pratiques) **et/ou sous forme de QCM.**
L'évaluation en fin de formation est réalisée de la même façon et/ou via **le questionnaire d'auto-évaluation** qui permet de mesurer l'évolution par rapport au début de la formation et/ou par le passage de l'examen de certification, le cas échéant.
Les convocations, avec horaires définitifs, lieu et plan d'accès, sont envoyées deux semaines avant le début de la formation.
Les participants en classe virtuelle reçoivent leurs éléments de connexion par e-mail.
La feuille de présence numérique est à signer par demi-journée.
En fin de formation, les participants remplissent un questionnaire de satisfaction global.
Une attestation de réalisation est remise à la fin de la formation.
Si les conditions le permettent, nous pouvons inscrire jusqu'à 24h avant le début de la session. En cas d'inscription via le site Moncompteformation, un délai de 11 jours ouvrés minimum est à respecter entre la proposition de commande et l'entrée en formation.

INSCRIVEZ-VOUS
À CETTE FORMATION

PLB – 3-5 rue Maurice Ravel – 92 300 Levallois-Perret – Tél. : 01 43 34 90 94 – www.plb.fr
SAS au capital de 100 000 € – RCS Nanterre B 421 694 779 – APE 6202A – Siret : 42169477900057
N° Déclaration d'activité : 119 211 300 92 – Cet enregistrement ne vaut pas agrément de l'État.