+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 31/08/2026

S'inscrire

Formation Certification GIAC GCLD®

5 jours (35 heures)

Présentation

La certification officielle GIAC Cloud Security Essentials valide votre capacité à protéger des environnements cloud grâce à des contrôles préventifs, détectifs et réactifs.

La formation Formation Certification GIAC GCLD prépare à la certification officielle GIAC Cloud Security Essentials, dédiée aux professionnels chargés de sécuriser des charges de travail dans des environnements cloud publics et multicloud. Vous développerez une vision opérationnelle des risques, des responsabilités partagées et des mécanismes de défense adaptés aux services cloud.

Vous apprendrez à évaluer les modèles de services, à sécuriser les identités, les accès externes, les réseaux, les ressources de calcul, les conteneurs, le stockage et les données sensibles. La formation couvre également la journalisation, la supervision réseau, la gestion des secrets, l'automatisation et les pratiques DevSecOps.

Les mises en situation vous permettront d'appliquer les objectifs de l'examen à des cas de configuration, d'audit et de réponse à incident. Vous saurez analyser une exposition cloud, sélectionner des contrôles adaptés et interpréter les traces utiles à la détection d'une activité suspecte.

À l'issue de la formation, vous disposerez d'une méthode structurée pour préparer l'examen GIAC Cloud Security Essentials, organiser vos révisions et valider les compétences attendues en sécurité cloud. Vous serez également en mesure de mobiliser ces acquis dans vos activités de protection, de conformité et d'amélioration continue.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Maîtriser les domaines de compétences évalués par la certification GIAC Cloud Security Essentials.
- Analyser les responsabilités partagées et les principaux risques des environnements cloud et multicloud.
- Sécuriser les identités, les accès, les réseaux, les ressources de calcul et les données cloud.
- Exploiter la journalisation, la supervision et les mécanismes de réponse à incident dans le cloud.
- Préparer efficacement l'examen grâce à des cas pratiques et des entraînements ciblés.

Public visé

- Ingénieur sécurité cloud
- Analyste sécurité
- Administrateur systèmes et cloud
- Ingénieur DevOps
- Auditeur sécurité

Pré-requis

- Connaissances des fondamentaux de la sécurité des systèmes d'information.
- Expérience des concepts d'administration réseau, de segmentation et de contrôle d'accès.
- Compréhension des services cloud, des comptes, des rôles et des politiques d'accès.
- Notions de scripts ou d'automatisation avec Python, PowerShell ou un langage équivalent.

Pré-requis techniques

- Ordinateur équipé de Windows 10 ou 11, macOS ou Linux, avec 8 Go de RAM minimum.
- Navigateur récent Google Chrome, Mozilla Firefox ou Microsoft Edge.
- Connexion Internet stable autorisant l'accès aux consoles et environnements de laboratoire cloud.
- Compte de messagerie professionnel et droits permettant de créer ou d'utiliser des comptes de démonstration cloud.

Programme de notre formation GIAC GCLD®

[Jour 1 - Matin]

Fondamentaux et stratégie de préparation

- Présentation de la certification GIAC Cloud Security Essentials et des compétences évaluées.
- Structure de l'examen, typologie des questions et stratégie de gestion du temps.
- Panorama des modèles IaaS, PaaS, SaaS et des environnements multicloud.
- Répartition des responsabilités entre fournisseur cloud et client.
- Identification des actifs, des menaces et des surfaces d'attaque cloud.

- Atelier pratique : analyser un scénario de migration cloud et établir la matrice de responsabilités partagées.

[Jour 1 - Après-midi]

Identités, comptes et accès externes

- Principes de gestion des identités et des accès dans les plateformes cloud.
- Comptes humains, comptes de service, rôles, fédération et authentification multifacteur.
- Application du moindre privilège et conception de politiques d'autorisation.
- Sécurisation des intégrations tierces, des accès API et des relations de confiance.
- Détection des erreurs fréquentes liées aux privilèges excessifs et aux secrets exposés.

[Jour 2 - Matin]

Sécurisation des réseaux cloud

- Architecture des réseaux virtuels, sous-réseaux, routage et points d'exposition.
- Groupes de sécurité, listes de contrôle d'accès et filtrage des flux.
- Segmentation, microsegmentation et isolation des environnements sensibles.
- Accès distant sécurisé, bastions, VPN et réduction de la surface d'attaque.
- Principales attaques réseau contre les ressources cloud et contre-mesures adaptées.
- Atelier pratique : auditer une architecture réseau cloud et corriger les règles de filtrage à risque.

[Jour 2 - Après-midi]

Calcul, images et déploiements sécurisés

- Principes de durcissement des machines virtuelles et des services de calcul.
- Évaluation des images, gestion des correctifs et réduction de la surface d'attaque.
- Sécurité des fonctions serverless et maîtrise des permissions d'exécution.
- Conteneurs, orchestration et isolation des charges de travail.
- Bonnes pratiques de déploiement sécurisé et contrôles de conformité initiaux.

[Jour 3 - Matin]

Protection des données et gestion des secrets

- Classification des données et risques spécifiques aux environnements mutualisés.
- Chiffrement des données au repos et en transit, gestion des clés et rotation.
- Sécurisation du stockage objet, bloc et fichier avec des politiques d'accès adaptées.
- Prévention des fuites de données et découverte des informations sensibles.
- Gestion des secrets, jetons, certificats et informations d'identification applicatives.

- Atelier pratique : sécuriser un stockage cloud contenant des données sensibles et mettre en place une stratégie de secrets.

[Jour 3 - Après-midi]

Journalisation et supervision de sécurité

- Sources de journaux cloud, événements d'audit et conservation des traces.
- Centralisation, normalisation et protection de l'intégrité des journaux.
- Journaux d'identité, d'administration, de réseau et d'accès aux données.
- Flux réseau, captures de paquets et indicateurs utiles à la détection.
- Interprétation des alertes et construction de cas d'usage de supervision.

[Jour 4 - Matin]

Automatisation et sécurité intégrée

- Principes d'Infrastructure as Code et reproductibilité des déploiements.
- Automatisation des contrôles de configuration et détection de la dérive.
- Intégration de la sécurité dans les cycles CI/CD et DevSecOps.
- Évaluation continue des ressources, politiques et pratiques de remédiation.
- Cadres de développement sécurisé, modélisation des menaces et sécurité par défaut.
- Atelier pratique : examiner un modèle d'infrastructure et identifier les contrôles de sécurité à automatiser.

[Jour 4 - Après-midi]

Risque, conformité et assurance sécurité

- Gouvernance de la sécurité cloud et gestion du risque métier.
- Évaluation des fournisseurs, des exigences contractuelles et des dépendances tierces.
- Notions de conformité, de preuve d'audit et de contrôle continu.
- Priorisation des vulnérabilités selon l'exposition, l'impact et la vraisemblance.
- Construction d'un plan d'amélioration de la posture de sécurité cloud.

[Jour 5 - Matin]

Détection, réponse et investigation

- Cycle de réponse à incident appliqué aux ressources cloud.
- Analyse d'une compromission de compte, d'une clé exposée ou d'une ressource publique.
- Collecte des preuves, préservation des journaux et investigation initiale.
- Actions de confinement, d'éradication et de remédiation dans un environnement cloud.
- Introduction aux considérations de test d'intrusion et de défense informée par les menaces.

- Atelier pratique : traiter un scénario d'incident cloud à partir de journaux, d'alertes et d'indicateurs d'exposition.

[Jour 5 - Après-midi]

Révision et préparation finale à l'examen

- Révision transversale des objectifs officiels de la certification.
- Analyse des pièges fréquents sur les identités, réseaux, données, journaux et automatisation.
- Méthode de lecture des questions, élimination des réponses incohérentes et arbitrage sous contrainte de temps.
- Organisation des révisions et préparation des ressources autorisées pour l'examen.
- Évaluation des acquis et définition des axes de consolidation individuels.
- Atelier pratique : réaliser un examen blanc ciblé, corriger les réponses et établir un plan de révision final.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.