+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 GCPN®

5 jours (35 heures)

Présentation

La formation Certification GIAC GCPN prépare à la certification officielle GIAC Cloud Penetration Tester et valide votre capacité à conduire des tests d'intrusion cloud sur des environnements modernes.

La certification GIAC Cloud Penetration Tester évalue les compétences nécessaires pour analyser la sécurité des systèmes, réseaux, architectures et services cloud. Elle couvre la découverte d'environnements, l'identification des surfaces d'attaque et l'exploitation contrôlée de faiblesses dans des contextes AWS, Azure et cloud natif.

Notre formation Certification GIAC GCPN vous permet de structurer votre préparation à l'examen, d'assimiler les domaines évalués et de consolider les méthodes de raisonnement attendues. Vous apprendrez à cartographier une cible cloud, à évaluer les identités et permissions, à analyser les configurations exposées et à documenter des scénarios d'attaque réalistes.

Vous étudierez les attaques sur les services cloud, les applications web, les fonctions serverless, les conteneurs et les chaînes CI/CD. Les ateliers mettent en pratique les techniques de reconnaissance, d'escalade de privilèges, de pivot, de contournement et de remédiation dans un cadre autorisé.

À l'issue de la formation, vous serez en mesure d'aborder l'examen avec une méthode efficace, d'identifier les objectifs à réviser et de mobiliser les compétences validées par la certification GIAC Cloud Penetration Tester dans des missions de pentest cloud.

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

Objectifs

- Maîtriser les domaines et le format de l'examen GIAC Cloud Penetration Tester
- Cartographier une surface d'attaque dans des environnements AWS et Azure
- Évaluer les identités, permissions, configurations et services cloud exposés
- Analyser les risques liés aux applications cloud natives, aux conteneurs et aux pipelines CI/CD
- Appliquer une méthodologie de test d'intrusion cloud éthique et produire des recommandations de remédiation
- Construire une stratégie de préparation efficace pour la certification

Public visé

- Pentester
- Consultant cybersécurité
- Analyste vulnérabilités
- Ingénieur sécurité cloud
- Ingénieur DevOps

Pré-requis

- Expérience pratique des tests d'intrusion et de la reconnaissance réseau
- Connaissances des services, identités et permissions AWS ou Azure
- Maîtrise des commandes Linux et des bases du scripting Python ou Bash
- Compréhension des protocoles réseau, du HTTP, du DNS et du TLS
- Notions de sécurité des conteneurs Docker et des pipelines CI/CD

Pré-requis techniques

- Ordinateur doté d'un processeur récent, de 16 Go de RAM recommandés et de 50 Go d'espace disque disponible
- Système d'exploitation Windows 11, macOS récent ou distribution Linux compatible avec la virtualisation
- Solution de virtualisation VirtualBox 7 ou VMware Workstation installée et fonctionnelle
- Navigateur Google Chrome ou Mozilla Firefox à jour, avec une connexion Internet stable
- Accès autorisé à un environnement de laboratoire cloud et absence de filtrage bloquant les outils pédagogiques

Programme de notre formation GIAC GCPN®

[Jour 1 - Matin]

Cadre de certification et méthodologie du pentest cloud

- Présentation de la certification GIAC Cloud Penetration Tester, des domaines évalués et des compétences validées

- Compréhension du format d'examen, de la gestion du temps et de l'exploitation méthodique des ressources autorisées
- Principes du test d'intrusion cloud, cadre légal, règles d'engagement et périmètre d'autorisation
- Cycle d'un audit offensif, de la reconnaissance à la restitution des résultats
- Modélisation des responsabilités partagées et des surfaces d'attaque dans le cloud

[Jour 1 - Après-midi]

Reconnaissance et cartographie des environnements cloud

- Collecte de renseignements publics, empreinte numérique et identification des actifs exposés
- Découverte des domaines, sous-domaines, adresses IP, services web et endpoints d'API
- Énumération des ressources cloud accessibles et analyse des métadonnées utiles au pentest
- Priorisation des cibles selon leur exposition, leur criticité et les chemins d'attaque possibles
- Constitution d'une cartographie exploitable pour les cas pratiques et les questions d'examen
- Atelier pratique : cartographier la surface d'attaque d'une organisation fictive et produire un inventaire priorisé des actifs cloud

[Jour 2 - Matin]

Identités, permissions et attaques AWS

- Rappels sur les modèles d'identité, rôles, politiques et mécanismes d'authentification AWS IAM
- Recherche de secrets, clés d'accès, jetons temporaires et informations d'identification exposées
- Analyse des erreurs de configuration relatives aux permissions, aux rôles de service et aux relations d'approbation
- Énumération des services AWS et identification des vecteurs d'escalade de privilèges
- Bonnes pratiques de remédiation, principe du moindre privilège et journalisation des actions sensibles

[Jour 2 - Après-midi]

Stockage, réseau et exposition des services AWS

- Évaluation de la sécurité des stockages objets, volumes, instantanés et sauvegardes AWS
- Analyse des groupes de sécurité, listes de contrôle réseau, routes et points d'entrée exposés
- Recherche de configurations faibles dans les services de calcul et les services managés
- Identification des risques liés aux métadonnées d'instance et aux rôles associés aux workloads
- Lecture de scénarios de certification portant sur les chemins d'accès et les impacts métier
- Atelier pratique : analyser un environnement AWS de laboratoire, identifier les mauvaises configurations et proposer un plan de correction priorisé

[Jour 3 - Matin]

Identités, ressources et attaques Azure

- Architecture des identités Microsoft Entra ID, rôles, applications et principaux de service
- Recherche des chemins d'accès entre identités, abonnements, groupes de ressources et workloads Azure
- Évaluation des droits excessifs, consentements d'applications et secrets de comptes de service
- Découverte des ressources Azure et analyse des expositions de services courants
- Identification des mécanismes de défense, de journalisation et de limitation des privilèges

[Jour 3 - Après-midi]

Scénarios d'attaque et pivot dans Azure

- Analyse des vecteurs d'attaque sur les machines virtuelles, comptes de stockage, fonctions et services web
- Exploitation contrôlée de secrets exposés, de permissions déléguées et de configurations réseau faibles
- Techniques de pivot, de relais et d'obfuscation adaptées à un environnement cloud autorisé
- Corrélation des observations techniques avec les risques sur les données et les services métier
- Préparation de réponses synthétiques aux scénarios de type examen
- Atelier pratique : suivre un chemin d'attaque Azure en laboratoire, de l'identité exposée à l'accès à une ressource sensible

[Jour 4 - Matin]

Applications web et services cloud natifs

- Spécificités des attaques sur les applications web déployées dans le cloud
- Étude des vulnérabilités d'authentification, de contrôle d'accès, d'injection et de gestion de session
- Analyse des API, des passerelles d'API et des fonctions serverless
- Compréhension des mécanismes de redirection, de proxy, de contournement et d'obfuscation de commandes
- Identification des contrôles de sécurité applicatifs et des pistes de remédiation

[Jour 4 - Après-midi]

Conteneurs, orchestration et chaînes CI/CD

- Surface d'attaque des images, registres, conteneurs et plateformes d'orchestration
- Recherche de secrets, privilèges excessifs et erreurs de configuration dans les manifestes et images
- Risques liés aux comptes de service, volumes montés et communications interservices
- Évaluation de la sécurité des pipelines CI/CD, dépôts de code et mécanismes de livraison
- Mise en place de contrôles de prévention, détection et durcissement adaptés
- Atelier pratique : auditer une chaîne CI/CD et un déploiement conteneurisé afin d'identifier les secrets et privilèges à risque

[Jour 5 - Matin]

Consolidation des compétences et stratégie d'examen

- Révision transversale des objectifs : reconnaissance, services cloud, identités, applications et cloud natif
- Analyse de cas de certification associant AWS, Azure, applications web et conteneurs
- Méthode de lecture des questions, qualification des indices et élimination des réponses non pertinentes
- Organisation d'un index de révision et repérage rapide des notions à consolider
- Gestion du temps, des points de blocage et de la progression pendant l'épreuve surveillée

[Jour 5 - Après-midi]

Mise en situation de certification et restitution

- Résolution de scénarios couvrant la découverte, l'exploitation, le pivot et la remédiation
- Correction collective des raisonnements techniques et clarification des notions sensibles
- Revue des erreurs fréquentes relatives aux identités, aux stockages, aux réseaux et aux services managés
- Préparation finale au passage de la certification GIAC Cloud Penetration Tester
- Formalisation d'un plan de révision individuel après la formation
- Atelier pratique : réaliser une simulation sur un cas de pentest cloud complet, puis justifier les choix techniques et les recommandations

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.