+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 GCIH®

Présentation

La formation Certification GIAC GCIH prépare au passage de la certification officielle GIAC Certified Incident Handler et valide votre capacité à détecter, analyser, contenir et résoudre des incidents de sécurité informatique.

La certification GIAC GCIH s'adresse aux professionnels impliqués dans la réponse aux incidents, l'investigation technique et la défense des systèmes. Elle évalue des compétences opérationnelles couvrant les techniques d'attaque, l'analyse des traces et la remédiation face à des scénarios réalistes.

Notre formation Certification GIAC GCIH vous permettra de structurer votre préparation à l'examen, de réviser les domaines évalués et de consolider votre maîtrise des méthodes de traitement d'incident. Vous apprendrez à identifier les vecteurs d'intrusion, à qualifier les activités malveillantes et à appliquer des mesures de confinement adaptées.

Vous travaillerez les sujets essentiels de la certification, dont le scan réseau, les attaques sur les mots de passe, les services SMB, les outils tels que Nmap, Metasploit et Netcat, ainsi que les attaques visant les applications web, les API et les environnements cloud.

À l'issue de la formation, vous serez en mesure de préparer efficacement l'examen GIAC Certified Incident Handler, de mobiliser les bons réflexes lors d'un incident et de démontrer des compétences pratiques en détection, investigation, confinement et remédiation.

Objectifs

- Maîtriser les domaines techniques évalués par la certification GIAC Certified Incident Handler
- Identifier et qualifier les techniques d'attaque courantes afin d'accélérer la réponse aux incidents
- Analyser des traces réseau et système avec les outils essentiels de l'investigation
- Appliquer des stratégies de confinement, d'éradication et de remédiation adaptées
- Préparer une stratégie de révision, d'indexation et de gestion du temps pour l'examen GIAC GCIH

Public visé

- Analyste SOC
- Incident Responder
- Administrateur système
- Ingénieur cybersécurité
- Consultant sécurité

Pré-requis

- Connaissances des fondamentaux de la cybersécurité et de la réponse aux incidents
- Maîtrise courante des environnements Windows et Linux
- Connaissances des réseaux TCP/IP, des services réseau et des journaux système
- Notions d'administration des comptes, des droits et des services SMB

Pré-requis techniques

- Ordinateur équipé de Windows 10 ou 11, macOS ou Linux, avec droits d'installation locaux
- Processeur compatible virtualisation, au moins 16 Go de RAM et 80 Go d'espace disque disponible
- Installation de VMware Workstation Player, VMware Fusion ou VirtualBox dans une version récente
- Connexion Internet stable, sans filtrage bloquant les téléchargements, les machines virtuelles et les services de laboratoire

Programme de notre formation GIAC GCIH®

[Jour 1 - Matin]

Cadre de la certification et réponse aux incidents

- Positionnement de la certification GIAC Certified Incident Handler et compétences validées
- Format de l'examen, gestion du temps, politique open book et préparation des supports papier
- Cycle de vie de la réponse aux incidents : préparation, détection, analyse, confinement, éradication et retour d'expérience
- Qualification d'une alerte, collecte initiale des informations et préservation des éléments utiles
- Construction d'un plan de révision par objectifs et création d'un index de référence exploitable le jour de l'examen

[Jour 1 - Après-midi]

Reconnaissance, scan et cartographie réseau

- Principes de reconnaissance, d'énumération et de cartographie des actifs exposés
- Lecture des échanges TCP/IP, identification des ports, services, bannières et erreurs de configuration
- Utilisation de Nmap pour le scan d'hôtes, de ports, de versions et de scripts ciblés
- Interprétation des résultats de scan et priorisation des risques pour l'investigation
- Atelier pratique : cartographier un réseau de laboratoire avec Nmap, identifier les services exposés et produire une première hypothèse d'investigation

[Jour 2 - Matin]

Exploitation, shells et communications furtives

- Panorama des vulnérabilités exploitables et articulation entre exploitation, post-exploitation et réponse défensive
- Fonctionnement de Metasploit, modules, charges utiles et limites d'usage dans un contexte d'analyse
- Rôle de Netcat, shells distants, redirections de ports et communications de commande et contrôle
- Détection des comportements anormaux liés aux connexions sortantes, aux tunnels et aux services inattendus
- Préparation aux questions de certification sur les outils d'exploitation et les canaux de communication covert

[Jour 2 - Après-midi]

Détection et analyse des techniques d'évasion

- Indicateurs de compromission, chronologie d'attaque et corrélation entre événements réseau et système
- Persistance, élévation de privilèges, dissimulation de processus et techniques de post-exploitation
- Analyse des mécanismes d'évasion : encodage, obfuscation, suppression de traces et contournement des contrôles
- Mesures de défense : journalisation, surveillance des processus, règles de détection et validation des alertes
- Atelier pratique : analyser un scénario de persistance et d'évasion, reconstituer la chronologie puis définir les actions de confinement

[Jour 3 - Matin]

Attaques sur les mots de passe et les identifiants

- Fonctionnement des mots de passe, empreintes, salage et principales faiblesses d'authentification
- Techniques d'attaque : dictionnaire, force brute, réutilisation d'identifiants et interception de secrets
- Reconnaissance des artefacts d'attaque et choix de mesures de protection adaptées
- Gestion des identifiants privilégiés, rotation des secrets et réponse à une compromission de comptes

- Points de vigilance pour les objectifs de certification relatifs à la compréhension et à la sécurisation des mots de passe

[Jour 3 - Après-midi]

SMB et investigation sur les services internes

- Architecture et usages du protocole SMB dans les environnements Windows
- Énumération des partages, permissions, accès anonymes et risques de configuration
- Techniques d'attaque sur SMB : accès aux partages, mouvement latéral et abus d'identifiants
- Détection des activités SMB suspectes et mesures de durcissement du service
- Atelier pratique : investiguer un partage SMB de laboratoire, identifier une exposition de données et proposer un plan de remédiation priorisé

[Jour 4 - Matin]

Attaques web et sécurité des API

- Principes de fonctionnement des applications web, requêtes HTTP, sessions et mécanismes d'authentification
- Vecteurs d'attaque courants : injection, contournement d'accès, manipulation de paramètres et exposition de données
- Spécificités des API : jetons, autorisations, contrôle d'accès objet et validation des entrées
- Identification des traces d'exploitation dans les journaux applicatifs et les flux réseau
- Révision orientée certification des scénarios de compromission d'applications web et d'API

[Jour 4 - Après-midi]

Identifiants et données dans le cloud

- Risques liés aux identifiants cloud, aux secrets exposés et aux stockages insuffisamment protégés
- Analyse des erreurs de configuration, des droits excessifs et des accès non autorisés aux données
- Détection des abus de comptes, de clés d'accès et de jetons dans un environnement cloud
- Actions de confinement : révocation, rotation des secrets, réduction des privilèges et collecte des journaux
- Atelier pratique : traiter un incident de fuite d'identifiants cloud, qualifier l'impact, contenir l'accès et formaliser les actions correctives

[Jour 5 - Matin]

Conduite d'incident et consolidation des acquis

- Organisation d'une investigation : hypothèses, périmètre, priorités, preuves et décisions de réponse
- Stratégies de confinement et d'éradication selon le vecteur d'attaque et le niveau de compromission
- Communication technique, documentation des actions et préparation du retour d'expérience
- Synthèse transversale des objectifs GCIH® et identification des sujets à renforcer
- Atelier pratique : piloter une réponse à incident de bout en bout à partir d'un cas multi-vecteurs, de l'alerte initiale à la remédiation

[Jour 5 - Après-midi]

Préparation finale à l'examen

- Révision ciblée des domaines de l'examen : scan, exploitation, évasion, mots de passe, SMB, cloud, web et API
- Méthode de lecture des questions, élimination des distracteurs et arbitrage face aux cas ambigus
- Optimisation de l'index personnel, classement des références et gestion du temps sur quatre heures
- Préparation aux mises en situation CyberLive et aux exigences du passage surveillé
- Atelier pratique : réaliser un examen blanc chronométré, corriger les réponses et finaliser son plan de préparation à la certification

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.