+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 GCFA®

5 jours (35 heures)

Présentation

La formation Certification GIAC GCFA vous prépare à la certification officielle GIAC Certified Forensic Analyst et vous permet de maîtriser les méthodes avancées de forensic numérique, de réponse à incident et de threat hunting.

Cette formation vous accompagne dans la préparation de l'examen GIAC GCFA, une certification reconnue pour valider votre capacité à conduire des investigations formelles sur des systèmes compromis. Vous développerez une approche rigoureuse pour analyser les intrusions, identifier les techniques adverses et produire des conclusions exploitables.

Vous apprendrez à examiner les artefacts Windows, les structures NTFS, les traces d'exécution, les données de restauration et les éléments volatils présents en mémoire. Les mises en situation vous aideront à reconstruire l'activité d'un attaquant, à détecter des mécanismes d'anti-forensic et à prioriser les preuves utiles.

À l'issue de la formation, vous serez en mesure de conduire une investigation à l'échelle d'un environnement d'entreprise, de construire des frises chronologiques, d'analyser les indicateurs de compromission et de documenter une réponse adaptée. Vous préparerez également votre stratégie d'examen, vos supports papier et votre gestion du temps face aux exercices pratiques CyberLive.

La formation aborde enfin les conditions de passage de la certification GIAC Certified Forensic Analyst, les réflexes attendus lors d'un examen surveillé et les bonnes pratiques permettant de consolider vos acquis avant la présentation à l'examen.

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

Objectifs

- Maîtriser les compétences évaluées par la certification GIAC Certified Forensic Analyst
- Analyser les artefacts Windows et les structures NTFS dans le cadre d'une investigation
- Examiner la mémoire vive afin d'identifier processus, connexions et activités malveillantes
- Reconstruire une chronologie d'intrusion et qualifier les techniques d'un attaquant
- Conduire une réponse à incident structurée dans un environnement d'entreprise
- Préparer efficacement l'examen GIAC GCFA et ses mises en situation pratiques

Public visé

- Analyste forensic
- Analyste SOC
- Analyste réponse à incident
- Threat hunter
- Consultant cybersécurité

Pré-requis

- Expérience en investigation sur systèmes Windows
- Connaissances des fondamentaux de la réponse à incident et de l'analyse de journaux
- Maîtrise des notions de base des systèmes de fichiers NTFS
- Connaissances pratiques des processus, services et mécanismes de persistance Windows
- Lecture technique de documentation en anglais

Pré-requis techniques

- Poste sous Windows 10 ou Windows 11 avec droits d'installation locaux
- Processeur compatible virtualisation matérielle et au moins 16 Go de RAM
- Outil de virtualisation VMware Workstation ou VirtualBox installé et fonctionnel
- Au moins 80 Go d'espace disque libre pour les images et jeux de preuves
- Connexion Internet stable, sans filtrage bloquant les téléchargements de logiciels et de machines virtuelles

Programme de notre formation GIAC GCFA®

[Jour 1 - Matin]

Cadre de la certification et démarche forensic

- Présentation de la certification GIAC Certified Forensic Analyst et des compétences évaluées
- Format de l'examen, environnement surveillé, gestion du temps et préparation des supports autorisés
- Rôle de l'analyste dans la réponse à incident et articulation avec le SOC
- Cycle d'investigation : préparation, collecte, analyse, qualification et restitution
- Chaîne de conservation, intégrité des preuves et traçabilité des actions

- Atelier pratique : analyser un scénario d'intrusion et définir un plan d'investigation priorisé

[Jour 1 - Après-midi]

Fondamentaux des artefacts Windows

- Architecture Windows, comptes, services, processus et emplacements clés
- Sources de preuves sur disque, en mémoire et dans les journaux système
- Artefacts d'exécution et de persistance : principes d'interprétation
- Collecte ciblée et distinction entre activité normale, suspecte et malveillante
- Méthode de prise de notes et construction d'un index de révision pour l'examen
- Atelier pratique : identifier les artefacts pertinents dans une image Windows compromise

[Jour 2 - Matin]

Analyse NTFS et investigation sur disque

- Organisation du système de fichiers NTFS et couches de données, métadonnées et noms de fichiers
- Lecture des entrées de la MFT et interprétation des attributs principaux
- Analyse des horodatages et détection des incohérences temporelles
- Fichiers supprimés, données résidentes et non résidentes, liens et flux alternatifs
- Recherche d'indices de dissimulation et d'anti-forensic sur le stockage

[Jour 2 - Après-midi]

Exécution, persistance et traces utilisateur

- Analyse des preuves d'exécution de programmes et de scripts
- Artefacts liés aux utilisateurs, aux documents récents et aux périphériques
- Points de persistance : registre, tâches planifiées, services et dossiers de démarrage
- Corrélation des traces pour caractériser une chaîne d'attaque
- Préparation aux questions de certification portant sur les artefacts Windows
- Atelier pratique : reconstituer l'exécution d'un outil malveillant et son mécanisme de persistance

[Jour 3 - Matin]

Forensic mémoire et activité volatile

- Principes d'acquisition et d'analyse de la mémoire vive
- Processus, threads, handles, pilotes et connexions réseau en mémoire
- Détection des processus anormaux, des injections de code et des rootkits
- Analyse des lignes de commande, objets résidents et artefacts réseau volatils
- Qualification des preuves mémoire au regard du contexte système

[Jour 3 - Après-midi]

Détection des techniques adverses

- Étapes d'une intrusion avancée et raisonnement fondé sur les comportements adverses
- Identification des accès initiaux, mouvements latéraux et élévations de privilèges
- Techniques d'évasion, de camouflage et d'anti-forensic
- Indicateurs de compromission et hypothèses de chasse aux menaces
- Passage de l'observation technique à la qualification d'un incident
- Atelier pratique : analyser une capture mémoire pour identifier une injection de code et une connexion suspecte

[Jour 4 - Matin]

Chronologie et corrélation des preuves

- Construction d'une timeline multi-sources pour une investigation
- Normalisation des horodatages, fuseaux horaires et gestion des dérives temporelles
- Corrélation des données disque, mémoire, registre et journaux
- Détection des séquences d'attaque et des ruptures dans une chronologie
- Priorisation des événements et formulation de conclusions vérifiables

[Jour 4 - Après-midi]

Réponse à incident à l'échelle entreprise

- Évaluation rapide d'un périmètre compromis dans un environnement d'entreprise
- Stratégies de collecte et d'analyse à grande échelle
- Coordination entre analystes, équipes systèmes, réseau et sécurité
- Confinement, éradication et validation de la remédiation
- Production d'un rapport d'investigation clair, factuel et exploitable
- Atelier pratique : prioriser les actions de réponse à incident dans un scénario de compromission multi-postes

[Jour 5 - Matin]

Préparation ciblée à l'examen GCFA

- Révision structurée des domaines évalués par la certification GIAC GCFA®
- Analyse des pièges fréquents et des critères de décision dans les cas forensic
- Organisation d'un index papier efficace pour un examen en ressources documentaires
- Stratégies de résolution pour les questions théoriques et les exercices CyberLive
- Gestion du temps, contrôle des réponses et maintien de la rigueur analytique

[Jour 5 - Après-midi]

Mise en situation de certification

- Rappel des objectifs, du format et des règles de passage de l'examen
- Résolution de cas transverses combinant disque, mémoire et artefacts Windows
- Justification des conclusions à partir de preuves techniques corrélées
- Auto-évaluation des acquis et identification des axes de révision individuels
- Plan de préparation final avant la présentation à la certification officielle
- Atelier pratique : réaliser une simulation d'investigation, puis restituer la chronologie et les conclusions

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.