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

Mis à jour le 03/03/2026

S'inscrire

Formation Certification Ec-council CIH™

3 jours (21 heures)

Présentation

La formation EC-Council CIH™ vous prépare à conduire des investigations numériques de bout en bout : collecte, analyse et restitution. Elle s’adresse aux contextes d’incident de sécurité, de fraude ou de litige nécessitant des preuves exploitables.

Vous apprenez à appliquer une méthodologie forensique rigoureuse : préservation de la scène, chaîne de possession, acquisition fiable, analyse et reporting. L’objectif est de produire des résultats défendables, en limitant les biais et en respectant les contraintes légales et organisationnelles.

L’approche de notre formation est résolument pratique : ateliers guidés, démos d’outils, mini-cas réalistes (poste de travail, artefacts système, traces réseau). Les livrables incluent des checklists d’intervention, un modèle de rapport, et des procédures d’acquisition/triage réutilisables.

Objectifs

- Structurer une investigation selon une méthodologie forensique.
- Préserver et documenter les preuves (chaîne de possession).
- Réaliser des acquisitions et un triage en sécurité.
- Analyser des artefacts système et des journaux pertinents.
- Rédiger un rapport clair, reproductible et exploitable.

Public visé

- Analystes SOC / CSIRT
- Administrateurs systèmes et réseaux
- Consultants cybersécurité / réponse à incident
- Auditeurs techniques

Pré-requis

- Bases solides en Windows et/ou Linux (process, fichiers, permissions)
- Notions de réseaux TCP/IP et de logs
- Compréhension des concepts sécurité (IOC, malware, persistance)
- Rigueur documentaire et bonnes pratiques d’investigation

Pré-requis techniques

- PC avec 16 Go RAM recommandés (8 Go minimum) et 40 Go libres
- Windows 10/11 ou Linux (VM autorisée), droits d’installation
- Virtualisation activée (Hyper-V/VirtualBox/VMware)
- Outils : éditeur de texte, terminal, utilitaires de hash (SHA-256)

Programme de notre formation EC-Council CIH™ : Incident Handling & Forensics

[Jour 1 - Matin]

Méthodologie IH et Préparation de l'Environnement

- Le cycle de vie de l'incident (NIST vs SANS) : Préparation, Détection, Confinement
- Cadre légal et éthique : Intégrité des preuves et chaîne de conservation (Chain of Custody)
- Poste d'analyse : Mise en place d'une machine virtuelle d'enquête (SIFT Workstation)
- Collecte de preuves : Ordre de volatilité et acquisition (Disque vs RAM)
- Atelier pratique : Création d'un kit d'enquête et acquisition d'une image avec validation par Hash.

[Jour 1 - Après-midi]

Forensique Système : Windows & Linux

- Artefacts Windows : Registre (Run keys), Prefetch, Shimcache et Journaux d'événements
- Traces Linux : Cronjobs, SSH keys, Systemd services et Bash history
- Analyse de la chronologie : Création d'une Super-Timeline pour corréler les événements
- Gestion des artefacts volatils : processus, connexions et sessions actives
- Atelier pratique : Analyse d'une image disque pour identifier le vecteur d'entrée et la persistance.

[Jour 2 - Matin]

Analyse Mémoire et Détection de Malwares

- Analyse RAM avancée : Utilisation de Volatility (Processus, DLL, Sockets)
- Détection d'anomalies : Injections de code et processus orphelins
- Triage de Malware : Analyse statique rapide (Strings, Entropy, Capa)
- Analyse dynamique en Sandbox et extraction d'indicateurs (IOCs)
- Atelier pratique : Extraction d'un malware depuis un dump mémoire et analyse de ses capacités.

[Jour 2 - Après-midi]

Investigation Réseau et Flux de Données

- Analyse de trafic (PCAP) : Identification des balises de Command & Control (C2)
- Protocoles critiques : Analyse DNS, HTTP/S (certificats) et tunnels
- Corrélation avec les logs d'infrastructure : Firewall, Proxy et SIEM
- Reconstruction de sessions et extraction de fichiers transférés
- Atelier pratique : Analyse d'une capture réseau pour reconstruire un scénario d'exfiltration.

[Jour 3 - Matin]

Forensique Applicative et Cloud

- Traces Utilisateurs : Navigateurs Web (historique, cache) et Mail (Phishing)
- Introduction aux incidents Cloud : Spécificités des logs AWS/Azure (CloudTrail)
- Automatisation du triage : Scripts de collecte rapide pour les IOCs
- Corrélation utilisateur : Retracer le "qui, quoi, quand" depuis le contexte applicatif
- Atelier pratique : Retracer le parcours d'une infection via artefacts navigateur.

[Jour 3 - Après-midi]

Post-Incident, Reporting et Certification

- Éradication et Remédiation : Nettoyage et stratégies d'évolution
- Reporting professionnel : Synthèse managériale et annexes techniques
- Préparation à l'examen CIH : Revue des concepts, quizz et pièges fréquents
- Checklist de clôture d'incident et partage d'informations (MISP)
- Atelier pratique : Rédaction d'une synthèse d'enquête (Timeline + IOCs) et debriefing.

FAQ – QUESTIONS / RÉPONSES

Dans quelle langue la formation CIH™ vous est enseignée ?

La formation est en français.

L’examen est-il compris dans le prix de la formation ?

Oui, le prix de la certification est inclus au coût de la formation ($450 à titre indicatif). Vous pourrez passer l'examen à la fin de la session.

Comment se déroule l'examen pour la certification CIH™ ?

L'examen consiste en un QCM basé sur la performance composé de 100 **questions** maximum.

Il s'effectue en ligne dans un centre d'examen agréé Pearson Vue.

Cet examen dure **180 minutes**, les langues disponibles sont l'anglais

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.