EXPERT

FORMATION CERTIFIANTE

COMPUTER HACKING FORENSIC INVESTIGATOR V11

La certification de l'investigation numérique

Code : CHFIv11

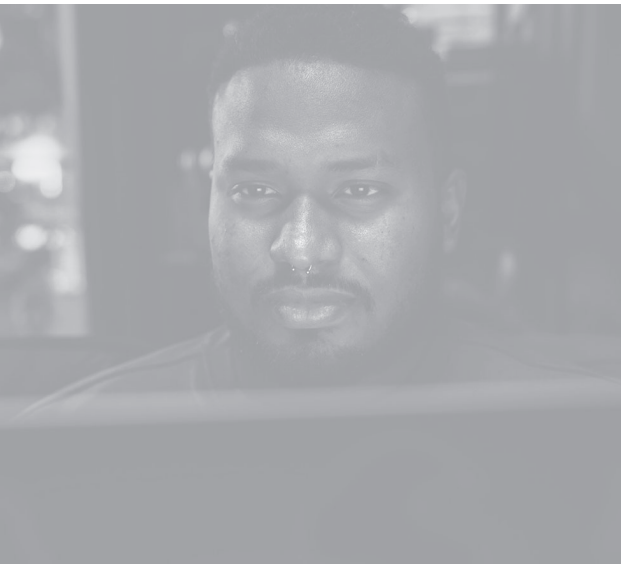
Les nouvelles technologies sont en train de changer le monde professionnel. Les entreprises s'accommodant rapidement aux technologies numériques comme le cloud, le mobile, le big data ou encore l'IoT, rendent l'étude du forensique numérique dorénavant nécessaire.
Le cours CHFIv11 a été développé pour des professionnels en charge de la collecte de preuves numériques après un cyber crime. Il a été conçu par des experts sur le sujet et des professionnels du secteur, il présente les normes mondiales en matière de bonnes pratiques forensiques. En somme, il vise également à élever le niveau de connaissances, de compréhension et de compétences en cybersécurité des acteurs du forensique.
Le programme CHFIv11 offre une approche méthodologique détaillée du forensique et de l'analyse de preuves numériques. Il apporte les compétences nécessaires à l'identification de traces laissées par un intrus mais également à la collecte de preuves nécessaires à sa poursuite judiciaire. Les outils et savoirs majeurs utilisés par les professionnels du secteur sont couverts dans ce programme. La certification renforcera le niveau de connaissances de toutes les personnes concernées par l'intégrité d'un réseau et par l'investigation numérique.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afi n de favoriser l'acquisiti on des savoirs du programme (cf. Ressources).

Modalités d'évaluation : En amont de la formation, une évaluation des compétences de l'apprenant est effectuée.

Puis, les objectifs sont régulièrement évalués tout au long de la formation (20% de cas pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur, ainsi que par le passage de la certification.



PLAN DE COURS

- **Module 1 :** Computer Forensics in Today's World
- **Module 2 :** Computer Forensics Investigation Process
- **Module 3 :** Understanding hard disks and file systems
- **Module 4 :** Data acquisition and duplication
- **Module 5 :** Defending anti-forensics techniques
- **Module 6 :** Operating system forensics
- **Module 7 :** Network forensics
- **Module 8 :** Investigating web attacks
- **Module 9 :** Database forensic
- **Module 10 :** Cloud forensic
- **Module 11 :** Malware forensic
- **Module 12 :** Investigating email crimes
- **Module 13 :** Mobile forensic
- **Module 14 :** Forensic report writing and presentation

PASSAGE DE L'EXAMEN

L'examen CHFIv11 (312-49) aura lieu à distance dans le lieu de votre choix.

Pour passer l'examen à distance, vous devrez alors disposer d'un PC, d'une webcam et d'une bonne connexion à internet.

- **Titre de l'examen :** CHFI
- **Format de l'examen :** QCM
- **Nombre de questions :** 150
- **Durée :** 4 heures
- **Langue :** anglais
- **Score requis :** il se situe entre 70% et 78%, selon la difficulté du set de questions proposées.

RÉSULTAT

Directement disponible en fin d'examen.

MAINTIEN DE LA CERTIFICATION

Pour maintenir la certification, il faudra obtenir 120 crédits dans les 3 ans avec un minimum de 20 points chaque année. Pour plus d'informations, vous pouvez consulter le site d'EC-Council.

PROCHAINES DATES

10 mars 2025
16 juin 2025
15 septembre 2025
17 novembre 2025

OBJECTIFS

- Donner aux participants les qualifications nécessaires pour identifier et analyser les traces laissées lors de l'intrusion d'un système informatique par un tiers et pour collecter correctement les preuves nécessaires à des poursuites judiciaires
- Se préparer à l'examen CHFI

INFORMATIONS GÉNÉRALES

Code : CHFIv11
Durée : 5 jours
Prix : 4 650 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) ou en distanciel
Examen : inclus. Valable 12 mois pour un passage de l'examen à distance.
Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

Toutes les personnes intéressées par le cyber forensique, avocats, consultants juridiques, forces de l'ordre, officiers de police, agents fédéraux et gouvernementaux, personnes en charge de la défense, militaires, détectives et enquêteurs, membres des équipes de réponse après incident, managers IT, défenseurs réseaux, professionnels IT, ingénieurs système/réseau, analystes/consultants/auditeurs sécurité…

PRÉ-REQUIS

- Avoir des connaissances basiques en cybersécurité forensique et gestion d'incident
- L'obtention préalable de la certification CEH est un plus

RESSOURCES

- Support de cours officiel en anglais
- Accès au cours en version numérique pendant un an
- Cours donnés en français
- 20% d'exercices pratiques
- 1 PC par personne
- Environnement Windows de démonstration et de mise en pratique