Organisme de formation professionnelle continue
Numero agrément 91 30 03332 30
France : +33 (0)188 24 70 33 / 34
Site : www.oo2.fr
Mail : contact@oo2.fr

Devenir enquêteur judiciaire certifié en piratage informatique (C|HFI)

Date et durée

Code formation : CHFI-V10
Durée : 5 jours
Nombre d'heures : 35 heures

Formation avec certification

C|HFI : Certified Hacking Forensic Investigator

Description

Le monde informatique évolue avec les nouvelles technologies et dans un contexte de transition numérique, les entreprises se tournent rapidement vers les solutions cloud, les applications mobiles, le big data et les objets connectés (IoT). Cette évolution conduit à considérer **l'étude du digital forensics** comme une véritable priorité. Développé par des experts en cybersécurité et des professionnels du domaine, cette formation CHFI v10 est une référence mondiale pour **se former aux meilleures pratiques de l'informatique légale**. Les cours sont est également conçu pour améliorer les connaissances et les compétences des personnes impliquées dans les enquêtes médico-légales dans le domaine de la cybersécurité.
À l'issue de ce **programme Hacking Forensic Investigator**, vous acquerrez une approche méthodologique complète de la criminalistique et de l'analyse des preuves numériques. Vous serez alors en mesure de transposer ces nouvelles compétences lorsque **vous passerez l'examen officiel CHFI** notre partenaire certificateur EC-Council *(plus d'infos dans l'onglet certification)*.

Objectifs

En participant à la **formation CHFI v10**, vous atteindrez les objectifs suivants :

- comprendre ce que représente l'investigation numérique ;
- connaître les techniques de récupération de fichiers supprimés et de décryptage de mots de passe ;
- agir en tant que premier intervenant lors d'une attaque informatique ;
- sécuriser et analyser la surface d'une zone d'attaque ;
- mener des enquêtes préparatoires ;
- identifier les traces numériques laissées par des attaquants et rassembler des preuves suffisantes pour engager une action en justice ;
- rédiger des rapports d'enquête complets ;
- collecter et stocker en toute sécurité des preuves numériques ;
- réussir l'examen ECHO 312-49 et obtenir la certification C|HFI du EC-Council.

Oo2 est accrédité par EC-Council pour dispenser la formation CHFI. Ce statut garantit la prestation d'un formateur agréé, des supports de cours officiels et des examens de certifications organisés immédiatement en fin de formation.

Points forts

Une formation qui aborde les rôles clés de la criminalistique numérique et qui présente les derniers outils, techniques et méthodologies. Un formateur certifié en cybersécurité. Un programme de certification reconnu par l'ANSI.

Certification

Informations générales

Cette formation de préparation à la certification CHFI vous permet de passer l'examen officiel disponible en ligne sur la plateforme EC-Council ECC Exam. **Les frais d'inscription sont inclus dans le prix de cette formation**. Vous recevrez un bon d'examen (voucher). Une fois l'examen réussi, vous obtiendrez le titre de Certified Hacking Forensic Investigator.

Détail de l'examen C|HFI

Code de l'examen : ECO 312-49
Nombres de questions : 150 QCM
Durée : 4 heures
Score de réussite : entre 60 et 85 %
Validité de la certification : permanente

Modalités d'évaluation

Travaux Pratiques
Etude de cas

Pré-requis

Suivre la **formation CHFI v10**, nécessite les prérequis suivants :

- avoir des connaissances avancées sur les systèmes d'exploitation Windows et Linux (systèmes de fichiers, permissions, sécurité, pare-feu, etc.) ;
- maîtriser les fondamentaux des réseaux, tels que les protocoles TCP/IP ;
- connaître les rôles et les services qui sont utilisés par les serveurs au niveau du réseau.
- avoir suivi la formation CEH v12 et être titulaire du titre de Certified Ethical Hacking est chaudement conseillé.

Public

Cette formation s'adresse aux publics suivants :

- les professionnels de l'informatique qui sont chargés de la sécurité des SI, des analyses criminalistiques et de la gestion des incidents ;
- les analystes forensiques, les investigateurs cybercriminalité, les cyber analystes judiciaires, les auditeurs informatiques, les analystes spécialisés dans les programmes malveillants, les consultants en sécurité et les RSSI ;
- toute personne souhaitant se former aux techniques d'investigation informatique légale.

Cette formation s'adresse aux profils suivants

Administrateur système
Analyste cybersécurité
Ingénieur système
Ingénieur logiciel

Programme

Module 1 :

- Comprendre ce qu'est la criminalistique informatique de nos jours.

Module 2 :

- Mettre en œuvre des procédures d'investigation numérique (Computer Forensics).

Module 3 :

- Connaître le fonctionnement des disques durs et des systèmes de fichiers.

Module 4 :

- Collecter et dupliquer des données avec précision.

Module 5 :

- Contourner les dispositifs anti-forensic.

Module 6 :

- Mener des analyses numériques sur un système Windows.

Module 7 :

- Mener des analyses numériques sur des systèmes Linux et Mac.

Module 8 :

- Mener des analyses numériques sur un réseau de communication.

Module 9 :

- Mener des investigations sur des attaques provenant du web.

Module 10 :

- Mener des investigations sur des attaques provenant du dark web.

Module 11 :

- Mener des investigations à partir de bases de données.

Module 12 :

- Mener des investigations sur des attaques provenant du cloud.

Module 13 :

- Mener des investigations sur des attaques provenant de courriers électroniques.

Module 14 :

- Mener des investigations sur des attaques provenant de logiciels malveillants.

Module 15 :

- Mener des investigations sur des attaques provenant d’appareils mobiles.

Module 16 :

- Mener des investigations sur des attaques provenant de systèmes IoT.