EC-Council Computer Hacking Forensic Investigator (CHFI) + Voucher d'examen

Durée: 5 Jours **Réf de cours: CHFI** **Version: V10** **Méthodes d'apprentissage: Virtual Learning**

Résumé:

The Computer Hacking Forensic Investigator (CHFI) course delivers the security discipline of digital forensics from a vendor-neutral perspective. CHFI is a comprehensive course covering major forensic investigation scenarios and enabling students to acquire necessary hands-on experience with various forensic investigation techniques and standard forensic tools necessary to successfully carry out a computer forensic investigation leading to the prosecution of perpetrators.
The CHFI certification gives participants (Law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of the network infrastructure.) the necessary skills to perform an effective digital forensics investigation.
CHFI presents a methodological approach to computer forensics including searching and seizing, chain-of-custody, acquisition, preservation, analysis and reporting of digital evidence.
CHFI v10 captures all the essentials of digital forensics analysis and evaluation required for the modern world — tested and approved by veterans and top practitioners of the cyber forensics industry. From identifying the footprints of a breach to collecting evidence for a prosecution, CHFI v10 handholds students through every step of the process with experiential learning. CHFI v10 is engineered by industry practitioners for professionals including those such as forensic analysts, cybercrime investigator, cyber defense forensic analyst, incident responders, information technology auditor, malware analyst, security consultant, chief security officers and aspirants alike.
CHFI Course Benefits
- Inclusion of critical modules in Darkweb forensic and IoT Forensics
- Significant coverage of forensic methodologies for public cloud infrastructure, including Amazon AWS and Microsoft Azure
- Massive updates on all modules in CHFI
- Inclusion of latest forensic tools including Splunk, DNSQuerySniffer etc
- Addition of new techniques such as Defeating Anti-forensic technique, Windows ShellBags including analyzing LNK files and Jump Lists
- Extensive coverage of Malware Forensics (latest malware samples such as Emotet and EternalBlue)
- Now more than 50GB of crafted evidence files for investigation purposes
- More than 50% of new and advanced forensic labs
- In-depth focus on Volatile and Non-volatile data acquisition and examination process (RAM Forensics, Tor Forensics, etc.
- Accepted and trusted by cybersecurity practitioners across Fortune 500 globally.

Public visé:

Who Should Attend?
Police and other law enforcement personnel
Defense and Military personnel
e-Business Security professionals
Systems administrators
Legal professionals
Banking, Insurance and other professionals
Government agencies
IT managers
Job Roles
Cyber Threat Analyst Tier 2
Cyber Threat Intelligence Analyst
Mid Level Penetration Tester
Cyberspace Analyst II
Cybersecurity Engineer II Red Team
Forensic Analyst, Senior
Cyber Security Analyst Advisor
Cyber Security Analyst
Application Security Analyst
Senior Cyber Security Analyst
Digital Forensics Analyst- Junior level
Security Architect
Cybersecurity Auditor
Senior Network Security Engineer
Information Security Engineer
Manager Information Security management
Principal Cyber Security Engineer
Information Security Risk Program Manager
Cybersecurity Systems Engineer
Information Assurance/Security Specialist
Principal Cyber Operator
Information Security Cyber Risk Defense Analyst
Senior Forensic Analyst

Objectifs pédagogiques:

- Establish threat intelligence and key learning points to support pro-active profiling and scenario modeling
- Perform anti-forensic methods detection
- Perform post-intrusion analysis of electronic and digital media to determine the who, where, what, when, and how the intrusion occurred
- Extract and analyze of logs from various devices like proxy, firewall, IPS, IDS, Desktop, laptop, servers, SIM tool, router, firewall, switches AD server, DHCP logs, Access Control Logs & conclude as part of investigation process.
- Identify & check the possible source / incident origin.
- Recover deleted files and partitions in Windows, Mac OS X, and Linux
- Conduct reverse engineering for known and suspected malware files
- Collect data using forensic technology methods in accordance with evidence handling procedures, including collection of hard copy and electronic documents

Pré-requis:

- CEH - EC-Council Certified Ethical Hacker (CEH) + Voucher d'examen

Test et certification

EXAM

Passing Score

In order to maintain the high integrity of our certification exams, EC-Council Exams are provided in multiple forms (I.e. different question banks). Each form is carefully analyzed through beta testing with an appropriate sample group under the purview of a committee of subject matter experts that ensure that each of our exams not only has academic rigor but also has “real world” applicability. We also have a process to determine the difficulty rating of each question. The individual rating then contributes to an overall “Cut Score” for each exam form. To ensure each form has equal assessment standards, cut scores are set on a “per exam form” basis. Depending on which exam form is challenged, cut scores can range from 60% to 78%.

Number of Questions: 150

Test Duration: 4 Hours

Test Format: Multiple Choice

Test Delivery: ECC Exam Portal

Contenu:

- Computer Forensics in Today’s World
- Computer Forensics Investigation Process
- Understanding Hard Disks and File Systems
- Data Acquisition and Duplication
- Defeating Anti-forensics Techniques
- Windows Forensics
- Linux and Mac Forensics
- Network Forensics
- Investigating Web Attacks
- Dark Web Forensics
- Database Forensics
- Cloud Forensics
- Investigating Email Crimes
- Malware Forensics
- Mobile Forensics
- IoT Forensics

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s’auto-évaluer sur l’atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d’inscription :

• Vous pouvez vous inscrire sur l’une de nos sessions planifiées en inter-entreprises jusqu’à 5 jours ouvrés avant le début de la formation