EC-Council Computer Hacking Forensic Investigator CHFI

Lernen Sie verschiedene Arten der digitalen forensischen Untersuchung durch Python Scripting kennen und beherrschen Sie ein methodisches Forensik-Framework.

CBT Training & Consulting GmbH ist EC-Council Accredited Training Center (ATC)

Listenpreis

3.950,00 € exkl. MwSt

4.700,50 € inkl. MwSt

Dauer

5 Tage

Leistungen Präsenz

- Schulung im Trainingscenter
- Verpflegung
- Teilnahmebestätigung / Zertifikat

Leistungen bei VCL Training

- Technischer Support
- Online Zugang
- Teilnahmebestätigung / Zertifikat

Ihre Ansprechpartnerin

Manuela Krämer
Leitung
Informationssicherheit

Kontakt/Fragen:
m.kraemer@cbt-training.de
Telefon: +49 (0)89-4576918-12

Inhalte

Der CHFI Kurs findet in deutscher Kurssprache mit englischen Herstellerunterlagen in der aktuellsten Version v11 (02-2024) und englischem Examen statt.
Business Englisch erforderlich

Erwerben Sie fundierte Kenntnisse in:

- Social Media Forensics
- Mobile Forensics Analysis
- Wireless Network Forensics
- RAM forensics and Tor forensics
- Electron Application and Web Browser Forensics
- Malware Forensics Process and Malware Analysis
- Forensic Methodologies for Cloud Infrastructure (AWS, Azure, and GCP)
- Dark Web and IoT Forensics

Course Outline:

- Module 01: Computer Forensics in Today?s World
- Module 02: Computer Forensics Investigation Process
- Module 03: Understanding Hard Disks and File Systems
- Module 04: Data Acquisition and Duplication
- Module 05: Defeating Anti-forensics Techniques
- Module 06: Windows Forensics
- Module 07: Linux and Mac Forensics
- Module 08: Network Forensics
- Module 09: Malware Forensics
- Module 10: Investigating Web Attacks
- Module 11: Dark Web Forensics
- Module 12: Cloud Forensics
- Module 13: Email and Social Media Forensics

- Module 14: Mobile Forensics
- Module 15: IoT Forensics

Ziele

Das CHFI-Programm des EC-Council bereitet Cybersicherheitsexperten auf das Wissen und die Fähigkeiten vor, um effektive digitale forensische Untersuchungen durchzuführen und ihre Organisation in einen Zustand forensischer Bereitschaft zu versetzen.
Dazu gehört die Festlegung des forensischen Prozesses, des Labors, der Beweisverfahren sowie der Untersuchungsverfahren, die zur Validierung/Selektierung von Vorfällen erforderlich sind und die Einsatzteams für die Reaktion auf Vorfälle in die richtige Richtung zu leiten. Forensische Bereitschaft könnte den Unterschied zwischen einem kleinen Vorfall und einem großen Cyberangriff ausmachen, der ein Unternehmen in die Knie zwingt.

CHFI präsentiert einen methodischen Ansatz zur Computerforensik, einschließlich Durchsuchung und Beschlagnahme, Chain-of-Custody, Erfassung, Aufbewahrung, Analyse und Meldung digitaler Beweise. Sie erlernen verschiedene forensische Untersuchungstechniken und standardmäßige forensische Werkzeuge. Während Sie lernen, wie man Beweise in verschiedenen Betriebsumgebungen beschafft und verwaltet, lernen Sie auch die Beweiskette und die rechtlichen Verfahren, die erforderlich sind, um Beweise zu sichern und ihre Zulässigkeit vor Gericht sicherzustellen, was die letztendliche Strafverfolgung von Cyberkriminellen ermöglicht und die Haftung des Opfers eindämmt.

Das Programm vermittelt glaubwürdige Fachkenntnisse mit weltweit anerkannter Zertifizierung, die für eine erfolgreiche Karriere im Bereich digitale Forensik und DFIR erforderlich sind, und erhöht so Ihre Karrierechancen.

Zielgruppe

- Jeder, der sich für Cyber-Forensik/Ermittlungen interessiert
- Rechtsanwälte, Rechtsberater und Anwälte
- Strafverfolgungsbeamte
- Polizisten
- Bundes-/Regierungsvertreter
- Verteidigung und Militär
- Detektive/Ermittler
- Mitglieder des Incident-Response-Teams
- Informationssicherheitsmanager
- Netzwerkverteidiger
- IT-Experten, IT-Direktoren/Manager
- System-/Netzwerk-Ingenieure
- Sicherheits-Analysten/Architekt/Prüfer/Berater

Voraussetzungen

- IT-/Forensik-Experten mit Grundkenntnissen in IT-/Cybersicherheit, Computerforensik und Reaktion auf Vorfälle
- Der vorherige Abschluss einer CEH-Schulung wäre von Vorteil:EC-Council Certified Ethical Hacker CEH oder EC-Council Certified Ethical Hacker CEH - INTENSIV
- Business Englisch erforderlich

Prüfung/Zertifizierung

EC-Council Computer Hacking Forensic Investigator (CHFI) Examen 312-49
Multiple-Choice Prüfung mit 150 Fragen, Dauer 4 Stunden
ECC Examensgebühr im Kurspreis enthalten.

Die ECC Examen werden je nach Kurs entweder direkt am Seminarende Nachmittags oder zu einem späteren Zeitpunkt absolviert.
Informationen hierzu erhalten Sie nach Buchung.