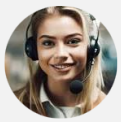
EC-Council Computer Hacking Forensic Investigator (CHFI)

Meistern Sie die Digitale Forensik, Beweissicherung und Ursachenanalyse

Kurs ID: ECCHFI Dauer: 1 Tag ab: € 3.950,00 zzgl. MwSt.

In der praxisbezogenen Schulung EC-Council Computer Hacking Forensic Investigator (CHFI) werden dir verschiedene Lerninhalte der digitalen Computerforensik sowie die aktuellsten forensischen Techniken vermittelt. Während des Seminars erfährst du anhand von praktischen Übungen, wie man nach einem Angriff durch Cyber-Kriminelle in einem IT- System die Beweissicherung durchführt und die Ergebnisse anhand von Datensicherungen sicherstellt. Mit der zunehmenden Bedrohung durch Cyber-Angriffe erkennen Unternehmen die Notwendigkeit, digitale forensische Praktiken in ihre täglichen Aktivitäten einzubeziehen. Computerforensische Praktiken spielen eine wichtige Rolle bei der Untersuchung von Angriffen und Systemanomalien sowie bei der Unterstützung von Systemadministratoren bei der Erkennung von Problemen durch Überprüfung von normalen Funktionsspezifikationen und ungewöhnlichem Verhalten. Es ist entscheidend, dass Untersuchungen von Cyber-Angriffen oder -Vorfällen auf forensisch fundierte Weise durchgeführt werden, um Beweise im Falle eines Gesetzesverstoßes zu sichern. Der EC-Council Computer Hacking Forensic Investigator (CHFI) Kurs vermittelt dir das nötige Wissen, um ein Experte in der digitalen Forensik zu werden und ein wertvolles Mitglied von Incident Handling und Incident Response Teams zu sein.



Sie haben Fragen?

+43 50 4510-0
Mo-Do 8-17 Uhr, Fr. 8-14 Uhr

Kursdetails

tecTrain ist ein zertifiziertes Schulungsinstitut nach Ö-Cert, dem Qualitätsrahmen für die Erwachsenenbildung in Österreich

Kursinhalte

- **Module 01: Computer Forensics in Today’s World**
  - Understand the Fundamentals of Computer Forensics
  - Understand Cybercrimes and their Investigation Procedures
  - Understand Digital Evidence and eDiscovery
  - Understand Forensic Readiness
  - Understand the Role of Various Processes and Technologies in Computer Forensics
  - Identify the Roles and Responsibilities of a Forensic Investigator
  - Understand the Challenges Faced in Investigating Cybercrimes
  - Understand Various Standards and Best Practices Related to Computer Forensics
  - Understand Laws and Legal Compliance in Computer Forensics
- **Module 02: Computer Forensics Investigation Process**
  - Understand the Forensic Investigation Process and its Importance
  - Understand First Response
  - Understand the Pre-investigation Phase
  - Understand the Investigation Phase
  - Understand the Post-investigation Phase
- **Module 03: Understanding Hard Disks and File Systems**
  - Describe Different Types of Disk Drives and their Characteristics
  - Explain the Logical Structure of a Disk
  - Understand the Booting Process of Windows, Linux, and macOS Operating Systems
  - Understand Various File Systems of Windows, Linux, and macOS Operating Systems
  - Understand File System Analysis
  - Understand Storage Systems
  - Understand Encoding Standards and Hex Editors

- Analyze Popular File Formats Using Hex Editor

- **Module 04: Data Acquisition and Duplication**
  - Understand Data Acquisition Fundamentals
  - Understand eDiscovery
  - Understand Data Acquisition Methodology
  - Prepare an Image File for Examination
- **Module 05: Defeating Anti-forensics Techniques**
  - Understand Anti-forensics Techniques
  - Discuss Data Deletion and Recycle Bin Forensics
  - Illustrate File Carving Techniques and Ways to Recover Evidence from Deleted Partitions
  - Explore Password Cracking/Bypassing Techniques
  - Detect Steganography, Hidden Data in File System Structures, Trail Obfuscation, and File Extension Mismatch
  - Understand Techniques of Artifact Wiping, Overwritten Data/Metadata Detection, and Encryption
  - Detect Program Packers and Footprint Minimizing Techniques
- **Module 06: Windows Forensics**
  - Understand Windows Forensics
  - Collect Volatile Information
  - Collect Non-volatile Information
  - Perform Windows Memory Analysis
  - Perform Windows Registry Analysis
  - Perform Electron Application Analysis
  - Perform Web Browser Forensics
  - Examine Windows Files and Metadata
  - Understand ShellBags, LNK Files, and Jump Lists
  - Understand Text-based Logs and Windows Event Logs
- **Module 07: Linux and Mac Forensics**
  - Collect Volatile Information in Linux
  - Collect Non-volatile Information in Linux
  - Understand Linux Memory Forensics
  - Understand Mac Forensics
  - Collect Volatile Information in Mac
  - Collect Non-volatile Information in Mac
  - Understand Mac Memory Forensics and Mac Forensics Tools
- **Module 08: Network Forensics**
  - Understand Network Forensics
  - Summarize Event Correlation Concepts

    - Identify Indicators of Compromise (IoCs) from Network Logs
    - Investigate Network Traffic
    - Perform Incident Detection and Examination Using SIEM Tools
    - Understand Wireless Network Forensics
    - Detect and Investigate Wireless Network Attacks
- **Module 09: Malware Forensics**
    - Understand Malware Concepts
    - Understand Malware Forensics
    - Perform Static Malware Analysis
    - Analyze Suspicious Documents
    - Perform System Behavior Analysis
    - Perform Ransomware Analysis
- **Module 10: Investigating Web Attacks**
    - Understand Web Application Forensics
    - Understand Internet Information Services (IIS) Logs
    - Understand Apache Web Server Logs
    - Detect and Investigate Various Attacks on Web Applications
- **Module 11: Dark Web Forensics**
    - Understand the Dark Web and Dark Web Forensics
    - Determine How to Identify the Traces of Tor Browser during Investigation
    - Perform Tor Browser Forensics
- **Module 12: Cloud Forensics**
    - Understand Cloud Computing Concepts
    - Understand Cloud Forensics
    - Understand Amazon Web Services (AWS) Fundamentals
    - Perform AWS Forensics
    - Understand Microsoft Azure Fundamentals
    - Perform Microsoft Azure Forensics
    - Understand Google Cloud Fundamentals
    - Perform Google Cloud Forensics
- **Module 13: Email and Social Media Forensics**
    - Understand Email Basics
    - Explain Email Crime Investigation and its Steps
    - Understand U.S. Laws Against Email Crime
    - Explain Social Media Forensics
- **Module 14: Mobile Forensics**
    - Understand Mobile Device Forensics

    - Understand Android and iOS Architecture, Boot Process, and File Systems
    - Understand Mobile Forensics Process
    - Investigate Cellular Network Data
    - Perform File System Acquisition
    - Understand Phone Locks, Rooting, and Jailbreaking of Mobile Devices
    - Perform Logical and Physical Acquisition on Mobile Devices
    - Perform Android and iOS Forensic Analysis
- **Module 15: IoT Forensics**
    - Understand IoT Concepts
    - Perform Forensics on IoT Devices

Voraussetzungen

Für deinen Besuch unserer Schulung EC-Council Computer Hacking Forensic Investigator (CHFI) sind:

- Netzwerk, Linux und Windows Grundwissen
- Security Grundwissen ist von Vorteil
- CEH Ethical Hacker Kurs ist von Vorteil

Zielgruppe

Die Schulung EC-Council Computer Hacking Forensic Investigator (CHFI) richtet sich an

- System-und-Netzwerkadministratoren
- Polizeiliche/staatliche Ermittlungsbehörden
- Verteidigungs- und Militärpersonal
- E-Business Sicherheitsexperten
- Systemadministratoren
- Juristen
- IT-Manager

Abschluß

Nach Seminarabschluss erhalten Sie ein tecTrain-Teilnahmezertifikat.