EC-Council Computer Hacking Forensic Investigator (CHFI)

ID CHFI **Preis** CHF 5'500.– (exkl. MwSt.) **Dauer** 5 Tage

Zielgruppe

- Analytiker für digitale Forensik
- Computerforensischer Analyst/Praktiker/Prüfer/Spezialist/Techniker/Kriminalbeamter/Labor-Projektleiter
- Ermittler für Cyberkriminalität
- Ermittler für Computerkriminalität
- Cyber Defense Forensics Analyst
- Strafverfolgung/Abwehr der Spionageabwehr Forensischer Analyst
- Forensischer Ermittler für Daten
- Spezialist für digitale Kriminalität
- Forensischer Ermittler für Computersicherheit
- Forensischer Analyst/Spezialist für Netzwerk/Technologie
- Ingenieur für digitale Forensik und Reaktion auf Zwischenfälle
- Spezialist für forensische Bildgebung
- Analyst für Forensik und eDiscovery
- Computerforensik und Intrusion Analyst
- Forensischer Leiter für Einbrüche
- Sicherheitsingenieur - Forensik
- Malware Analyst
- Mobiler forensischer Analyst/Experte
- Analyst für mobile Ausbeutung
- Fachmann/Analytiker für die Sicherheit von Informationssystemen
- Prüfer für Informationstechnologie
- Kryptoanalytiker
- Kryptograph
- Experte für Katastrophenschutz
- Intelligenz-Technologie-Analyst
- Analyst für Cybersicherheitsvorfälle und Angriffe
- Analyst für Cloud-Sicherheit
- Forensik-KMU
- Forensischer Buchhalter
- Forensischer IT-Sicherheitsanalytiker
- Analyst für Cybersicherheit/Verteidigungsforensik

Voraussetzungen

- IT-/Forensik-Fachleute mit Grundkenntnissen in den Bereichen IT-/Cybersecurity, Computerforensik und Reaktion auf Vorfälle.
- Kenntnisse über Bedrohungsvektoren.

Kursziele

- Grundlagen der Computerforensik, verschiedene Arten von Cyberkriminalität und deren Ermittlungsverfahren sowie Vorschriften und Normen, die den computerforensischen Ermittlungsprozess beeinflussen.
- Die verschiedenen Phasen der computerforensischen Untersuchung.
- Verschiedene Arten von Festplattenlaufwerken und ihre Eigenschaften, Boot-Prozess und Dateisysteme in Windows-, Linux- und Mac-Betriebssystemen, Tools zur Untersuchung von Dateisystemen, RAID- und NAS/SAN-Speichersysteme, verschiedene Kodierungsstandards und Dateiformatanalyse.
- Grundlagen der Datenerfassung und Methodik, eDiscovery und Vorbereitung von Bilddateien für die forensische Untersuchung.
- Verschiedene Anti-Forensik-Techniken, die von Angreifern eingesetzt werden, verschiedene Möglichkeiten, sie zu erkennen, sowie entsprechende Tools und Gegenmassnahmen.
- Erfassung flüchtiger und nichtflüchtiger Daten in Windows-Betriebssystemen, Analyse von Windows-Speicher und -Registrierung, Analyse elektronischer Anwendungen, Webbrowser-Forensik und Untersuchung von Windows-Dateien, ShellBags, LNK-Dateien und Jump Lists sowie Windows-Ereignisprotokollen.
- Erfassung flüchtiger und nichtflüchtiger Daten und Speicherforensik in Linux- und Mac-Betriebssystemen.
- Grundlagen der Netzwerkforensik, Konzepte der Ereigniskorrelation, Indikatoren für Sicherheitslücken (Indicators of Compromise, IOCs) und deren Unterscheidung in Netzwerkprotokollen, Techniken und Tools für die Untersuchung des Netzwerkverkehrs, Erkennung und Untersuchung von Vorfällen sowie Erkennung und Untersuchung von drahtlosen Angriffen.
- Konzepte der Malware-Forensik, statische und dynamische Malware-Analyse, Analyse des System- und Netzwerkverhaltens und Ransomware-Analyse.
- Forensik von Webanwendungen und ihre Herausforderungen, Bedrohungen und Angriffe auf Webanwendungen, Webanwendungsprotokolle (IIS-Protokolle, Apache-Webserver-Protokolle usw.) und wie man verschiedene Angriffe auf Webanwendungen erkennt und untersucht.
- Die Arbeitsmethodik des Tor-Browsers und die Schritte, die in den forensischen Prozess des Tor-Browsers involviert

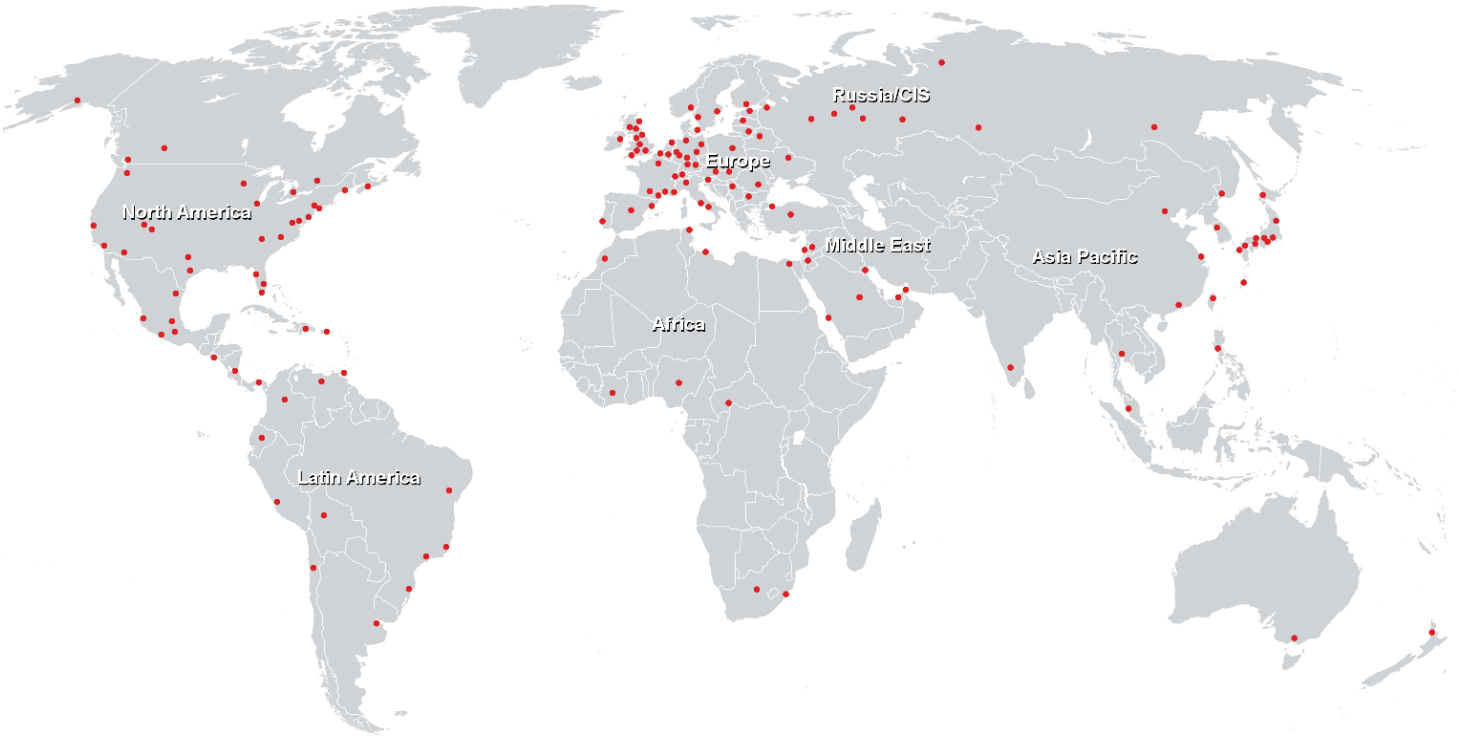
sind.
- Cloud-Computing-Konzepte, Cloud-Forensik und -Herausforderungen, Grundlagen von AWS, Microsoft Azure und Google Cloud sowie deren Ermittlungsverfahren.
- Komponenten der E-Mail-Kommunikation, Schritte bei der Untersuchung von E-Mail-Kriminalität und Forensik der sozialen Medien.
- Architekturschichten und Boot-Prozesse von Android- und iOS-Geräten, mobile forensische Prozesse, verschiedene Mobilfunknetze, SIM-Dateisystem sowie logische und physische Erfassung von Android- und iOS-Geräten.
- Verschiedene Arten von IoT-Bedrohungen, Sicherheitsprobleme, Schwachstellen und Angriffsflächen, IoT-Forensik-Prozess und Herausforderungen.

Kursinhalt

- Computerforensik in der Welt von heute
- Prozess der computerforensischen Untersuchung
- Verstehen von Festplatten und Dateisystemen
- Datenerfassung und -vervielfältigung
- Abwehr von Anti-Forensik-Techniken
- Windows-Forensik
- Linux- und Mac-Forensik
- Netzwerk-Forensik
- Malware Forensics
- Untersuchen von Web-Angriffen
- Forensik im Dark Web
- Cloud-Forensik
- Forensik von E-Mails und sozialen Medien
- Mobile Forensik
- IoT-Forensik

EC-Council Computer Hacking Forensic Investigator (CHFI)

Weltweite Trainingscenter



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch