EC-Council Computer Hacking Forensic Investigator (CHFI)

ID CHFI **Preis** 3.950,– € (exkl. MwSt.) **Dauer** 5 Tage

Dieser Text wurde automatisiert übersetzt. Um den englischen Originaltext anzuzeigen, klicken Sie bitte hier.

Kursüberblick

Kein Cybersicherheitsteam ist ohne digitale Forensik vollständig. Digitale Forensik und Untersuchungen sind entscheidend für die erfolgreiche Bewältigung eines Cybervorfalls, wenn dieser eintritt.

Das CHFI-Programm von EC-Council bereitet Cybersicherheitsexperten mit dem Wissen und den Fähigkeiten vor, die erforderlich sind, um effektive digitale forensische Untersuchungen durchzuführen und ihre Organisation in einen Zustand forensischer Bereitschaft zu versetzen. Dazu gehören die Einrichtung des forensischen Prozesses, des Labors, der Verfahren zur Handhabung von Beweisen sowie der Untersuchungsverfahren, die für die Validierung/Sortierung von Vorfällen erforderlich sind und den Reaktionsteams auf Vorfälle den richtigen Weg weisen. Forensische Bereitschaft kann den Unterschied zwischen einem kleinen Vorfall und einem großen Cyberangriff ausmachen, der ein Unternehmen in die Knie zwingt.

Dieses intensive, praxisorientierte Programm für digitale Forensik lässt die Studierenden in über 68 forensische Labore eintauchen, in denen sie an selbst erstellten Beweisdateien arbeiten und die von den weltweit führenden Experten für digitale Forensik eingesetzten Tools nutzen können. Die Studierenden gehen über die traditionelle Hardware- und Speicherforensik hinaus und lernen aktuelle Themen wie Cloud-Forensik, Mobile und IoT, die Untersuchung von Angriffen auf Webanwendungen und Malware-Forensik kennen. CHFI stellt einen methodischen Ansatz für die Computerforensik vor, der die Suche und Beschlagnahme, die Beweiskette, die Beschaffung, die Aufbewahrung, die Analyse und die Berichterstattung über digitale Beweise umfasst Die Studierenden lernen, wie man Beweise in verschiedenen Betriebsumgebungen beschafft und verwaltet, sowie die Beweiskette und die rechtlichen Aspekte Verfahren, die erforderlich sind, um Beweise zu sichern und ihre Zulässigkeit vor Gericht zu gewährleisten. Dieses Wissen wird ihnen helfen, Cyberkriminelle zu verfolgen und die Haftung für die Zielunternehmen zu begrenzen.

Dieses Programm kombiniert glaubwürdiges Fachwissen mit einer weltweit anerkannten Zertifizierung, die für eine Karriere in der digitalen Forensik, digitalen Ermittlungen und DFIR erforderlich ist.

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

Über Fast Lane

Fast Lane ist weltweiter, mehrfach ausgezeichneter Spezialist für Technologie und Business-Trainings sowie Beratungsleistungen zur digitalen Transformation. Als einziger globaler Partner der drei Cloud-Hyperscaler Microsoft, AWS und Google und Partner von 30 weiteren führenden IT-Herstellern bietet Fast Lane beliebig skalierbare Qualifizierungslösungen und Professional Services an. Mehr als 4.000 erfahrene Fast Lane Experten trainieren und beraten Kunden jeder Größenordnung in 90 Ländern weltweit in den Bereichen Cloud, künstliche Intelligenz, Cybersecurity, Software Development, Wireless und Mobility, Modern Workplace sowie Management und Leadership Skills, IT- und Projektmanagement.

Fast Lane Services

- ✓ Highend-Technologietraining
- ✓ Business- & Softskill-Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digitale Lernlösungen
- ✓ Content-Entwicklung
- ✓ Remote Labs
- ✓ Talentprogramme
- ✓ Eventmanagement-Services

Trainingsmethoden

- ✓ Klassenraumtraining
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Klassenraum und ILO kombiniert
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobiles Lernen

Technologien und Lösungen

- ✓ Digitale Transformation
- ✓ Artificial Intelligence (AI)
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center

Weltweit vertreten
mit High-End-Trainingszentren rund um den Globus

Mehrfach ausgezeichnet
von Herstellern wie AWS, Microsoft, Cisco, Google, NetApp, VMware

Praxiserfahrene Experten
mit insgesamt mehr als 19.000 Zertifizierungen

Deutschland
Fast Lane Institute for Knowledge Transfer GmbH
Tel. +49 40 25334610
info@flane.de / www.flane.de

Österreich
ITLS GmbH
(ITLS ist ein Partner von Fast Lane)
Tel. +43 1 6000 8800
info@itls.at / www.itls.at

Schweiz
Fast Lane Institute for Knowledge Transfer (Switzerland) AG
Tel. +41 44 8325080
info@flane.ch / www.flane.ch