Fortgeschrittenenkurs IT-Forensik für Datenträger und RAM

IT-Forensik-Untersuchungen selbst durchführen

Dieser Kurs vermittelt praxisnah die Analyse von Datenträgern und Arbeitsspeicher. Teilnehmende lernen, digitale Beweise unter Windows und Linux forensisch zu sichern, auszuwerten und Informationsverluste zu verhindern. Ideal für IT-Sicherheitsbeauftragte, Forensikerinnen und Ermittlerinnen.

Fortgeschrittene IT-Sicherheits- und Forensikkenntnisse praxisnah erwerben

Der Fortgeschrittenenkurs richtet sich an IT-Sicherheitsbeauftragte, IT-Administratorinnen, Forensikerinnen sowie Ermittler*innen in Unternehmen und Behörden.

Ziel des Kurses ist es, tiefgehendes Fachwissen über die Betriebssysteme Windows und Linux sowie deren Dateisysteme NTFS, FAT und ext zu vermitteln. Darüber hinaus lernen die Teilnehmenden, wie sie diese Systeme im Rahmen von Sicherheitsanalysen, forensischen Untersuchungen und Incident-Response-Szenarien effizient untersuchen, Schwachstellen identifizieren und Sicherheitsmaßnahmen gezielt implementieren.

Praxisnahe Übungen und Fallbeispiele runden den Kurs ab und ermöglichen eine direkte Anwendung des erworbenen Wissens im beruflichen Umfeld.

Kursdetails auf einen Blick

- Für **IT-Sicherheitsbeauftragte, IT-Administrator*innen, Forensiker*innen, Ermittler*innen**
- **offene Schulung** oder I**nhouse Training**
- Dauer: **5 Tage**
- Format: **Präsenz**
- Kosten: 2.900,00 Euro (zzgl. MwSt.)

IT-Forensik praxisnah anwenden – Datenträger sichern, analysieren und Risiken minimieren

Die Teilnehmenden lernen, Datenträger forensisch zu sichern, auszuwerten und Arbeitsspeicher-Analysen professionell durchzuführen. Dabei werden speziell Methoden der IT-Forensik für SSDs, Festplatten, RAM sowie hybride Speicherlösungen vermittelt. Praxisnahe Übungsbeispiele mit vorbereiteter IT-Forensik-Software ergänzen das theoretische Wissen und fördern die direkte Anwendung im beruflichen Alltag.

Nach Abschluss des Seminars sind die Teilnehmenden in der Lage, Informationsverluste im Unternehmen effektiv zu verhindern, standardisierte Sicherungsprotokolle konsequent einzusetzen, forensische Untersuchungen selbstständig durchzuführen oder gezielt extern zu beauftragen.

Darüber hinaus erwerben sie die Fähigkeit, forensische Analysen kritisch zu bewerten, Risiken frühzeitig zu erkennen und organisatorische Maßnahmen zur Verbesserung der IT-Sicherheitsprozesse zu empfehlen.

Nach dem Seminar können Sie:

- **Datenträger** und **Arbeitsspeicher forensisch** sichern und analysieren.
- **Dateisysteme** wie NTFS, FAT und ext unter Windows und Linux **untersuchen.**
- **IT-forensische Untersuchungen** selbstständig durchführen oder externe Dienstleister beauftragen.

Alle Kursdetails und die Anmeldung finden Sie hier:

https://s.fhg.de/IT-Forensic-Investigations

Kursinhalte

Das Spektrum der behandelten Themen umfasst:

- Definitionen, Vorgehensmodell der IT-Forensik (BSI, NIST),
- Vorbereitung Ihrer Untersuchungen
- Datensammlung auf physischen Datenträgern (SSD, USB-Sticks usw.)
- Dateisysteme (FAT*, NTFS, ext*)
- Betriebssysteme (Windows, Linux)
- File Recovery und File Carving
- Spurensuche im RAM
- IT-forensische Sofortmaßnahmen (Live-Forensik, Triage)
- Verlaufsdokumentation, Abschlussbericht und Gerichtsgutachten
- Umgang mit IT-Forensik-Tools auf der Kommandozeile und mit GUI-Werkzeugen
- Übersicht Software-Werkzeuge (kommerziell und Open Source)
- Übungsaufgaben zur Datensammlung (Image erstellen, Writeblocker)
- Übungsaufgaben zur IT-forensischen Analyse auf Linux-Servern und Windows-Clients
- Aufbereitung Ihrer Ergebnisse aus den Übungsaufgaben
- Nützliche Informationsquellen, Literatur, Konferenzen usw.
- Zusammenfassung, Abschlussdiskussion

Zugangsvoraussetzung:

Grundkenntnisse auf der Kommandozeile (Windows, Linux)

Fachlicher Ansprechpartner am Fraunhofer SIT

Dr. Sascha Zmudzinski
Tel. +49 6151 869-321
sascha.zmudzinski@sit.fraunhofer.de

Fraunhofer SIT
Rheinstraße 75
64295 Darmstadt

Lernlabor
Cybersicherheit