IT-Forensik Spezialist (ZITF)

ID ZITF **Preis** auf Anfrage **Dauer** 4 Tage

Zielgruppe

- Erfahrene SOC Mitarbeiter
- Junior Forensiker / CERT Mitarbeiter
- Sicherheitsbeauftragte mit Technikaffinität
- Erfahrene Administratoren mit Bezug zu IT-Sicherheit

Voraussetzungen

MUSS:

- Detaillierte Kenntnisse Microsoft Windows
- Grundkenntnisse über IT-Netzwerke

SOLLTE:

- Grundkenntnisse Linux
- Praktische Erfahrung im Umgang mit Sicherheitsvorfällen

NICE TO HAVE:

- Hacking Grundlagen (Metasploit, Mimikatz, Kali, Web Applikationen, usw.)

Kursziele

Cyber-Angriffe, Betrug und andere Sicherheitsvorfälle sowie deren Erkennungsrate bei Unternehmen nimmt zu. Doch die richtige Vorgehensweise bei der Beweissicherung und Analyse dieser Vorfälle stellt viele Unternehmen vor grosse Herausforderungen.

Dieser Workshop für Sicherheitsverantwortliche und CERT-Mitarbeiter vermittelt, wie Sicherheitsvorfälle technisch aufgeklärt werden können und ggf. strafbare Handlungen nachgewiesen können.

Der Fokus liegt dabei auf den Themen Umgang mit Beweismitteln und den technischen Möglichkeiten von forensischen Analysen.

Durch viele Übungen werden die theoretischen Inhalte sofort vertieft, damit die Komplexität und die praktischen Einsatzszenarien durch die Teilnehmer besser verstanden werden.

Am Ende des Kurses werden die Teilnehmer fähig sein:

- Sicherheitsvorfälle besser einschätzen zu können
- Beweisobjekte gerichtsfest zu sichern
- Einzelne Analyseschritte eigenständig durchzuführen.

Das Seminar wird abgerundet von einer rechtlichen Betrachtung der IT-Forensik durch unseren Referenten Rechtsanwalt für IT-Recht & Datenschutz.

Dem Teilnehmer wird vermittelt, welche rechtlichen Anforderungen an die Beweisführung in den verschiedenen Rechtsgebieten zu stellen sind und wo Verwertungsverbote drohen können. Anhand der rechtlichen Anforderungen wird mit den Teilnehmern eine Methodik für strukturelle Untersuchungen erarbeitet. Der Teilnehmer erhält Handlungsempfehlungen für den Umgang mit Ermittlungsbehörden sowohl für die Rechtsverfolgung als auch für die Rechtsverteidigung.

Kursinhalt

Tag 1 - 3 Technische Grundlagen mit vielen ÜBUNGEN Referent Senior Cyber Security Consultant

Einführung

- Was sind Cyber Angriffe
- Das Big Picture: SIMP und IT-Forensik im Unternehmen
- Aktuelle Bedrohungslage
- Fallbeispiele aus der Praxis

IT-Forensik

- Incidentkategorien & Best Practice Vorgehensweise
- Incident handling anhand der SIMP-Phasen
  - Assessment
  - Analyse
  - Remediation

Beweisobjekte und Sicherung

- Live Response

- Arbeitsspeicher
- Festplaten
- Virtuelle Maschinen
- Sonderfälle

Forensik Deep-Dive: Analysetechniken

- Dateisysteme
- Windows Analyse
- Linux Analyse
- Mobile Geräte am Beispiel iPhone
- Timeline Analyse
- Malware Analyse
- Arbeitsspeicher Analyse

Abschluss der Analyse

- IOCs und Threat Intelligence
- IOC Breitensuche und Exkurs SIEM
- Lessons learned
- Berichtserstellung

Prüfungsvorbereitung & 1. Teil-Prüfung 60 Minuten Multiple-Choice mit Freitext(Optional)

ACHTUNG 4. Tag

Der Rechts-Part ist auch im Kurs Cyber Security Incident Manager enthalten. Haben Sie diesen Kurs bei uns absolviert, teilen Sie uns dies bei der Buchung mit, damit wir den 4. Tag aus Ihrer Buchung inkl. Kosten dafür, entnehmen. Die Modul-Prüfung IT-Recht Incident Manager wird dann anerkannt und angerechnet.

Tag 4: IT-Recht Referent Rechtsanwalt Schwerpunkte Datenschutz & IT-Recht

Aufgaben und Exponierung des IT-Verantwortlichen

Organisationsverpflichtung

Überblick über das Recht der IT-Sicherheit

Technische und organisatorische Massnahmen nach § 9 BDSG

Beweiswürdigungsgrundsätze

- Gerichtliche Beweisführung
- Rechtliche Aspekte der digitalen Beweissicherung

Umgang mit Behörden

- Strafanzeige
- Akteneinsicht
- Durchsuchungen
- Beschlagnahmungen

Prüfungsvorbereitung & 2. Teil-Prüfung 20 Minuten Multiple-Choice (Optional)

PRÜFUNG:

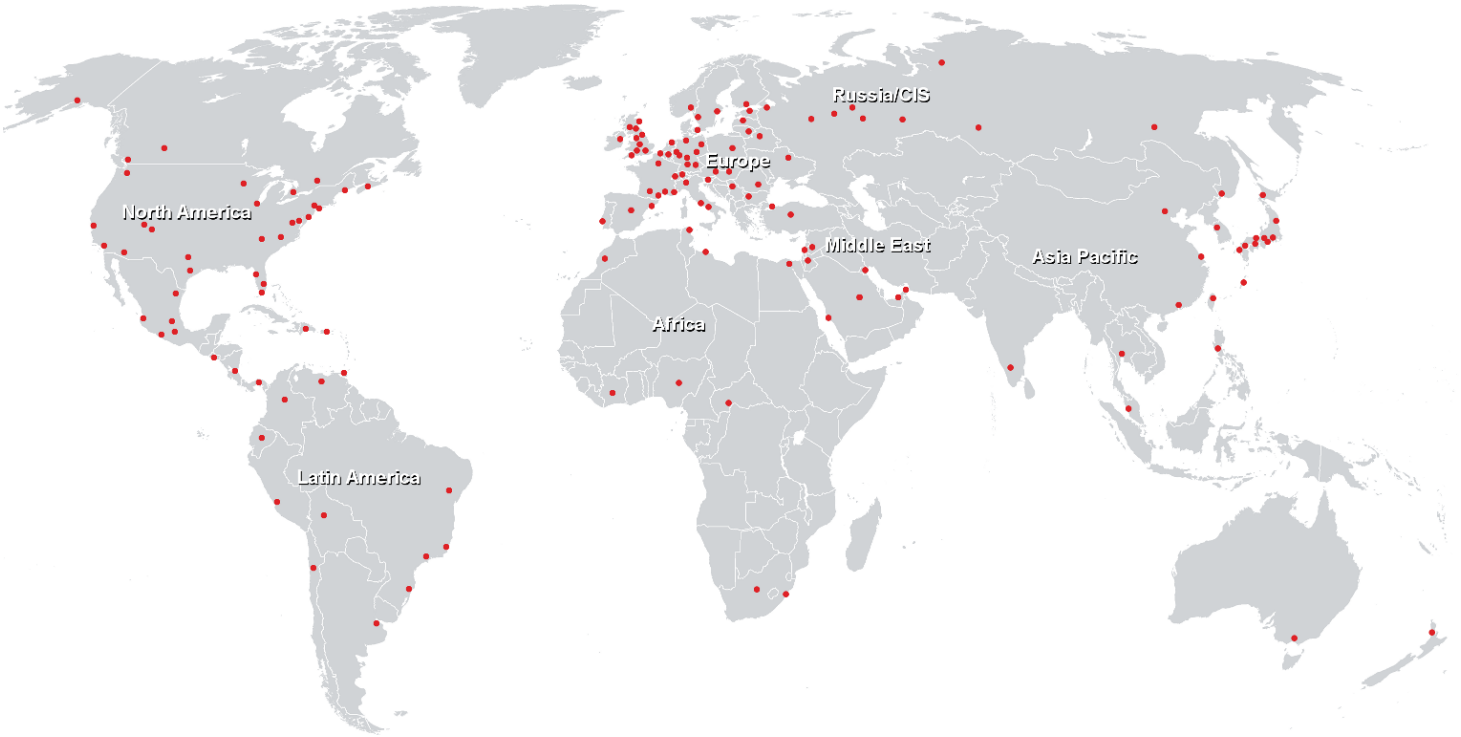
Zum Bestehen der Prüfung ist ein Gesamt-Durchschnitt beider Teilprüfungen von mind. 70% nötig.

1. Part Dauer 60 Minuten Multiple-Choice mit Freitext
2. Part IT-Recht 20 Minuten Multiple-Choice.

Bei Bestehen der Prüfung wird den Teilnehmern ein persönliches Zertifikat CERT überreicht. Eine Teilnahmebestätigung mit den Seminarinhalten wird ebenso übergeben.

IT-Forensik Spezialist (ZITF)

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