IT-Forensik Spezialist CERT/ITFS

Dieser Kurs vermittelt, wie Sicherheitsvorfälle technisch aufgeklärt werden und ggf. strafbare Handlungen nachgewiesen werden können. Eine rechtliche Betrachtung am 4. Seminartag, durch unseren Rechtsanwalt für IT-Recht und Datenschutz, runden das Seminar IT-Forensik ab.

Am Ende des Kurses werden die Teilnehmer fähig sein:

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

Bitte beachten Sie zur Ergänzung auch den Kurs: CSIM - Cyber Security Incident Manager

Deutsche Kursunterlagen / Zertifikat "IT-Forensik Spezialist"
Unser Experten-Zertifikat, das die Teilnehmer nach bestandener Prüfung erhalten, ermöglicht es erfahrenen Beratern und Mitarbeitern im Umfeld der IT-Sicherheit, ihre Kompetenz eindeutig zu belegen.

Listenpreis

3.390,00 € exkl. MwSt

4.034,10 € inkl. MwSt

Dauer

4 Tage

Gebühr für Prüfungen/Examen

420,00 € exkl. MwSt / 499,80 € inkl. MwSt

Leistungen Präsenz

- Schulung im Trainingscenter
- Verpflegung
- Teilnahmebestätigung / Zertifikat

Leistungen bei VCL Training

- Technischer Support
- Online Zugang
- Teilnahmebestätigung / Zertifikat

Ihre Ansprechpartnerin

Manuela Krämer
Leitung Informationssicherheit

Kontakt/Fragen:
m.kraemer@cbt-training.de
Telefon: +49 (0)89-4576918-12

Inhalte

Tag 1 - 3 Technische Grundlagen mit vielen Übungen & Praxisbeispielen, Referent Senior Cyber Security Consultant

- **Einführung**
  - Was sind Cyber Angriffe
  - Aktuelle Bedrohungslage
  - Fallbeispiele aus der Praxis & Übungen (Ramsonware, DarkSide, Wirtschaftsspionage)
- **IT-Forensik**
  - Generische Vorgehensweise bei einer forensischen Analyse
  - Security Incident Management Process nach ISO 27035
  - Incidentkategorien & Incident Handling mit Runbooks
- **Beweisobjekte und Sicherung**
  - Live Response
  - Arbeitsspeicher
  - Festplatten
  - Log Daten und Triage Pakete
  - Virtuelle Maschinen
  - Sonderfälle (M365, Azure, Cloud Dienste...)
- **Forensik Deep-Dive: Analysetechniken**
  - Festplatten und Dateisysteme

  - Dateiwiederherstellung und -analyse
  - Volltextsuche und Indizierung
  - Windows Forensik
  - Linux Forensik
  - Internetnutzung / Browser Analyse
  - Mobile Geräte am Beispiel iPhone
  - Malware Analyse
  - Arbeitsspeicher Analyse
- **Incident Response**
  - Major Incident Management
  - IOCs und Threat Intelligence
  - Live Forensik
- **Case Study: APT at DBMG**
  - Memory Analyse eines Clients
  - Post Mortem Analyse eines Clients
  - Lösung: ENISA Szenario
- **Verhaltensregeln bei Sicherheitsvorfällen**
- **Zusammenfassung der Schulung, Besprechung der noch offenen Fragen, Prüfung (Optional)**

Bitte beachten Sie Tag 4:

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

Tag 4: Rechtsfragen in der IT-Forensik, Datenschutz & IT-Recht, Referent Rechtsanwalt

- Überblick Recht in der IT-Sicherheit
- Technische, organisatorische, strategische und rechtliche Aspekte der IT-Sicherheit
- Organisationsverpflichtung
- Maßgebliche Rechtsbereiche der IT-Forensik
- Arbeitnehmermitbestimmung
- Datenschutz Grundverordnung DSGVO
- Beschäftigtendatenschutz (§ 26 BDSG)
- IT-Forensische Ermittlungen bei Outsourcing
- Meldepflichten & Bussgelder
- Strafrecht u.a. Hackerparagraph § 202c StGB
- Beweiswürdigungsgrundsätze
- Kooperation mit den Behörden
- Fazit & Disskussionsrunde
- Zusammenfassung der Schulung, Besprechung der noch offenen Fragen, Prüfung (Optional)

Weiterführende Kurse:

- Cyber Securtiy Incident Manager für SOC/CDC

Ziele

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.

Dieses Seminar IT-Forensik für Sicherheitsverantwortliche und CERT-Mitarbeiter vermittelt, wie Sicherheitsvorfälle technisch aufgeklärt werden 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 mit Tätigkeitsschwerpunkt IT-Recht und Datenschutz mit IAPP Datenschutz Zertifizierungen

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.

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.)

Prüfung/Zertifizierung

CERT ITFS IT-Forensik Spezialist

Prüfung, deutsch
1. Part Dauer 60 Minuten Multiple-Choice mit Freitext
2. Part IT-Recht 25 Minuten Multiple-Choice

Prüfung zum CBT CERT Zertifikat:

Die Prüfung erfolgt schriftlich als Multiple-Choice/Freitext Prüfung. Die **CBT CERT Prüfung** wird direkt nach Kursende abgenommen. Sie gilt als bestanden, wenn mindestens 70% der Fragen richtig beantwortet wurden.

Nach Bestehen der Prüfung erhalten Sie ein personenbezogenes **CBT CERT Zertifikat,** das Ihnen die erfolgreiche Kursteilnahme inklusive bestandener Prüfung bestätigt.

Hat ein Teilnehmer die **CBT CERT Prüfung** nicht bestanden, so kann er diese entweder direkt im Anschluss an die erste Prüfung oder während unserer Öffnungszeiten Online Live mit Prüfungsüberwachung (Kamerapflicht, MS-Teams) nach vorheriger schriftlicher Anmeldung (mind. 14 Tage vor Termin) gegen die genannte Prüfungsgebühr wiederholen.

Die Prüfung kann höchstens 2-mal wiederholt werden. Die Prüfungswiederholung muss innerhalb von 3 Monaten nach Kursbesuch erfolgt sein.

Gültigkeit CBT CERT:

Das **CBT CERT ZERTIFIKAT** ist 3 Jahre gültig und muss anschließend durch eine erneute Prüfung bei CBT Training & Consulting GmbH aktualisiert / verlängert werden.

Alle Prüfungsunterlagen werden 3 Jahre aufbewahrt.
