
# Cyber Security Incident Manager für SOC/CDC CERT/CSIM

**inkl. 1 Tag IT-Recht in der Forensik mit Rechtsanwalt für IT-Recht & Datenschutz**

Dieser Kurs vermittelt den Teilnehmern ein tiefgehendes Verständis wie die organisationsinternen Fähigkeiten und Kapazitäten für Incident Response optimiert werden können.
Bitte beachten Sie zur Ergänzung auch den Kurs:"IT-Forensik Spezialist"

**Zertifikat "CyberSecurity Incident Manager"**
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
3.290,00 € exkl. MwSt
3.915,10 € 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

### Ihr Ansprechpartner


**Manuela Krämer**
Leitung Informationssicherheit

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

## Inhalte
### Tag 1 - 3 Security Incident Management im Unternehmen, Referent Senior Cyber Security Consultant

- **Einleitung & Definitionen**
  - Über dieses Training
  - Was versteht man unter Cyber Angriffen?
  - Aktuelle Bedrohungslage
  - Einheitliche Begriffsdefinition
- **Security Incident Management Process (SIMP)**
  - Warum benotigt es Prozesse?
  - Bekannte Ausprägungen von SIMP
  - Vom high level SIMP zum pragmatischen Workflow
  - Anhängige und zugrundeliegende Prozesse
  - Zusammenfassung und Fazit
- **Incident Response organisieren**
  - Security Incident Management im Unternehmen
  - Zielsetzung und Strategie eines CDCs
  - Die Herausforderung Security Monitoring und Incident Handling
  - Ressourcen
  - Technologien
  - Zusammenfassung und Fazit
- **Bearbeitung alltäglicher Security Incidents**
  - Standardisierung und Automatisierung von Incident Response
  - Zusammenarbeit mit IT Operations
  - Lessons Learned
  - Zusammenfassung und Fazit


- **Bearbeitung Major Security Incidents**
  - Detektion und Eskalation
  - Grundlagen Krisenmanagement
  - CSIRT Planung und Etablierung
  - Koordination
  - Monitoring
  - Sofortmaßnahmen
  - Forensische Analysen
  - Remediation
  - Durchführung von Lessons Learned
- **Zusammenfassung der Schulung, Besprechung der noch offenen Fragen, Prüfung (Optional)**

**ACHTUNG 4. Tag**
Der Rechts-Part ist auch im Kurs "IT-Forensik Spezialist" 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 IT-Forensik 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
- Zusammenfassung der Schulung, Besprechung der noch offenen Fragen, Prüfung (Optional)

**Weiterführende Kurse:**
Für eine Beratung rufen Sie uns gerne an!

- IT-Forensik
- Advanced Privacy & Counter Surveillance Training
- IT-GRC Governance, Risk & Compliance Management Systems
- CISO
- CISO.PROF
- Change Management
- ISO 27001 Lead Implementer & Auditor
- Risikomanagement
- BCM
- ISO27701 DSMS / PIMS
- Hacking Einführung

---


## Ziele

Cyber-Angriffe nehmen immer mehr zu und immer mehr Unternehmen implementieren SIEM Systeme und andere Tools zur Erkennung von Sicherheitsvorfällen. Die größte Herausforderung dabei: Wie geht man professionell mit den erkannten Sicherheitsvorfällen um, um die Spreu vom Weizen zu trennen und eine ordnungsgemäße Abarbeitung und Behebung sicherstellen?Dieser Kurs vermittelt den Teilnehmern ein tiefgehendes Verständnis wie die organisationsinternen Fähigkeiten und Kapazitäten für Incident Response optimiert werden können. Neben der theoretischen Erläuterung von Konzepten, Methodiken und Taktiken werden diese auch anhand von persönlichen Erfahrungen reflektiert. Mit verschiedenen Übungen, die das Wissen vertiefen und für erste Praxisanwendung sorgen, wird der Kurs abgerundet.**Am Ende des Kurses werden die Teilnehmer fähig sein:**

- Security Incident Management Prozesse (SIMP) zu verstehen und zu entwickeln.
- Response Strategien für verschiedene Sicherheitsvorfälle zu entwerfen.
- Den Lead bei der Bearbeitung von schwerwiegenden Vorfällen zu übernehmen.
- Eine leitende Rolle im CERT oder SOC auszuführen.**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.

---

## Zielgruppe

- Leiter von Cyber Security Incidents Response Teams (CSIRT)
- Manager von CERT oder SOC
- Senior CERT Mitarbeiter
- Senior oder 3rd level SOC Analysten
- Senior Forensik Spezialisten

---

## Voraussetzungen

**MUSS:**

- Grundkenntnisse über IT-Systeme und Informationssicherheit
- Praktische Erfahrung im Umgang mit Sicherheitsvorfällen (SOC oder digitale Forensik)

**SOLLTE:**

- Fähigkeit zum abstrakten Denken
- Organisations und Planungs Talent

**NICE TO HAVE:**

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

---


## Prüfung/Zertifizierung

CERT CSIM Cyber Security Incident Manager

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

---