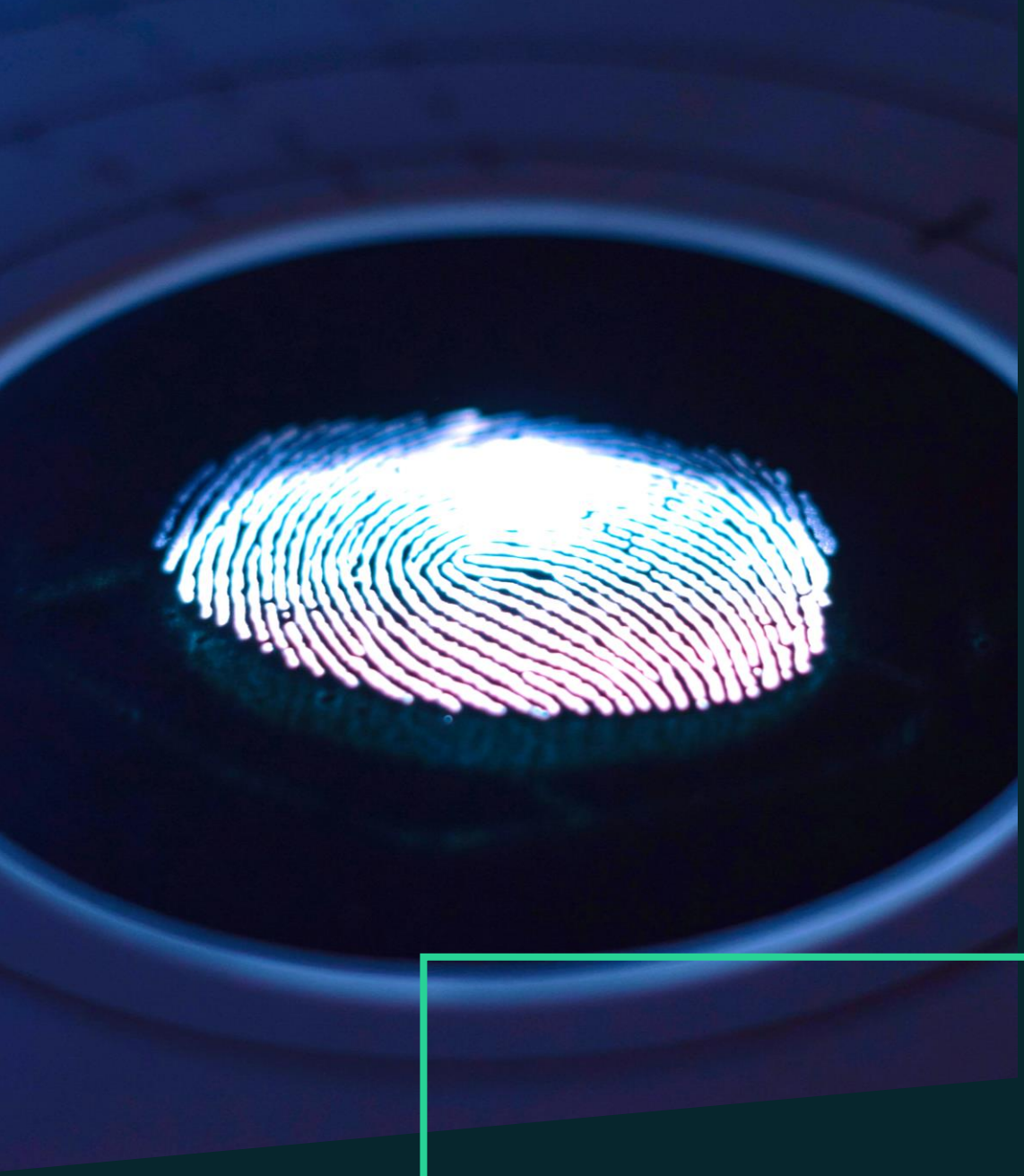
bitkom
akademie



IT-Forensik & Cybercrime Expert

Zertifikatslehrgang

IT-Forensik & Cybercrime Expert

Bekämpfung von Cyberkriminalität: IT-Forensik für Professionals

Kurzbeschreibung

Kommt es zu einem IT-Sicherheitsvorfall im Unternehmen, ist eine **rasche und professionelle Aufarbeitung** erforderlich. So werden nicht nur größere Schäden vermieden, es können auch digitale Beweise gesichert werden, die in der Aufklärung des Cyberangriffs als Beweismittel genutzt werden können – denn oftmals hinterlassen Cyberkriminelle digitale Spuren, die sichergestellt werden müssen. Diese wichtige Aufgabe übernehmen IT-Forensiker und IT-Forensikerinnen.

In diesem Zertifikatslehrgang lernen Sie das notwendige Rüstzeug, um als IT-Forensik & Cybercrime Expert zu agieren. Dafür werden Sie zum einen umfassend geschult: von den Grundlagen der IT-Forensik über Angriffsprozesse bis hin zur richtigen Handhabung bei Sicherheitsvorfällen. Zum anderen lernen Sie forensische Analysetools kennen und wenden das erlernte Wissen im Lehrgang praktisch an. Damit sind Sie im Anschluss in der Lage, **Beweise fachkundig zu sichern, IT-forensische Untersuchungen durchzuführen und Cyberangriffe aufzuarbeiten**. Nach dem Lehrgang haben Sie die Möglichkeit, sich zertifizieren zu lassen und das Zertifikat „IT-Forensik & Cybercrime Expert“ zu erwerben.

Inhalt

- Einführung in die Konzepte der IT-Forensik und relevante Systeme
- Methoden zur Identifizierung und Behandlung von Cyberbedrohungen mit einer Vertiefung der Angriffstechniken und -prozesse
- Daten- und Festplattenforensik
- Ergreifen von Notfallmaßnahmen und Bewältigen von Sicherheitsvorfällen
- Spezifische Forensik wie die Arbeitsspeicher-, Cloud- und Mobile-Forensik
- Anwendung von Analysetools wie Wireshark

Was lernen Sie in diesem Lehrgang?

Sie erlernen, wie Sie IT-forensische Untersuchungen durchführen und wie Sie IT-forensische Methoden sicher und legal in Ihrem beruflichen Umfeld einsetzen. Am Ende des Lehrgangs sind Sie in der Lage, **Daten effektiv zu sichern und so zur Aufklärung von IT-Sicherheitsvorfällen beizutragen**. Sie lernen wichtige Tools für die IT-forensische Ersthilfe kennen und werden mit grundlegenden Konzepten aus der IT-Forensik vertraut gemacht. Darüber hinaus entwickeln sie ein Verständnis für Speichermedienforensik, Cyberhygiene und die Implementierung von IT-forensischen Notfallplänen.

bitkom akademie

IT-Forensik & Cybercrime Expert

Bekämpfung von Cyberkriminalität: IT-Forensik für Professionals

Zielgruppe

Dieser Lehrgang richtet sich an **Mitarbeitende im IT-Sicherheitsbereich und IT-Bereich**, die ihr Verständnis von IT-Forensik und Cyberkriminalität erweitern möchten. Vorerfahrungen in IT, IT-Sicherheit, Forensik und Hacking sind hilfreich.

Didaktischer Aufbau

Der Lehrgang vereint aufeinander aufbauende Module mit Theorie- und Praxisteilen, beginnend mit einer grundlegenden Einführung in die IT-Forensik. Durch die Kombination aus **Vorträgen, interaktiven Workshops und der Bearbeitung von Fallbeispielen** wird ein hoher Praxis-Bezug gegeben. In den späteren Modulen werden Spezialgebiete wie Datenbankforensik, Arbeitsspeicher- und Festplattenforensik thematisiert. Die Teilnehmenden werden dazu ermutigt, aktiv teilzunehmen.

Zertifikat

Der Lehrgang schließt mit einer Prüfung ab, die an einem separaten Termin stattfindet. Mit Bestehen der Prüfung erhalten Sie ein Zertifikat, das Ihre **Fachkenntnisse im Bereich IT-Forensik** nachweist. Die Zertifizierung beruht auf einem Qualitätsstandard, den sich die Bitkom Akademie und ihre Partner als Qualitätssiegel für ihre Ausbildungslehrgänge gesetzt haben.

Zusatzinformationen

- Der Lehrgang findet im kleinen Kreis mit einer Maximalteilnehmerzahl von **16 Personen** statt. Die Mindestteilnehmerzahl beträgt fünf.
- Der Online-Lehrgang wird mit Zoom durchgeführt. Systemvoraussetzungen und unterstützte Betriebssysteme können Sie hier einsehen. Für die Einwahl in Zoom über die verschiedenen Anwendungen (Desktop Client, App oder Web-Client) bietet Ihnen diese Tabelle einen zusätzlichen Vergleich zu den Eigenschaften.
- Die Bitkom Akademie ist anerkannter Bildungsträger in Baden-Württemberg und Nordrhein-Westfalen. Teilnehmende haben im Rahmen des Bildungszeitgesetzes die Möglichkeit, Bildungsurlaub bzw. eine Bildungsfreistellung zu beantragen. Auf Anfrage erstellen wir auch Anträge auf Anerkennung unserer Veranstaltungen in anderen Bundesländern.
- Wir erklären ausdrücklich, dass beim Bitkom – Unterzeichner der Charta der Vielfalt – jede Person, unabhängig von Geschlecht, Nationalität, ethnischer Herkunft, Religion oder Weltanschauung, Behinderung, Alter, sexueller Orientierung und Identität willkommen ist.

bitkom akademie

Seminarprogramm

IT-Forensik & Cybercrime Expert

Tag 1

Grundlagen der IT-Forensik
- Veranschaulichung eines typischen Hacking-Angriffs
- Forensische Rechtsgrundlagen (u. a. StGB und UrHG)

Typischer Hackingangriff
- Durchlaufen der Phasen von Aufklärung bis Bewaffnung
- Vishing
- Erzeugung von Phishing-Mails und -Websites
- Erstellen von fiktiven Identitäten

Spezifische Anwendung von Hacking
- Darknet
- Passwort-Leaks
- Funktionsweise von Google Hacking

Zustellung, Ausnutzung und Einrichtung von C&C
- Physical Access
- Vorstellung gängiger Angriffstechniken und –tools
- Ransomware

Tag 2

Verständnis und Anwendung von Offense und Defense-Strategien
- Vertiefung des Command and Control & Angriffsprozesses
- Darstellung der 'Action on Objectives‘

Einführung in die ISMS-Grundlagen
- Historische Entwicklung und Aufbau eines ISMS
- ISO-270XX
- Leitfaden für präventive Informationssicherheitsmaßnahmen
- Beurteilen, Reaktion und Erkenntnisse aus Informationssicherheitsvorfall
- Sammeln von Beweismaterial
- Compliance-Vorschriften

Aufbau und Verständnis von ISO 27035
- Normbestandteile:
  - 1: Grundlagen des Vorgehens
  - 2: Vor- und Nachbereitung
  - 3: Forensische ICT-Untersuchung
- Die fünf Hauptphasen:
  - Planung und Vorbereitung
  - Aufspüren und Melden
  - Bewertung und Entscheidung
  - Reaktion
  - Lessons Learned

bitkom akademie

Seminarprogramm

IT-Forensik & Cybercrime Expert

Tag 3

Vertiefung der Forensik in Datenbanksystemen
- Überblick zur Forensik in relationalen Datenbanken
- Erläuterung von SQL-Injektion
- Abgrenzung zur allgemeinen Forensik
- Artefaktauswertung

Ram- und Festplattenforensik
- Forensik im RAM
- Anwendung von Hunter-Tools
- Erstellung von RAM-Dumps
- Windows-Ram Anwendungsbeispiel
- Runbooks & Playbooks

Vertiefung der Forensik auf Festplatten
- Festplattenformate
- Datenquellen
- Data Artifacts & Analysis Results

Tag 4

Notfallplanung und -organisation
- Einführung in Notfallmaßnahmen und organisatorische Präventionen
- Incident Handling
- Preparation
- Detection and Analysis
- Containment Eradication Recovery
- Post-Incident Activity
- Darstellung von Best Practices

Durchführung von IT-forensischen Untersuchungen
- Beweisermittlung anhand von Liveforensik, Deadforensik/Postforensik
- Validierung von IP-Adressen und Dateien
- Identifikation und Decryptor von Ransomware

Forensik im Arbeitsspeicher und Einführung in weitere Forensik-Felder
- Feldübergreifende Forensik und Analysewerkzeuge
- Methoden und Techniken zur Spurensuche und Analyse
- Anwendung und Funktion von Wireshark
- Einführung in die Cloud- und Mobile Forensik

bitkom akademie

Ihr Referent

Julian Stumpe

IT-Security Consultant
BREDEX GmbH

Julian Stumpe bringt eine fundierte Ausbildung und umfangreiche praktische Erfahrung in den Bereichen IT-Forensik und IT-Sicherheit mit. Er hat einen breiten beruflichen Hintergrund, unter anderem drei Jahre als Full-Stack Web-Developer und gegenwärtig als IT-Security Consultant. Neben seiner Rolle als IT-Security Consultant ist er auch zertifizierter Scrum-Master, Cybersecurity-Trainer und Ethical Hacker und bringt damit wertvolle Kenntnisse und Fähigkeiten in diesen spezialisierten Bereichen der IT-Sicherheit mit. Diese Erfahrungen, kombiniert mit seinem Masterabschluss in IT-Sicherheit & Forensik, ermöglicht ihm, sowohl fundiertes theoretisches Wissen als auch praktische Einblicke in die IT-Sicherheit zu bieten.

Shortfacts

Termine, Ort und Preise
Die aktuellen Informationen entnehmen Sie bitte der ↗ Website der Bitkom Akademie.

Kontaktieren Sie uns – wir beraten Sie gern.

Bitkom Akademie | Albrechtstraße 10 | 10117 Berlin
T 030 27576-540 | info@bitkom-akademie.de
Weitere Seminare finden Sie unter **www.bitkom-akademie.de**

bitkom akademie