IT-Forensik.

Grundlagen und Praxis

Seminar	1 Termin verfügbar	Teilnahmebescheinigung
Präsenz / Virtual Classroom	24 Unterrichtseinheiten	

Seminarnummer: 31201

Stand: 01.11.2026. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/31201

Als Sicherheitsverantwortlicher für IT-Security, Mitarbeiter in einem CERT oder SOC, oder Berater werden Sie regelmäßig mit IT-forensischen Fragestellungen konfrontiert. In unserer Schulung erlernen Sie den multidisziplinären Ansatz der **IT-Forensik, der Techniken aus den Bereichen der Kriminalistik, Informatik und Rechtswissenschaften kombiniert, um digitale Beweise zu sammeln, zu analysieren und zu interpretieren.**

Nutzen

In dieser umfangreichen, dreitägigen Schulung werden bewusst theoretische und praktische Anteile gemischt, sodass Sie nicht nur das Wissen erlangen, sondern direkt den Bezug zur Praxis der IT-Sicherheit herstellen können. Unsere Referenten sind langjährig in Unternehmen mit der Bearbeitung von IT-Sicherheitsvorfällen sowie dem Erstellen von forensischen Gutachten tätig und ergänzen die Theorieeinheiten mit Beispielen aus der Praxis. Dadurch profitieren Sie von einer praxisnahen Schulung mit Branchenexperten, die Ihnen anhand realer Fallbeispiele vermitteln, wie Sie souverän auf Cyberangriffe und Datenschutzverletzungen reagieren. Auf diese Weise stärken Sie nicht nur Ihre Krisenreaktion auf Sicherheitsvorfälle, sondern reduzieren auch das Risiko finanzieller und reputationsbezogener Schäden. Zudem erhalten Sie Best Practices und klare Prozessabläufe an die Hand, mit denen Sie das Incident-Management effizient strukturieren können.

Zielgruppe

(System-)Administratoren, IT-Mitarbeiter, IT-Führungskräfte, IT-Sicherheitsbeauftragte, Personen aus dem Bereich IT/Netzwerksicherheit

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

Inhalte des Seminars

- Begriffe/Terminologie
- IT-Forensik im Kontext
- Rechtliche Grundlagen und Einordnung
- Digitaler Tatort
- Forensisches Imaging
- Werkzeuge im Überblick
- Beweismittel
- Von der Spur zum Ereignis
- Order of Volatility
- IT-forensische Fragestellungen und Ziele
- Vorgehen und Prozesse
- Festplatten und Partitionen
- Dateisysteme
- Metadaten und Zeitstempel
- Priorisierung von Beweismitteln
- Registry
- Datenrekonstruktion (Carving)
- Artefakte (Evidence of ...)
- Prozessanalyse
- Loganalyse
- Registryanalyse
- Internetnutzungsartefakte
- Netzwerkanalyse
- Memory-Forensics

Diese Schulung eignet sich als Weiterführung der Schulungsangebotes Cybersecurity Incident – First Response

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

Wichtige Hinweise

Die Schulung ist so konzipiert, dass auch Teilnehmende ohne vorherige technische IT-forensische Erfahrung den Beispielen folgen können. Für Teilnehmende mit erster Erfahrung bieten die Aufgabenstellungen genügend Raum, um über die initialen Fragestellungen hinaus Untersuchungen zu tätigen.

Um in vollem Umfang an der Schulung teilzunehmen, benötigen Sie einen eigenen Laptop mit aktuellem Betriebssystem und ca. 100 GB freiem Speicherplatz für VM´s und zu analysierende Images.

Das Seminar wird in Kooperation mit unserer langjährigen Tochtergesellschaft der isits AG in gewohnter TÜV-Rheinland-Qualität durchgeführt.

Sollte ein von uns beauftragter Partner zur Leistungserbringung Unterauftragnehmer einsetzen, stellen wir sicher, dass diese den erforderlichen Standards entsprechen.

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/31201 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- Persönliches Kundenkonto
- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.