# Cyber Threat Intelligence Training.

**Lernen Sie Cyber-Bedrohungen zu analysieren, Angreifer taktisch zu verstehen und Ihr SOC durch Threat Intelligence zu stärken.**

| | | |
|---|---|---|
| Seminar | Zurzeit keine Termine | Teilnahmebescheinigung |
| Präsenz / Virtual Classroom | 16 Unterrichtseinheiten | |

Seminarnummer: 31131

Stand: 09.06.2026. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/31131

In einer dynamischen Bedrohungslandschaft reicht rein reaktiver Schutz nicht mehr aus. Diese praxisnahe **Cyber Threat Intelligence Schulung** versetzt IT-Sicherheitsverantwortliche in die Lage, Angriffe nicht nur abzuwehren, sondern proaktiv vorherzusehen. Sie lernen, wie Sie strategische, taktische und operative Bedrohungsinformationen effektiv sammeln, auswerten und für eine **proaktive IT Sicherheit** anwenden. Werden Sie vom Gejagten zum Jäger und verstehen Sie die Absichten der Angreifer, bevor Schaden entsteht.

## Nutzen

- **Vom Reagieren zum Agieren:** Sie wandeln Ihre Verteidigung in eine proaktive Einheit um, indem Sie lernen, komplexe **Cyber-Bedrohungen zu analysieren** und Angreifern einen Schritt voraus zu sein.
- **Drastische Reduktion der MTTR:** Durch fundierte **Incident Response Threat Intelligence** verkürzen Sie die Zeit bis zur Erkennung und Behebung von Sicherheitslücken auf ein Minimum.
- **Gezielte SOC-Entlastung:** Ihr Team lernt, Fehlalarme (False Positives) durch präzise Cyber-Bedrohungsanalysen schneller zu filtern und Ressourcen effizient zu bündeln.
- **Optimiert für die Praxis:** Die Schulung richtet sich maßgeschneidert an IT-Sicherheitsmitarbeiter, Netzwerkadministratoren und SOC-Analysten, die direkt anwendbares Expertenwissen benötigen.

## Zielgruppe

IT-Sicherheitsmitarbeiter, Netzwerkadministratoren und SOC (Security Operations Center) Analysten

# Abschluss

**Teilnahmebescheinigung**

Teilnahmebescheinigung der Isits AG.

# Inhalte des Seminars

Die Fachausbildung deckt alle Kernbereiche der modernen, datengestützten Bedrohungsabwehr ab:

- **Grundlagen & Threat Intelligence Datenquellen**
  - Einführung in den Intelligence-Lebenszyklus und die Klassifizierung globaler Angreifergruppen (Advanced Persistent Threats).
  - Systematische Evaluierung kommerzieller und Open-Source **Threat Intelligence Datenquellen** sowie deren Nutzbarmachung im Unternehmen.
- **Angriffsrahmenwerke & Kompromittierung**
  - **Cyber-Bedrohungen erkennen** und tiefgehend analysieren mithilfe des weltweit etablierten **MITRE ATT&CK Framework Kurs**-Modells.
  - Identifikation von Angreifer-Taktiken und präzise **Indicators of Compromise Analyse** (IoCs) zur schnellen Aufklärung von Sicherheitsvorfällen.
- **Prozessintegration & SOC-Operationen**
  - Nahtlose Einbindung von CTI in bestehende Sicherheitsprozesse und das IT-Risikomanagement.
  - **Threat Hunting im SOC:** Optimierung von Security Operations Center-Abläufen durch die proaktive Jagd nach versteckten Schadprogrammen im Netzwerk.
- **Infrastrukturanalyse & Best Practices im Reporting**
  - **Incident Response Threat Intelligence:** Einsatz von Echtzeit-Bedrohungsdaten zur schnellen Eindämmung und Isolation von Cyber-Angriffen.
  - Praktische Infrastrukturanalyse mit aktuellen Methoden sowie die Erstellung zielgruppengerechter Intelligence-Reports für das Management (Reporting).

# Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/31131 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.