# 3785 IT Forensik und Incident Response

## Ermittlung von Sicherheitsvorfällen und Beweissicherung

Sie lernen, angemessen auf Notfälle zu reagieren und vorbereitende forensische Maßnahmen einzuleiten, um die Situation zu stabilisieren. Außerdem lernen Sie, wichtige Daten zu sichern, bis Fachleute eintreffen.

**Die Zielgruppe:**
Fachpersonal im IT-Umfeld
Security Spezialisten

**Die Inhalte:**

- Einführung in die digitale Forensik
  - Bedeutung und Grundlagen der digitalen Forensik
  - Rechtliche Aspekte und Ethik
  - Chain of Custody: Beweissicherung und Protokollierung
- Arten digitaler Beweise und Methoden
  - Unterschiedliche Arten von digitalen Beweismitteln (Netzwerk, Betriebssysteme, Dateien, Mobilgeräte)
  - Grundlegende forensische Untersuchungsmethoden (Computer, Mobile, Malware, Memory, Network)
- Betriebssysteme, Dateistrukturen und Netzwerke
  - Grundlagen der Betriebssysteme und Dateistrukturen
  - Analyse von Netzwerkaktivitäten und -spuren.
- Notfallplan und Incident Management
  - Einführung in den Incident Response Prozess
  - Angriffsphasen/Lifecycle und aktuelle Angriffstechniken
  - Integration digitaler Forensik in den Notfallplan
  - Erstellung von Leitlinien für den Umgang mit digitalen Vorfällen
- Notfallbetrieb und Wiederherstellungsstrategien
  - Wie könnte ein Notfallbetrieb nach digitalen Vorfällen aussehen
  - Welche Wiederherstellungsstrategien gibt es?