# Sicherheitsanalytik und IT-Forensik

## Allgemeine Angaben

| | |
|---|---|
| **Kürzel** | M_SIF |
| **Modulverantwortliche** | Prof. |
| **Dozenten** | Prof. Dr. Koch, Prof. Dr. Stehr, Dr. Löser, Dr. Speth |
| **Lehrsprache** | Deutsch |
| **Semester** | 1 |
| **ECTS-Punkte** | 5 |
| **Kontaktstunden** | 40 |
| **Selbststudium** | 85 |
| **Dauer** | 1 Semester |
| **Art** | Pflicht |
| **Häufigkeit** | jedes Studienjahr |
| **Gewichtung** | 5/120 |
| **Prüfungsleistung** | **K**RS90 |

## Stichwörter

- Sicherheitsanalysen und -bewertungen
- Sicherheitskonzepte
- Durchführung IT-Forensischer Analysen

## Zugangsvoraussetzungen

- Grundlagen im Bereich IT-Sicherheit und Riskmanagement sind vorhanden.

## Verwendbarkeit

- Verwendbar in weiteren Spezialisierungsmodulen Cyber Security, in den Transfermodulen, im Seminar zu ausgewählten Forschungsthemen und in der Master-Thesis.

## Qualifikations- und Kompetenzziele

Die Studierenden sind in der Lage, Bedrohungen und Angriffsvektoren der heutigen Zeit richtig einzuschätzen. Sie wissen, wie Verhaltensanalyse und Netzwerkanalyse erfolgt. Zudem kennen sie die typischen Schwachstellen von Unternehmen und können darauf eine fundierte Sicherheitsanalyse durchführen und Bewertungen vornehmen. Die Studierenden sind ebenso befähigt, an die jeweilige Situation angepasste Sicherheitskonzepte zu entwickeln.
Die Studierenden kennen erforderlichen Schritte zur Durchführung einer forensischen Analyse und sind befähigt, vergangene und laufende Attacken zu bewerten, verstehen wie die Systeme kompromittiert wurden und erkennen offen Schwachstellen.

## Lehr- und Lernmethoden

Vorlesungen, Gruppenarbeit, Fallstudien, vertiefende und explorative Übungen, evtl. Einsatz von Software.

## Inhalte

- Sicherheitsanalyse und -bewertungen
  - Datenanalysen
  - Verhaltensanalysen (z.B. UBA, UEBA)
  - Netzwerkanalysen (z.B. Wireshark)
  - Technischen Analysen, Pen-Tests, etc.
- Sicherheitskonzepte

    - KI-basierter Schutz vor Malware und Viren
    - Firewalls und Next Generation Firewalls (NGF)
    - Intrusion Detection and Prevention Systems (IDS, IPS)
    - Data Leakage/Loss Prevention (DLP)
    - etc.
- IT-Forensik
    - Ziele und Grundbegriffe
    - Vorgehensweise und Werkzeuge
    - Sammlung, Analyse und Aufbereitung
    - Beispiele: Live Response (Sicherung flüchtiger Daten)
    - Smartphone Forensik

## Grundlegende Literaturhinweise

Eckert, C.: IT-Sicherheit: Konzepte - Verfahren - Protokolle, De Gruyter Studium, 2018
Pohlmann, N.: Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung, Springer Vieweg, 2022
Labudde, D. und Spranger, M.: Forensik in der digitalen Welt, Springer Verlag, 2017

## Ergänzende Literaturempfehlungen

Lang, M. und Löhr, H.: IT-Sicherheit: Technologien und Best Practices für die Umsetzung im Unternehmen, Hanser Verlag, 2022