Lerninhalte & Ziele des Moduls „Monitoring“

Inhalte

- **Wieso und weshalb Monitoring der IT-Infrastruktur?**
  - Möglichkeiten im Betrieb – Was kann/soll überwacht werden?
  - Was passiert bei Ausfall/IT-Problemen? – Benachrichtigung
- **Überwachungsmöglichkeiten/Protokolle**
  - Pingen
  - http(s)-Requests
  - TCP-Port Scans
  - DNS-Auflösung
  - Agent
  - SNMP/WIM
  - etc.
- **Blacklist-Monitoring [ist mein Mailserver blockiert?]**
- **Installation und Konfiguration von IT-Monitoring Produkten inkl. Praktische Übungen mit diversen Systemen und Clients**
  - Remote Monitoring & Management (RMM) - Software
    - NinjaOne (Demoversion)
  - Checkmk https://checkmk.com/de
  - Uptime Kuma https://uptime.kuma.pet/
  - Prometheus https://prometheus.io/
  - Grafana https://grafana.com/
  - Tactical RMM https://docs.tacticalrmm.com/
- **Profi-OpenSource-Anwendungen (Intrusion Detection System: IDS)**
  - Snort https://www.snort.org/
  - Zeek https://zeek.org/