Uge 15 – Introduktion til SIEM og Wazuh

I denne uge introduceres begrebet **SIEM (Security Information and Event Management)** samt værktøjet **Wazuh**, som anvendes resten af semesteret til central logindsamling, analyse og detektering af sikkerhedshændelser.

Ugen bygger videre på arbejdet med logning, audit og efterforskning fra de foregående uger og samler disse elementer i et samlet overvågnings- og detekteringsperspektiv.
Der arbejdes både med færdige detektioner og med forståelsen af, hvordan logdata bevæger sig gennem et SIEM-system.

Forberedelse

- Se kolonen *Forberedelse og pædagogisk tilrettelæggelse* i planen på It's learning

---

♂ Øvelser

- Øvelse 33 – Overvåg ændringer i filer med Wazuh
- Øvelse 34 – Detekter forsøg på SQL-injection med Wazuh
- Øvelse 35 – Detekter forsøg på Shellshock-angreb med Wazuh
- Øvelse 36a – Wazuh som logserver
- Øvelse 36b – Tilpasset detektering af kommandoer med Wazuh
- Øvelse 18.1 – Eftermiddagsøvelse: Opsætning af webservere på Proxmox

---

Læringsmål der arbejdes med i faget denne uge

I denne uge arbejdes der med følgende læringsmål fra studieordningen:

- **Viden**
  - Kendskab til relevante it-trusler
- **Færdigheder**
  - Implementere systematisk logning og monitorering af enheder
  - Kan analyser logs for hændelser og følge et revision spo

- **Kompetencer**
  - Kan håndtere enheder på command line-niveau
  - håndtere værktøjer til at identificere og fjerne/afbøde forskellige typer af endpoint trusler
  - Håndtere udvælgelse, anvendelse og implementering af praktiske mekanismer til at forhindre, detektere og reagere over for specifikke it-sikkerhedsmæssige hændelser.

Afleveringer

- Ingen.

Skema

Tirsdag

Tid	Aktivitet
08:15	Introduktion til dagen
08:35	Oplæg: Introduktion til SIEM
08:50	Gruppeøvelser: Wazuh-øvelser
09:45	Pause
10:20	Wazuh-øvelser fortsat
11:20	Opsamling og status
11:30	Pause
12:15	Eftermiddagsøvelser

Kommentarer

- Fokus i denne uge er forståelse af SIEM-arkitektur og logflow – ikke fuld beherskelse af alle Wazuh-funktioner.
- Det er forventeligt, at nogle detektioner virker komplekse første gang – de genbesøges senere i forløbet.

Last update: 2026-03-25 13:21:47