# Uge 16 – Overvågning med SIEM systemer

I denne uge arbejder I med **overvågning, detektering og analyse af sikkerhedshændelser ved hjælp af et SIEM-system**, med Wazuh som det centrale værktøj.

Ugen har fokus på at skabe en **sammenhængende forståelse af detection engineering** – fra idé og modellering til konkret implementering og visualisering.

I løbet af ugen kommer I til at:

- modellere detektering ved hjælp af *detekteringens 7 abstraktionslag*
- diskutere og kvalificere detekteringsdesign i grupper
- implementere egne dekodere og regler i Wazuh
- arbejde med logdata som grundlag for hændelser og alarmer
- visualisere sikkerhedshændelser i Wazuh Dashboards

Ugen kombinerer **analyse, praktisk arbejde og refleksion** og danner et vigtigt fundament for arbejdet med overvågning, hændelseshåndtering og eksamensprojektet.

---

## Forberedelse

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

---

## ♂ Øvelser

- Detekterings 7 abstraktionslag og detekterings pipeline
- Opsamling på Detekterings 7 abstraktionslag i grupper
- Detektering i Wazuh, med egen tilpasset regler
- Visualisering i Wazuh
- Eftermiddagsøvelse: Reaktivt svar med Wazuh
- Ekstra Eftermiddagsøvelse: Udvikle en tilpasset regel ud fra detekterings pipeline modellering

---

## Læringsmål der arbejdes med i faget denne uge

I denne uge arbejdes der med følgende læringsmål fra studieordningen:

- **Viden**
  - Viden om relevante it-trusler
- **Færdigheder**
  - Implementere systematisk logning og monitorering af enheder
- **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.

---

## Praktiske mål

- Alle studerende har modelleret en detection pipeline
- Alle studerende har implementeret en dekoder i Wazuh
- Alle studerende har implementeret en regel i Wazuh
- Alle studerende har implementeret en visualisering i Wazuh

---

## Skema – Tirsdag

| Tid | Aktivitet |
|---|---|
| 08:15 | Introduktion til dagen |
| 08:35 | Individuel øvelse: Detekteringens 7 abstraktionslag |
| 09:35 | Gruppeøvelse: Opsamling og diskussion af detekteringsmodeller |
| 10:00 | Pause |
| 10:15 | Introduktion til Wazuh-øvelser |

| Tid | Aktivitet |
|---|---|
| 10:20 | Praktisk arbejde med Wazuh: dekodere, regler og visualisering |
| 11:20 | Opsamling og status på Wazuh-øvelser |
| 11:30 | Lektion slut |

## Kommentarer

- Fokus er på **sammenhæng mellem modellering og implementering**
- Der forventes eksperimentering og iterativ afprøvning
- Øvelserne kan med fordel kobles direkte til semesterprojektet

Last update: 2026-04-12 17:32:46