

# Uge 14 - Introduktion til SIEM

## Emner

Ugens emner er:

- Introduktion til SIEM systemer.
- Introduktion til Wazuh.

## Mål for ugen

Herunder kan du læse ugens forskellige mål

### Praktiske mål

- At hver studerende har grundlæggende forståelse for hvad et SIEM system er.
- At hver studerende har lavet simple filtering af sikkerheds hændelser i Wazuh

### Læringsmål der arbejdes med i faget denne uge

#### Overordnede læringsmål fra studie ordningen:

- **Viden:**
  - Viden om relevante it-trusler
- **Færdigheder:**
  - Kan implementerer systematisk logning og monitorering af enheder
  - Kan analyser logs for hændelser og følge et revision spor
- **Kompetencer:**
  - Kan håndtere enheder på command line-niveau

### Øvelser

- [Uge 14 - Overvåg filer i directory for ændringer med Wazuh](#)
- [Uge 14 - Detekter SQL injection med Wazuh](#)
- [Uge 14 - Detekter Shellshock angreb med Wazuh](#)
- [Uge 14 - Wazuh som log server](#)

- [Uge 14 - Tilpasset dektekering af kommandoer](#)
- [Uge 14 - Eftermiddag - Opsætning af webserver](#)

## Tirsdag

Tid	Aktivitet
08:15	Introduktion til dagen
08:25	Udfyldelse af semester evaluering
08:35	Oplæg: Intro til SIEM
08:50	Gruppe øvelser: Wazuh opgaver
09:45	Pause
10:00	Samling og status på øvelserne
10:20	Wazuh opgaver forsat
11:20	Samling og status på øvelserne
11:30	Pause
12:00	Wazuh eftermiddags opgaver

🕒 2025-04-03 05:55:59