Uge 15 - *Overvågning med SIEM systemer*

Emner

Ugens emner er:

- Monitorering med Wazuh.
- Wazuh regler og dekoder.

Mål for ugen

Herunder kan du læse ugens forskellige mål

Praktiske mål

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

Læringsmål der arbejdes med i faget denne uge

Overordnede læringsmål fra studie ordningen:

- **Viden:** ..
- **Færdigheder:**
- Kan implementerer systematisk logning og monitering af enheder
- Kan analyser logs for hændelser og følge et revision spor
- **Kompetencer:**
- Kan håndtere enheder på command line-niveau
- Håndtere udvælgelse, anvendelse og implementering af praktiske mekanismer til at forhindre, detektere og reagere over for specifikke it-sikkerhedsmæssige hændelser.
- håndtere værktøjer til at identificere og fjerne/afbøde forskellige typer af endpoint trusler

Øvelser

- Uge 15 - Detekterings 7 abstraktionslag og dekterings pipeline
- Uge 15 - Opsamling på Detekterings 7 abstraktionslag i grupper
- Uge 15 - Detektering i Wazuh, med egen tilpasset regler
- Uge 15 - Visualisering i Wazuh
- Uge 15 - Eftermiddags opgave: Udvikle en tilpasset regle udfra detekterings pipeline modellering

Tirsdag

Tid	Aktivitet
08:15	Introduktion til dagen
08:35	Individuel Øvelse med detekterings 7 abstraktionslag
09:35	Gruppe øvelse med opsamling i grupperne på detekterings 7 abstraktionslag
10:00	Pause
10:15	Introduktion til Wazuh øvelser
10:20	Wazuh øvelser
11:20	Opsamling og status på Wazuh øvelser
11:30	Lektion slut

2025-04-08 05:23:58