

□ Øvelse 55 – Opsamling i grupper

Del og diskuter jeres detekteringspipelines

□ Formål med øvelsen

Denne gruppeøvelse bygger videre på jeres individuelle arbejde med detekteringspipelines. Målet er at sammenligne, diskutere og videreudvikle jeres modeller, så I får en fælles forståelse for, hvordan man strukturerer detektion i praksis.

Formålet med øvelsen er at styrke jeres evne til at vurdere og kvalificere designet af en detekteringspipeline.

I skal sammenligne jeres individuelle løsninger og i fællesskab identificere styrker, svagheder og potentielle forbedringer.

Øvelsen træner jeres evne til at: - analysere og diskutere detektionsdesigns kritisk - anvende fagbegreber i dialog - sammenfatte bedste praksis i en fælles model

Det er samtidig en vigtig øvelse i perspektivering og samarbejde, der afspejler arbejdet i virkelige Blue Team-situationer.

□ Instruktioner

Denne øvelse udføres i grupper og bygger direkte på jeres individuelle arbejde med de 7 detekteringslag.

Øvelsens tidsramme er ca. 25 minutter.

□ Trin 1 – Del jeres løsninger

Hver deltager fremlægger sin individuelle pipeline (brug skabelonen).

Gennemgå jeres scenarie lag-for-lag – max 3 minutter per person.

□ Trin 2 – Diskuter jeres observationer

Diskuter følgende spørgsmål i gruppen:

- Hvor var jeres løsninger forskellige – og hvorfor?
 - Hvilke valg medfører risiko for falske positive?
 - Hvilken løsning ville være nemmest for en angriber at undgå?
 - Har nogen af jer tænkt på automatisk reaktion eller udelukkende alarmering?
 - Hvilke logkilder og data var mest centrale for jeres scenarie?
-

□ Trin 3 – Byg en fælles pipeline

Vælg ét af jeres scenarier og sammensæt gruppens bedste pipeline.

Kombiner de stærkeste elementer fra jeres individuelle løsninger og brug skabelonen:

Angreb:

...

1. Feature Selection

Hvordan manifesterer angrebet sig?

2. Feature Extraction

Hvor kan informationen hentes? (logkilder, processer, sockets)

3. Event Selection

Hvordan udvælger I det relevante?

4. Event Detection

Hvordan identificeres en begivenhed teknisk?

5. Attack Detection

Hvordan bestemmes, at det er et angreb?

6. Attack Classification

Hvordan navngives og kategoriseres hændelsen?

7. Attack Alarming

Hvordan og til hvem alarmeres der?

□ Refleksionsspørgsmål

- Hvilket lag var sværest at blive enige om?
 - Hvordan balancerer man følsomhed og præcision i detektering?
 - Hvilke logkilder er mest kritiske i jeres scenarie?
 - Hvordan kan I bruge denne metode i jeres semesterprojekt?
-

Tip: Jeres fælles pipeline kan danne grundlag for en Wazuh-regel, I implementerer senere – eller for et afsnit i jeres rapport om overvågning og hændeshåndtering.

□ Perspektiv – Brug af modellen i jeres projekt

Når I arbejder videre med semesterprojektet, kan I bruge modellen med de 7 lag til at:

- dokumentere jeres overvågningsstrategi
- strukturere udviklingen detection pipeline, Som blandt andet redegøre for Hændelses regler i fx Wazuh
- forklare hvordan I sikrer både detection in depth og detection in breadth
- analysere, hvorfor visse angreb kunne undgå detektion – og hvordan det kunne forbedres

Modellen er altså ikke bare et øvelsesværktøj – men en metode til systematisk og reflekteret sikkerhedsdesign.

Last update: 2026-04-14 07:08:04