Uge 16 – Eftermiddagsøvelse: Vælg en PoC til detektering (Gruppeøvelse)

Information

Formålet med denne eftermiddagsøvelse er, at I som studiegruppe arbejder selvstændigt med **Proof of Concept (PoC)-guides** fra Wazuhs officielle dokumentation.

En **Proof of Concept (PoC)** er en demonstration, der viser hvordan en specifik sikkerhedsteknik, sårbarhed eller angrebsmetode kan detekteres i et system.

En **detektering** er en regel eller mekanisme, der identificerer en specifik type aktivitet eller angreb i systemets logs.

I skal vælge **én detektering**, som ikke tidligere er gennemgået i undervisningen, og implementere den praktisk i jeres eget miljø.

Øvelsen giver jer erfaring med:

- at arbejde ud fra teknisk dokumentation
- at implementere sikkerhedsdetektering
- at teste og validere sikkerhedshændelser
- at dokumentere jeres arbejde

Øvelsen udføres som **selvstændigt gruppearbejde uden for undervisningen**.

Denne øvelse minder om en rigtig opgave i et **Security Operations Center (SOC)**, hvor analytikere implementerer og tester nye detekteringer i et SIEM-system.

Baggrund

Wazuhs dokumentation indeholder en række **Proof of Concept-guides**, der viser hvordan specifikke angreb, teknikker eller sikkerhedshændelser kan detekteres.

Disse PoC-guides er ofte relateret til:

- kendte sårbarheder
- MITRE ATT&CK-teknikker
- almindelige angrebsmønstre

Ved at implementere disse guides får man praktisk erfaring med hvordan sikkerhedsdetektering kan konfigureres i et SIEM-system.

Øvelsen bygger videre på jeres tidligere arbejde med:

- loganalyse
- Wazuh-agenter
- sikkerhedshændelser

Instruktioner

Øvelsen løses i studiegrupper og kræver dokumentation af arbejdet.

---

1 Udvælg en Proof of Concept-guide

1. Gå til Wazuhs Proof of Concept Guide: https://documentation.wazuh.com/current/proof-of-concept-guide/index.html
2. Udvælg **én PoC-guide** som virker realistisk at implementere i jeres miljø.

Tip: Da dette er jeres første arbejde med PoC-guides, bør I undgå de mest avancerede scenarier.

---

2 Implementér detekteringen

1. Følg den valgte PoC-guide trin for trin.
2. Implementér detekteringen i jeres Wazuh-miljø.
3. Udløs den aktivitet eller hændelse som PoC'en beskriver.
4. Verificér at Wazuh registrerer hændelsen korrekt.

---

3 Dokumentation

I skal dokumentere følgende:

- Hvilken PoC-guide I har valgt
- Hvad detekteringen forsøger at opdage
- Hvilken konfiguration der var nødvendig:
  - relevante logfiler

  - Wazuh-regler
  - agent- eller serverkonfiguration
- Hvordan I testede detekteringen
- Screenshots eller loguddrag fra **Wazuh-dashboardet**, der viser hændelsen

---

4 Refleksion

Diskutér i gruppen og besvar følgende spørgsmål i jeres dokumentation:

- Hvad gjorde den valgte guide nem eller svær at implementere?
- Hvad lærte I om Wazuhs opbygning ved at følge guiden?
- Hvordan kunne jeres detektering udbygges med automatiseret respons?
- Hvilke overvejelser ville I gøre jer, hvis dette skulle anvendes i et produktionsmiljø?
- Hvilken **MITRE ATT&CK-teknik** relaterer jeres PoC til?

Links

Proof of Concept guides – Wazuh

Last update: 2026-03-20 13:58:28