Uge 16 – Eftermiddagsøvelse: Vælg en POC til detektering

Formål

I denne øvelse skal du og din gruppe arbejde med *Proof of Concept*-guides fra Wazuhs officielle dokumentation. I vælger to forskellige detekteringer, som ikke tidligere er gennemgået i undervisningen, og implementerer dem praktisk i jeres eget miljø. Øvelsen giver jer erfaring med at arbejde med færdige vejledninger og giver idéer til, hvordan man strukturerer detektering i praksis.

Baggrund

Wazuhs dokumentation indeholder en række *Proof of Concept*-guides, der viser, hvordan man kan detektere bestemte angreb, teknikker og trusler. Disse guides er detaljerede og ofte relateret til kendte sårbarheder eller angrebsformer, som I også kan møde i virkelige scenarier.

Denne øvelse bygger videre på tidligere erfaringer fra kurset og giver jer mulighed for at eksperimentere med flere avancerede regler, logkilder og reaktioner.

Opgavebeskrivelse

1. Gå til Wazuhs Proof of Concept Guide
2. Udvælg to forskellige detekteringer, som **ikke er brugt i tidligere øvelser**
3. Implementér begge detekteringer i jeres miljø
4. Dokumentér:
5. Hvilke PoC-guides I har valgt og hvorfor
6. Hvad konfigurationen krævede (logfiler, regler, agent/server)
7. Hvordan I testede detekteringen
8. Screenshots eller log-uddrag fra Wazuh-dashboardet

 Det anbefales at vælge to forskellige typer detekteringer – fx én der overvåger filsystemet og én der overvåger netværksadfærd.

Nyttige links

- Proof of Concept guides – Wazuh

Refleksionsspørgsmål

- Hvad gjorde de valgte guides nemme eller svære at implementere?
- Hvad lærte I om Wazuhs opbygning ved at følge disse guides?
- Hvordan kunne en af jeres valgte detekteringer udbygges med automatiseret respons?
- Hvilke overvejelser ville I gøre jer, hvis I skulle bruge dette i et rigtigt produktionsmiljø?

2025-04-03 05:55:59