Øvelse 37 – Active Response i Wazuh (automatisk handling)

Information

I denne øvelse arbejder du med **Active Response** i Wazuh.

Hvor du tidligere har arbejdet med: `log → analyse → detection → alarm`

arbejder du nu med: **log → analyse → detection → alarm → handling**

Formålet er at forstå:

- hvordan Wazuh kan reagere automatisk på hændelser
- hvordan man omsætter en detection til en konkret handling
- hvordan sikkerhedssystemer kan stoppe angreb i realtid

Dette er et første skridt mod **Security orchestration and response (SOAR)**

I øvelsen skal du arbejde selvstændigt ud fra Wazuh dokumentationen.

Baggrund

Active Response gør det muligt for Wazuh at udføre handlinger som:

- blokere IP-adresser
- deaktivere brugere
- genstarte services
- køre scripts på den overvågede host

Handlingerne trigges af specifikke regler.

Eksempel:

log → analyse → detection → alarm → blokér IP

IDS vs IPS perspektiv:

Indtil nu har Wazuh-agenten primært fungeret som et **IDS (Intrusion Detection System)**:

- Den indsamler logs
- Sender dem til Wazuh-manageren
- Hvor de analyseres og evt. bliver til alarmer

 Systemet opdager altså hændelser – men reagerer ikke automatisk.

Med **Active Response** ændrer dette sig:

- Wazuh-manageren analyserer logdata
- Trigger en alarm
- Sender en kommando tilbage til agenten
- Agenten udfører en handling (fx blokering eller deaktivering)

 Active Response skaber et feedback-loop mellem analyse og handling.

 Systemet går dermed fra: **detection → til → detection + handling**

Dette betyder, at Wazuh nu får egenskaber, der minder om et **IPS (Intrusion Prevention System)**, da det ikke kun opdager angreb – men også aktivt forsøger at stoppe dem.

 Dette kan også ses som et *closed-loop security system*, hvor detection automatisk fører til respons.

 Bemærk: Active Response skal bruges med omtanke, da automatiske handlinger kan påvirke legitime brugere eller systemer.

 Perspektiv: I denne øvelse arbejder du med et konkret eksempel på Active Response.

Det er vigtigt at forstå, at Active Response i Wazuh er en generel mekanisme, som kan anvendes i mange forskellige scenarier – ikke kun de eksempler du arbejder med her.

Du kan f.eks.: - blokere IP-adresser - deaktivere brugere - stoppe processer - køre egne scripts - reagere på næsten alle typer detections

 Active Response er derfor et centralt værktøj i Security orchestration and response (SOAR), hvor systemer ikke kun opdager angreb – men også reagerer på dem.

Hvis du vil dykke dybere ned i mulighederne, kan du læse mere her:
Wazuh - active response

Instruktioner

I denne øvelse skal du bruge **Wazuh dokumentation** til selv at konfigurere en Active Response.

Du arbejder ikke med en fast guide – men med at forstå og anvende dokumentation i praksis.

 Du arbejder med hele kæden:

detection → beslutning → response → validering

---

1 Find relevant dokumentation

Vælg en af følgende use cases fra Wazuh dokumentationen:

- Blocking SSH brute force
- Restarting Wazuh agent
- Disabling user account

 Bemærk: Dokumentationen tager ofte udgangspunkt i Red Hat-baserede Linux-distributioner.
Selvom du arbejder med Ubuntu, er den overordnede tilgang den samme:

- Wazuh-konfiguration er identisk
- Forskelle er fx `apt` vs `yum`

 Fokusér på konceptet – ikke copy/paste.

---

2 Vælg en use case

Du skal vælge én af følgende:

 Blocking SSH brute force

- Blokerer angriberens IP
- Klassisk sikkerhedsrespons

 Disabling user account

- Deaktiverer en bruger
- Relaterer til identity security

 Restarting Wazuh agent (valgfri)

- Genstarter service
- Fokus på drift og stabilitet

---

3 Implementér Active Response

Følg dokumentationen og opsæt:

- Active Response konfiguration
- Kobling til en regel (rule.id eller gruppe)

 Sørg for at forstå:

- hvad der trigger din response
- hvad systemet gør

---

4 Test din løsning

1. Udfør en handling der trigger din detection
2. Verificér at:
3. detection bliver trigget
4. Active Response bliver udført

---

5 Dokumentation

Dokumentér:

- hvilken use case du valgte
- hvordan du implementerede den
- hvordan du testede den
- hvad resultatet var

 Din løsning er korrekt når:

- din detection laver en alarm
- din Active Response udføres
- du kan forklare sammenhængen

Refleksion

- Hvad er forskellen på detection og response?
- Hvornår er automatisk respons en fordel – og hvornår en risiko?

- Kan legitime brugere blive ramt af din løsning?
- Hvordan kunne en angriber forsøge at omgå din response?
- Hvilken type hændelser bør automatiseres?
- Hvornår bør et system fungere som IDS vs IPS?
- Hvad kan konsekvensen være af en forkert konfigureret Active Response?

CIS Controls – Relevans

CIS Control	Titel	Relevans
8	Audit Log Management	Detection som input til handling
17	Incident Response Management	Automatiseret respons
13	Network Monitoring and Defense	Blokering af netværksaktivitet

---

Links

- Wazuh - active response
- Blocking SSH brute force
- Restarting Wazuh agent
- Disabling user account

Last update: 2026-04-08 17:33:07