Øvelse 33 – Overvåg ændringer i filer med Wazuh

Information

Formålet med denne øvelse er at lære, hvordan **Wazuh-agenten** kan anvendes til at opdage ændringer i filer gennem **File Integrity Monitoring (FIM)**.

Du arbejder dermed med en central sikkerhedsfunktion:
at kunne identificere uautoriserede ændringer i systemet og omsætte dem til konkrete sikkerhedshændelser (detections).

Overvågning af filintegritet er en central del af systemovervågning og anvendes bredt i professionelle it-miljøer, både til sikkerhed og fejlfinding.

Tidligere i forløbet har du arbejdet med auditd, som også kan anvendes til overvågning af filaktiviteter.
Auditd og Wazuhs **File Integrity Monitoring (FIM)** har hver deres styrker:

- Auditd giver meget detaljeret lavniveau-logging af systemkald
- Wazuh er stærk til realtidsrapportering, central loghåndtering og korrelation

De to værktøjer anvendes ofte sammen, hvor Wazuh analyserer og reagerer på hændelser baseret på auditd-logs. I denne øvelse fokuseres der dog udelukkende på Wazuhs egen File Integrity Monitoring (FIM).

Alle Wazuh øvelser er gruppe øvelser, da de skal udføres på proxmox serveren

---

Forudsætninger

- Wazuh-agenten er installeret og aktiv på hosten
- Du har terminaladgang og root-rettigheder
- Adgang til Wazuh Dashboard

> Wazuh har også sin egen guide til opsætning af FIM, Den kan findes her.

Instruktioner

I denne øvelse skal du arbejde med Wazuhs File Integrity Monitoring (FIM) i praksis.

Du vil konfigurere Wazuh-agenten til at overvåge et directory, udføre ændringer i filer og analysere de hændelser, som genereres i Wazuh Dashboard.

Formålet er at forstå:

- hvordan ændringer i filer bliver til sikkerhedshændelser (events)
- hvordan Wazuh registrerer og præsenterer disse hændelser
- hvordan filovervågning kan bruges til detektion af uautoriseret aktivitet

Du arbejder altså ikke kun med konfiguration – men med hele kæden:

ændring → event → detection → analyse

---

1 Forstå Wazuh-konfigurationen

Wazuh-agentens konfigurationsfil findes her: `/var/ossec/etc/ossec.conf`

Konfigurationen er skrevet i XML-format. File Integrity Monitoring konfigureres i `<syscheck>`-blokken.

Undersøg konfigurationfilen, og skab et overblik over strukturen.

---

2 Opret et folder der skal overvåges

Opret en folder som Wazuh skal overvåge for ændringer i filer. Folderen skal have følgende sti: `/home/SecretFolder`

---

3 Tilføj folder til Wazuh File Integrity Monitoring konfigurationen

Nu skal Wazuh-agenten konfigureres til at detektere ændringer i filer i folderen.

1. Åbn konfigurationsfilen `/var/ossec/etc/ossec.conf` i en text editor.
2. Find `<syscheck>`-blokken og tilføj følgende linje til sidst inde i den: `<directories check_all="yes" report_changes="yes" realtime="yes">/home/SecretFolder</directories>`
   Forklaring
   - check_all="yes" → Overvåg alle filtyper
   - report_changes="yes" → Rapporter ændringer i filindhold
   - realtime="yes" → Overvåg ændringer i realtid

> `<syscheck>-blokken konfigurerer Wazuhs File Integrity Monitoring (FIM), herunder hvilke filer og mapper der overvåges, samt hvilke hændelser der genereres og sendes som logevents.`

3. Gem og luk filen

---

4 Genstart Wazuh-agenten

For at Wazuh-agenten genindlæser konfigurationen. Genstart Wazuh agenten med kommandoen `systemctl restart wazuh-agent`

---

5 Udfør ændringer i det overvågede directory

Nu skal du teste, om din konfiguration virker ved at udføre ændringer i det overvågede directory.

1. Opret en fil: `/home/SecretFolder/secretFile.txt`
2. Tilføj tekst til filen: `echo "Hello security world" | sudo tee /home/SecretFolder/secretFile.txt > /dev/null`
3. Slet filen igen: `rm /home/SecretFolder/secretFile.txt`

---

6 Analyse i Wazuh Dashboard

1. Log ind i Wazuh Dashboard
2. Gå til Threat hunting → Events
3. Søg efter følgende ved at bruge filteret `rule.groups: syscheck`
4. Verificér at følgende hændelser er registreret:
   - Fil oprettet
   - Fil ændret
   - Fil slettet

 Dette er konkrete eksempler på detections, hvor en ændring i systemet bliver omsat til en sikkerhedshændelse i Wazuh.

 Tip: Hvis du ikke ser nogen hændelser, så prøv at: - opdatere siden - udvide tidsintervallet

---

7 Udforsk hændelserne

Klik på forstørrelsesglasset ved hver hændelse for at åbne *Document Details*.

Undersøg:

- Hvilken regel udløste hændelsen?
- Hvilken fil blev påvirket?
- Hvilken bruger udførte handlingen?
- Hvilke alternative søgeparametre kan anvendes i dashboardet?

Refleksion

Overvej følgende spørgsmål:

- Hvad er fordelene ved at overvåge følsomme filer med Wazuh?
- Hvordan adskiller Wazuhs File Integrity Monitoring sig fra auditd?
- Hvordan kan realtidsalarmer bruges til hurtig reaktion på angreb eller fejl?
- Hvilke filer eller directories ville være kritiske at overvåge i et produktionsmiljø?
- Hvornår er en filændring legitim, og hvornår er den mistænkelig?

CIS Controls – Relevans

CIS Control	Titel	Relevans
8	Audit Log Management	Wazuh FIM genererer strukturerede logevents
17	Incident Response Management	Filændringer kan indikere kompromittering
3	Data Protection	Overvågning understøtter dataintegritet

Links

-Wazuh FIM configuration

Last update: 2026-03-25 11:45:21