Opgave 33 – Overvåg ændringer i filer med Wazuh

Formål

Formålet med denne øvelse er at lære, hvordan man kan bruge **Wazuh-agenten** til at overvåge ændringer i filer og mapper på en host. Det giver mulighed for at opdage uønskede eller mistænkelige ændringer, som kan være tegn på fx malware, uautoriseret adgang eller konfigurationsændringer.

Dette er en vigtig del af systemovervågning og bruges i mange professionelle it-miljøer, både til sikkerhed og fejlfinding.

Tidligere i forløbet har du arbejdet med `auditd`, som også kan bruges til overvågning af filaktiviteter. `auditd` og Wazuhs File Integrity Monitoring (FIM) har hver deres styrker. Hvor Wazuh er stærk til realtidsrapportering og central loghåndtering, tilbyder `auditd` meget detaljeret kontrol og lavniveau-logging af systemkald.

Derfor bliver de to værktøjer ofte brugt sammen. Wazuh kan fx analysere og reagere på hændelser direkte fra `auditd`-loggen – så man får det bedste fra begge verdener.

Introduktion

Wazuh-agenten kan overvåge ændringer i både enkeltfiler og hele directories. I denne øvelse skal du konfigurere Wazuh til at overvåge en mappe og derefter se, hvordan ændringer automatisk bliver registreret og vist i dashboardet.

Wazuhs overvågningsfunktion kaldes *file integrity monitoring*, og den konfigureres i filen `/var/ossec/etc/ossec.conf`, som er skrevet i XML-format. Det betyder, at man tilføjer nye indstillinger inde i bestemte "blokke" – f.eks. `<syscheck>...</syscheck>`, som du kommer til at arbejde med her.

Forudsætninger

- Øvelsen skal udføres på en host (computer), hvor **Wazuh-agenten er installeret og aktiv**.

- Du skal have adgang til terminalen og kunne redigere konfigurationsfiler med root-rettigheder.

Trin for trin – Sådan gør du

1. Forstå konfigurationen

Konfigurationsfilen findes her:

```
/var/ossec/etc/ossec.conf
```

Filens struktur er i XML-format, og de fleste relevante indstillinger findes inde i `<syscheck>`-blokken.

---

2. Opret et directory, der skal overvåges

```
mkdir /home/SecretFolder
```

---

3. Tilføj mappen til Wazuhs overvågning

1. Åbn konfigurationsfilen med en teksteditor:

```
sudo nano /var/ossec/etc/ossec.conf
```

1. Find blokken `<syscheck>` og indsæt følgende linje 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 indholdsændringer - `realtime="yes"` → Overvåg i realtid

1. Gem og luk filen

---

4. Genstart Wazuh-agenten

```
sudo systemctl restart wazuh-agent
```

---

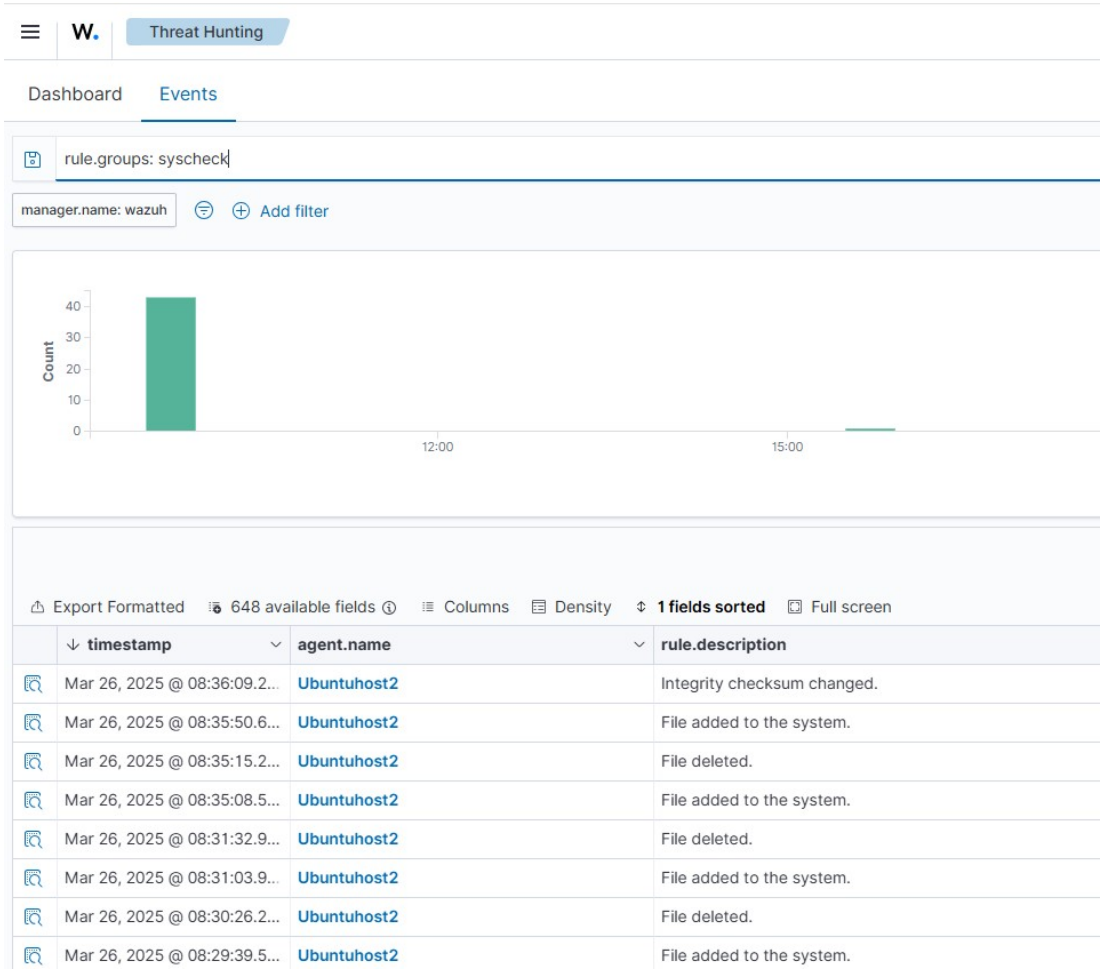
5. Udfør ændringer i mappen

```
# Opret fil
sudo touch /home/SecretFolder/secretFile.txt

# Tilføj tekst til filen
echo "Hello security world" | sudo tee /home/SecretFolder/secretFile.txt >
/dev/null

# Slet fil igen
sudo rm /home/SecretFolder/secretFile.txt
```

---

6. Se resultatet i Wazuh Dashboard

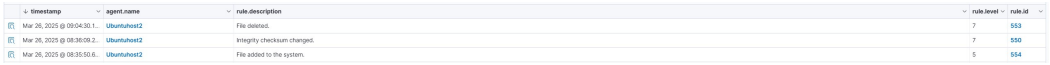
1. Log ind i **Wazuh Dashboard**
2. Gå til **Threat hunting → Events**



3. I søgefeltet øverst, skriv:

```
rule.groups: syscheck
```

1. Du bør nu se tre hændelser:
   - Fil oprettet
   - Fil ændret
   - Fil slettet



> *Integritetscheck på filer er en ressourcekrævende operation. Derfor udføres de ikke konstant, hvilket kan betyde, at hændelser (fx filændringer) tager lidt tid om at blive vist i dashboardet.*

---

1. Udforsk hændelserne:

Klik på forstørrelsesglasset til venstre for hver af de 3 hændelser for at åbne *Document Details*. Her kan du se detaljerede oplysninger om hændelsen.

Undersøg fx:

- Hvor kommer søgeparameteren `rule.groups: syscheck` fra?
- Kan du finde alternative søgeparametre?

Ekstra viden og links

- File Integrity Monitoring – Wazuh PoC-guide
- Wazuh Ruleset – Regler og alarmer

Refleksionsspørgsmål

- Hvad er fordelene ved at overvåge følsomme filer med Wazuh?
- Hvordan adskiller Wazuh sig fra `auditd`, som du tidligere har arbejdet med?
- Hvordan kan man bruge realtidsalarmer til at reagere hurtigt på angreb eller fejl?

CIS Controls – Kobling

Denne øvelse understøtter følgende CIS Controls (v8):

CIS Control	Titel	Relevans
8 – Audit Log Management	Overvågning og analyse af logs	Wazuhs FIM genererer strukturerede logevents, der kan bruges til at opdage systemændringer
17 – Incident Response Management	Håndtering af sikkerhedshændelser	Hændelser som filændringer eller sletninger kan bruges som indikatorer for kompromittering
3 – Data Protection	Beskyttelse af følsomme data	Ved at overvåge ændringer i kritiske filer og mapper understøttes dataens integritet og fortrolighed

 Du kan bruge denne viden til at relatere øvelsen til praksisnære sikkerhedsrammeværk og compliance-arbejde – fx i eksamensrapporten eller til dokumentation af forsvarslag.

2025-04-03 05:55:59