Øvelse 56 – Simpel visualisering i Wazuh Dashboards

Formål

Formålet med denne øvelse er at gøre dig i stand til at filtrere, analysere og visualisere sikkerhedshændelser i Wazuh Dashboard, samt anvende visualiseringer til at identificere mønstre og støtte hændelseshåndtering.

Baggrund

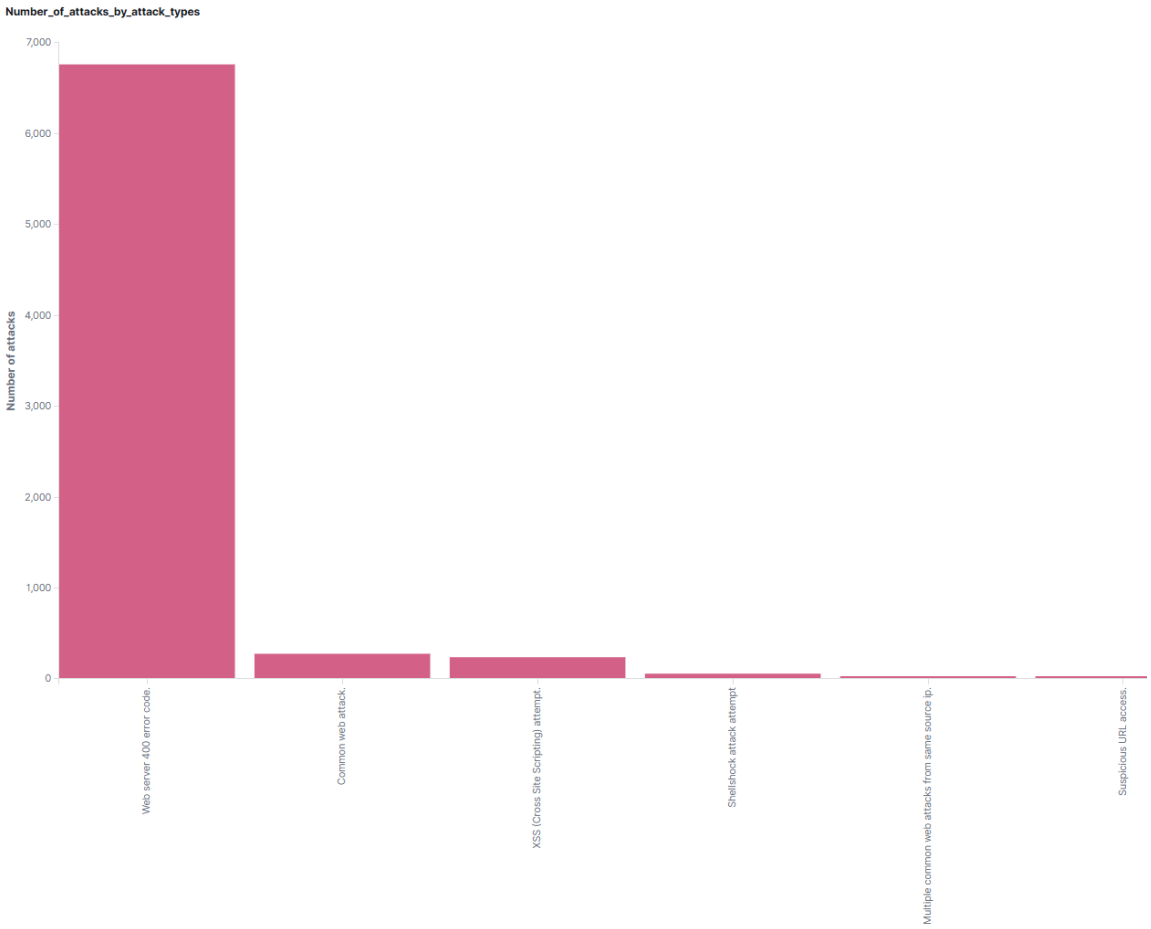
Hvis man skal kigge igennem store mængder logfiler eller hændelser, kan det være svært at danne sig et overblik
over, hvad der sker i de systemer, som Wazuh monitorerer. Visualisering er en metode til at gøre store datamængder
overskuelige, så det bliver lettere at identificere mønstre, afvigelser og mulige trusler.

I Wazuh Dashboards kan du oprette visualiseringer på baggrund af hændelser (alerts) eller rå logdata. Disse
visualiseringer kan hjælpe med at svare på spørgsmål som:

- Hvilke brugere fejler ofte login?
- Er der flere angreb på bestemte tidspunkter?
- Hvilke IP-adresser genererer flest hændelser?

Visualiseringerne kan vises som søjlediagrammer, tidslinjer eller tabeller og samles i dashboards til løbende overvågning.

I nedstående billede vises en visualisering fra Wazuh, der viser antallet er detekteret angreb, fordelt ud fra angrebstype:



Antal angreb fordelt på angrebstype

I det konkrete tilfælde, hjælper visualiseringen med at skabe et hurtigt overblik over hvilket type angreb, systemet oftes bliver udsat for.

Fra data til visualisering

Når man skal skabe en visualisering i Wazuh, er der to hovedtrin:

1. **Definér datasættet**:
   Find de relevante hændelser eller logs med en forespørgsel i fx *Discover* eller *Threat Hunting*.
2. **Opret en visualisering**:
   Brug Dashboards til at præsentere resultaterne – f.eks. i et søjlediagram, tidslinje eller tabel.

Wazuh indekserer mange felter, du kan søge på – fx:

- `rule.groups` – kategorisering af hændelser
- `full_log` – hele loglinjen fra agenten

- `agent.name` – hvilken maskine hændelsen kommer fra
- `rule.id`, `level`, `srcip`, `user.name` – og mange flere

> Brug disse felter til at bygge præcise forespørgsler og visualiseringer.

Eksempel: Failed logins

Hvis du vil undersøge fejlede loginforsøg på din Ubuntu-host, kan du gøre det på to måder:

- Brug hændelser fra Wazuh-regler:

```
rule.groups: "authentication_failed"
```

- Brug en søgning på den rå loglinje (fra fx `auth.log`):

```
full_log: "*Failed password for*"
```

I begge tilfælde kan du bruge datofilter og fx gruppere efter IP-adresse eller bruger for at skabe et overblik.

Begge metoder giver forskellige styrker: hændelsesbaseret søgning udnytter eksisterende regler,
mens logbaseret søgning giver mere fleksibilitet og dækker ikke-standard hændelser.

Eksempler på visualiseringstyper

Når du har defineret dit datasæt, kan du visualisere det på forskellige måder:

- **Søjlediagram** – Antal hændelser pr. time, dag eller uge
- **Tidslinje** – Overblik over aktivitet over tid
- **Tabel** – Vis hvilke brugere eller IP'er der optræder hyppigst
- **Histogram** – Aktivitet fordelt over timer, dage eller uger

Du kan kombinere flere visualiseringer i ét dashboard og tilføje filtre eller søgefelter for interaktiv analyse.

Dashboards i Wazuh

Et **dashboard** i Wazuh er en samling af visualiseringer, som præsenterer systemdata og hændelser i et samlet overblik.
Det kan fx bestå af:

- en søjlegraf med failed logins fordelt over tid
- en tabel over brugere med flest fejlforsøg
- et histogram med aktivitet fra en bestemt IP

Dashboards er særligt nyttige til **kontinuerlig overvågning** og til hurtigt at kunne reagere på ændringer i mønstre.
Når du arbejder med hændelseshåndtering eller sikkerhedsmonitorering, kan dashboards fungere som et **situationsbillede**
– både historisk og i realtid.

 I Wazuh kan du tilpasse dashboards med filtre, søgninger og datointervaller, så de matcher dine behov og cases.

Instruktioner

For at gøre øvelsen konkret, bruger vi eksemplet "fejlede autentificeringsforsøg" – men du opfordres til selv at vælge en anden hændelsestype, som er relevant for dit projekt eller dit miljø.

Alt afhæning er jeres konfiguration, skal i måske undersøge hvilket loglinjer der bliver generet ved den hændelse i ønsker at visualiserer, så vær forberedt på at der skal eksperimenters lidt

---

Trin 1: Forbered et datasæt

Start med at vælge en hændelsestype, du gerne vil visualisere. Det kan være noget, du allerede har genereret – fx brute force, reverse shell eller sudo-misbrug.

1. Gå til **Threat Hunting** → **Events** og find en hændelse, du vil analysere.
2. Udvælg et felt, du vil filtrere på – fx `rule.groups`, `rule.id`, `srcip` eller `agent.name`.
3. Skift til **Discover** og opret en forespørgsel.
   Eksempel (fejlede logins):

   ```
   rule.groups: "authentication_failed"
   ```

4. Justér datointervallet, så du er sikker på at der vises resultater.
5. Klik på **Save** i øverste højre hjørne og gem din søgning med et passende navn.

 Sørg for at der faktisk er data i forespørgslen – ellers bliver visualiseringen tom.

Trin 2: Opret en visualisering

1. Gå til **Visualize** (via menuen i øverste venstre hjørne).
2. Klik på **Create visualization** og vælg **Vertical bar**.
3. Under *Choose a source*, vælg det datasæt du gemte i trin 1.

Nu skal du konfigurere visualiseringen:

- **Metrics (Y-akse)**
  - Aggregation: `Count`
  - Dette viser antallet af hændelser
- **Buckets (X-akse)**
  - Klik "Add"
  - Aggregation: `Terms`
  - Field: fx `agent.name` eller `srcip`
  - Klik **Update** for at se resultatet
- Klik **Save as** og giv visualiseringen et sigende navn.

Trin 3: Byg et dashboard (valgfrit)

Et dashboard samler flere visualiseringer i ét overblik.

1. Gå til **Dashboards** via menuen og klik **Create new dashboard**
2. Klik på **Add** i øverste højre hjørne og vælg den visualisering du netop har lavet
3. Klik **Save**, og giv dashboardet et navn

 Du kan tilføje flere visualiseringer efter behov – fx forskellige datakilder, filtrering på tid, bruger eller IP. Brug dashboards til at danne situationsbilleder i praksis.

Trin 4: Udforsk selv

Der er mange muligheder i Wazuh Dashboards. Prøv fx at:

- Skifte diagramtype (fx pie chart eller table)
- Gruppere efter forskellige felter

- Tilføje interaktive filtre
- Kombinere visualiseringer i dashboards

Du lærer mest ved at eksperimentere og prøve ting af.

Refleksionsspørgsmål

```
- Hvad kan du hurtigt få overblik over med visualisering?
- Hvilke felter var mest nyttige i din forespørgsel?
- Hvad kunne du ikke se i visualiseringen – og hvorfor?
- Hvordan kan dashboards bruges i praksis i et SOC eller Blue Team?
```

CIS Controls – Kobling

CIS Control	Titel	Relevans
08 – Audit Log Management	Brug logdata aktivt	Visualisering skaber overblik over hændelser og trends
06 – Access Control Management	Identificér misbrugsmønstre	Visualisering kan vise autentificerings fejl, privilege-escalation mv.
17 – Incident Response Management	Understøt analyser og efterforskning	Dashboards kan bruges til at identificere mønstre og reagere hurtigt

---

Nyttige links

- Wazuh – Dashboards documentation
- Opensearch - Dashboards documentation

2025-04-08 05:23:58