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

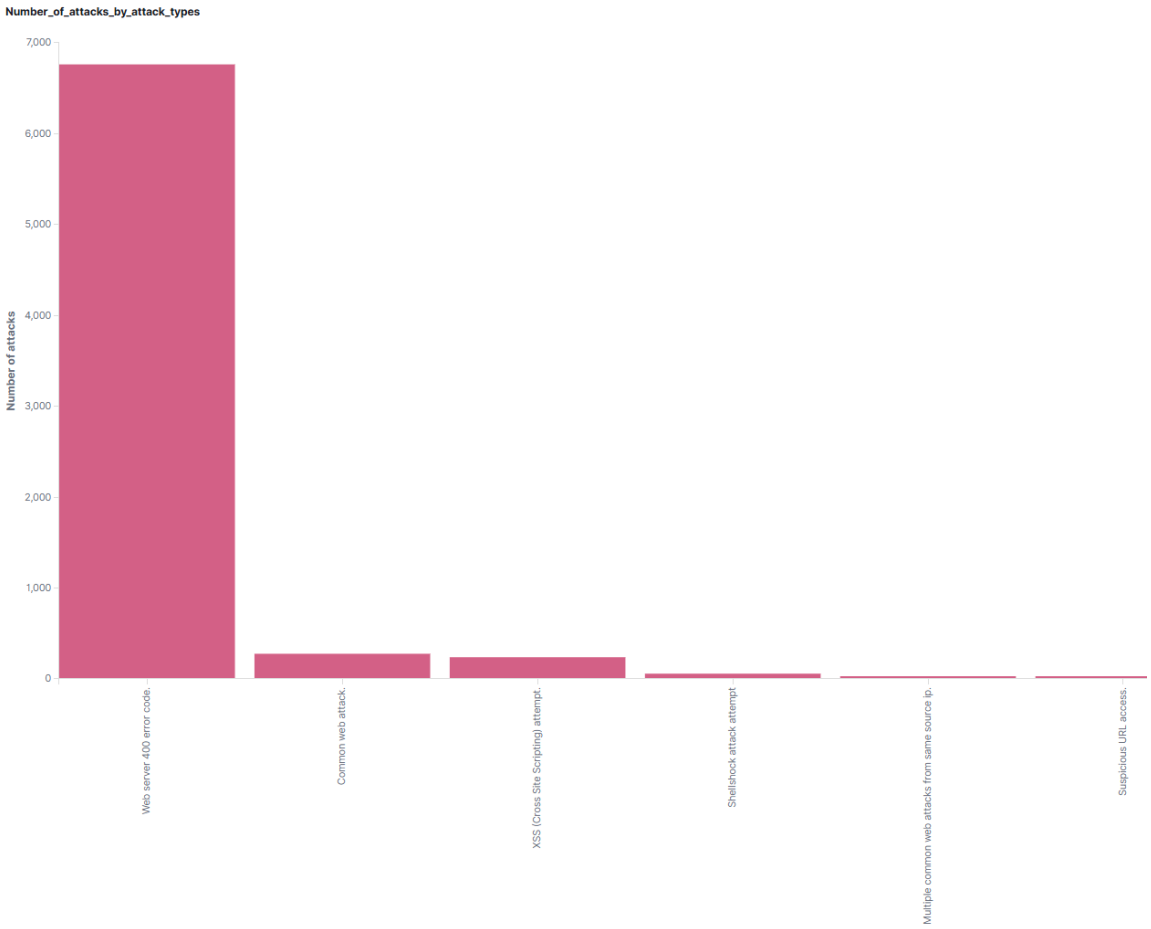
Hvis man skal kigge igennem store mængder logfiler eller hændelser, kan det være svært at danne sig et overblik
over, hvad der sker i de systemer, som Wazuh monitorerer. Visualisering er en metode til at gøre store datamængder
overskuelige, så det bliver lettere at identificere mønstre, afvigelser og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



Antal angreb fordelt på angrebstype

I det konkrette 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 alert indekset 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:

1. Brug hændelser fra Wazuh-regler: rule.groups: "authentication_failed" i indekset *wazuh-archives*
2. Eller 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 bruges 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 hvilke 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

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: rule.groups: "authentication_failed"
4. Justér datointervallet, så der vises resultater.
5. Klik Save og gem søgningen.

Trin 2 – Opret en visualisering

1. Gå til Visualize og klik Create visualization.
2. Vælg Vertical bar.
3. Vælg datasættet fra trin 1.

Konfiguration: - Metrics (Y-akse): Count - Buckets (X-akse): Terms → fx agent.name eller srcip

Gem visualiseringen med et passende navn.

Trin 3 – Byg et dashboard (valgfrit)

1. Gå til Dashboards og klik Create new dashboard.
2. Klik Add og vælg visualiseringen.
3. Gem dashboardet.

Trin 4 – Udforsk selv

Prøv fx at:

- Skifte diagramtype
- Gruppere efter andre felter
- Tilføje filtre
- Kombinere flere visualiseringer

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: 08 – Audit Log Management
Relevans: Visualisering skaber overblik over hændelser og trends

CIS Control: 17 – Incident Response Management
Relevans: Dashboards kan bruges til at identificere mønstre og reagere hurtigt

---

Nyttige links

- Wazuh – Dashboards documentation

Last update: 2026-04-12 17:32:46