Kibana: Dashboard dla logów Windows z Winlogbeat – instrukcja krok po kroku

Poniższy przewodnik przeprowadzi Cię od weryfikacji dopływu danych po zbudowanie kompletnego dashboardu w Kibanie dla logów Windows zbieranych przez Winlogbeat.

# 0) Warunki wstępne

* Dane z Winlogbeat wpływają do Elasticsearch (istnieje data stream/indeks: „winlogbeat-\*”).
* Masz dostęp do Kibany (odpowiednia rola, np. kibana\_user + odczyt indeksów winlogbeat-\*).
* Czas serwera/hostów jest zsynchronizowany (NTP).

# 1) Utwórz Data View (jeśli nie istnieje)

1. Stack Management → Data Views → Create data view.
2. Name: „winlogbeat-\*”.
3. Time field: „@timestamp”.
4. Zapisz.

# 2) Szybka weryfikacja danych

1. Wejdź w Discover (lub Observability → Logs).
2. Ustaw zakres czasu na „Last 24 hours”.
3. Użyj filtra: winlog.channel: ("Security" or "System" or "Application").
4. Sprawdź, czy widać dokumenty oraz dostępne pola (host.name, user.name, event.code, log.level, winlog.provider\_name, message).

# 3) Utwórz Dashboard i pierwszy panel (Lens)

1. Analytics → Dashboard → Create dashboard.
2. Create panel → Lens.
3. Po skonfigurowaniu każdego panelu użyj „Save to library”, aby łatwo dodawać go na innych dashboardach.
4. Na końcu zapisz cały dashboard (nadaj nazwę, np. „Winlog – Security & System Overview”).

# 4) Proponowany zestaw paneli (KQL + konfiguracja)

## A. Logowania (Security)

**1) Logowania: sukces vs porażka (trend) – Area chart**

KQL: winlog.channel: "Security" and event.code: ("4624" or "4625")

Y: Count; Split series: event.code (4624 = sukces, 4625 = nieudane).

Opcjonalny podział (Break down by): host.name.

**2) Nieudane logowania – TOP hosty – Bar (horizontal)**

KQL: winlog.channel: "Security" and event.code: "4625"

Terms: host.name, Size 10.

**3) Nieudane logowania – TOP użytkownicy – Bar (horizontal)**

KQL: winlog.channel: "Security" and event.code: "4625"

Terms: user.name (lub winlog.event\_data.TargetUserName, jeśli user.name nie jest wypełnione).

**4) Logowania z przywilejami – Bar**

KQL: winlog.channel: "Security" and event.code: "4672"

Terms: host.name.

## B. Procesy / usługi (System/Security)

**5) Tworzenie procesów (4688) – trend – Line**

KQL: event.code: "4688"

Y: Count over time; opcjonalny Split: host.name.

**6) Instalacje usług (4697) – tabela ostatnich 24 h**

KQL: event.code: "4697"

Kolumny: @timestamp, host.name, winlog.event\_data.ServiceName, winlog.event\_data.ImagePath, user.name.

## C. Zmiany kont (jeśli logowane)

**7) Zmiany kont – licznik i typ – Bar**

KQL: event.code: ("4720" or "4726" or "4740" or "4723" or "4724" or "4725")

Split series: event.code.

## D. Jakość/poziom logów (Application/System)

**8) Poziom logów – rozkład – Donut**

KQL: winlog.channel: ("Application" or "System")

Terms: log.level.

**9) Najczęstsze źródła (provider) – Bar**

KQL: \*

Terms: winlog.provider\_name, Size 10.

## E. „Ostatnie błędy” – tabela z Discover

**10) Ostatnie błędy (System+Application) – Saved search**

Discover → KQL: log.level: ("error" or "critical") and winlog.channel: ("System" or "Application")

Kolumny: @timestamp, host.name, winlog.provider\_name, event.code, message

Save (np. „Winlog – Ostatnie błędy”), następnie dodaj do dashboardu: Add → From library → Saved search.

# 5) Kontrolki (filtrowanie na dashboardzie)

* Add panel → Controls → Options list: host.name, user.name, winlog.channel, event.code, log.level.
* Ustaw Time Picker na „Last 24 hours” i Auto-refresh (np. 1–5 min).

# 6) (Opcjonalnie) Gotowe panele

* Uruchom na hoście: winlogbeat setup – wgra wzorce i predefiniowane dashboardy.
* Jeśli używasz Elastic Agent (Windows integration), w Integrations → Windows znajdziesz prebuilt dashboards.

# 7) Dobre praktyki

* Redukuj „szum”: NOT event.code: ("5156" or "5158") (Windows Filtering Platform) w panelach, gdzie to zasadne.
* Korzystaj z event.outcome: ("success" or "failure") oraz event.category: authentication (jeśli ECS mapping to wspiera).
* Regularnie sprawdzaj dostępne pola w Discover → dokument → „View surrounding fields”.
* Zadbaj o uprawnienia: rola z odczytem indeksów winlogbeat-\* oraz dostęp do dashboardów.