Kibana — wykorzystanie danych z Winlogbeat

Propozycja dokumentu: gotowe widoki, KQL, Lens, alerty i korelacje dla zdarzeń Windows z Winlogbeat.  
*Data: 2025-08-21 07:31*

# 1) Cel dokumentu

* Pokazać co i jak wyciągać z danych Winlogbeat w Kibanie, gdy agent już wysyła zdarzenia.
* Dostarczyć gotowe widoki, zapytania KQL, przepisy Lens i alerty do szybkiego użycia.
* Zakres: kanały Security/System/Application, PowerShell, Sysmon, ForwardedEvents (WEF).

# 2) Gdzie są dane i jak je przeglądać

* Data view: winlogbeat-\* (w nowszych wdrożeniach także logs-\*)
* Najważniejsze pola (ECS + Winlog): @timestamp, host.name, winlog.channel, winlog.event\_id, winlog.provider\_name, log.level, user.name, process.\* (jeśli dotyczy), event.code (czasem duplikat event\_id).
* Szybki start: Kibana → Discover → wybierz data view → ustaw Timepicker (np. “Last 24 hours”).

# 3) Gotowe widoki (po imporcie dashboardów)

* Winlogbeat Overview / Windows Security — logony, błędy logowania, podsumowanie zdarzeń bezpieczeństwa.
* PowerShell — podgląd zdarzeń operacyjnych (4104 Script Block, 4103, itp.).
* Processes / Sysmon — jeśli Sysmon jest włączony i wysyłany (Event ID 1, 3, 7, …).

# 4) Typowe pytania, na które odpowie Kibana

* Czy mamy wzrost nieudanych logowań (4625)? Dla jakich kont i z jakich IP?
* Kto wyczyścił logi audytu (1102) i na jakim hoście?
* Czy dodano użytkownika do uprzywilejowanej grupy (4728/4732)?
* Czy zainstalowano nową usługę (4697/7045)? Z jakiej ścieżki EXE?
* Jakie polecenia PowerShell były wykonywane (4104)?
* Jakie procesy powstały (4688 / Sysmon 1) i jakie nawiązano połączenia (Sysmon 3)?

# 5) Przepisy „Lens” (wizualizacje 30–90 s)

A. Brute-force — trend 4625 (nieudane logowania)

* Filter: winlog.channel:"Security" and winlog.event\_id:4625; Metric: Count; Break down by: user.name; Line/Area (interval 1m/5m).

B. Administracyjne działania (dodanie do grup)

* Filter: winlog.channel:"Security" and winlog.event\_id:(4728 or 4732); Metric: Count; Break down by: user.name (lub winlog.event\_data.TargetUserName); Bar.

C. Instalacja nowych usług

* Filter: winlog.event\_id:(4697 or 7045); Table: @timestamp, host.name, user.name, winlog.event\_data.ServiceName, winlog.event\_data.ImagePath.

D. PowerShell — skrypty

* Filter: winlog.channel:"Microsoft-Windows-PowerShell/Operational" and winlog.event\_id:4104; Table: @timestamp, host.name, user.name, message (lub script block).

E. Sysmon — procesy i połączenia (jeśli dostępne)

* Filter: winlog.channel:"Microsoft-Windows-Sysmon/Operational" and winlog.event\_id:1; Table: @timestamp, host.name, process.executable, process.command\_line.
* Dodatkowo: winlog.event\_id:3 (połączenia sieciowe) → top destination.ip / destination.port.

# 6) Propozycje dashboardów własnych

„Windows Security — incydenty” — panele:

* Trend 4625 per user.name/source.ip; mapa/heatmap host.name × winlog.event\_id.
* Tabela „ostatnie zdarzenia krytyczne”: 1102 (clear logs), 4697/7045 (usługi), 4728/4732 (grupy).
* Rozkład typów logowań (4624) po LogonType (jeśli parsowane w event\_data).

„PowerShell — obserwacja” — panele:

* Trend 4104 (Script Block Logging) per host.name; tabela ostatnich poleceń (user.name, host.name, skrócone message).

„Sysmon — procesy & sieć” — panele:

* Top process.executable / parent.process.executable; trend połączeń (event\_id:3) per destination.ip/port.
* Heatmap host.name × process.name (uwaga na kardynalność).

# 7) KQL — gotowe „cookbook” (kopiuj-wklej)

winlog.channel : "Security" and winlog.event\_id : 4625 and @timestamp >= now-15m # nieudane logowania

winlog.channel : "Security" and winlog.event\_id : 1102 # wyczyszczenie logów audytu

winlog.channel : "Security" and winlog.event\_id : 4697 # instalacja nowej usługi (Security)

winlog.event\_id : 7045 and winlog.provider\_name : "Service Control Manager" # instalacja usługi (System)

winlog.event\_id : (4728 or 4732) # dodanie do grup (global/local)

winlog.channel : "Microsoft-Windows-PowerShell/Operational" and winlog.event\_id : 4104 # PowerShell Script Block

winlog.channel : "Microsoft-Windows-Sysmon/Operational" and winlog.event\_id : 1 # utworzenie procesu (Sysmon)

host.name : "dc-01" and winlog.channel : "Security" # zdarzenia tylko z DC

user.name : "svc\_deploy" and winlog.channel : "Security" and @timestamp >= now-24h # działania konkretnego konta serwisowego

# 8) Alerty — gotowy pakiet reguł

A. Brute-force / nieudane logowania

* KQL: winlog.channel:"Security" and winlog.event\_id:4625; Okno: 5–10 min; Group by: user.name/source.ip; Warunek: liczba prób > N.

B. Czyszczenie logów audytu

* KQL: winlog.channel:"Security" and winlog.event\_id:1102; Typ: natychmiastowy alert; Group by: host.name.

C. Instalacja/usługa

* KQL: (winlog.event\_id:4697 or (winlog.event\_id:7045 and winlog.provider\_name:"Service Control Manager")); Powiadamiaj z pełnym ImagePath.

D. Zmiany w grupach

* KQL: winlog.event\_id:(4728 or 4732); Group by: winlog.event\_data.TargetUserName/winlog.event\_data.TargetSid.

E. PowerShell — skrypty/ciągi podejrzane

* KQL: winlog.event\_id:4104 and message : ("Invoke-WebRequest" or "FromBase64String" or "IEX") — dopasuj do polityki.

F. „Silence” (brak zdarzeń z hosta)

* Typ: Less than 1 match; KQL: host.name:"\*" (lub konkretny host) i winlog.channel:"Security"; Okno: 10–15 min.

# 9) Korelacje i łączenie z innymi danymi

* Filebeat: koreluj błędy aplikacji (error logs) z działaniami systemowymi (restarty/usługi).
* Metricbeat: podczas wzrostu 4625 sprawdź CPU/Network na DC (czy DoS/atak słownikowy).
* APM/RUM: zestawiaj incydenty systemowe z regresjami wydajności usług.
* Packetbeat: nietypowe połączenia z hostów w czasie nowych usług/procesów (4697, Sysmon 1/3).

# 10) Raportowanie i współdzielenie

* Saved Search: „Security — 4625 (Last 24h)”, „Audit cleared (1102)”, „New services (4697/7045)”.
* Dashboard PDF: tygodniowy raport bezpieczeństwa hostów i DC.
* Skrócone linki do widoków z filtrami (np. host.name, user.name).

# 11) Dobre praktyki pracy ze zdarzeniami Windows

* Kardynalność: uważaj na terms po user.name/host.name w dużych domenach — ogranicz top N i filtry.
* Czas: wybieraj okna 15m/1h/24h; agregacje Auto/1m/5m zależnie od wolumenu.
* Normalizacja: używaj spójnych `fields.env`, `fields.role`; rozważ tagowanie WEF (tags:["wef"]).
* Uprawnienia: pamiętaj, że dostęp do kanału Security bywa ograniczony — w analizie uwzględnij brak zdarzeń jako sygnał.
* Retencja/ILM: ustal okresy dla `winlogbeat-\*` (prod/stage/test osobno).

# 12) „Starter pack” (do importu / odtworzenia)

Saved Searches:

SEC — 4625 (Last 24h): winlog.channel:"Security" and winlog.event\_id:4625 and @timestamp >= now-24h

SEC — 1102 (Audit cleared): winlog.channel:"Security" and winlog.event\_id:1102

SEC — New services: winlog.event\_id:(4697 or 7045)

Dashboardy:

* Windows Security — Incidents (sekcja 6).
* PowerShell — Script Blocks (sekcja 6).
* Sysmon — Processes & Network (sekcja 6).

Alerty:

* SEC\_BRUTEFORCE\_4625, SEC\_AUDIT\_CLEARED\_1102, SEC\_NEW\_SERVICE, SEC\_GROUP\_CHANGE, PS\_SCRIPT\_INDICATORS, HOST\_SILENCE.

# 13) Aneks — przydatne Event ID (wybór)

* Security: 4624 (logon), 4625 (failed logon), 4634 (logoff), 4648 (explicit credentials), 4688 (process created), 4697 (service installed), 4720/4726 (user add/remove), 4728/4732 (group add), 1102 (audit log cleared).
* System (SCM): 7045 (service installed).
* PowerShell (Operational): 4104 (script block), 4103 (module logging).
* Sysmon (Operational): 1 (process create), 3 (network connect), 7 (image loaded), 11 (file created), 13 (registry), 15 (file stream created).

# Co dalej?

Mogę przygotować pakiet Saved Objects (dashboardy, saved searches, alerty) dopasowany do Twoich hostów (DC/serwery), zaprojektować reguły progowe oraz raport PDF tygodniowy.