Winlogbeat — dokumentacja wdrożeniowa (PL)

Wersja: Windows (ZIP/offline), integracja z Kibana Dashboards  
*Data: 2025-08-21 06:45*

# 1) Cel i korzyści

* Zbieranie zdarzeń z Dziennika Zdarzeń Windows (Security, System, Application, PowerShell, Sysmon, ForwardedEvents).
* Wykrywanie incydentów (nieudane logowania, zmiany grup, czyszczenie logów, instalacje usług) i korelacja w ECS.
* Gotowe dashboardy Winlogbeat (Windows Security/Processes/PowerShell) oraz praca w Discover/Lens.

# 2) Wymagania i przygotowanie

* Windows x64; uruchomienie usługi najlepiej jako LocalSystem (dostęp do kanału Security).
* Dostęp do Kibany/Elasticsearch (adresy, konto do Saved Objects i indeksów).
* TLS: jeśli własne CA — wskaż plik CA w konfiguracji; nie wyłączaj weryfikacji w produkcji.
* Jeśli korzystasz z WEF (Windows Event Forwarding) — skonfiguruj odbiór w kanale ForwardedEvents.

# 3) Instalacja (ZIP/offline) — Windows

1) Rozpakuj paczkę ZIP do katalogu, np. C:\Elastic\winlogbeat.

2) Zainstaluj usługę i uruchom:

cd C:\Elastic\winlogbeat  
.\install-service-winlogbeat.ps1  
Start-Service winlogbeat

# 4) Konfiguracja minimalna (przykłady)

## 4A) Podstawowe kanały (Application/System/Security)

winlogbeat.event\_logs:  
 - name: Application  
 ignore\_older: 72h  
 - name: System  
 - name: Security  
 processors:  
 - drop\_event.when.not.or:  
 - equals:  
 winlog.event\_id: [4624, 4625, 4634, 4648, 4688, 4697, 4720, 4726, 4728, 4732, 1102]  
  
processors:  
 - add\_fields:  
 target: "win"  
 fields:  
 env: "prod"  
 role: "server"  
  
output.elasticsearch:  
 hosts: ["https://<ES\_HOST>:9200"]  
 username: "<USER>"  
 password: "<PASS>"  
  
setup.kibana:  
 host: "https://<KIBANA\_HOST>:5601"  
 username: "<USER>"  
 password: "<PASS>"

## 4B) PowerShell i Sysmon (jeśli włączone)

winlogbeat.event\_logs:  
 - name: Microsoft-Windows-PowerShell/Operational  
 ignore\_older: 168h  
 - name: Microsoft-Windows-Sysmon/Operational  
 ignore\_older: 168h

## 4C) ForwardedEvents (WEF) — centralizacja z DC/serwerów

winlogbeat.event\_logs:  
 - name: ForwardedEvents  
 tags: ["wef"]

## 4D) Test konfiguracji i połączeń

.\winlogbeat.exe test config -e  
.\winlogbeat.exe test output -e

# 5) Dashboardy w Kibanie (auto-import lub ręcznie)

A) Auto-import (rekomendowane):

C:\Elastic\winlogbeat\winlogbeat.exe setup --dashboards ^  
 -E setup.kibana.host=https://<KIBANA\_HOST>:5601 ^  
 -E setup.kibana.username=<USER> ^  
 -E setup.kibana.password=<PASS> ^  
 -E output.elasticsearch.hosts=["https://<ES\_HOST>:9200"] ^  
 -E output.elasticsearch.username=<USER> ^  
 -E output.elasticsearch.password=<PASS>

(Jeśli używasz Spaces: dodaj -E setup.kibana.space.id=<SPACE\_ID>)

B) Ręczny import: Kibana → Stack Management → Saved Objects → Import → pliki z katalogu 'kibana/' w paczce Winlogbeat.

Po imporcie: Analytics → Dashboard → „Winlogbeat …”. Discover: data view `winlogbeat-\*` (ew. `logs-\*`).

# 6) Kibana — gdzie patrzeć i jak wyciągać wnioski

* Dashboards: „Winlogbeat Security” (logony, błędy), „PowerShell”, „Processes/Sysmon” (jeśli włączone).
* Discover: kluczowe pola — `winlog.event\_id`, `winlog.channel`, `winlog.provider\_name`, `user.name`, `host.name`, `process.\*`.
* Lens: trend błędów logowania (4625) per `user.name`/`source.ip`, top zdarzeń administracyjnych, korelacja z hostami.

# 7) KQL — gotowe filtry

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

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

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

winlog.event\_id : 4720 or winlog.event\_id : 4726 # utworzenie/usunięcie użytkownika

winlog.channel : "Microsoft-Windows-PowerShell/Operational" and winlog.event\_id : 4104 # script block logging

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

# 8) Alerty — wzorce reguł

* Brute-force logowania: `winlog.event\_id:4625` → próg liczby zdarzeń per `user.name` lub `source.ip` w 5–10 min.
* Czyszczenie logów audytu: `winlog.event\_id:1102` → natychmiastowy alert, Group by `host.name`.
* Zmiany uprawnień: `winlog.event\_id:(4728 or 4732)` → dodanie do grup (global/local).
* Instalacja usług: `winlog.event\_id:4697` → weryfikuj ścieżkę binarną i `user.name`.
* PowerShell 4104 (script block): alertuj tylko nietypowe hosty/środowiska lub gdy regex wykrywa podejrzane komendy.

# 9) Dobre praktyki

* Uruchamiaj jako LocalSystem, aby mieć dostęp do kanału Security; na serwerach RDP rozważ osobny agent per rola.
* Filtruj `event\_id` w Security, aby ograniczyć wolumen (allowlista najważniejszych ID; resztę zbieraj okresowo).
* Włącz PowerShell Script Block Logging (4104) oraz — jeśli możesz — Sysmon (kanał Operational).
* Konsystencja nazw hostów (`host.name`), dodaj `fields.env`/`fields.role` do identyfikacji środowiska.
* Plan retencji/ILM na `winlogbeat-\*`; rozdziel prod/stage/test tagami lub osobnymi pipeline’ami.

# 10) Troubleshooting

* Brak zdarzeń z Security: sprawdź uprawnienia usługi (LocalSystem) i zasady audytu (Local/Domain Policy → Audit).
* Duży wolumen i opóźnienia: ogranicz zakres `event\_id`, zwiększ batch/queue, wyłącz zbędne kanały.
* Błędy TLS/403: dodaj CA w `output.elasticsearch.ssl.certificate\_authorities` i analogicznie dla `setup.kibana`.
* Puste dashboardy: sprawdź data view `winlogbeat-\*` i zakres czasu w Timepickerze.
* Błędy w `install-service-winlogbeat.ps1`: uruchom PowerShell jako Administrator i sprawdź ExecutionPolicy.

# 11) Szybki checklist (TL;DR)

* Rozpakuj ZIP → `install-service-winlogbeat.ps1` → `Start-Service winlogbeat`.
* Skonfiguruj `winlogbeat.event\_logs` (Security/System/Application + opcjonalnie PowerShell/Sysmon/ForwardedEvents).
* Skonfiguruj output do ES i `setup.kibana`; wgraj dashboardy `winlogbeat.exe setup --dashboards`.
* Sprawdź w Kibanie: Dashboards + Discover; dodaj alerty (4625, 1102, 4697, 4720/4732, 4104).