Winlogbeat → Kibana: widoczność logów Windows

# Streszczenie

Tak — logi Windows będą widoczne w Kibanie, o ile Winlogbeat przesyła zdarzenia do klastra Elasticsearch. Kibana nie łączy się z Winlogbeatem bezpośrednio; pokazuje dane, które już znajdują się w Elasticsearch.

# 1) Minimalny przepływ

Winlogbeat (serwer Windows) → Elasticsearch (opcjonalnie przez Logstash) → Kibana.

# 2) Kluczowe ustawienia w winlogbeat.yml

* output.elasticsearch.hosts — adres(y) klastra Elasticsearch.
* Uwierzytelnienie — użytkownik/hasło lub API key (jeden z mechanizmów).
* event\_logs — lista dzienników do zbierania, np. Application, System, Security.
* setup.kibana.host — opcjonalnie, do jednorazowego wgrania wzorców/dashboards komendą „winlogbeat setup”.

# 3) Uprawnienia do logu „Zabezpieczenia” (Security)

* Usługa Winlogbeat powinna działać jako LocalSystem lub konto z przywilejem SeSecurityPrivilege.
* Członkostwo w grupie „Event Log Readers” może nie wystarczyć bez przyznanego przywileju odczytu logów zabezpieczeń.

# 4) Gdzie to widać w Kibanie

* Discover — utwórz Data View z wzorcem indeksu „winlogbeat-\*” (pole czasu: @timestamp).
* Observability → Logs (Logs Explorer) — wybierz źródło „winlogbeat-\*”.
* Dashboards — po „winlogbeat setup” dostępne gotowe panele Windows/Winlogbeat.

# 5) Zbieranie z wielu hostów

* Najprościej: Winlogbeat na każdym hoście → Elasticsearch.
* Alternatywa: Windows Event Forwarding (WEF) do serwera kolektora → Winlogbeat czyta dziennik „ForwardedEvents” → Elasticsearch.

# 6) Diagnostyka i szybkie checki

* winlogbeat test output — sprawdź połączenie z Elasticsearch.
* Logi agenta: C:\ProgramData\winlogbeat\logs\.
* W Kibanie sprawdź istnienie indeksu/data stream „winlogbeat-\*” i czy masz Data View.
* Zsynchronizuj czas (NTP) — zły zegar = puste zakresy czasu w widokach.
* Błędy 401/403 — konto musi mieć uprawnienia do tworzenia indeksów i zapisu (np. rola „beats\_writer” lub równoważna).

# Checklist: szybki start

* Skonfiguruj output.elasticsearch.hosts oraz uwierzytelnienie w winlogbeat.yml.
* Zdefiniuj event\_logs (Application/System/Security według potrzeb).
* Uruchom usługę Winlogbeat i zweryfikuj „winlogbeat test output”.
* Opcjonalnie wykonaj „winlogbeat setup” (wzorce, dashboardy).
* W Kibanie utwórz Data View „winlogbeat-\*” i sprawdź dane w Discover / Logs.