Packetbeat — dokumentacja wdrożeniowa (PL)

Wersja: Windows (ZIP/offline), integracja z Kibana Dashboards  
*Data: 2025-08-21 06:42*

# 1) Cel i korzyści

* Pasywna obserwacja ruchu sieciowego z hosta (lub na porcie mirror/SPAN): HTTP, TLS (metadane), DNS, wybrane bazy (MySQL/PostgreSQL), Redis itd.
* Widoczność opóźnień, błędów i top talkers bez zmian w aplikacjach.
* Integracja z Kibana Dashboards (Packetbeat Overview/HTTP/DNS/TLS) i Lens; korelacja przez ECS (source/destination/network.\*).

# 2) Wymagania i przygotowanie

* Windows x64; wymagany Npcap (WinPcap-compatible) do przechwytywania pakietów.
* Uprawnienia administratora do instalacji i uruchomienia usługi z dostępem do interfejsu sieciowego.
* Rekomendowany port mirror/SPAN lub TAP dla pełnego obrazu ruchu.
* Kibana/Elasticsearch: adresy + konto z uprawnieniami Saved Objects i indeksów.
* TLS/CA: jeśli własne CA — wskaż plik w konfiguracji; nie wyłączaj weryfikacji w produkcji.

# 3) Instalacja (ZIP/offline) — Windows

1) Zainstaluj Npcap na hoście (z obsługą WinPcap API).

2) Rozpakuj paczkę ZIP do katalogu, np. C:\Elastic\packetbeat.

3) Zainstaluj usługę i uruchom:

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

Listę interfejsów/adapterów sprawdzisz w PowerShell:

Get-NetAdapter | Where-Object {$\_.Status -eq 'Up'} | Select-Object Name, InterfaceDescription, ifIndex

Następnie ustaw `packetbeat.interfaces.device` na numer/ nazwę interfejsu (patrz sekcja 4).

# 4) Konfiguracja minimalna (przykłady)

## 4A) Podstawowe protokoły + flows (HTTP/TLS/DNS)

packetbeat.interfaces.device: 0 # lub nazwa interfejsu, np. "Ethernet"  
packetbeat.interfaces.bpf\_filter: 'port 53 or port 80 or port 443' # ogranicz ruch do istotnych portów  
  
packetbeat.flows:  
 enabled: true  
 timeout: 30s  
 period: 10s  
  
packetbeat.protocols:  
 - type: http  
 ports: [80, 8080, 8000, 5000, 8002]  
 - type: tls  
 ports: [443, 8443]  
 - type: dns  
 ports: [53]  
  
output.elasticsearch:  
 hosts: ["https://<ES\_HOST>:9200"]  
 username: "<USER>"  
 password: "<PASS>"  
  
setup.kibana:  
 host: "https://<KIBANA\_HOST>:5601"  
 username: "<USER>"  
 password: "<PASS>"

## 4B) Bazy danych (MySQL/PostgreSQL) — opcjonalnie

packetbeat.protocols:  
 - type: mysql  
 ports: [3306]  
 - type: postgresql  
 ports: [5432]

## 4C) Test konfiguracji i połączeń

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

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

A) Auto-import (rekomendowane):

C:\Elastic\packetbeat\packetbeat.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 Packetbeat.

Po imporcie: Analytics → Dashboard → „Packetbeat …” (HTTP/DNS/TLS/Overview). Discover: data view `packetbeat-\*` (ew. `network-\*`).

# 6) Kibana — gdzie patrzeć i jak wyciągać wnioski

* Dashboards: „Packetbeat Overview” (wolumen, top talkers, error rates), „HTTP”, „DNS”, „TLS”.
* Discover: kluczowe pola ECS — source.\* / destination.\* / network.\*, `url.\*`, `http.\*`, `dns.\*`, `tls.\*`, `event.duration`.
* Lens: trend p95 `event.duration` per usługa (HTTP), udział protokołów, top klienci wg `source.ip`/`client.bytes`.

# 7) KQL — gotowe filtry

event.dataset : "http" and http.response.status\_code >= 500 and @timestamp >= now-15m # HTTP 5xx w 15 min

event.category : "network" and event.type : "connection" and network.bytes >= 10000000 # ciężkie przepływy (flows)

event.dataset : "dns" and dns.response\_code : "NXDOMAIN" # problemy DNS / typosquatting

event.dataset : "tls" and tls.version : "1.0" # przestarzałe wersje TLS

# 8) Alerty — wzorce reguł

* Spike HTTP 5xx: KQL jak wyżej; okno 5–10 min; Group by `url.domain` lub `destination.ip`.
* Wysoki odsetek NXDOMAIN: `event.dataset:dns AND dns.response\_code:NXDOMAIN` → próg procentowy > X%.
* Degradacja latencji: średnia `event.duration` dla `event.dataset:http` > próg przez 5 min, Group by `url.path`/`service.name` (jeśli dostępne).
* Cisza ruchu: Less than 1 match dla `event.dataset:http` (lub flows) z danej lokalizacji w 10–15 min.

# 9) Dobre praktyki

* Zacznij od BPF filtra (porty/protokóły) aby ograniczyć wolumen i narzut.
* Ustal interfejs `device` właściwy dla ruchu SPAN/TAP; na Windows bywa inny niż interfejs routingu.
* Wyłącz zbędne protokoły w `packetbeat.protocols`; zostaw tylko te, które analizujesz.
* Flows: włączone pomagają w top talkers i anomaliach; dostosuj `period` i `timeout`.
* TLS: Packetbeat widzi metadane (SNI, wersje, cert), nie deszyfruje treści; to normalne.
* Pamiętaj o retencji/ILM na indeksach `packetbeat-\*`/`network-\*`.

# 10) Troubleshooting

* Brak danych: sprawdź Npcap, uprawnienia admina, poprawny `device`, brak zbyt restrykcyjnego `bpf\_filter`.
* Wysokie zużycie CPU/IO: zawężaj BPF, wyłącz zbędne protokoły, zwiększ `period` flows, zmniejsz liczbę portów.
* Błędy TLS/połączenia do ES: dodaj CA w `output.elasticsearch.ssl.certificate\_authorities` i w `setup.kibana`.
* Puste dashboardy: brak data view (`packetbeat-\*`) albo zły zakres czasu.
* Kolizja z inną aplikacją sniffującą: wyłącz inne sniffery/IDS na tym samym interfejsie.

# 11) Szybki checklist (TL;DR)

* Zainstaluj Npcap → rozpakuj ZIP → `install-service-packetbeat.ps1` → `Start-Service packetbeat`.
* Ustaw `interfaces.device` + opcjonalny `bpf\_filter`; włącz protokoły (HTTP/TLS/DNS/DB).
* Skonfiguruj output do ES i `setup.kibana`; wgraj dashboardy `packetbeat.exe setup --dashboards`.
* Sprawdź w Kibanie: Dashboards + Discover; dodaj alerty (5xx, NXDOMAIN, latency).