Kibana — wykorzystanie danych z Packetbeat

Propozycja dokumentu: gotowe widoki, KQL, Lens, alerty i korelacje dla ruchu sieciowego z Packetbeat.  
*Data: 2025-08-21 07:28*

# 1) Cel dokumentu

* Pokazać co i jak wyciągać z danych Packetbeat w Kibanie, gdy agent już wysyła ruch.
* Dostarczyć gotowe widoki, zapytania KQL, przepisy Lens i alerty do szybkiego użycia.
* Zakres: HTTP, DNS, TLS (metadane), wybrane DB (MySQL/PostgreSQL), flows (top talkers, wolumen, opóźnienia).

# 2) Gdzie są dane i jak je przeglądać

* Data view: packetbeat-\* (w nowszych wdrożeniach także network-\*).
* Najważniejsze pola (ECS + Packetbeat): @timestamp, event.dataset (http/dns/tls/flow), event.category (network), event.type (connection).
* Źródła/cele i sieć: source.\*, destination.\*, network.\* (bytes, packets, protocol, latency).
* HTTP: http.request.method, http.response.status\_code, url.\*; DNS: dns.question.name, dns.response\_code; TLS: tls.version, tls.server.x509.\* (np. not\_after).
* Szybki start: Kibana → Discover → wybierz data view → ustaw Timepicker (np. “Last 24 hours”).

# 3) Gotowe widoki (po imporcie dashboardów)

* Packetbeat Overview — wolumen ruchu, top protokoły, top rozmówcy.
* HTTP — statusy, metody, domeny, ścieżki, p95 latency.
* DNS — top domeny, NXDOMAIN, opóźnienia odpowiedzi.
* TLS — wersje protokołu, błędy handshake, wygasanie certyfikatów.

# 4) Typowe pytania, na które odpowie Kibana

* Gdzie są piki błędów HTTP (5xx)? Które ścieżki/domeny je generują?
* Jakie są „top talkers” w sieci (source/destination IP)?
* Czy DNS zwraca dużo NXDOMAIN/ServFail?
* Czy używamy przestarzałego TLS (1.0/1.1)? Kiedy wygasają certyfikaty?
* Czy rosną opóźnienia (latency) na ścieżkach HTTP lub usługach DB?

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

A. Piki 5xx per ścieżka (HTTP)

* Filter: event.dataset:"http" and http.response.status\_code >= 500; Metric: Count; Break down by: url.path (Top 10); Bar (desc).

B. p95 latencji HTTP per domena

* Filter: event.dataset:"http"; Metric: 95th percentile of event.duration (przeskaluj do ms); Break down by: url.domain; Line/Bar.

C. Top rozmówcy (flows)

* Filter: event.category:"network" and event.type:"connection"; Metric: Sum network.bytes; Break down by: source.ip (Top 10); Bar. Drugi panel: destination.ip.

D. DNS — problemy

* Filter: event.dataset:"dns"; Panel 1: Count by dns.response\_code (Pie); Panel 2: Count (dns.response\_code:"NXDOMAIN") by dns.question.name (Top 10).

E. TLS — higiena

* Filter: event.dataset:"tls"; Panel 1: Count by tls.version (Bar); Panel 2: Table z tls.server.x509.subject.common\_name i tls.server.x509.not\_after (sort ASC).

# 6) Propozycje dashboardów własnych

„HTTP — jakość usług” — panele:

* p95 event.duration per url.domain (trend).
* Top url.path dla 5xx (bar).
* Rozkład http.response.status\_code (stacked area 2xx/4xx/5xx).
* Top client.ip (jeśli dostępne).
* Tabela „ostatnie 5xx”: @timestamp, url.full, http.response.status\_code, host.name.

„Network — top talkers & flows” — panele:

* Sum network.bytes per source.ip i per destination.ip.
* Top network.packets per source.ip.
* Heatmap source.ip × destination.ip (uwaga na kardynalność).
* Trend wolumenu per network.transport (tcp/udp).

„DNS & TLS — higiena” — panele:

* Top dns.response\_code + top dns.question.name dla NXDOMAIN.
* tls.version rozkład + lista certyfikatów wg not\_after.

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

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

event.dataset : "http" and event.duration >= 2000000 # Wolne HTTP (≥ 2 s)

event.category : "network" and event.type : "connection" and source.ip : \* # Top ruch od IP źródłowego (flows)

event.dataset : "dns" and dns.response\_code : "NXDOMAIN" # DNS — NXDOMAIN

event.dataset : "tls" and tls.version : ("1.0" or "1.1") # TLS — przestarzałe wersje

event.dataset : "tls" and tls.server.x509.not\_after <= now+30d # TLS — certyfikat wygasa w 30 dni

event.dataset:"http" and url.domain:"api.twojadomena.pl" and url.path:"/orders" # HTTP — konkretna domena/ścieżka

# 8) Alerty — gotowy pakiet reguł

A. Spike HTTP 5xx

* KQL: event.dataset:"http" and http.response.status\_code >= 500; Okno: 5–10 min; Group by: url.path/url.domain; Warunek: ratio 5xx > X%.

B. Latency threshold (HTTP)

* KQL: event.dataset:"http" and event.duration >= 2000000; Group by: url.path/url.domain; Warunek: „More than N matches” w 5 min.

C. NXDOMAIN surge (DNS)

* KQL: event.dataset:"dns" and dns.response\_code:"NXDOMAIN"; Group by: dns.question.name; Warunek: wzrost powyżej progu.

D. TLS hygiene

* KQL: event.dataset:"tls" and tls.version:("1.0" or "1.1"); KQL (expiry): event.dataset:"tls" and tls.server.x509.not\_after <= now+30d; Harmonogram: 1×/dzień; Group by: CN/domain.

E. Heavy flows (egress/ingress)

* KQL: event.category:"network" and event.type:"connection" and network.bytes >= 100000000; Group by: source.ip/destination.ip; Okno: 5–15 min.

F. „Silence” (brak danych)

* Typ: Less than 1 match; KQL: event.category:"network" (lub zawęż do http); Okno: 10–15 min.

# 9) Korelacje i łączenie z innymi danymi

* APM: porównaj p95 latency (event.duration) z danymi APM; sprawdź, czy 5xx są widoczne także w APM.
* Heartbeat: zestaw monitor.status:down z pikami 5xx/latency (czy awarie przekładają się na błędy).
* Metricbeat: host-level CPU/dysk/sieć podczas pików network.bytes/latency.
* Filebeat: logi aplikacji w tym samym czasie (korelacja po host.name, url.\*, IP).

# 10) Raportowanie i współdzielenie

* Saved Search: „HTTP 5xx — last 24h”, „TLS expiry < 30d”, „Top source.ip by bytes”.
* Dashboard PDF (Reporting): tygodniowy raport jakości ruchu (HTTP/DNS/TLS).
* Skrócone linki z predefiniowanymi filtrami (domena, ścieżka, IP).

# 11) Dobre praktyki pracy z danymi Packetbeat

* Kardynalność: unikaj pełnego url.full w terms; preferuj url.domain/url.path.
* Jednostki: event.duration to mikrosekundy — formatuj jako ms (÷1000).
* Interwał: dopasuj okno czasu (15m/1h/24h) i agregacje (Auto/1m/5m).
* Higiena TLS: monitoruj wersje, błędy handshake i wygaśnięcia certów.
* Heatmapy IP: top N i filtry po podsieciach, by utrzymać wydajność.

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

Saved Searches:

HTTP 5xx — Last 1h: event.dataset:"http" and http.response.status\_code >= 500 and @timestamp >= now-1h

DNS NXDOMAIN — 24h: event.dataset:"dns" and dns.response\_code:"NXDOMAIN" and @timestamp >= now-24h

TLS Expiry < 30d: event.dataset:"tls" and tls.server.x509.not\_after <= now+30d

Dashboardy:

* HTTP — Quality & Latency (sekcje 5A/5B + tabela 5xx).
* Network — Top Talkers & Flows (sekcja 5C).
* DNS/TLS — Hygiene (sekcje 5D/5E).

Alerty:

* HTTP\_5XX\_SPIKE, HTTP\_LATENCY\_P95\_THRESHOLD, DNS\_NXDOMAIN\_SURGE, TLS\_DEPRECATED/EXPIRY, HEAVY\_FLOWS, PACKETBEAT\_SILENCE.

# 13) Aneks — pola przydatne w analizie

* HTTP: http.request.method, http.response.status\_code, url.domain, url.path, event.duration.
* DNS: dns.question.name, dns.response\_code, dns.op\_code.
* TLS: tls.version, tls.cipher, tls.server.x509.not\_after, tls.server.x509.subject.common\_name.
* Flows: source.ip/port, destination.ip/port, network.bytes, network.packets, network.transport, event.type:"connection".

# Co dalej?

Mogę przygotować pakiet Saved Objects (dashboardy, saved searches, alerty) dopasowany do Twoich domen/ścieżek/IP oraz wersji Kibany.