Kibana — wykorzystanie danych z Heartbeat

Propozycja dokumentu: Uptime + Discover/Lens, KQL, alerty i korelacje dla danych z Heartbeat.  
*Data: 2025-08-21 07:18*

# 1) Cel dokumentu

* Pokazać jak analizować dane z Heartbeat w Kibanie (gdy monitory już wysyłają dane).
* Dostarczyć gotowe widoki w Uptime, zapytania KQL, przepisy Lens i alerty do szybkiego użycia.
* Zakres: monitory HTTP/TCP/ICMP; pola TLS, lokalizacje, czas odpowiedzi i dostępność.

# 2) Gdzie są dane i jak je przeglądać

* Aplikacja: Observability → Uptime (główny widok dla Heartbeat).
* Data view: heartbeat-\* (ew. synthetics-\* w nowszych wdrożeniach synthetics).
* Najważniejsze pola (ECS + Heartbeat): @timestamp, monitor.status (up/down), monitor.id, monitor.name, monitor.type (http/tcp/icmp), monitor.duration.us, url.full/url.domain/url.path (HTTP), observer.geo.\* (lokalizacja), tls.server.x509.\* (ważność certyfikatu), error.\* (opis błędu).

# 3) Gotowe widoki (Uptime + dashboardy)

* Uptime Overview — status monitorów, historia, lokalizacje/geo, p95 czasu odpowiedzi.
* TLS certs — lista certyfikatów i ich ważność, ostrzeżenia o zbliżającym się wygaśnięciu.
* (Opcjonalnie) „Heartbeat Overview”/inne dashboardy — jeśli zaimportowano przez setup --dashboards.

# 4) Typowe pytania, na które odpowie Kibana

* Czy monitor jest DOWN i od kiedy? (monitor.status, historia w Uptime).
* Czy czas odpowiedzi rośnie/ulega degradacji? (monitor.duration.us, p95/p99).
* Czy problem dotyczy konkretnej lokalizacji? (observer.geo.name/geo.location).
* Które URL-e/hosty najczęściej zawodzą? (url.domain, url.full).
* Kiedy wygasają certyfikaty TLS? (tls.server.x509.not\_after).

# 5) Przepisy „Lens” (wizualizacje 30–60 s)

A. Trend dostępności (UP vs DOWN)

* Metric: Count; Break down by: monitor.status; Format: Stacked area/column; Filter: monitor.name:"<Twoj monitor>" (opcjonalnie).

B. p95 czasu odpowiedzi per monitor

* Metric: 95th percentile of monitor.duration.us (przeskaluj do ms: /1000); Break down by: monitor.name; Filter: monitor.type:"http".

C. Top awaryjne URL-e (HTTP)

* Filter: monitor.type:"http" and monitor.status:"down"; Metric: Count; Break down by: url.full (Top 10).

D. Różnice między lokalizacjami

* Metric: Median of monitor.duration.us (→ ms); Break down by: observer.geo.name; Filter: monitor.name:"<Twoj monitor>".

E. Histogram czasów odpowiedzi (rozrzut)

* Metric: monitor.duration.us (Distribution); Filter: monitor.type:"http" and monitor.name:"<Twoj monitor>".

# 6) Propozycje dashboardów własnych

„Uptime — SLO & dostępność” — panele:

* Availability (100 \* up/(up+down)) per monitor.name za ostatnie 7/30 dni.
* p95 monitor.duration.us (ms) per monitor.name.
* Top DOWN incidents (Count) per url.full.
* Mapa/lokalizacje: median monitor.duration.us per observer.geo.name.
* Tabela „ostatnie awarie”: @timestamp, monitor.name, url.full, observer.geo.name, error.message.

„TLS — ważność i higiena” — panele:

* Lista certyfikatów z tls.server.x509.not\_after (sort ASC).
* Wykres liczby certyfikatów wygasających w oknach 30/14/7 dni.
* Tabela wyjątków TLS (error.type/message związane z handshake).

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

monitor.status : "down" and @timestamp >= now-15m # monitory w dół w ostatnich 15 min

monitor.name : "My API Health" and monitor.status : "down" # konkretny monitor

monitor.type : "http" and monitor.duration.us >= 1000000 # HTTP wolniej niż 1 s

url.domain : "api.twojadomena.pl" and monitor.status : "down" # awarie dla konkretnej domeny

observer.geo.name : "Warsaw" and monitor.status : "down" # problemy lokalizacyjnie

tls.server.x509.not\_after <= now+30d # certyfikat wygasa w 30 dni

http.response.status\_code >= 500 and monitor.type : "http" # błędy HTTP 5xx (jeśli rejestrowane)

error.message : \* and monitor.status : "down" # zdarzenia z opisanym błędem

# 8) Alerty — gotowy pakiet reguł

A. Monitor DOWN

* KQL: monitor.status:"down"; Okno: 1–5 min; Group by: monitor.id/monitor.name; Powiadom: e-mail/Teams/Slack.

B. Degradacja czasu odpowiedzi

* KQL: monitor.type:"http" and monitor.duration.us >= 1000000; Okno: 5 min; Group by: monitor.name/url.full.

C. Wygasający certyfikat TLS

* KQL: tls.server.x509.not\_after <= now+30d; Harmonogram: raz dziennie; Group by: url.domain/monitor.name.

D. Spadek dostępności (SLO)

* Metryka: Availability (100\*up/(up+down)) w 7d < 99.9%; można zbudować jako Lens + Threshold rule albo zapytanie KQL o liczbę DOWN per całkowita liczba checków.

E. Seria nieudanych prób (consecutive failures)

* Reguła o warunku „More than N matches” w 5–10 min + Group by monitor.name i observer.geo.name (lokacja).

# 9) Korelacje i łączenie z innymi danymi

* APM/Backend: porównaj godziny awarii z błędami 5xx i pikami opóźnień w APM/Metricbeat.
* Metricbeat: sprawdź CPU/dysk/ sieć hostów backend przy wzrostach monitor.duration.us.
* Packetbeat: koreluj wzrost latency HTTP/DNS z problemami sieci (flows, retransmisje, 5xx).
* Filebeat: przeglądaj logi aplikacyjne w tym samym oknie czasu (trace lub korelacja po host.name/url).

# 10) Raportowanie i współdzielenie

* Uptime status report: tygodniowy PDF z dostępności i p95 latencji.
* Saved Search: „DOWN last 24h” i „TLS expiry < 30d”.
* Skrócone linki z predefiniowanymi filtrami (np. monitor.name, observer.geo.name).

# 11) Dobre praktyki pracy z danymi Heartbeat

* Unikalne monitor.id i spójne monitor.name; tagi: env/team/system.
* Czas: dopasuj Timepicker (15m/1h/7d) i interwał agregacji (Auto/1m/5m).
* Skalowanie: ogranicz liczbę lokalizacji i częstotliwość checków w zależności od krytyczności.
* TLS: nie wyłączaj weryfikacji; utrzymuj listę CA i regularny przegląd certyfikatów.
* Kardynalność: unikaj wykresów po pełnym url.full, używaj url.domain/url.path.

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

Saved Searches:

DOWN — Last 15m: monitor.status : "down" and @timestamp >= now-15m

TLS — Expiry <30d: tls.server.x509.not\_after <= now+30d

SLOW — HTTP >1s: monitor.type : "http" and monitor.duration.us >= 1000000

Dashboardy:

* Uptime — SLO & Availability (sekcja 6).
* TLS — Expiry & Errors (sekcja 6).

Alerty:

* UPTIME\_DOWN (sekcja 8A).
* UPTIME\_SLOW (sekcja 8B).
* TLS\_EXPIRY\_30D (sekcja 8C).
* UPTIME\_AVAILABILITY\_SLO (sekcja 8D).

# 13) Aneks — pola przydatne w analizie

* monitor.status, monitor.id, monitor.name, monitor.type, monitor.ip, monitor.duration.us.
* url.full, url.scheme, url.domain, url.path (HTTP).
* observer.geo.name, observer.geo.location (lokacje).
* tls.server.x509.not\_after, tls.version, tls.cipher, tls.\*.
* error.type, error.message, http.response.status\_code (gdy dostępne).

# Co dalej?

Mogę przygotować pakiet Saved Objects (dashboardy, saved searches, alerty) pod Twoje monitory i lokalizacje oraz dodać kalkulację Availability/SLO.