**KQL – przykłady dla Beats (Filebeat, Metricbeat, Winlogbeat, Packetbeat, Heartbeat)**

*Format: Co robi → KQL (bez stylizacji kodu, z filtrem agent.type).*

*Data: 21 sierpnia 2025*

# Filebeat (logi) – 30 przykładów

1) **Co robi:** Pokaż tylko logi z Filebeat.

**KQL:** agent.type : "filebeat"

2) **Co robi:** Logi (bez metryk) z Filebeat.

**KQL:** agent.type : "filebeat" and data\_stream.type : "logs"

3) **Co robi:** Tylko błędy/krytyczne logi.

**KQL:** agent.type : "filebeat" and log.level : ("error" or "fatal")

4) **Co robi:** Syslog – ostrzeżenia i błędy.

**KQL:** agent.type : "filebeat" and event.dataset : "system.syslog" and log.level : ("warn" or "error")

5) **Co robi:** Nginx – odpowiedzi 5xx.

**KQL:** agent.type : "filebeat" and event.dataset : "nginx.access" and http.response.status\_code >= 500

6) **Co robi:** Apache – żądania POST.

**KQL:** agent.type : "filebeat" and event.dataset : "apache.access" and http.request.method : "POST"

7) **Co robi:** IIS – błędy 404.

**KQL:** agent.type : "filebeat" and event.dataset : "iis.access" and http.response.status\_code : 404

8) **Co robi:** Błędy w konkretnym serwisie aplikacyjnym.

**KQL:** agent.type : "filebeat" and service.name : "orders-api" and log.level : "error"

9) **Co robi:** Linijki zawierające „Exception”.

**KQL:** agent.type : "filebeat" and message : "\*Exception\*"

10) **Co robi:** Logi z hosta web-01.

**KQL:** agent.type : "filebeat" and host.name : "web-01"

11) **Co robi:** Dane z przestrzeni `prod`.

**KQL:** agent.type : "filebeat" and data\_stream.namespace : "prod"

12) **Co robi:** Tylko moduł „system”.

**KQL:** agent.type : "filebeat" and event.module : "system"

13) **Co robi:** Logi zawierające identyfikator śladu (korelacja z APM).

**KQL:** agent.type : "filebeat" and trace.id : \*

14) **Co robi:** Web API – GET na /api/\*

**KQL:** agent.type : "filebeat" and http.request.method : "GET" and url.path : "/api/\*"

15) **Co robi:** Logi, gdzie rozpoznano użytkownika.

**KQL:** agent.type : "filebeat" and user.name : \*

16) **Co robi:** Ruch z prywatnych adresów źródłowych 10/8.

**KQL:** agent.type : "filebeat" and source.ip : "10.0.0.0/8"

17) **Co robi:** Tagi zawierające „prod”.

**KQL:** agent.type : "filebeat" and tags : "prod"

18) **Co robi:** Logi z kontenerów (container.id).

**KQL:** agent.type : "filebeat" and container.id : \*

19) **Co robi:** Logi z namespace K8s „default”.

**KQL:** agent.type : "filebeat" and kubernetes.namespace : "default"

20) **Co robi:** Logi pochodzące z plików „…\logs\…”.

**KQL:** agent.type : "filebeat" and log.file.path : "\*\\logs\\\*"

21) **Co robi:** Żądania do plików .php.

**KQL:** agent.type : "filebeat" and url.extension : "php"

22) **Co robi:** Sukcesy HTTP (2xx–3xx).

**KQL:** agent.type : "filebeat" and http.response.status\_code >= 200 and http.response.status\_code < 400

23) **Co robi:** GeoIP – źródła z Polski.

**KQL:** agent.type : "filebeat" and source.geo.country\_iso\_code : "PL"

24) **Co robi:** User-Agent = Chrome.

**KQL:** agent.type : "filebeat" and user\_agent.name : "Chrome"

25) **Co robi:** Dane z chmury AWS.

**KQL:** agent.type : "filebeat" and cloud.provider : "aws"

26) **Co robi:** Log zawiera event.original.

**KQL:** agent.type : "filebeat" and event.original : \*

27) **Co robi:** Błędy parsowania/ingestu.

**KQL:** agent.type : "filebeat" and error.message : \*

28) **Co robi:** Logi Nginx dla ścieżki /health.

**KQL:** agent.type : "filebeat" and event.dataset : "nginx.access" and url.path : "/health"

29) **Co robi:** Apache – odpowiedzi 4xx.

**KQL:** agent.type : "filebeat" and event.dataset : "apache.access" and http.response.status\_code >= 400 and http.response.status\_code < 500

30) **Co robi:** IIS – żądania z określonego IP.

**KQL:** agent.type : "filebeat" and event.dataset : "iis.access" and source.ip : "192.168.1.10"

# Metricbeat (metryki) – 30 przykładów

1) **Co robi:** Tylko metryki z Metricbeat.

**KQL:** agent.type : "metricbeat"

2) **Co robi:** CPU > 90% (znormalizowane).

**KQL:** agent.type : "metricbeat" and event.dataset : "system.cpu" and system.cpu.total.norm.pct > 0.9

3) **Co robi:** RAM > 90%.

**KQL:** agent.type : "metricbeat" and event.dataset : "system.memory" and system.memory.actual.used.pct > 0.9

4) **Co robi:** Load1 > 2 na Linuksach.

**KQL:** agent.type : "metricbeat" and event.dataset : "system.load" and system.load.1 > 2 and host.os.type : "linux"

5) **Co robi:** Dyski > 80% zajętości (nie tmpfs).

**KQL:** agent.type : "metricbeat" and event.dataset : "system.filesystem" and system.filesystem.used.pct > 0.8 and system.filesystem.type != "tmpfs"

6) **Co robi:** Inody > 80%.

**KQL:** agent.type : "metricbeat" and event.dataset : "system.filesystem" and system.filesystem.inodes.used.pct > 0.8

7) **Co robi:** Wejściowy ruch na interfejsie > 10 MB.

**KQL:** agent.type : "metricbeat" and event.dataset : "system.network" and system.network.in.bytes > 10000000

8) **Co robi:** Straty pakietów na interfejsie.

**KQL:** agent.type : "metricbeat" and event.dataset : "system.network" and (system.network.in.dropped > 0 or system.network.out.dropped > 0)

9) **Co robi:** Procesy dotnet z wysokim CPU.

**KQL:** agent.type : "metricbeat" and event.dataset : "system.process" and process.name : "dotnet" and process.cpu.total.pct > 0.5

10) **Co robi:** Liczba procesów > 300.

**KQL:** agent.type : "metricbeat" and event.dataset : "system.process\_summary" and system.process.summary.total > 300

11) **Co robi:** Uptime hosta > 7 dni.

**KQL:** agent.type : "metricbeat" and event.dataset : "system.uptime" and system.uptime.duration.ms > 604800000

12) **Co robi:** Mount C:\ ma wolnego < 10%.

**KQL:** agent.type : "metricbeat" and event.dataset : "system.filesystem" and system.filesystem.mount\_point : "C:\" and system.filesystem.available.pct < 0.10

13) **Co robi:** CPU „system” > 30% na hostach db-\*.

**KQL:** agent.type : "metricbeat" and event.dataset : "system.cpu" and host.name : "db-\*" and system.cpu.system.pct > 0.3

14) **Co robi:** Liczba rdzeni CPU >= 8.

**KQL:** agent.type : "metricbeat" and event.dataset : "system.cpu" and system.cpu.cores >= 8

15) **Co robi:** Windowsowe hosty z małą wolną pamięcią.

**KQL:** agent.type : "metricbeat" and host.os.type : "windows" and event.dataset : "system.memory" and system.memory.free < 2147483648

16) **Co robi:** Swap > 50%.

**KQL:** agent.type : "metricbeat" and event.dataset : "system.memory" and system.memory.swap.used.pct > 0.5

17) **Co robi:** Duże opóźnienia dysku (read).

**KQL:** agent.type : "metricbeat" and event.dataset : "system.diskio" and system.diskio.read.time > 500

18) **Co robi:** Duży zapis na dysk (bytes).

**KQL:** agent.type : "metricbeat" and event.dataset : "system.diskio" and system.diskio.write.bytes > 52428800

19) **Co robi:** Interfejs „Ethernet” – wysoki OUT.

**KQL:** agent.type : "metricbeat" and event.dataset : "system.network" and system.network.name : "Ethernet" and system.network.out.bytes > 10000000

20) **Co robi:** Usługi w stanie „stopped”.

**KQL:** agent.type : "metricbeat" and event.dataset : "system.service" and system.service.state : "stopped"

21) **Co robi:** Hosty w AWS.

**KQL:** agent.type : "metricbeat" and cloud.provider : "aws"

22) **Co robi:** Hosty architektury x86\_64.

**KQL:** agent.type : "metricbeat" and host.architecture : "x86\_64"

23) **Co robi:** Średni load5 > 1.

**KQL:** agent.type : "metricbeat" and event.dataset : "system.load" and system.load.5 > 1

24) **Co robi:** Load15 > 0.8 i CPU > 70%.

**KQL:** agent.type : "metricbeat" and event.dataset : "system.load" and system.load.15 > 0.8 and system.cpu.total.norm.pct > 0.7

25) **Co robi:** Partycje tylko typu „ext4”.

**KQL:** agent.type : "metricbeat" and event.dataset : "system.filesystem" and system.filesystem.type : "ext4"

26) **Co robi:** Hosty Linux z uptime < 1h (niedawny restart).

**KQL:** agent.type : "metricbeat" and host.os.type : "linux" and system.uptime.duration.ms < 3600000

27) **Co robi:** Najcięższe procesy Java.

**KQL:** agent.type : "metricbeat" and event.dataset : "system.process" and process.name : "java" and (process.cpu.total.pct > 0.4 or process.memory.rss.bytes > 1073741824)

28) **Co robi:** Hosty bez swapu (0 bajtów).

**KQL:** agent.type : "metricbeat" and event.dataset : "system.memory" and system.memory.swap.total : 0

29) **Co robi:** Liczba socketów (sumarycznie) > 5000.

**KQL:** agent.type : "metricbeat" and event.dataset : "system.socket\_summary" and system.socket.summary.all.count > 5000

30) **Co robi:** Interfejsy nazwane „eth\*”.

**KQL:** agent.type : "metricbeat" and event.dataset : "system.network" and system.network.name : "eth\*"

# Winlogbeat (Windows/Sysmon/PowerShell) – 30 przykładów

1) **Co robi:** Dane tylko z Winlogbeat.

**KQL:** agent.type : "winlogbeat"

2) **Co robi:** Nieudane logowania (Security 4625).

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.security" and event.code : 4625

3) **Co robi:** Udane logowania typu 10 (zdalne).

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.security" and event.code : 4624 and winlog.event\_data.LogonType : "10"

4) **Co robi:** Przydział uprawnień specjalnych (4672).

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.security" and event.code : 4672

5) **Co robi:** Utworzenie konta (4720).

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.security" and event.code : 4720

6) **Co robi:** Usunięcie konta (4726).

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.security" and event.code : 4726

7) **Co robi:** Dodanie do lokalnej grupy (4732).

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.security" and event.code : 4732

8) **Co robi:** Logon z jawnymi poświadczeniami (4648).

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.security" and event.code : 4648

9) **Co robi:** Wyczyszczenie dziennika audytu (1102).

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.security" and event.code : 1102

10) **Co robi:** Utworzenie procesu – Sysmon EID 1.

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.sysmon" and event.code : 1

11) **Co robi:** Połączenia sieciowe – Sysmon EID 3.

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.sysmon" and event.code : 3

12) **Co robi:** Ładowanie bibliotek – Sysmon EID 7.

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.sysmon" and event.code : 7

13) **Co robi:** Dostęp do procesu – Sysmon EID 10.

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.sysmon" and event.code : 10

14) **Co robi:** Tworzenie pliku – Sysmon EID 11.

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.sysmon" and event.code : 11

15) **Co robi:** Zdarzenia rejestru – Sysmon EID 12/13/14.

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.sysmon" and event.code : (12 or 13 or 14)

16) **Co robi:** DNS query – Sysmon EID 22.

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.sysmon" and event.code : 22

17) **Co robi:** Uruchomienia PowerShell (kanał PS).

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.powershell"

18) **Co robi:** PowerShell – ScriptBlock z frazą „Invoke-WebRequest”.

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.powershell" and winlog.event\_data.ScriptBlockText : "\*Invoke-WebRequest\*"

19) **Co robi:** Instalacja nowej usługi (System 7045).

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.system" and event.code : 7045

20) **Co robi:** Zmiana stanu usługi (System 7036).

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.system" and event.code : 7036

21) **Co robi:** Start usługi Event Log (System 6005).

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.system" and event.code : 6005

22) **Co robi:** Stop usługi Event Log (System 6006).

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.system" and event.code : 6006

23) **Co robi:** Utworzenia procesu PowerShell (Sysmon + executable).

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.sysmon" and event.code : 1 and process.executable : "\*\\powershell.exe"

24) **Co robi:** Rodzic procesu to cmd.exe.

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.sysmon" and event.code : 1 and process.parent.executable : "\*\\cmd.exe"

25) **Co robi:** Proces uruchomiony z katalogu temp.

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.sysmon" and event.code : 1 and process.executable : "\*\\AppData\\Local\\Temp\\\*"

26) **Co robi:** Logowania interaktywne (4624 typ 2).

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.security" and event.code : 4624 and winlog.event\_data.LogonType : "2"

27) **Co robi:** Reset hasła (4724).

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.security" and event.code : 4724

28) **Co robi:** Zmiana hasła (4723).

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.security" and event.code : 4723

29) **Co robi:** Zdarzenia tylko z kanału Sysmon.

**KQL:** agent.type : "winlogbeat" and winlog.channel : "Microsoft-Windows-Sysmon/Operational"

30) **Co robi:** Zdarzenia Security dla użytkownika Administrator.

**KQL:** agent.type : "winlogbeat" and event.dataset : "windows.security" and user.name : "Administrator"

# Packetbeat (sieć/protokoły) – 30 przykładów

1) **Co robi:** Tylko dane z Packetbeat.

**KQL:** agent.type : "packetbeat"

2) **Co robi:** TCP port 443 (HTTPS).

**KQL:** agent.type : "packetbeat" and network.transport : "tcp" and destination.port : 443

3) **Co robi:** Żądania HTTP metodą POST.

**KQL:** agent.type : "packetbeat" and http.request.method : "POST"

4) **Co robi:** HTTP 5xx.

**KQL:** agent.type : "packetbeat" and http.response.status\_code >= 500

5) **Co robi:** Ruch do domeny example.com.

**KQL:** agent.type : "packetbeat" and url.domain : "example.com"

6) **Co robi:** Zapytania DNS o example.com.

**KQL:** agent.type : "packetbeat" and dns.question.name : "example.com"

7) **Co robi:** DNS – NXDOMAIN.

**KQL:** agent.type : "packetbeat" and dns.response\_code : "NXDOMAIN"

8) **Co robi:** Ruch z podsieci 10/8 na porty wysokie.

**KQL:** agent.type : "packetbeat" and source.ip : "10.0.0.0/8" and destination.port >= 1024

9) **Co robi:** Transakcje z ≥ 1 MB danych.

**KQL:** agent.type : "packetbeat" and network.bytes >= 1000000

10) **Co robi:** TLS – wildcard CN \*.example.com.

**KQL:** agent.type : "packetbeat" and tls.server.x509.subject.common\_name : "\*.example.com"

11) **Co robi:** TLS – certyfikat wygaśnie w 14 dni.

**KQL:** agent.type : "packetbeat" and tls.server.x509.not\_after < now+14d

12) **Co robi:** HTTP – Chrome jako UA.

**KQL:** agent.type : "packetbeat" and user\_agent.original : "\*Chrome\*"

13) **Co robi:** HTTP/2.

**KQL:** agent.type : "packetbeat" and http.version : "2"

14) **Co robi:** URL zaczyna się od /api/.

**KQL:** agent.type : "packetbeat" and url.path : "/api/\*"

15) **Co robi:** Odpowiedzi 401/403 (auth).

**KQL:** agent.type : "packetbeat" and http.response.status\_code : (401 or 403)

16) **Co robi:** Długa transakcja (>1 s).

**KQL:** agent.type : "packetbeat" and event.duration > 1000000000

17) **Co robi:** Ruch do kraju US (dest).

**KQL:** agent.type : "packetbeat" and destination.geo.country\_iso\_code : "US"

18) **Co robi:** Ruch z kraju PL (src).

**KQL:** agent.type : "packetbeat" and source.geo.country\_iso\_code : "PL"

19) **Co robi:** HTTP – brak referera.

**KQL:** agent.type : "packetbeat" and http.request.referrer : ""

20) **Co robi:** HTTP – typ treści JSON.

**KQL:** agent.type : "packetbeat" and http.response.mime\_type : "application/json"

21) **Co robi:** DNS do resolvera 8.8.8.8.

**KQL:** agent.type : "packetbeat" and destination.ip : "8.8.8.8" and dns.question.name : \*

22) **Co robi:** Ogranicz do protokołu MySQL.

**KQL:** agent.type : "packetbeat" and network.protocol : "mysql"

23) **Co robi:** Ogranicz do protokołu PostgreSQL.

**KQL:** agent.type : "packetbeat" and network.protocol : "pgsql"

24) **Co robi:** Ogranicz do Redis.

**KQL:** agent.type : "packetbeat" and network.protocol : "redis"

25) **Co robi:** Klient → Serwer (pola roli).

**KQL:** agent.type : "packetbeat" and client.ip : \* and server.ip : \*

26) **Co robi:** TCP z resetem (RST).

**KQL:** agent.type : "packetbeat" and tcp.flags : "RST"

27) **Co robi:** HTTP – host „api.example.com”.

**KQL:** agent.type : "packetbeat" and url.domain : "api.example.com"

28) **Co robi:** HTTP – metody inne niż GET/POST.

**KQL:** agent.type : "packetbeat" and http.request.method : \* and not http.request.method : ("GET" or "POST")

29) **Co robi:** TLS – issuer zawiera „Let's Encrypt”.

**KQL:** agent.type : "packetbeat" and tls.server.x509.issuer.common\_name : "\*Let's Encrypt\*"

30) **Co robi:** Transakcje, gdzie user\_agent jest pusty.

**KQL:** agent.type : "packetbeat" and not user\_agent.original : \*

# Heartbeat (Uptime/Synthetics) – 30 przykładów

1) **Co robi:** Tylko dokumenty Heartbeat.

**KQL:** agent.type : "heartbeat"

2) **Co robi:** Monitory down (niedostępne).

**KQL:** agent.type : "heartbeat" and monitor.status : "down"

3) **Co robi:** Tylko HTTP.

**KQL:** agent.type : "heartbeat" and monitor.type : "http"

4) **Co robi:** Tylko ICMP (ping).

**KQL:** agent.type : "heartbeat" and monitor.type : "icmp"

5) **Co robi:** Tylko TCP.

**KQL:** agent.type : "heartbeat" and monitor.type : "tcp"

6) **Co robi:** HTTP z błędami (>=400).

**KQL:** agent.type : "heartbeat" and monitor.type : "http" and http.response.status\_code >= 400

7) **Co robi:** Długie odpowiedzi HTTP (>2 s).

**KQL:** agent.type : "heartbeat" and monitor.type : "http" and monitor.duration.us > 2000000

8) **Co robi:** Co najmniej jedno „down” w podsumowaniu.

**KQL:** agent.type : "heartbeat" and summary.down > 0

9) **Co robi:** Monitory dla konkretnego URL.

**KQL:** agent.type : "heartbeat" and url.full : "https://twojadomena.pl/\*"

10) **Co robi:** Po porcie 8443.

**KQL:** agent.type : "heartbeat" and url.port : 8443

11) **Co robi:** TLS – certyfikat wygaśnie < 14 dni.

**KQL:** agent.type : "heartbeat" and tls.server.x509.not\_after < now+14d

12) **Co robi:** TLS – wystawca „Let's Encrypt”.

**KQL:** agent.type : "heartbeat" and tls.server.x509.issuer.common\_name : "\*Let's Encrypt\*"

13) **Co robi:** Tylko monitory z tagiem „prod”.

**KQL:** agent.type : "heartbeat" and tags : "prod"

14) **Co robi:** Monitory z nazwą zawierającą „API”.

**KQL:** agent.type : "heartbeat" and monitor.name : "\*API\*"

15) **Co robi:** Up tylko z danej lokalizacji.

**KQL:** agent.type : "heartbeat" and monitor.status : "up" and observer.geo.name : "eu-central-1"

16) **Co robi:** TCP – porty otwarte.

**KQL:** agent.type : "heartbeat" and monitor.type : "tcp" and monitor.status : "up"

17) **Co robi:** HTTP – 3xx (redirecty).

**KQL:** agent.type : "heartbeat" and monitor.type : "http" and http.response.status\_code >= 300 and http.response.status\_code < 400

18) **Co robi:** HTTP – JSON w odpowiedzi.

**KQL:** agent.type : "heartbeat" and monitor.type : "http" and http.response.mime\_type : "application/json"

19) **Co robi:** HTTP – wysoki TTFB (proxy: duration).

**KQL:** agent.type : "heartbeat" and monitor.type : "http" and monitor.duration.us > 1000000

20) **Co robi:** Browser/Synthetics – nieudane kroki.

**KQL:** agent.type : "heartbeat" and synthetics.type : "step/end" and synthetics.step.status : "failed"

21) **Co robi:** Browser – konkretna nazwa kroku.

**KQL:** agent.type : "heartbeat" and synthetics.type : "step/end" and synthetics.step.name : "\*Login\*"

22) **Co robi:** Browser – konkretna nazwa journey.

**KQL:** agent.type : "heartbeat" and synthetics.journey.name : "\*Checkout\*"

23) **Co robi:** Browser – testy z konkretnej lokacji.

**KQL:** agent.type : "heartbeat" and synthetics.type : "journey/start" and observer.geo.name : "eu-west-1"

24) **Co robi:** HTTP – brak certyfikatu TLS (plain).

**KQL:** agent.type : "heartbeat" and monitor.type : "http" and not tls.server.x509.subject.common\_name : \*

25) **Co robi:** ICMP – hosty niedostępne.

**KQL:** agent.type : "heartbeat" and monitor.type : "icmp" and monitor.status : "down"

26) **Co robi:** HTTP – monitoruje host „api.example.com”.

**KQL:** agent.type : "heartbeat" and url.domain : "api.example.com"

27) **Co robi:** HTTP – port 80.

**KQL:** agent.type : "heartbeat" and monitor.type : "http" and url.port : 80

28) **Co robi:** HTTP – kod 200.

**KQL:** agent.type : "heartbeat" and monitor.type : "http" and http.response.status\_code : 200

29) **Co robi:** Browser – tylko zakończenia kroków.

**KQL:** agent.type : "heartbeat" and synthetics.type : "step/end"

30) **Co robi:** Monitory z konkretnym ID.

**KQL:** agent.type : "heartbeat" and monitor.id : "monitor-123"