Winlogbeat / Windows Event Logs – przewodnik po polach (ECS + winlog.event\_data)

Ta ściąga opisuje najczęściej używane pola w zdarzeniach Windows zbieranych przez Winlogbeat (ECS + winlog.\*), w prostym języku i z podpowiedzią, do czego są przydatne w analizie/alertach/dashboardach Kibany. Uwaga: nie każde pole występuje w każdym zdarzeniu – wiele kluczowych atrybutów znajduje się w winlog.event\_data.\* i zależy od event.code.

# Jak czytać nazwy pól

• ECS (uniwersalne): @timestamp, event.\*, host.\*, user.\*, process.\*, log.level, message – wspólny schemat dla całego stacka.

• Specyficzne dla Windows: winlog.\* (np. winlog.channel, winlog.provider\_name) oraz oryginalne atrybuty zdarzeń w winlog.event\_data.\* (np. NewProcessName).

# A) Rdzeń zdarzenia

• @timestamp — Chwila wystąpienia zdarzenia. Po co: Oś czasu, korelacja incydentów. KQL: @timestamp > now()-24h

• message — Pełny opis zdarzenia (tekst). Po co: Szybkie czytanie, często zawiera brakujące detale

• log.level — Poziom logu (information/warning/error/critical). Po co: Filtrowanie „szumu”, fokus na błędy. KQL: log.level: ("error" or "critical")

• event.code — Numer zdarzenia Windows (np. 4624, 4625, 4688, 4697). Po co: Precyzyjne reguły i panele. KQL: event.code: "4688"

• event.action — Opis akcji (np. logon, process\_started). Po co: Ujednolicone filtry między systemami

• event.category — Kategoria (authentication/process/configuration...). Po co: Szybki przegląd typów aktywności. KQL: event.category: authentication

• event.type — Typ w ramach kategorii (start/end/info/change). Po co: Rozróżnienie fazy (np. start procesu). KQL: event.type: start and event.category: process

• event.outcome — Wynik akcji (success/failure). Po co: Odróżnianie udanych/nieudanych logowań. KQL: event.category: authentication and event.outcome: failure

• event.sequence — Licznik/sekwencja źródła. Po co: Porządkowanie powiązanych wpisów

• event.original — Surowy tekst/XML (jeśli włączone). Po co: Forensyka, weryfikacja mapowania

# B) Źródło i środowisko (host/agent)

• host.name — Nazwa komputera. Po co: Drill‑down na maszynę, rankingi TOP. KQL: host.name: "SRV-AD-01"

• host.id / host.hostname — Identyfikatory hosta. Po co: Rozróżnianie podobnych nazw

• host.os.\* — Informacje o systemie operacyjnym. Po co: Różnice w logach/podatnościach

• agent.\* — Wersja/typ agenta (Winlogbeat). Po co: Zdrowie telemetryki, debugging

# C) Kanał i „provider” (Windows)

• winlog.channel — Dziennik: Security/System/Application/Microsoft-\*. Po co: Kierowanie do paneli/alertów. KQL: winlog.channel: "Security"

• winlog.provider\_name — Źródło zdarzenia (provider). Po co: Identyfikacja komponentu

• winlog.record\_id — ID rekordu w dzienniku. Po co: Deduplikacja, odwołanie na hoście

• winlog.task / opcode / keywords — Meta-opis akcji Windows. Po co: Zaawansowane filtrowanie

• winlog.level — Poziom Windows. Po co: Alternatywa dla log.level

• winlog.computer\_name — Nazwa z wpisu. Po co: Spójność nazw/domen

• winlog.activity\_id — GUID korelacyjny. Po co: Łączenie wpisów jednej operacji

• winlog.user.\* — Użytkownik wg subsystemu. Po co: Pomocnicze, gdy user.\* brak

# D) Użytkownicy i konta

• user.name — Nazwa konta (np. DOMAIN\user). Po co: Kto wykonał/objęty zdarzeniem. KQL: user.name: "DOMAIN\\admin"

• user.domain — Domena/komputer lokalny. Po co: Rozróżnienie kont lokalnych/domenowych

• user.id / user.sid — SID użytkownika. Po co: Jednoznaczna identyfikacja

• winlog.event\_data.TargetUserName / SubjectUserName — Użytkownik cel/wykonawca. Po co: Analiza logowań/zmian kont. KQL: winlog.event\_data.TargetUserName: "\*admin\*"

• winlog.event\_data.TargetDomainName / SubjectDomainName — Domena celu/wykonawcy. Po co: Rozróżnienie stref/OU

# E) Logowanie i sesje (Security)

• winlog.event\_data.LogonType — Typ logowania (2=interactive, 3=network, 10=RDP). Po co: Wykrywanie RDP/psExec itp.. KQL: event.code: "4624" and winlog.event\_data.LogonType: "10"

• winlog.event\_data.IpAddress / IpPort / WorkstationName — Źródło logowania. Po co: Pivot sieciowy, geolokacja. KQL: event.code: "4625" and winlog.event\_data.IpAddress: \*

• event.outcome — success/failure. Po co: Brute force / nieudane próby. KQL: event.category: authentication and event.outcome: failure

• Kody często używane — 4624 OK, 4625 FAIL, 4634 logoff, 4672 przywileje, 4648 explicit creds. Po co: Gotowe reguły

# F) Procesy i pliki

• process.entity\_id — Stabilny identyfikator procesu. Po co: Korelacja rodzic‑dziecko

• process.pid / process.parent.pid — PID procesu i rodzica. Po co: Drzewo procesów

• process.name / process.executable — Nazwa/pełna ścieżka EXE. Po co: Allow/Deny, LOLBiny. KQL: process.executable: "C:\\Windows\\System32\\cmd.exe"

• process.command\_line — Pełna linia poleceń. Po co: Parametry akcji (np. -enc). KQL: process.command\_line: "\*-nop\*"

• winlog.event\_data.\* (4688) — NewProcessName, CommandLine, ParentProcessName, ProcessId, ParentProcessId. Po co: Uzupełnienie process.\*. KQL: event.code: "4688"

# G) Usługi i sterowniki

• winlog.event\_data.\* (4697) — ServiceName, ImagePath, ServiceType, StartType. Po co: Wykrywanie persystencji. KQL: event.code: "4697"

• SCM 7045 (System) — Instalacja usługi/sterownika (w message). Po co: Low‑level persystencja. KQL: winlog.provider\_name: "Service Control Manager"

# H) Uprawnienia i dostęp do obiektów

• winlog.event\_data.Privileges (4672) — Lista przywilejów (np. SeDebugPrivilege). Po co: Eskalacja uprawnień. KQL: event.code: "4672"

• winlog.event\_data.ObjectName/ObjectType/AccessMask — Jaki obiekt i jakie prawa. Po co: Śledzenie zmian rejestru/plików

# I) Sieć (gdy występuje w logu)

• source.ip / destination.ip (+ port) — Adresy źródłowy/docelowy. Po co: Pivot sieciowy. KQL: source.ip: 10.0.0.\*

• related.ip / related.user / related.hash — Skróty do pivotów (ECS). Po co: Szybkie łączenie kontekstu

# J) Korelacja i porządkowanie

• trace.id / transaction.id — Identyfikatory transakcji/śledzenia. Po co: Łączenie zdarzeń w jedną operację

• tags / labels.\* — Twoje własne etykiety. Po co: Oznaczanie wyjątków/kampanii

# Najważniejsze winlog.event\_data.\* (wg event.code)

• Logowanie (4624/4625/4648): LogonType, TargetUserName, TargetDomainName, SubjectUserName, IpAddress, WorkstationName, AuthenticationPackageName, FailureReason, Status, SubStatus.

• Proces (4688): NewProcessName, CommandLine, ParentProcessName, ProcessId, ParentProcessId.

• Usługa (4697 / SCM 7045): ServiceName, ImagePath, ServiceType, StartType, AccountName.

• Zmiany kont (4720/4726/4723/4724/4725/4740): TargetUserName, SubjectUserName, SamAccountName, UserPrincipalName, UserAccountControl.

# Mini‑tabela: „pole → przydatność → przykład KQL”

|  |  |  |
| --- | --- | --- |
| Pole | Po co / Przydatność | Przykładowy KQL |
| event.code | Numer zdarzenia; budowa reguł | event.code: "4688" |
| event.outcome | Sukces/porażka; KPI i alerty | event.category: authentication and event.outcome: failure |
| host.name | Drill‑down; TOP hosty | host.name: "SRV-AD-01" |
| user.name / TargetUserName | Kto wykonał/cel akcji | winlog.event\_data.TargetUserName: "\*admin\*" |
| winlog.channel | Segmentacja Security/System/Application | winlog.channel: "Security" |
| process.command\_line / CommandLine | Podejrzane parametry | process.command\_line: "\*-enc\*" |
| ServiceName / ImagePath | Persystencja usług | event.code: "4697" |
| IpAddress / WorkstationName | Źródło logowania | event.code: "4625" and winlog.event\_data.IpAddress: \* |
| log.level | Cięcie szumu błędów | log.level: ("error" or "critical") |

# Szybkie filtry KQL (kopiuj‑wklej)

• Nieudane logowania (24h): event.category: authentication and event.outcome: failure

• RDP logins (4624 typ 10): event.code: "4624" and winlog.event\_data.LogonType: "10"

• Tworzenie procesu cmd/powershell: event.code: "4688" and (winlog.event\_data.NewProcessName: "\*\\cmd.exe" or winlog.event\_data.NewProcessName: "\*\\powershell.exe")

• Nowe usługi: event.code: "4697"

• Błędy krytyczne System+Application: log.level: ("error" or "critical") and winlog.channel: ("System" or "Application")