CERTYX



AUTONOMOUS CERTIFICATE LIFECYCLE MANAGEMENT

Integracja SIEM

Eksport dziennika bezpieczeństwa do Splunk, Cribl, IBM QRadar, ArcSight, Microsoft Sentinel i webhooków

JĘZYK
Polski

WERSJA
8550060f

DATA
1 listopada 2026

Spis treści

1 Co eksportuje CERTYX 5
1.1 Potok przetwarzania 5
1.2 Transporty 6
1.3 Formaty 6
1.4 Profile schematu 7
2 Dozwolone kombinacje 7
2.1 Miejsca docelowe z pierwszego wydania 8
3 Szybki start 8
4 Eksportowane zdarzenia 8
5 Zanim zaczniesz 10
6 Dodawanie miejsca docelowego w CERTYX 10
7 TLS i zaufane certyfikaty główne 12
7.1 Certyfikat klienta (mTLS) 12
7.2 Sprawdzanie unieważnienia 13
8 Podpisany webhook HTTPS 13
8.1 Strona odbiorcy 13
8.2 Weryfikacja podpisu 13
8.3 Strona CERTYX 15
9 Splunk HTTP Event Collector 15
9.1 Wybór ścieżki do Splunk 15
9.2 Strona odbiorcy (Splunk) 16
9.3 Strona CERTYX 17
9.4 props.conf 18
9.5 Splunk CIM 18
10 Syslog przez TLS 19
10.1 Nagłówek RFC 5424 formatów kanonicznych 19
10.2 Ramkowanie 20
10.3 Strona CERTYX (wszystkie formaty syslog) 20
10.4 Ogólny odbiorca syslog (rsyslog, syslog-ng) 20
11 Cribl Stream 21
11.1 Wybór źródła Cribl 21
11.2 Strona odbiorcy (źródło syslog Cribl) 21
11.3 Strona odbiorcy (źródło Splunk HEC w Cribl) 22
11.4 Strona CERTYX 22
12 Wejście TCP-SSL Splunk 22
12.1 Strona odbiorcy (Splunk) 22
12.2 Strona CERTYX 23
13 IBM QRadar 23
13.1 Wybór formatu LEEF 23
13.2 Strona odbiorcy (QRadar) 23
13.3 Strona CERTYX 24
14 ArcSight 24
14.1 Wybór formatu CEF 24
14.2 Strona odbiorcy (ArcSight SmartConnector) 25
14.3 Strona CERTYX 25

15 Elastic (ECS) 25
16 Odbiorcy OCSF i Amazon Security Lake 26
17 Microsoft Sentinel 26
17.1 Co otrzymuje tabela 27
17.2 Strona odbiorcy (Azure) 27
17.3 Strona CERTYX 28
18 OpenTelemetry Logs (OTLP/HTTP) 29
18.1 Co otrzymuje odbiorca 29
18.2 Strona odbiorcy (OpenTelemetry Collector) 30
18.3 Grafana Alloy i Loki 31
18.4 Inne systemy OTLP 31
18.5 Strona CERTYX 31
19 Sprawdzenie połączenia i zdarzenie testowe 32
20 Dostarczanie, ponowienia i zaległości 32
20.1 Odrzucone zdarzenia 33
20.2 Limity 33
21 Ponowne wysyłanie od numeru sekwencyjnego lub czasu 33
22 Usuwanie duplikatów według event_id 34
23 Wysyłaj tylko: mniej danych do SIEM 35
23.1 Łączenie filtrów 35
24 Kształtowanie zdarzeń: rozmiar i postać 35
25 Mapowanie pól 37
26 Pola wzbogacenia 38
27 Wiele organizacji w jednym SIEM 39
28 Archiwa plikowe 40
28.1 Konfiguracja 40
28.2 Pliki 41
28.3 Pobieranie 41
28.4 Dostarczanie, ponowne uruchomienia i miejsce na dysku 41
29 Uprawnienia 42
30 Rozwiązywanie problemów 42
30.1 Incydenty 42
30.2 Wyniki sprawdzenia i zdarzenia testowego 42
30.3 Odbiorca pokazuje fragmenty lub dane binarne 44
30.4 Kody Splunk HEC 44
30.5 Stan dostarczania na karcie miejsca docelowego 45
30.6 Komunikaty formularza i uprawnień 45
31 Przykładowe zdarzenia 46
31.1 Webhook HTTPS 46
31.2 Splunk HEC 47
31.3 Syslog przez TLS 48
31.4 Microsoft Sentinel 50
31.5 OpenTelemetry Logs 50
31.6 Archiwum plikowe 51
32 Opis pól 52
32.1 Zdarzenie kanoniczne 52
32.2 Rekord JSON 53

32.3 Pola CEF (pierwsze wydanie) 54
32.4 Pola LEEF (pierwsze wydanie) 54
32.5 Kolumny Sentinel 55
33 Katalog kodów zdarzeń 55
33.1 Wybierane według wyniku 56
33.2 Akcje dziennika 56

CERTYX w sposób ciągły eksportuje swój dziennik bezpieczeństwa do używanego już przez Ciebie systemu SIEM. Ten przewodnik wyjaśnia, co jest eksportowane, jak wybiera się format, profil schematu i transport oraz jak krok po kroku skonfigurować obie strony — system odbierający i CERTYX — dla Splunk, Cribl Stream, IBM QRadar, ArcSight, Elastic, odbiorców OCSF, Microsoft Sentinel, systemów OpenTelemetry i własnego kolektora.

1 Co eksportuje CERTYX

Każde miejsce docelowe otrzymuje te same zdarzenia z dziennika bezpieczeństwa. Miejsce docelowe jest określone przez trzy niezależne wybory:

- **Transport** — sposób przesyłania zdarzeń: podpisany webhook HTTPS, Splunk HTTP Event Collector, syslog przez TLS, Azure Monitor Logs Ingestion API (Microsoft Sentinel), OpenTelemetry Logs przez OTLP/HTTP albo pliki dzienne w archiwum na serwerze.
- **Format** — sposób zakodowania jednego zdarzenia: JSON, NDJSON, syslog RFC 5424, CEF, LEEF 1.0, LEEF 2.0, Generic KV, CSV, wiersz tabeli Sentinel albo żądanie dzienników OTLP (protobuf lub OTLP/JSON).
- **Profil schematu** — nazwy pól używane w dokumencie JSON: zdarzenie kanoniczne CERTYX (`native`), Elastic Common Schema (`ecs`), OCSF (`ocsf`) albo zdarzenie kanoniczne z polami indeksowanymi Splunk CIM (`splunk-cim`).

Zapisać można tylko kombinacje wymienione w sekcji Dozwolone kombinacje. Każde miejsce docelowe jest dostępne dla administratora organizacji w widoku **Eksport do SIEM**, a dla operatora platformy w **Dziennik zdarzeń bezpieczeństwa → Eksport do SIEM**. Każde miejsce docelowe ma własną pozycję w dzienniku: dostarczanie jest ciągłe, co najmniej jednokrotne (at least once), a po błędzie nic nie zostaje pominięte.

Wyłącznie szyfrowany transport. CERTYX zawsze używa TLS i zawsze weryfikuje certyfikat odbiorcy — względem magazynu zaufanych certyfikatów systemu operacyjnego albo dokładnie tych certyfikatów głównych, które wkleisz dla danego miejsca docelowego — oraz sprawdza unieważnienie. Zwykły TCP, syslog przez UDP ani TLS bez weryfikacji nie są dostępne. OpenTelemetry Logs są przesyłane przez OTLP/HTTP z TLS; OTLP przez gRPC nie jest dostępny.

1.1 Potok przetwarzania

1. **Dziennik.** Każde zdarzenie bezpieczeństwa jest zapisywane w dzienniku bezpieczeństwa powiązanym łańcuchem skrótów w bazie platformy. Dziennik jest trwałą kolejką każdego miejsca docelowego.
2. **Zdarzenie kanoniczne.** Podczas eksportu każdy wpis dziennika jest mapowany na jedno zdarzenie kanoniczne w wersji schematu `certyx.event/1.0`, razem z kontekstem eksportu (identyfikator instalacji, wersja produktu, środowisko, host) i wzbogaceniem wpisu (identyfikator śledzenia, port źródłowy, adres serwera, rola, identyfikator korelacji sesji — zob. Pola wzbogacenia). Sam rekord dziennika objęty skrótem nigdy nie jest zmieniany.
3. **Redakcja.** Zapisane zmiany przechodzą przez etap redakcji, który na każdym poziomie zagnieżdżenia usuwa każdą właściwość, której nazwa wskazuje na hasło, sekret, token, klucz, plik cookie lub poświadczenie; `changes_redacted` ma wartość `true`, gdy coś usunięto.
4. **Filtry.** Sondy kondycji, wyniki, minimalna ważność, kategorie i kody zdarzeń decydują, czy miejsce docelowe otrzyma zdarzenie (zob. Wysyłaj tylko). Archiwa plikowe zachowują każde zdarzenie.
5. **Mapowanie pól.** Własne reguły miejsca docelowego zmieniają nazwy pól zdarzenia kanonicznego, usuwają je, zachowują albo dodają — jeden raz, zanim zapisze je którykolwiek format (Mapowanie pól).
6. **Serializator.** Format i profil schematu zamieniają zdarzenie w wiersz lub dokument.
7. **Transport.** Paczka zostaje wysłana; pozycja miejsca docelowego przesuwa się dopiero po jej przyjęciu przez odbiorcę.

Każde zdarzenie ma globalnie unikalny `event_id = <installation id>:<journal sequence>`, na przykład `7d4c2a10-…-9e1f:48213`. Identyfikatorem instalacji jest `Clm:Siem:InstallationId`, jeśli operator go ustawi, a w przeciwnym razie UUID wygenerowany jednorazowo i zapisany w bazie platformy, więc każda instancja i każde ponowne uruchomienie używa tego samego. Odbiorcy usuwają duplikaty według `event_id` (zob. Usuwanie duplikatów).

1.2 Transporty

Transport	Identyfikator	Działanie	Typowy odbiorca
Podpisany webhook HTTPS	`https`	HTTPS `POST` z paczką, podpisany HMAC-SHA256 w `X-Certyx-Signature`	Własny kolektor, Logstash, SOAR, funkcja bezserwerowa, źródło HTTP Cribl
Splunk HTTP Event Collector	`splunk-hec`	HTTPS do `/services/collector/event` z tokenem HEC, opcjonalne potwierdzanie indeksowania	Splunk Enterprise, Splunk Cloud, źródło Splunk HEC w Cribl
Syslog przez TLS	`syslog-tls`	Komunikaty RFC 5424 przez TCP z TLS, ramkowanie zliczaniem oktetów (RFC 5425) lub nową linią	Cribl Stream, QRadar, ArcSight SmartConnector, wejście TCP Splunk, rsyslog, syslog-ng, Logstash, Elastic Agent
Microsoft Sentinel	`azure-monitor`	Logs Ingestion API przez regułę zbierania danych, uwierzytelnianie aplikacją Microsoft Entra	Microsoft Sentinel, Log Analytics
OpenTelemetry Logs	`otlp-http`	HTTPS `POST` z żądaniem OTLP `ExportLogsServiceRequest` (protobuf lub OTLP/JSON, opcjonalnie gzip i jeden nagłówek uwierzytelniania)	OpenTelemetry Collector, Grafana Alloy i Loki, każdy system z punktem końcowym dzienników OTLP/HTTP
Archiwum plikowe	`file`	Pliki dzienne w katalogu archiwum na serwerze, do pobrania z konsoli	Długoterminowe przechowywanie, import wsadowy (na przykład potoki OCSF)

1.3 Formaty

Format	Identyfikator	Zawartość
Rekord JSON	`json`	Rekord dziennika CERTYX z pierwszego wydania (`Sequence` , `At` , `Category` , `EventCode` , `Tenant` , ...) z dodanym `EventId` ; tablica JSON na żądanie webhooka, `event` HEC albo tekst komunikatu syslog. Cudzysłowy w napisach są zapisywane jako `\"` , a znaki takie jak `+` pozostają bez zmian (nie `\u0022` ani `\u002B`), więc wyodrębnianie par klucz-wartość nie tworzy fałszywych pól, a wyszukiwanie tekstu działa. `Changes` zawiera zagnieżdżone obiekty, a nie ciągi z cudzysłowami poprzedzonymi ukośnikiem (także dla starszych zdarzeń)
NDJSON	`ndjson`	Jeden dokument JSON profilu schematu na wiersz (`application/x-ndjson`), UTF-8 bez znacznika kolejności bajtów
RFC 5424	`rfc5424`	Komunikat syslog RFC 5424 z danymi strukturalnymi, którego MSG jest dokumentem JSON profilu schematu
CEF	`cef`	ArcSight CEF 0 ze zdarzenia kanonicznego (Device Event Class ID = kod zdarzenia, `externalId` = identyfikator zdarzenia)
LEEF 1.0	`leef-1.0`	IBM QRadar LEEF 1.0 z atrybutami rozdzielonymi tabulatorem
LEEF 2.0	`leef-2.0`	IBM QRadar LEEF 2.0 z separatorem atrybutów zadeklarowanym w nagłówku (domyślnie tabulator)
Generic KV	`kv`	Udokumentowany profil `certyx-kv/1.0` : każde pole kanoniczne jako `key=value` w stałej kolejności; nie jest to CEF ani LEEF
CSV	`csv`	Kanoniczne wiersze CSV zgodne z RFC 4180, z wersjonowanym nagłówkiem (archiwum plikowe)
Wiersz Sentinel	`sentinel`	Kolumny niestandardowej tabeli Sentinel z dodanym `EventId`
OTLP protobuf	`otlp-protobuf`	Żądanie OpenTelemetry Logs w binarnym protobuf (`application/x-protobuf`), jeden rekord dziennika na zdarzenie kanoniczne
OTLP/JSON	`otlp-json`	To samo żądanie w kodowaniu OTLP/JSON (`application/json`)
CEF (pierwsze wydanie)	`cef-compat`	Układ CEF z pierwszego wydania z dodanym `certyxEventId=`
LEEF (pierwsze wydanie)	`leef-compat`	Układ LEEF 2.0 z pierwszego wydania (separator `^`) z dodanym `eventId=`
CSV (pierwsze wydanie)	`csv-compat`	Kolumny archiwum CSV z pierwszego wydania (`certyx-security-YYYY-MM-DD.csv`) bez zmian

1.4 Profile schematu

Profil	Identyfikator	Nazwy pól
Kanoniczny	`native`	Zdarzenie kanoniczne CERTYX `certyx.event/1.0` w notacji snake_case (`event_id` , `event_code` , `category` , `outcome` , ...); zob. Opis pól
Elastic Common Schema	`ecs`	ECS 8.11.0: `@timestamp` , `event.*` (`event.id` = identyfikator zdarzenia, `event.code` = kod zdarzenia, `event.dataset = certyx.security`), `user.*` , `source.ip` , `host.hostname` , `service.*` , `http.*` , `url.path` , `organization.*` , `labels.*`
OCSF	`ocsf`	OCSF 1.1.0, klasa wybierana dla każdego zdarzenia i weryfikowana: Authentication (3002), Account Change (3001), API Activity (6003), w pozostałych przypadkach Base Event (0); `metadata.uid` = identyfikator zdarzenia
Splunk CIM	`splunk-cim`	Zdarzenie kanoniczne jako `event` HEC, a do tego pola Splunk CIM (modele danych Authentication i Change) jako pola indeksowane HEC; tylko transport HEC

Pełne mapowanie każdego pola kanonicznego na klucze CEF, atrybuty LEEF, ECS, OCSF i CIM zawiera dokument opisu pól `docs/SIEM-EXPORT-FIELDS.md` w dokumentacji CERTYX; najważniejsze pola podsumowano w sekcji Opis pól.

2 Dozwolone kombinacje

Najpierw wybierz transport; formularz zaproponuje wtedy jego formaty, a dla każdego formatu — jego profile.

Transport	Format	Profile
`https`	`ndjson`	`native` , `ecs` , `ocsf`
`https`	`json`	`native`
`splunk-hec`	`ndjson`	`native` , `ecs` , `ocsf` , `splunk-cim`
`splunk-hec`	`json`	`native`
`syslog-tls`	`rfc5424`	`native` , `ecs` , `ocsf`
`syslog-tls`	`cef`	`native`
`syslog-tls`	`leef-1.0`	`native`
`syslog-tls`	`leef-2.0`	`native`
`syslog-tls`	`kv`	`native`
`syslog-tls`	`json`	`native`
`syslog-tls`	`cef-compat`	`native`
`syslog-tls`	`leef-compat`	`native`
`azure-monitor`	`sentinel`	`native`
`otlp-http`	`otlp-protobuf`	`native`
`otlp-http`	`otlp-json`	`native`
`file`	`ndjson`	`native` , `ecs` , `ocsf`
`file`	`csv`	`native`
`file`	`csv-compat`	`native`

Każda inna kombinacja jest odrzucana komunikatem *Format, profil schematu i transport: wybierz transport, a następnie jeden z oferowanych dla niego formatów i profili.* Archiwa plikowe można skonfigurować wyłącznie w konsoli, a nie w konfiguracji serwera.

2.1 Miejsca docelowe z pierwszego wydania

Miejsca docelowe zapisane, zanim format, profil i transport stały się osobnymi wyborami — oraz miejsca docelowe z konfiguracji, które ustawiają tylko `Kind` — zachowują swój układ i pola. Ich nagłówek syslog zawiera identyfikator procesu i `[timeQuality tzKnown="1"]` tam, gdzie wcześniej był symbol zastępczy `-`. Ich rodzaj jest aliasem trasy:

Rodzaj (pierwsze wydanie)	Transport	Format	Dodany identyfikator zdarzenia
`webhook`	`https`	`json`	`EventId` w każdym rekordzie
`syslog`	`syslog-tls`	`json`	`EventId` w każdym rekordzie
`cef`	`syslog-tls`	`cef-compat`	rozszerzenie `certyxEventId=`
`leef`	`syslog-tls`	`leef-compat`	atrybut `eventId=`
`splunk-hec`	`splunk-hec`	`json`	pole indeksowane `event_id`
`sentinel`	`azure-monitor`	`sentinel`	kolumna `EventId`
`csv-archive`	`file`	`csv-compat`	brak: układ się nie zmienia; `Sequence` razem z identyfikatorem instalacji daje identyfikator zdarzenia

Pola identyfikatora zdarzenia są tylko dodawane: parsery napisane dla pierwszego wydania nadal działają. Aby otrzymywać kanoniczny kod zdarzenia, kategorię i pozostałe pola kanoniczne, wybierz format kanoniczny (`ndjson`, `rfc5424`, `cef`, `leef-1.0`, `leef-2.0`, `kv`, `csv`). Aby archiwum plikowe miało `event_id` w każdym wierszu, użyj kanonicznego `csv` lub archiwum `ndjson`.

3 Szybki start

1. Zaloguj się jako administrator (Admin) organizacji z MFA i otwórz **Eksport do SIEM** (operator: **Dziennik zdarzeń bezpieczeństwa → Eksport do SIEM**).
2. Przygotuj odbiorcę zgodnie z opisem w jego sekcji: Splunk, Cribl, QRadar, ArcSight, Elastic, OCSF, Sentinel lub webhook.
3. Wpisz nazwę i identyfikator miejsca docelowego, wybierz **Transport**, **Format** i **Profil schematu** (zalecane punkty wyjścia: Splunk `splunk-hec` × `ndjson` × `native` lub `splunk-cim`; Cribl `syslog-tls` × `rfc5424` × `native`; QRadar `syslog-tls` × `leef-2.0`; ArcSight `syslog-tls` × `cef`; Elastic `https` × `ndjson` × `ecs`; potoki OCSF `https` lub `file` × `ndjson` × `ocsf`; systemy OpenTelemetry `otlp-http` × `otlp-protobuf`, zob. OpenTelemetry Logs).
4. Wypełnij pola adresu, sekretu i zaufania, opcjonalnie filtry, wartości dostarczania i certyfikat klienta, a następnie zapisz.
5. Wybierz **Sprawdź połączenie**, a następnie **Wyślij zdarzenie testowe**. Wynik podaje `event_id` zdarzenia testowego (UUID); wyszukaj go u odbiorcy.
6. Obserwuj kartę miejsca docelowego: pokazuje pozycję, zdarzenia wciąż oczekujące, dostarczone zdarzenia, ostatni sukces i ostatni błąd.

4 Eksportowane zdarzenia

Eksport odczytuje dziennik bezpieczeństwa CERTYX. Miejsca docelowe i archiwum organizacji otrzymują wyłącznie zdarzenia tej organizacji i nigdy zapisy platformy, także te jej dotyczące: działania i wnioski operatorów, zawieszenie i przywrócenie z powodu rozliczeń, udostępnianie i ponowne szyfrowanie zapisanych sekretów. Organizacja czyta je w swojej konsoli. Logi platformy to osobny eksport ustawiany przez operatora platformy: zdarzenia operatorów (zakres *Operatorzy platformy*) albo wszystkie zdarzenia wszystkich organizacji (zakres *Wszystkie zdarzenia*).

Każde zdarzenie kanoniczne ma **kod zdarzenia** i **kategorię** z katalogu kodów zdarzeń, na przykład `AUTHN-002` (`authentication`, nieudane logowanie) lub `CONFIG-008` (`configuration-change`, zmiana miejsca docelowego SIEM). Kody są stałe i nigdy nie są przenumerowywane. Dziesięć kategorii to `authentication`, `authorization`, `user-management`,

`configuration-change`, `data-access`, `administrative`, `security`, `application-error`, `system` i `integration`.

Wynik (filtr w CERTYX)	Zawartość
Zdarzenia logowania (`authentication`)	Każdy krok logowania jako osobne zdarzenie: `authentication.sign-in.succeeded`, `authentication.sign-in.failed`, `authentication.sign-out`, `authentication.locked`, `authentication.mfa.enrolled`, `authentication.mfa.confirmed`, `authentication.mfa.reset`, `authentication.mfa.recovery-codes-regenerated`
Zmiany biznesowe (`business`)	Zmiany wprowadzone poza żądaniem użytkownika, na przykład zmiany kondycji agenta (`agent.health.changed`), decyzje o automatycznym odnowieniu, zdarzenia inwentaryzacji w tle i kolejki wykonania
Powodzenia (`success`)	Zakończone żądania API, konsoli, platformy i agentów wraz z wprowadzonymi przez nie zmianami biznesowymi (przed/po)
Odebrane żądania (`attempt`)	Rekord zapisywany w chwili nadejścia żądania, przed jego wykonaniem, dzięki czemu żądanie, które nigdy się nie zakończy, i tak pozostawia ślad; nie oznacza nieudanej próby. Wysyłany tylko po zaznaczeniu
Odrzucone żądania (`rejected`)	Żądania odrzucone z HTTP 4xx (innym niż 401/403), na przykład z powodu nieprawidłowych danych wejściowych
Odmowy dostępu (`denied`)	Żądania odrzucone z HTTP 401 lub 403
Błędy serwera (`error`)	Żądania zakończone błędem HTTP 5xx (typ wyjątku i identyfikator śledzenia, nigdy ślad stosu)

Kanoniczne `outcome` normalizuje te wartości do `success`, `failure` lub `unknown`; wynik z dziennika pozostaje dostępny jako `outcome_original`.

Zdarzenia logowania. Obejmują logowanie hasłem, hasłem z kodem MFA lub kodem odzyskiwania, logowanie firmowe przez OIDC lub SAML oraz aplikację mobilną CERTYX. Wylogowania obejmują sesje zakończone przez wygaśnięcie, brak aktywności, zmianę hasła, adresu e-mail lub MFA albo wylogowanie zażądane przez dostawcę tożsamości. Każde zdarzenie zawiera adres e-mail użytkownika, informację, czy ta tożsamość została zweryfikowana, organizację, źródłowy adres IP, agenta użytkownika, metodę, wynik (`success` lub `failure`) i stały kod przyczyny. Podane hasło, kod MFA, kod odzyskiwania ani token nigdy nie są zapisywane.

Pole	Wartości
Metoda	`password`, `password+mfa`, `password+recovery-code`, `oidc`, `saml`, `mobile-password` (także `+mfa`, `+recovery-code`), `mobile-oidc`, `mobile-saml`, `mobile-sso`, `totp` (zmiany MFA)
Wynik	`success`, `failure`
Przyczyna (niepowodzenia)	`unknown-account`, `invalid-credentials`, `disabled`, `locked`, `too-many-failures`, `mfa-required`, `mfa-invalid`, `mfa-enrollment-required`, `enrollment-expired`, `sso-required`, `not-operator`, `operator-entry`, `organization-unavailable`, `organization-mismatch`, `account-not-allowed`, `ticket-invalid`, `device-refused`, `invalid-request`, `sso-error`, `sso-disabled`, `sso-no-subject`, `sso-group-overage`, `sso-not-provisioned`, `sso-no-role`, `sso-expired`, `sso-not-configured`, `sso-unverified-domain`
Przyczyna (wylogowania)	`user`, `credentials-changed`, `idp-logout`, `session-ended`, `administrator-reset`

Nieudane logowanie, którego adres e-mail nie pasuje do żadnego konta, jest przypisywane organizacji, której zweryfikowana domena logowania firmowego pasuje do tego adresu, a w przeciwnym razie platformie; w tym drugim przypadku Twoja organizacja go nie otrzymuje.

Zmiany biznesowe. Zmiany konfiguracji i inwentarza zawierają akcję, zasób oraz wartości przed zmianą i po niej. Zmiana, która pozostawia rekordy bez zmian, np. ponowne zobaczenie przez agenta tego samego certyfikatu na punkcie końcowym (`endpoint.observe`), zawiera akcję i zasób z pustymi wartościami przed i po; rewizja grafu zaufania, która przesuwa tylko czasy ostatniego zobaczenia, nie jest zapisywana jako `trust-graph.updated`. Zmiana kondycji agenta (`agent.health.changed`, wykonawca `system:agent-health`) zawiera agenta, poprzednią i nową przyczynę oraz ważność, wyjaśnienie i kroki naprawcze. Sekrety, klucze prywatne i dane wyjściowe agentów nigdy nie są częścią zdarzenia.

Dwa rekordy na żądanie. Każde żądanie jest zapisywane w dzienniku dwukrotnie: rekord `attempt` przed jego wykonaniem (kod `SYSTEM-000`, dzięki czemu żądanie, które nigdy się nie zakończy, i tak pozostawia ślad) i rekord wyniku (`success`, `rejected`, `denied` lub `error`) po nim, oba z tym samym identyfikatorem korelacji (`correlation_id`, w rekordzie JSON `TraceId`). Miejsce docelowe otrzymuje rekord `attempt` tylko wtedy, gdy w *Wysyłaj tylko* zaznaczono *Odebrane żądania*: gdy

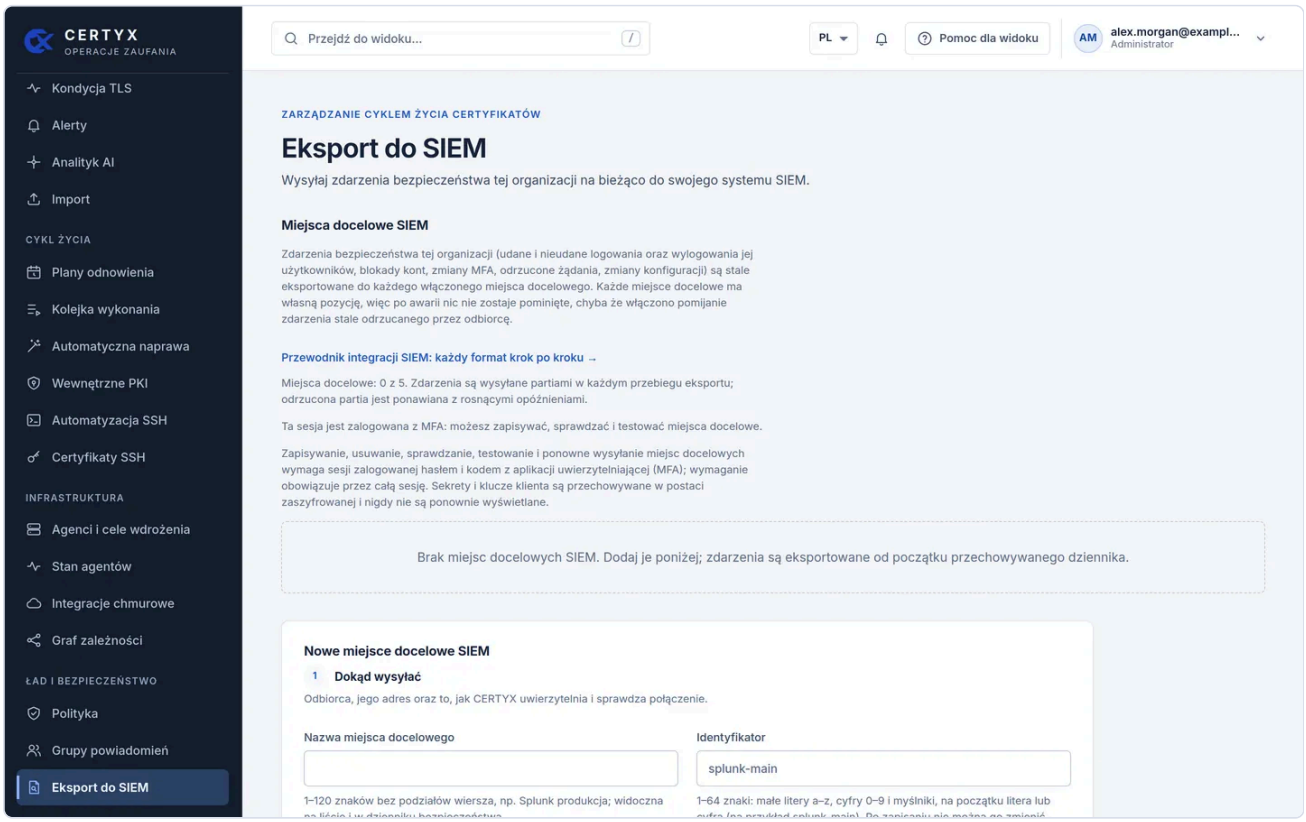
nie zaznaczono żadnego wyniku, dostaje każdy wynik oprócz `attempt`, czyli jeden rekord na żądanie. Zaznacz *Odebrane żądania* razem z pozostałymi wynikami, gdy SIEM ma widzieć żądania, które nigdy się nie kończą; rekord odebranego żądania pozostaje w dzienniku i w archiwum plikowym.

Sondy kondycji. Żądania do `/health/ready` i `/health/live` (sondy gotowości load balancera i kontenerów) są zapisywane w dzienniku — `/health/live` wcale, `/health/ready` z oboma rekordami i `Tenant unattributed` — ale nie są wysyłane do sieciowych miejsc docelowych. Operator może je wysyłać, ustawiając `Clm:Siem:ExportHealthProbes=true`. Archiwum plikowe je zachowuje.

5 Zanim zaczniesz

1. **Rola i MFA.** Zaloguj się jako administrator (Admin) organizacji hasłem i kodem z aplikacji uwierzytelniającej (albo przez logowanie firmowe, jeśli dostawca tożsamości zgłasza MFA). Zapisywanie, sprawdzanie, testowanie, ponowne wysyłanie i usuwanie miejsc docelowych wymaga sesji z MFA; gdy sesja nie spełnia tego warunku, widok dokładnie informuje, co zrobić. Sesje aplikacji mobilnej nie mogą zmieniać miejsc docelowych. Zob. Uprawnienia.
2. **Baza platformy.** Eksport do SIEM odczytuje dziennik z bazy platformy. Gdy instalacja przechowuje dziennik w pliku lokalnym, widok informuje, że eksport jest niedostępny; operator musi skonfigurować bazę platformy.
3. **Ścieżka sieciowa.** Połączenie otwiera serwer CERTYX (a nie Twój komputer). Zezwól na wychodzący ruch TCP z serwera CERTYX do portu odbiorcy i upewnij się, że nazwa hosta odbiorcy jest rozwiązywana w DNS używanym przez serwer CERTYX.
4. **Certyfikat odbiorcy.** Odbiorca potrzebuje certyfikatu serwera TLS, którego nazwy obejmują nazwę hosta wpisaną w CERTYX. Jeśli wystawiło go prywatne lub samopodpisane CA, przygotuj certyfikat główny tego CA (PEM) do pola *Zaufane certyfikaty główne*. Gdy odbiorca wymaga uwierzytelniania klienta, przygotuj certyfikat klienta i jego niezaszyfrowany klucz prywatny PEM (zob. Certyfikat klienta (mTLS)).
5. **Limity.** Każda organizacja może zdefiniować do 5 miejsc docelowych (ustawienie operatora `Clm:Siem:MaxDestinationsPerOrganization`). Operator współdzielonej instalacji może ograniczyć miejsca docelowe organizacji do publicznych adresów IP (`Clm:Siem:AllowPrivateDestinations`); domyślnie odbiorcy wewnętrzni są dozwoleni.

6 Dodawanie miejsca docelowego w CERTYX



Eksport do SIEM: formularz nowego miejsca docelowego i miejsca docelowe organizacji (dane przykładowe)

1. Otwórz **Eksport do SIEM** (operator platformy: **Dziennik zdarzeń bezpieczeństwa** → **Eksport do SIEM**, a następnie wybierz zakres).
2. Wpisz **Nazwa miejsca docelowego** (1–120 znaków, wyświetlana na liście i w dzienniku) oraz **Identyfikator** (1–64 małe litery, cyfry i łączniki, na przykład `splunk-main`; po zapisaniu nie można go zmienić).
3. Wybierz **Transport**, a następnie **Format** i **Profil schematu** spośród opcji dostępnych dla niego (Dozwolone kombinacje). Ramka *Czego potrzebuje strona odbierająca* podsumowuje ustawienia odbiorcy; odnośnik przy każdym polu otwiera odpowiednią sekcję tego przewodnika.
4. Wypełnij pola transportu: adres HTTPS i sekret (webhook, Splunk HEC, Sentinel), host syslog, port i ramkowanie (syslog) albo okres przechowywania i kompresję (archiwum plikowe). Dla `leef-2.0` opcjonalnie **Separator LEEF**.
5. Opcjonalnie: wklej **Zaufane certyfikaty główne** (TLS i zaufane certyfikaty główne), **Certyfikat klienta** z jego kluczem prywatnym (mTLS) i wybierz **Sprawdzanie odwołania** (Unieważnienie).

Formularz ma cztery numerowane sekcje: **1 Dokąd wysyłać** (kroki 2–5), **2 Co wysyłać** (krok 6), **3 Kształt i rozmiar zdarzenia** (krok 6a) i **4 Dostarczanie** (kroki 7–8). Części zaawansowane są zwinięte, dopóki ich nie otworzysz.

1. Opcjonalnie: **Wysyłaj tylko** — wyniki, minimalna ważność, **Wysyłaj tylko (kategorie)** i **Wysyłaj tylko (kody zdarzeń)**; w **Więcej filtrów** trasy do wysyłania lub nigdy niewysyłane, aktorzy, kategorie i kody zdarzeń, których nigdy nie wysyłać (Wysyłaj tylko).

6a. Opcjonalnie: **Kształtowanie zdarzeń** — karta gotowego ustawienia (**Pełne**, **Zrównoważone**, **Oszczędne**, **Własne**) i jej **Ustawienia szczegółowe** (Kształtowanie zdarzeń); **Mapowanie pól** — zmiana nazw, usuwanie, zachowanie lub dodawanie pól (Mapowanie pól); **Podgląd zdarzenia testowego** pokazuje, co wyśle miejsce docelowe i ile bajtów oszczędza kształtowanie. Dla OpenTelemetry: **Treść (Body) rekordu dziennika**, **Nazwa nagłówka uwierzytelniania** i **Kompresuj żądania gzip** (OpenTelemetry Logs).

1. Opcjonalnie: wartości dostarczania — **Próby przed alertem krytycznym**, **Pierwsze opóźnienie ponowienia (sekundy)**, **Najdłuższe opóźnienie ponowienia (sekundy)**, **Rozmiar partii (zdarzenia)**, **Alert zaległości powyżej (zdarzenia)** i **Pomiń zdarzenie, które odbiorca nadal odrzuca po powyższych próbach** (Dostarczanie). Puste pola oznaczają wartości domyślne serwera.
2. Pozostaw zaznaczone **Eksportuj do tego miejsca docelowego** (odznacz, aby wstrzymać miejsce docelowe bez utraty jego pozycji) i wybierz **Zapisz miejsce docelowe**.

3. Wybierz **Sprawdź połączenie**, a następnie **Wyślij zdarzenie testowe** (Sprawdzenie połączenia i zdarzenie testowe).

Nowe miejsce docelowe zaczyna od początku przechowywanego dziennika, więc odbiorca najpierw otrzymuje historię, a potem nowe zdarzenia na bieżąco. Usunięcie miejsca docelowego kasuje jego pozycję; ponowne dodanie zaczyna od początku. Aby ponownie wysłać wybrany okres, użyj **Wyślij ponownie od** (Ponowne wysyłanie).

Przy zmianie formatu podaj ponownie sekret. *Edytuj* wczytuje miejsce docelowe do formularza. Pozostawienie pustego pola sekretu zachowuje zapisany sekret; zmiana transportu wymaga ponownego wpisania sekretu. Sekrety (sekret podpisu HMAC, token HEC, klucz tajny klienta) i klucz prywatny klienta są przechowywane w postaci zaszyfrowanej, nigdy nie są ponownie wyświetlane ani zapisywane w dzienniku. Każda zmiana jest zapisywana w dzienniku jako `siem.destination.*` (kod `CONFIG-008`).

7 TLS i zaufane certyfikaty główne

CERTYX weryfikuje certyfikat odbiorcy przy każdym połączeniu i dla każdego transportu: certyfikat musi być w okresie ważności, musi zawierać wpisany host (nazwę DNS lub adres IP w alternatywnych nazwach podmiotu), musi prowadzić do zaufanego certyfikatu głównego i musi przejść sprawdzanie unieważnienia.

- **Bez zaufanych certyfikatów głównych** decyduje magazyn zaufanych certyfikatów systemu operacyjnego serwera CERTYX. Stosuj tę opcję dla odbiorców z certyfikatem publicznego CA (na przykład Splunk Cloud lub Azure).
- **Z zaufanymi certyfikatami głównymi** zaufane są dokładnie wklejone certyfikaty główne (własny magazyn zaufania): wklej jeden lub więcej bloków PEM (`-----BEGIN CERTIFICATE-----`), najwyżej 64 KiB, bez kluczy prywatnych. Stosuj tę opcję dla wewnętrznego CA lub samopodpisanego certyfikatu odbiorcy.

Weryfikacji nie można wyłączyć.

Aby odczytać łańcuch certyfikatów odbiorcy z komputera w tej samej sieci:

```
openssl s_client -connect siem.example.internal:6514 -servername siem.example.internal -showcerts </dev/null
```

Ostatni wyświetlony certyfikat to zwykle wystawiające CA; jego certyfikat główny należy wkleić.

7.1 Certyfikat klienta (mTLS)

Odbiorcy, którzy uwierzytelniają nadawców certyfikatem (Cribl *Authenticate client*, Logstash `ssl_client_authentication`, syslog-ng `peer-verify(required-trusted)`, serwer pośredniczący przed webhookiem), mogą wymagać, aby CERTYX przedstawił certyfikat klienta. Opcja jest dostępna dla `syslog-tls` i każdego transportu HTTPS (`https`, `splunk-hec`, `azure-monitor`); nie dotyczy archiwów plikowych.

1. Wystaw dla CERTYX certyfikat klienta z CA, któremu ufa odbiorca (użycie klucza *digital signature*, rozszerzone użycie klucza *client authentication*).
2. W formularzu miejsca docelowego wklej **Certyfikat klienta**: jeden certyfikat PEM (`-----BEGIN CERTIFICATE-----`), najwyżej 64 KiB.
3. Wklej jego **klucz prywatny**: niezaszyfrowany klucz PEM (`-----BEGIN PRIVATE KEY-----`, RSA lub EC), najwyżej 64 KiB. Klucz jest tylko do zapisu: jest przechowywany w postaci zaszyfrowanej pierścieniem kluczy Data Protection serwera, nigdy nie jest ponownie wyświetlany ani zapisywany w dzienniku. Przy edycji pozostaw pole puste, aby zachować zapisany klucz.
4. **Sprawdź połączenie** przedstawia certyfikat na etapie TLS.

Certyfikat bez pasującego klucza jest odrzucany przy zapisywaniu. Gdy zapisanego klucza nie można już odszyfrować (zmienił się pierścień kluczy), dostarczanie kończy się błędem *Nie można odczytać certyfikatu klienta ani jego klucza prywatnego; wpisz oba ponownie.*

Miejsca docelowe z konfiguracji używają `ClientCertificatePem` i `ClientKey` (odwołanie `secret:<name>`); zob. `docs/CONFIGURATION.md`.

7.2 Sprawdzanie unieważnienia

CERTYX sprawdza online status unieważnienia każdego certyfikatu z łańcucha odbiorcy poniżej certyfikatu głównego — przez punkty dystrybucji list CRL lub respondera OCSP wskazanego w certyfikatach — czekając najwyżej 10 sekund na każdy adres.

Tryb	Certyfikat unieważniony	Status nieznany (brak adresu CRL/OCSP, responder nieosiągalny)	Zastosowanie
Soft-fail (domyślnie)	odrzucany	akceptowany	Większość odbiorców, także wewnętrzne CA bez opublikowanej listy CRL
Hard-fail	odrzucany	odrzucany	Odbiorcy, których CA publikuje listę CRL lub responder OCSP osiągalny z serwera CERTYX

Aby sprawdzenie dało wynik, serwer CERTYX potrzebuje wychodzącego dostępu HTTP do adresów CRL i OCSP. Odrzucony certyfikat powoduje niepowodzenie etapu TLS sprawdzenia z kodem `tls-untrusted` (lub `tls-untrusted-roots` przy wklejonych certyfikatach głównych).

8 Podpisany webhook HTTPS

CERTYX wysyła żądania `POST` na Twój adres HTTPS. W formacie `json` treścią jest tablica JSON rekordów dziennika (`Content-Type: application/json`); w formacie `ndjson` treścią jest jeden dokument wybranego profilu na wiersz (`Content-Type: application/x-ndjson`, każdy wiersz zakończony znakiem LF). Żądanie zawiera najwyżej tyle zdarzeń, ile wynosi rozmiar paczki miejsca docelowego (domyślnie 200). Nagłówek `X-Certyx-Signature` zawiera `sha256=`, a po nim zapisany szesnastkowo małymi literami HMAC-SHA256 dokładnych bajtów treści, obliczony z kluczem w postaci sekretu podpisu. Każda odpowiedź HTTP 2xx oznacza przyjęcie paczki. HTTP 400, 413 lub 422 jest traktowane jako odrzucenie danych (Odrzucone zdarzenia); każda inna odpowiedź, przekroczenie czasu (domyślnie 20 sekund) lub błąd TLS powoduje, że CERTYX wyśle te same zdarzenia ponownie po upływie opóźnienia ponowienia (Dostarczanie).

8.1 Strona odbiorcy

1. Udostępnij punkt końcowy HTTPS, na przykład `https://siem.example.com/certyx`, z certyfikatem dla tej nazwy hosta.
2. Odczytaj surową treść żądania przed jej parsowaniem, oblicz HMAC-SHA256 z sekretem podpisu jako kluczem (ciąg sekretu zakodowany w UTF-8, użyty bez zmian — nie dekoduj tekstu szesnastkowego) i porównaj `sha256=<hex>` z `X-Certyx-Signature` w stałym czasie. W razie niezgodności odrzuć żądanie z kodem 401.
3. Sparsuj treść zgodnie z jej typem zawartości: tablica JSON (`application/json`) albo jeden dokument JSON na wiersz (`application/x-ndjson`).
4. Zapisz zdarzenia, a następnie odpowiedz kodem 2xx. Odpowiadaj 2xx dopiero wtedy, gdy paczka jest bezpiecznie zapisana.
5. Usuwaj duplikaty według identyfikatora zdarzenia: `EventId` w rekordzie JSON, `event_id` (native), `event.id` (ECS) lub `metadata.uid` (OCSF). Dostarczanie jest co najmniej jednokrotne, więc po przekroczeniu czasu ta sama paczka może dotrzeć dwukrotnie.
6. Przyjmuj zdarzenie testowe: jego identyfikator zdarzenia to UUID; rekord JSON: `Sequence` 0, `Actor` `siem-test`, `Method` `INTERNAL`, `Route` `business/siem.test`; zdarzenie kanoniczne: `event_code` `INTEGRATION-001`, `category` `integration`, `action` `siem.test`, `user_id` `siem-test`.

8.2 Weryfikacja podpisu

Python (biblioteka standardowa):

```
import hashlib, hmac, json, os
from http.server import BaseHTTPRequestHandler, HTTPServer

SECRET = os.environ["CERTYX_SIGNING_SECRET"].encode("utf-8")

def events(body, content_type):
```

```
    if content_type.startswith("application/x-ndjson"):
        return [json.loads(line) for line in body.decode("utf-8").splitlines() if line]
    return json.loads(body)

class CertyxReceiver(BaseHTTPRequestHandler):
    def do_POST(self):
        body = self.rfile.read(int(self.headers.get("Content-Length", "0")))
        expected = "sha256=" + hmac.new(SECRET, body, hashlib.sha256).hexdigest()
        if not hmac.compare_digest(expected, self.headers.get("X-Certyx-Signature", "")):
            self.send_response(401)
            self.end_headers()
            return
        for event in events(body, self.headers.get("Content-Type", "")):
            store(event)  # your storage; deduplicate by the event ID
        self.send_response(204)
        self.end_headers()

# Run behind a TLS-terminating reverse proxy, or wrap the socket with ssl.SSLContext.
HTTPServer(("0.0.0.0", 8080), CertyxReceiver).serve_forever()
```

Node.js (Express):

```
import crypto from 'node:crypto';
import express from 'express';

const secret = process.env.CERTYX_SIGNING_SECRET;
const app = express();

app.post('/certyx', express.raw({ type: ['application/json', 'application/x-ndjson'], limit: '20mb' }), (req, res) => {
  const expected = 'sha256=' + crypto.createHmac('sha256', secret).update(req.body).digest('hex');
  const given = req.get('X-Certyx-Signature') ?? '';
  const valid = given.length === expected.length && crypto.timingSafeEqual(Buffer.from(given), Buffer.from(expected));
  if (!valid) return res.sendStatus(401);
  const text = req.body.toString('utf8');
  const events = req.is('application/x-ndjson')
    ? text.split('\n').filter(Boolean).map(line => JSON.parse(line))
    : JSON.parse(text);
  for (const event of events) store(event); // deduplicate by the event ID
  res.sendStatus(204);
});
```

C# (minimalne API ASP.NET Core):

```
app.MapPost("/certyx", async (HttpRequest request) =>
{
    using var buffer = new MemoryStream();
    await request.Body.CopyToAsync(buffer);
    var body = buffer.ToArray();
    var key = Encoding.UTF8.GetBytes(Environment.GetEnvironmentVariable("CERTYX_SIGNING_SECRET")!);
    var expected = "sha256=" + Convert.ToHexString(HMACSHA256.HashData(key, body)).ToLowerInvariant();
    var given = request.Headers["X-Certyx-Signature"].ToString();
    if (!CryptographicOperations.FixedTimeEquals(Encoding.ASCII.GetBytes(expected), Encoding.ASCII.GetBytes(given)))
        return Results.Unauthorized();
    var text = Encoding.UTF8.GetString(body);
    var documents = request.ContentType?.StartsWith("application/x-ndjson") == true
        ? text.Split('\n', StringSplitOptions.RemoveEmptyEntries).Select(line => JsonDocument.Parse(line).RootElement)
```

```
        : JsonDocument.Parse(text).RootElement.EnumerateArray();
    foreach (var e in documents)
        Store(e); // deduplicate by the event ID
    return Results.NoContent();
});
```

Sprawdzenie przechwyconej treści w wierszu poleceń (`body.json` zapisany bajt w bajt):

```
printf 'sha256=%s\n' "$(openssl dgst -sha256 -hmac "$CERTYX_SIGNING_SECRET" -r body.json | cut -d' ' -f1)"
```

8.3 Strona CERTYX

1. Transport **Podpisany webhook HTTPS** (`https`); format `ndjson` z profilem `native` , `ecs` lub `ocsf` albo format `json` (rekord z pierwszego wydania).
2. **Adres HTTPS**: bezwzględny adres URL `https://` punktu końcowego (najwyżej 2048 znaków, bez nazwy użytkownika i hasła), na przykład `https://siem.example.com/certyx` .
3. **Sekret podpisu HMAC**: dla nowego webhooka pozostaw puste. CERTYX wygeneruje wtedy 64-znakowy sekret i po zapisaniu pokaże go jednokrotnie — skopiuj go do odbiorcy, zanim zamkniesz komunikat. Możesz też wpisać własny sekret (najwyżej 1024 znaki).
4. **Nowy sekret** na karcie miejsca docelowego natychmiast zastępuje sekret i jednokrotnie pokazuje nowy; poprzedni sekret przestaje działać przy następnym dostarczeniu, więc jednocześnie zaktualizuj odbiorcę.
5. Opcjonalnie: certyfikat klienta, gdy punkt końcowy wymaga mTLS.
6. Zapisz, **Sprawdź połączenie**, **Wyślij zdarzenie testowe**.

Oznaki powodzenia: sprawdzenie pokazuje DNS, TCP i TLS jako poprawne; wynik zdarzenia testowego informuje, że miejsce docelowe je przyjęło, i podaje jego identyfikator zdarzenia; odbiorca zarejestrował jedno zdarzenie z tym identyfikatorem. W ciągu następnego przebiegu karta pokazuje *ostatni sukces* i liczbę dostarczonych zdarzeń.

9 Splunk HTTP Event Collector

Zalecana droga do Splunk: każda paczka jest potwierdzana przez Splunk, a przy włączonym potwierdzaniu indeksowania (indexer acknowledgement) CERTYX czeka, aż zdarzenia zostaną zaindeksowane.

9.1 Wybór ścieżki do Splunk

Cel	Transport × format × profil	Sourcetype (domyślny)
Zdarzenia kanoniczne, wyszukiwalne według `event_id` , `event_code` , `category` bez parsowania	`splunk-hec` × `ndjson` × `native`	`certyx:event`
Modele danych Splunk CIM (Authentication, Change)	`splunk-hec` × `ndjson` × `splunk-cim`	`certyx:event`
Dokumenty ECS lub OCSF w Splunk	`splunk-hec` × `ndjson` × `ecs` / `ocsf`	`certyx:event`
Istniejące wyszukiwania oparte na rekordzie z pierwszego wydania	`splunk-hec` × `json` × `native`	`certyx:security`
Brak HEC, syslog bezpośrednio do indeksera	`syslog-tls` , ramkowanie nową linią (Wejście TCP-SSL Splunk)	ustawiany przez wejście

Gdy kilka miejsc docelowych CERTYX zapisuje do tego samego indeksu, używaj osobnego sourcetype dla każdego profilu (na przykład `certyx:event` , `certyx:event:cim` , `certyx:event:ecs`), aby `props.conf` mógł traktować każdy z nich oddzielnie.

9.2 Strona odbiorcy (Splunk)

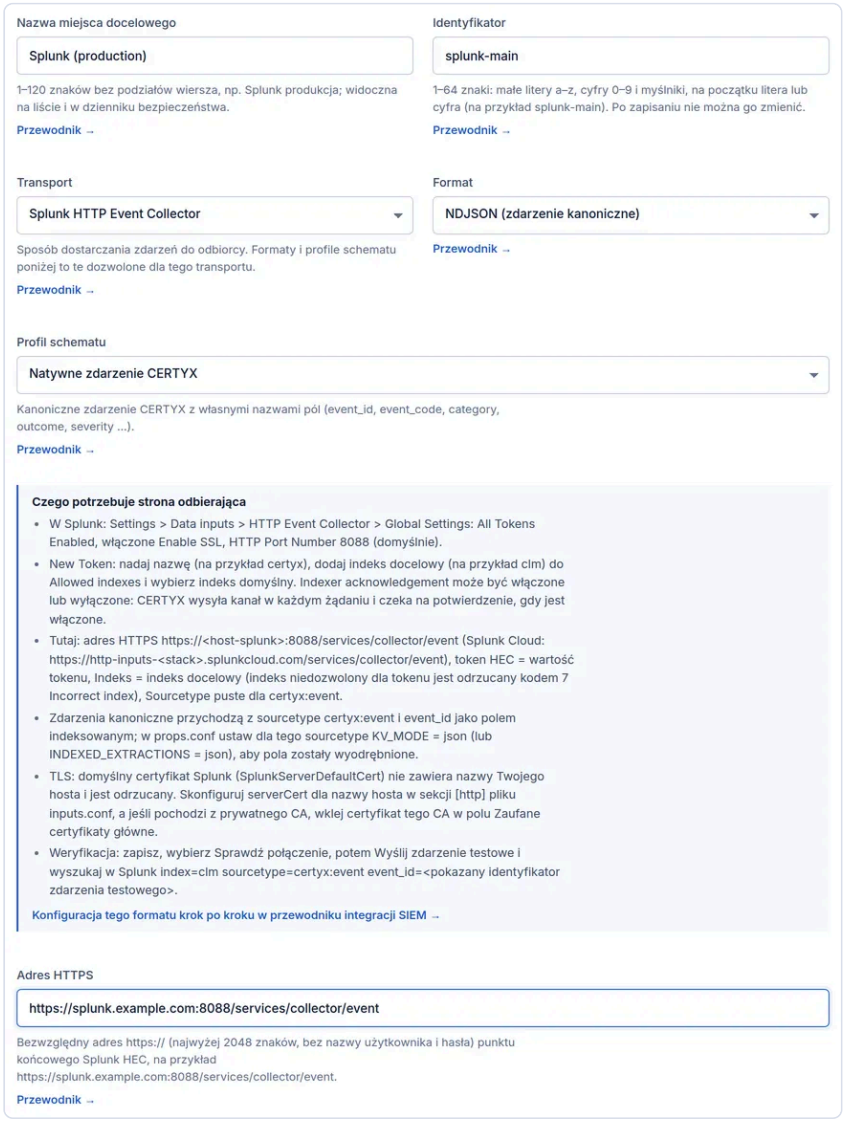
1. **Włącz HEC.** *Settings* → *Data inputs* → *HTTP Event Collector* → *Global Settings*: *All Tokens* **Enabled**, zaznaczone **Enable SSL**, *HTTP Port Number* 8088 (domyślnie). Zapisz.
2. **Utwórz indeks** (w razie potrzeby): *Settings* → *Indexes* → *New Index*, na przykład `clm`.
3. **Utwórz token.** *HTTP Event Collector* → *New Token*: nazwa `certyx`; pozostaw puste *Source name override*; *Input Settings*: opcjonalny domyślny *Source type* (CERTYX i tak ustawia sourcetype dla każdego zdarzenia), *Allowed Indexes* zawiera `clm`, *Default Index* `clm`. *Enable indexer acknowledgement* może być włączone lub wyłączone — CERTYX obsługuje oba warianty. Skopiuj **Token Value**.
4. **Certyfikat serwera.** Domyślny certyfikat Splunk (`SplunkServerDefaultCert`) nie zawiera nazwy Twojego hosta i jest odrzucany przez CERTYX. Skonfiguruj certyfikat dla nazwy hosta w sekcji `[http]` pliku `inputs.conf` (na przykład `$SPLUNK_HOME/etc/apps/splunk_httpinput/local/inputs.conf`) i uruchom ponownie Splunk:

```
[http]
disabled = 0
enableSSL = 1
port = 8088
serverCert = $SPLUNK_HOME/etc/auth/certyx/splunk-hec.pem
sslPassword = <password of the private key in the PEM file>
```

1. **Splunk Cloud.** Użyj `https://http-inputs-<stack>.splunkcloud.com/services/collector/event` (port 443). Jego certyfikat pochodzi od publicznego CA; zaufane certyfikaty główne nie są potrzebne.
2. **Zapora.** Zezwól na TCP 8088 (Splunk Cloud: 443) z serwera CERTYX.
3. **Ustawienia sourcetype** jak w sekcji props.conf.

Z komputera w tej samej sieci możesz potwierdzić, że HEC odpowiada: `curl https://splunk.example.com:8088/services/collector/health` zwraca `{"text":"HEC is healthy","code":17}`.

9.3 Strona CERTYX



Dodawanie miejsca docelowego Splunk HTTP Event Collector: nazwa, identyfikator, transport i adres kolektora (dane przykładowe)

1. Transport **Splunk HTTP Event Collector** (`splunk-hec`), format i profil wybrane zgodnie z powyższą tabelą.
2. **Adres HTTPS**: `https://<splunk-host>:8088/services/collector/event` — punkt końcowy `/event` , nie `/raw` .
3. **Token HEC**: wartość Token Value ze Splunk (`<HEC token>`).
4. **Indeks (opcjonalnie)**: indeks docelowy, na przykład `clm` . Musi należeć do indeksów dozwolonych dla tokenu (w przeciwnym razie Splunk odrzuca zdarzenie z kodem 7 *Incorrect index*); puste pole oznacza domyślny indeks tokenu.
5. **Sourcetype (opcjonalnie)**: puste pole oznacza `certyx:event` dla `ndjson` (ustawienie operatora `Clm:Siem:SplunkEventSourceType`) i `certyx:security` dla `json` (`Clm:Siem:SplunkSourceType`).
6. **Zaufane certyfikaty główne**: wklej CA, które wystawiło certyfikat HEC, jeśli jest to prywatne CA.
7. Zapisz, **Sprawdź połączenie**, **Wyślij zdarzenie testowe**.

Co wysyła CERTYX. `POST` z `Authorization: Splunk <HEC token>` , `X-Splunk-Request-Channel: <GUID>` (stały dla danego miejsca docelowego; wymagany przez tokeny z potwierdzaniem indeksowania, ignorowany przez pozostałe) i jedną kopertą na zdarzenie, połączonymi ze sobą. Każda koperta zawiera:

- `time` — czas zdarzenia, sekundy epoki z milisekundami;
- `host` — instancję CERTYX, która zapisała zdarzenie;
- `source` — `certyx:security-journal` ;
- `sourcetype` — zgodnie z konfiguracją; `index` — tylko gdy jest ustawiony;

- `event` — format `json`: rekord JSON (Rekord JSON); format `ndjson`: zdarzenie kanoniczne (`native`, `splunk-cim`), dokument ECS (`ecs`) lub dokument OCSF (`ocsf`);
- `fields` (pola indeksowane) — format `json`: `event_id`; format `ndjson`: zawsze `event_id`, `event_code` i `category`, a przy `splunk-cim` dodatkowo pola CIM (CIM).

Gdy odpowiedź zawiera `ackId`, CERTYX co sekundę odpytuje `/services/collector/ack`, aż Splunk potwierdzi indeksowanie, najdłużej przez 30 sekund (ustawienia operatora `Clm:Siem:HecAckPollInterval`, `Clm:Siem:HecAckTimeout`); niepotwierdzona paczka jest wysyłana ponownie. Kody HEC 5, 6, 12, 13 i 15 są traktowane jako odrzucenie danych (Odrzucone zdarzenia). Przykłady: Przykładowe zdarzenia.

Oznaki powodzenia: *Splunk HEC przyjął zdarzenie testowe (kod 0).* wraz z indeksem, sourcetype i identyfikatorem zdarzenia. Następnie wyszukaj:

```
index=clm event_id=<event ID shown by the test>
index=clm sourcetype=certyx:event category=authentication outcome=failure
| stats count by username, src_ip, reason
index=clm sourcetype=certyx:security Outcome=authentication SignIn.Result=failure
| stats count by SignIn.User, SourceIp, SignIn.Reason
```

9.4 props.conf

Zdarzenia z punktu końcowego `/event` biorą czas z pola `time` koperty; `TIME_PREFIX`, `TIME_FORMAT` i `TIMESTAMP_FIELDS` nie są potrzebne. Długie zdarzenia (wiele zmian, znaki narodowe) wymagają wartości `TRUNCATE` większej niż domyślne w Splunk 10 000 bajtów. Na search headach i indekserach (albo w Splunk Cloud przez własną aplikację):

```
[certyx:event]
KV_MODE = json
TRUNCATE = 0
SHOULD_LINEMERGE = false

[certyx:security]
KV_MODE = json
TRUNCATE = 0
SHOULD_LINEMERGE = false
```

`TRUNCATE = 0` usuwa limit; jeśli Twoje zasady wymagają limitu, ustaw dużą wartość (na przykład `200000`). Pola indeksowane (`event_id`, `event_code`, `category`) można też wyszukiwać szybką składnią `field::value`, na przykład `event_code::AUTHN-002`. Pole, które jest zarazem indeksowane i obecne w zdarzeniu JSON, może pokazywać swoją wartość dwukrotnie; użyj `| eval event_id=mvindex(event_id,0)` albo wyszukuj w postaci indeksowanej.

9.5 Splunk CIM

Przy profilu `splunk-cim` CERTYX zapisuje pola CIM każdego zdarzenia jako pola indeksowane: pola wspólne `vendor_product` (`CERTYX CLM`), `app` (`clm`), `signature` (komunikat), `signature_id` (kod zdarzenia), `severity` (informational, low, medium, high, critical), `severity_id`, `src`, `src_port`, `dest`, `user`, `user_id`, `session_id`; dla modelu danych Authentication (kategoria `authentication`) `action` (`success`, `failure`, `unknown`), `authentication_method`, `reason`; dla modelu danych Change (kategorie `user-management`, `configuration-change` oraz `administrative` z typem zmiany) `action` (`created`, `modified`, `deleted`), `change_type` (`AAA` dla zarządzania użytkownikami, w pozostałych przypadkach `application`), `object`, `object_category`, `object_id`, `command`, `status`, `result`; dla pozostałych zdarzeń `action` = akcja kanoniczna.

Zdarzenie kanoniczne w `event` używa niektórych z tych samych nazw (`action`, `severity`, `reason`, `user_id`). Dla sourcetype CIM nie pozwól, aby wyodrębnianie JSON podczas wyszukiwania nadpisywało wartości CIM, a pola kanoniczne w razie potrzeby odczytuj poleceniem `spath`:

```
[certyx:event:cim]
KV_MODE = none
```

```
TRUNCATE = 0
SHOULD_LINEMERGE = false
```

CERTYX nie dostarcza dodatku (add-on) Splunk: typy zdarzeń i tagi, które przypisują zdarzenia do modeli danych CIM, nie są dołączone. Utwórz je we własnej aplikacji, na przykład:

```
# eventtypes.conf
[certyx_authentication]
search = sourcetype=certyx:event:cim category::authentication

[certyx_change]
search = sourcetype=certyx:event:cim (category::user-management OR category::configuration-change OR category::administrative)

# tags.conf
[eventtype=certyx_authentication]
authentication = enabled

[eventtype=certyx_change]
change = enabled
```

Następnie sprawdź wynik poleceniem `| datamodel Authentication search | search sourcetype=certyx:event:cim`.

10 Syslog przez TLS

Wszystkie formaty syslog korzystają ze wspólnego transportu. CERTYX otwiera połączenie TLS z hostem i portem (przedstawiając certyfikat klienta, jeśli został ustawiony), zapisuje paczkę i zamyka połączenie. Syslog nie ma potwierdzenia dostarczenia: zakończony zapis TLS oznacza przyjęcie.

Formaty kanoniczne (`rfc5424`, `cef`, `leef-1.0`, `leef-2.0`, `kv`) to komunikaty RFC 5424 z opisanym poniżej nagłówkiem; MSG jest wierszem danego formatu. **Formaty z pierwszego wydania** (`json`, `cef-compat`, `leef-compat`) zachowują układ nagłówka: `<86>` (informational) lub `<84>` (warning), APP-NAME `clm`, MSGID to kategoria zdarzenia (na przykład `authentication`; przed 1.2.19 `security-journal`), bez danych strukturalnych. Każde miejsce docelowe syslog może w kształtowaniu zdarzeń wybrać własny MSGID (kategoria, kod zdarzenia, własny tekst, np. `security-journal`, albo brak) i APP-NAME; odbiorca filtruje wtedy po kategorii bez czytania wiadomości, na przykład `msgid=authentication` w Splunku.

10.1 Nagłówek RFC 5424 formatów kanonicznych

`<PRI>1 TIMESTAMP HOSTNAME APP-NAME PROCID MSGID STRUCTURED-DATA MSG`

- **PRI** = facility × 8 + ważność syslog. Facility z `Clm:Siem:Syslog:Facility` (domyślnie 10, authpriv; zwykłą alternatywą jest 16, local0). Ważność syslog wynika z ważności kanonicznej: 0–3 → 6 informational, 4–5 → 5 notice, 6–7 → 4 warning, 8 → 3 error, 9 → 2 critical, 10 → 1 alert.
- **VERSION** `1`; **TIMESTAMP** w UTC z milisekundami (`2026-10-18T08:15:02.417Z`).
- **HOSTNAME** to instancja CERTYX, która zapisała zdarzenie; **APP-NAME** `Clm:Siem:Syslog:AppName` (domyślnie `clm`); **PROCID** to identyfikator procesu instancji CERTYX; **MSGID** to kategoria zdarzenia (na przykład `authentication`) albo to, co wybiera kształtowanie zdarzeń miejsca docelowego (kod zdarzenia, własny tekst lub brak); miejsce docelowe może też ustawić własny APP-NAME. Wartości nagłówka są drukowalnymi znakami US-ASCII; pozostałe znaki są zamieniane na `_`.
- **STRUCTURED-DATA** zawsze `[timeQuality tzKnown="1"]` i `[origin software="CERTYX CLM" swVersion="<version>" ip="<server address>"]` (`ip` tylko wtedy, gdy jest znany). Gdy operator skonfiguruje numer IANA Private Enterprise Number (`Clm:Siem:Syslog:IanaPrivateEnterpriseNumber`), dodatkowo `[certyx@<PEN> eventId="…" eventCode="…" category="…" outcome="…" schemaVersion="…" organizationId="…"]` oraz `enterpriseId` w `origin`. CERTYX nie ma własnego zarejestrowanego numeru przedsiębiorstwa; SD-ID z `@` musi używać zarejestrowanego numeru, więc bez skonfigurowanego numeru element prywatny nie jest wysyłany. Numer 32473 (numer dokumentacyjny z RFC 5612) jest odrzucany. W wartościach znaki `"`, `\` i `]` są poprzedzane ukośnikiem odwrotnym.

- **MSG** — `rfc5424`: dokument JSON profilu (`native`, `ecs` lub `ocsf`) poprzedzony znacznikiem kolejności bajtów UTF-8, chyba że ustawiono `Clm:Siem:Syslog:ByteOrderMark=false`; `cef`, `leef-1.0`, `leef-2.0`, `kv`: wiersz danego formatu, bez znacznika kolejności bajtów.

Gdy odbiorca pokazuje `` lub `ï»¿` przed JSON, poproś operatora o ustawienie `Clm:Siem:Syslog:ByteOrderMark=false`.

10.2 Ramkowanie

Ramkowanie informuje odbiorcę, gdzie kończy się komunikat; musi być zgodne z wejściem odbierającym.

Ramkowanie w CERTYX	W transmisji	Zastosowanie
Zliczanie oktetów (RFC 5425) — domyślne	`<length> <message>`	Źródło syslog w Cribl Stream z *Octet count framing* Yes, syslog-ng, rsyslog, IBM QRadar, ArcSight
Nowa linia (RFC 6587, wejście TCP Splunk)	`<message>`, a po nim znak nowego wiersza; znaki nowego wiersza wewnątrz komunikatu są zapisywane jako `\n`	Wejście Splunk `[tcp-ssl:<port>]`, Logstash `tcp` z kodekiem `line`, wejście TCP Elastic Agent

Przy zliczaniu oktetów `<length>` to liczba bajtów UTF-8 komunikatu (nie znaków), a po niej jedna spacja; przed komunikatem ani po nim nie ma znaku nowego wiersza. CERTYX zapisuje każdy rekord — prefiks długości i komunikat razem — jedną operacją zapisu, więc rekord do 16 KiB jest przesyłany w jednym rekordzie TLS. Obie strony muszą używać tego samego ramkowania: odbiorca, który dzieli strumień na znakach nowego wiersza, podczas gdy CERTYX zlicza oktety, pokazuje długość następnego rekordu doklejoną do końca poprzedniego (`… }412`), rekordy zaczynające się od długości (`412 <84>1 …`) i rekordy ucięte w połowie. Zob. Rozwiązywanie problemów.

10.3 Strona CERTYX (wszystkie formaty syslog)

1. Transport **Syslog przez TLS** (`syslog-tls`), format zgodny z wymaganiami odbiorcy (`rfc5424`, `cef`, `leef-1.0`, `leef-2.0`, `kv` albo format z pierwszego wydania).
2. **Host syslog**: wyłącznie nazwa DNS lub adres IP — bez `https://` i bez `:port` (na przykład `cribl-worker1.example.internal`). Nazwa musi być rozwiązywana na serwerze CERTYX i musi występować w certyfikacie odbiorcy.
3. **Port**: port TLS wejścia odbierającego (na przykład 6514 lub 10514).
4. **Ramkowanie (framing)**: zgodnie z tabelą powyżej.
5. **Separator LEEF** (tylko `leef-2.0`): jeden znak lub jego kod szesnastkowy (`x09`, `0x5E`); puste pole oznacza tabulator. Dozwolone są tabulator i drukowalne znaki interpunkcyjne ASCII z wyjątkiem `=`, kreski pionowej i ukośnika odwrotnego.
6. **Zaufane certyfikaty główne**: CA certyfikatu odbiorcy, jeśli jest to prywatne CA; opcjonalnie certyfikat klienta.
7. Zapisz, **Sprawdź połączenie**, **Wyślij zdarzenie testowe**.

Oznaki powodzenia: *Zdarzenie testowe zapisane przez TLS (octet-counting).* wraz z identyfikatorem zdarzenia. Syslog nie ma potwierdzenia dostarczenia, więc potwierdza to DNS, TCP, TLS i zapis. Sprawdź u odbiorcy, czy zdarzenie z tym identyfikatorem trafiło do oczekiwanego indeksu lub tabeli.

10.4 Ogólny odbiorca syslog (rsyslog, syslog-ng)

rsyslog z nasłuchem TLS na porcie 6514 (zliczanie oktetów jest rozpoznawane automatycznie):

```
global(DefaultNetstreamDriver="gtls"
       DefaultNetstreamDriverCAFile="/etc/rsyslog.d/tls/ca.pem"
       DefaultNetstreamDriverCertFile="/etc/rsyslog.d/tls/siem.example.internal.pem"
       DefaultNetstreamDriverKeyFile="/etc/rsyslog.d/tls/siem.example.internal.key")
module(load="imtcp" StreamDriver.Name="gtls" StreamDriver.Mode="1" StreamDriver.AuthMode="anon")
input(type="imtcp" port="6514" ruleset="certyx")
ruleset(name="certyx") { action(type="omfile" file="/var/log/certyx/security.log") }
```

Aby wymagać certyfikatu klienta CERTYX, użyj `StreamDriver.AuthMode="x509/certvalid"` z wystawiającym CA w `DefaultNetstreamDriverCAFile`.

syslog-ng:

```
source s_certyx {
  syslog(transport("tls") port(6514)
         tls(key-file("/etc/syslog-ng/tls/siem.key") cert-file("/etc/syslog-ng/tls/siem.pem") peer-verify(optional-
untrusted)));
};
destination d_certyx { file("/var/log/certyx/security.log"); };
log { source(s_certyx); destination(d_certyx); };
```

Z certyfikatem klienta CERTYX użyj `peer-verify(required-trusted)` oraz `ca-dir()` lub `ca-file()` z wystawiającym CA. JSON w MSG można sparsować parserem JSON odbiorcy (rsyslog `mmjsonparse` w konfiguracji bez cookie, syslog-ng `json-parser()`); dane strukturalne są dostępne jako pola SDATA odbiorcy.

11 Cribl Stream

Cribl odbiera zdarzenia, parsuje je i przekazuje do Splunk lub innego miejsca docelowego. Cribl nie wybiera samodzielnie indeksu Splunk; ustaw go w trasie lub potoku.

11.1 Wybór źródła Cribl

Źródło Cribl	Transport × format CERTYX	Uwagi
Syslog (TCP z TLS)	`syslog-tls` × `rfc5424` (profil `native`, `ecs` lub `ocsf`) albo `cef`, `leef-2.0`, `kv`	Ramkowanie musi się zgadzać: zliczanie oktetów w CERTYX ↔ *Octet count framing* **Yes** w Cribl
Splunk HEC	`splunk-hec` × `ndjson`	Cribl odpowiada tak jak Splunk; CERTYX wysyła do `https://<worker>:8088/services/collector/event`
HTTP (raw)	`https` × `ndjson`	Cribl nie weryfikuje podpisu HMAC; uwierzytelniaj CERTYX certyfikatem klienta (mTLS)

11.2 Strona odbiorcy (źródło syslog Cribl)

1. **Certyfikat.** *Group Settings* → *Security* → *Certificates* → *Add certificate*: prześlij certyfikat (z łańcuchem) i klucz prywatny dla nazwy hosta workera, na przykład `cribl-worker1.example.internal`. Musi to być nazwa, którą wpisujesz w CERTYX jako host syslog.
2. **Jedno źródło na port CERTYX.** *Data* → *Sources* → *Syslog* → *Add Source*: Input ID `certyx_tls`, Address `0.0.0.0`, *TCP Port* `10514`, *UDP Port* puste. Nie współdziel tego portu z innymi nadawcami, którzy używają innego ramkowania lub nie używają TLS: ramkowanie i TLS dotyczą każdego połączenia źródła.
3. **TLS.** W ustawieniach źródła *TLS Settings (TCP Only)*: **Enabled** Yes, *Certificate name* — certyfikat z kroku 1. *Authenticate client (mutual auth)*: Yes, gdy CERTYX przedstawia certyfikat klienta (mTLS) — wtedy dodaj wystawiające go CA jako *CA certificate* — w przeciwnym razie No. Przy wyłączonym TLS Cribl indeksuje uzgadnianie TLS wykonywane przez CERTYX jako zdarzenia (dane binarne zaczynające się od `\x16\x03`, zawierające nazwę serwera).
4. **Ramkowanie.** W *Advanced Settings* źródła: **Octet count framing** Yes (ramkowanie CERTYX *Zliczanie oktetów (RFC 5425)*). Możesz też pozostawić No i wybrać w CERTYX ramkowanie *Nowa linia* — ale nigdy nie mieszaj obu wariantów.
5. **Przetwarzanie.** Potok na źródle lub trasie z: - *Parser* (typ JSON object) na polu `message` dla `rfc5424` i `json` z pierwszego wydania; dla CEF i LEEF — parser z Twojego pakietu Cribl; dla `kv` — *Parser* typu *Key=Value pairs*; - *Eval* z polami `index` = `'clm'` i `sourcetype` = `'certyx:syslog'` (miejsce docelowe Splunk w Cribl używa tych pól; bez nich zdarzenia trafiają do domyślnego indeksu miejsca docelowego).
6. **Trasa.** *Routing* → *Data Routes* → *Add Route*: Filter `__inputId=='syslog:certyx_tls:tcp'`, Pipeline jak w kroku 5, Output — Twoje miejsce docelowe Splunk. Umieść trasę nad trasami przechwytującymi cały ruch (catch-all).
7. **Zatwierdź i wdróż** (commit and deploy) konfigurację w grupie workerów oraz zezwól na TCP 10514 z serwera CERTYX do workerów.

11.3 Strona odbiorcy (źródło Splunk HEC w Cribl)

1. *Data* → *Sources* → *Splunk HEC* → *Add Source*: Input ID `certyx_hec`, Port `8088`, HEC endpoint `/services/collector`.
2. *Auth tokens*: dodaj token (`<HEC token>`) i opcjonalnie pola `index` i `sourcetype`, które mają być dodawane do jego zdarzeń.
3. *TLS Settings*: Enabled Yes, certyfikat workera; uwierzytelnianie wzajemne tak jak dla źródła syslog.
4. W CERTYX: transport `splunk-hec`, format `ndjson`, adres HTTPS `https://cribl-worker1.example.internal:8088/services/collector/event`, token oraz indeks, jeśli Twoja trasa Cribl go przekazuje.

11.4 Strona CERTYX

Host syslog `cribl-worker1.example.internal` (albo nazwa load balancera przed workerami, która musi występować w certyfikacie), Port `10514`, Ramkowanie **Zliczanie oktetów (RFC 5425)** (lub **Nowa linia**, gdy źródło Cribl ma *Octet count framing* No), Zaufane certyfikaty główne, jeśli certyfikat Cribl pochodzi z prywatnego CA. Następnie **Sprawdź połączenie** i **Wyślij zdarzenie testowe**, a w Cribl użyj *Live Data* na źródle, aby zobaczyć zdarzenie z identyfikatorem zdarzenia testowego.

Oznaki powodzenia: zdarzenie testowe pojawia się w podglądzie na żywo źródła w Cribl jako jedno zdarzenie, którego `message` zaczyna się od dokumentu JSON (dla `rfc5424`) lub wiersza CEF/LEEF/KV — bez długości na początku, bez danych binarnych — z `appname` `clm` i kategorią jako `msgid`; a następnie w Splunk w indeksie ustawionym przez trasę. Jeśli jest w Cribl, ale nie ma go w indeksie, sprawdź filtr trasy i pole `index`. Fragmenty lub zdarzenia binarne: zob. Odbiorca pokazuje fragmenty lub dane binarne.

12 Wejście TCP-SSL Splunk

Stosuj tę opcję, gdy strumień syslog ma trafiać bezpośrednio do indeksera Splunk lub heavy forwardera bez HEC. Splunk dzieli strumień TCP na końcach wierszy, więc CERTYX musi używać ramkowania **Nowa linia**.

12.1 Strona odbiorcy (Splunk)

1. Utwórz indeks (na przykład `clm`).
2. Zainstaluj certyfikat dla nazwy hosta i skonfiguruj wejście w `inputs.conf` (na przykład `$SPLUNK_HOME/etc/system/local/inputs.conf`):

```
[tcp-ssl:6514]
index = clm
sourcetype = certyx:syslog
disabled = 0

[SSL]
serverCert = $SPLUNK_HOME/etc/auth/certyx/splunk-syslog.pem
sslPassword = <password of the private key in the PEM file>
requireClientCert = false
```

1. Podział na wiersze i znaczniki czasu w `props.conf`:

```
[certyx:syslog]
SHOULD_LINEMERGE = false
LINE_BREAKER = ([\r\n]+)
TIME_PREFIX = ^<\d+>1\s
TIME_FORMAT = %Y-%m-%dT%H:%M:%S.%3NZ
TZ = UTC
MAX_TIMESTAMP_LOOKAHEAD = 30
TRUNCATE = 0
```

1. Uruchom ponownie Splunk i zezwól na TCP 6514 z serwera CERTYX.

12.2 Strona CERTYX

Transport `syslog-tls`, format `rfc5424` (lub `json`, `cef`, `kv`), Host syslog = nazwa hosta Splunk zawarta w jego certyfikacie, Port `6514`, Ramkowanie **Nowa linia**, Zaufane certyfikaty główne w przypadku prywatnego CA. **Sprawdź połączenie**, **Wyślij zdarzenie testowe**, a następnie wyszukaj (JSON zaczyna się od pierwszego znaku `{` komunikatu):

```
index=clm sourcetype=certyx:syslog "<event ID shown by the test>"
index=clm sourcetype=certyx:syslog
| rex "(?<payload>\{.*\})$"
| spath input=payload
| search category=authentication
```

13 IBM QRadar

QRadar odbiera LEEF przez syslog/TLS. Dostępne są trzy formaty LEEF:

13.1 Wybór formatu LEEF

Format	Identyfikator zdarzenia w nagłówku	Atrybuty	Zastosowanie
`leef-2.0` (zalecany)	kod zdarzenia	pola kanoniczne, domyślnie separator tabulator lub skonfigurowany	Nowe integracje z QRadar
`leef-1.0`	kod zdarzenia	pola kanoniczne rozdzielone tabulatorem	Wersje QRadar lub moduły DSM, które oczekują LEEF 1.0
`leef-compat`	`certyx:<outcome>` lub `certyx:<event name>`	atrybuty z pierwszego wydania z dodanym `eventId`, separator `^`	Istniejąca zawartość QRadar zbudowana na pierwszym wydaniu

Nagłówki:

```
LEEF:2.0|CERTYX|CLM|<version>|<event code>|<delimiter>|
LEEF:1.0|CERTYX|CLM|<version>|<event code>|
LEEF:2.0|CERTYX|CLM|<version>|certyx:<outcome or event name>|^|
```

Event ID w QRadar to identyfikator zdarzenia z nagłówka LEEF: kod zdarzenia (`AUTHN-002`, `CONFIG-008`, …) dla `leef-1.0` i `leef-2.0`. Czas: `devTime` z `devTimeFormat` `yyyy-MM-dd'T'HH:mm:ss.SSSZ`. Ważność: `sev` 1–10. Najważniejsze atrybuty: `cat` (kategoria), `usrName`, `src`, `identSrc` (zdarzenia logowania), `proto`, `eventId` (identyfikator zdarzenia), `schemaVersion`, `action`, `outcome`, `message`, `reason`, `userId`, `authMethod`, `method`, `resource`, `httpStatus`, `organization`, `organizationName`, `organizationKind`, `correlationId`, `resourceType`, `resourceId`, `changeType`, `instance`. W wartościach ukośnik odwrotny i separator są poprzedzane ukośnikiem odwrotnym; końce wierszy i tabulatory są zamieniane na spacje.

13.2 Strona odbiorcy (QRadar)

1. *Admin* → *Data Sources* → *Log Sources* → *Add* (aplikacja QRadar Log Source Management).
2. **Log Source Type**: *Universal LEEF* (albo własny DSM utworzony w DSM Editor). **Protocol**: *TLS Syslog*.
3. **Log Source Identifier**: identyfikator instancji CERTYX (`Clm:Instance:Id`; we wdrożeniu kontenerowym `CERTYX_INSTANCE_ID`, domyślnie nazwa hosta konsoli, np. `certyx.example.com`, taka sama we wszystkich wydaniach) — pole HOSTNAME każdego komunikatu syslog CERTYX. Przy kilku instancjach CERTYX dodaj jedno źródło dziennika na każdy identyfikator instancji albo pozwól QRadar wykryć je automatycznie.
4. **TLS Listen Port**: 6514 (domyślnie) lub inny port. **Authentication Mode**: TLS albo TLS z uwierzytelnianiem klienta, gdy CERTYX przedstawia certyfikat klienta. **Certificate Type**: certyfikat generowany przez QRadar albo *Provide Certificate* z certyfikatem dla nazwy hosta QRadar.
5. Wdróż zmiany i zezwól na TCP do portu nasłuchu z serwera CERTYX.

6. **DSM Editor.** Zmapuj identyfikatory zdarzeń (kody zdarzeń) na QID; katalog kodów zdarzeń wymienia każdy kod z jego kategorią. Utwórz niestandardowe właściwości zdarzeń dla kluczy CERTYX, według których chcesz wyszukiwać lub raportować, na przykład `eventId` (usuwanie duplikatów), `schemaVersion`, `organization`, `organizationName`, `correlationId`, `authMethod`, `reason`, `resourceType`, `resourceId`, `changeType`. QRadar bierze czas zdarzenia z `devTime`, gdy obecne jest `devTimeFormat`; sprawdź, czy *Log Activity* pokazuje czas CERTYX, a nie czas odbioru.

13.3 Strona CERTYX

Transport `syslog-tls`, format `leef-2.0` (lub `leef-1.0`, `leef-compat`), Host syslog = nazwa hosta kolektora zdarzeń QRadar (zawarta w jego certyfikacie), Port = TLS Listen Port, Ramkowanie **Zliczanie oktetów (RFC 5425)**, opcjonalny **Separator LEEF** dla `leef-2.0` (domyślnie tabulator; na przykład `^` lub `x5E`, gdy Twój DSM oczekuje daszka). Gdy QRadar używa wygenerowanego przez siebie certyfikatu lub prywatnego CA, wklej certyfikat główny tego certyfikatu (PEM) w polu **Zaufane certyfikaty główne**. **Sprawdź połączenie**, **Wyślij zdarzenie testowe**, a następnie znajdź zdarzenie w *Log Activity* z filtrem według źródła dziennika (Event ID `INTEGRATION-001`). Przykłady: Przykładowe zdarzenia.

14 ArcSight

CEF przez syslog/TLS przenosi ArcSight Common Event Format w wersji 0, producent `CERTYX`, produkt `CLM`.

14.1 Wybór formatu CEF

Format	Device Event Class ID	Zastosowanie
`cef` (zalecany)	kod zdarzenia (`AUTHN-002`, …); `externalId` = identyfikator zdarzenia	Nowe integracje z ArcSight, dowolny parser CEF
`cef-compat`	`certyx:<outcome>` lub `certyx:<event name>`; `externalId` = numer sekwencyjny w dzienniku, `certyxEventId` = identyfikator zdarzenia	Istniejąca zawartość ArcSight zbudowana na pierwszym wydaniu

Mapowanie formatu `cef` (wartości nieznane i puste są pomijane; w polach nagłówka ukośnik odwrotny i kreska pionowa są maskowane, a końce wierszy zamieniane na spacje; w wartościach rozszerzeń maskowane są `\`, `=`, CR i LF):

Klucz CEF	Pole kanoniczne
Device Event Class ID	`event_code`
Name	`message`
Severity	`severity` (0–10)
`rt`	`timestamp` (milisekundy epoki)
`externalId`	`event_id`
`act`, `cat`, `outcome`, `msg`, `reason`	`action`, `category`, `outcome`, `message`, `reason`
`src`	`src_ip`
`suser`, `suid`	`username` (w przeciwnym razie `user_id`), `user_id`
`requestMethod`, `request`, `requestClientApplication`	`http_method`, `http_route`, `user_agent`
`app`, `dvchost`	`protocol`, `hostname`
`cn1` (`httpStatus`)	`http_status`
`cs1` … `cs6`	`organization_id`, `organization_name`, `correlation_id`, `resource_type`, `resource_id`, `schema_version` (etykiety w `cs1Label` … `cs6Label`)
`flexString1` (`changeType`), `flexString2` (`authMethod`)	`change_type`, `authentication_method`

14.2 Strona odbiorcy (ArcSight SmartConnector)

1. Zainstaluj SmartConnector **Syslog NG Daemon** (typ konektora syslog przyjmujący TLS) na hoście osiągalnym z serwera CERTYX.
2. W konfiguracji konektora wybierz protokół **TLS** (Raw TCP over TLS) i port, na przykład 6514.
3. Zaimportuj certyfikat serwera i klucz dla nazwy hosta konektora do magazynu kluczy konektora zgodnie z dokumentacją SmartConnector; uwierzytelnianie certyfikatem klienta włączaj tylko wtedy, gdy CERTYX przedstawia certyfikat klienta (mTLS).
4. Zarejestruj konektor w ArcSight ESM lub Logger jako miejsce docelowe. Konektor parsuje komunikaty CEF bez nadpisywania parsera; etykiety `cs1`–`cs6` docierają jako etykiety *Device Custom String*.
5. Zezwól na TCP 6514 z serwera CERTYX.

14.3 Strona CERTYX

Transport `syslog-tls`, format `cef` (lub `cef-compat`), Host syslog = nazwa hosta konektora, Port 6514, Ramkowanie **Zliczanie oktetów (RFC 5425)**, Zaufane certyfikaty główne w przypadku prywatnego CA. **Sprawdź połączenie**, **Wyślij zdarzenie testowe** i wyszukaj zdarzenie z *Device Vendor* CERTYX, *Device Event Class ID* `INTEGRATION-001` i *External ID* równym identyfikatorowi zdarzenia testowego. Przykłady: Przykładowe zdarzenia.

15 Elastic (ECS)

Profil `ecs` zapisuje dokumenty Elastic Common Schema 8.11.0: `@timestamp`, `message`, `ecs.version`, `event.id` (identyfikator zdarzenia), `event.code` (kod zdarzenia), `event.kind` `event`, `event.category`, `event.type`, `event.action`, `event.outcome`, `event.severity`, `event.created`, `event.dataset` `certyx.security`, `event.provider`, `event.reason`, `user.id`, `user.name`, `source.ip`, `host.hostname`, `service.*`, `http.request.method`, `http.request.id`, `http.response.status_code`, `url.path` (szablon trasy), `organization.id`, `organization.name`, `labels.schema_version`, `labels.certyx_category`. Nieznane wartości są pomijane.

Opcja A — Logstash przez HTTPS (zalecana). CERTYX: transport `https`, format `ndjson`, profil `ecs`, certyfikat klienta dla mTLS. Logstash:

```
input {
  http {
    port => 8443
    ssl_enabled => true
    ssl_certificate => "/etc/logstash/tls/logstash.example.internal.pem"
    ssl_key => "/etc/logstash/tls/logstash.example.internal.key"
    ssl_client_authentication => "required"
    ssl_certificate_authorities => ["/etc/logstash/tls/certyx-client-ca.pem"]
    additional_codecs => { "application/x-ndjson" => "json_lines" }
    remote_host_target_field => "[@metadata][input][remote_host]"
    request_headers_target_field => "[@metadata][input][headers]"
  }
}
output {
  elasticsearch {
    hosts => ["https://elasticsearch.example.internal:9200"]
    data_stream => true
    data_stream_type => "logs"
    data_stream_dataset => "certyx.security"
    data_stream_namespace => "default"
    document_id => "%{[event][id]}"
  }
}
```

Wejście `http` Logstash nie sprawdza podpisu HMAC; zamiast tego CERTYX jest uwierzytelniany certyfikatem klienta (podpis jest nadal wysyłany). Dwie opcje `…_target_field` utrzymują metadane żądania dodawane przez wejście poza dokumentem, dzięki czemu nie mieszają się z własnymi polami ECS `http`, `url` i `host` dokumentu. Strumień danych to `logs-certyx.security-default`; nazwy strumieni danych muszą być pisane małymi literami, a zbiór danych (dataset) nie może zawierać `-`.

Opcja B — syslog przez TLS do Logstash lub integracji Elastic Agent *Custom TCP Logs* z TLS: w CERTYX transport `syslog-tls`, format `rfc5424`, profil `ecs`, ramkowanie **Nowa linia**; u odbiorcy podziel strumień na wiersze, usuń nagłówek syslog aż do pierwszego znaku `{` (oraz znacznik kolejności bajtów albo poproś operatora o ustawienie `Clm:Siem:Syslog:ByteOrderMark=false`) i zdekoduj JSON (filtr `json` w Logstash, procesor `decode_json_fields` w Agent).

Opcja C — archiwum plikowe w formacie `ndjson` z profilem `ecs`, importowane wsadowo (na przykład przez Filebeat lub Elastic Agent odczytujący pobrane pliki).

Usuwanie duplikatów. Używaj `event.id` jako `_id` dokumentu (`document_id` powyżej): ponownie wysłane zdarzenie zostaje odrzucone jako duplikat (`409`), zamiast zostać zaindeksowane dwukrotnie. Strumień danych sprawdza `_id` tylko w swoim bieżącym indeksie bazowym; po rolloverze spóźniony duplikat może zostać zaindeksowany ponownie, więc gdy liczą się dokładne liczby, wyszukuj według `event.id`. Alternatywnie `_id` może wytworzyć filtr `fingerprint` Logstash z `source => "[event][id]"`.

16 Odbiorcy OCSF i Amazon Security Lake

Profil `ocsf` zapisuje dokumenty JSON OCSF 1.1.0. Dla każdego zdarzenia CERTYX wybiera klasę i weryfikuje jej wymagane atrybuty:

Klasa	Zdarzenia
Authentication (3002)	kategoria `authentication`: aktywność 1 Logon (logowanie), 2 Logoff (wylogowanie), 99 Other
Account Change (3001)	zmiany kont i użytkowników SCIM, reset MFA: 1 Create, 5 Disable, 6 Delete, 11 MFA Factor Disable, 99 Other
API Activity (6003)	pozostałe zdarzenia żądań: 1 Create (POST), 2 Read (GET/HEAD), 3 Update (PUT/PATCH), 4 Delete (DELETE), 99 Other
Base Event (0)	wszystkie pozostałe oraz klasa zastępcza

Każdy dokument zawiera `class_uid`, `category_uid`, `activity_id`, `type_uid`, `severity_id`, `status_id`, `time` (milisekundy epoki), `message`, `metadata.uid` (identyfikator zdarzenia), `metadata.event_code`, `metadata.version`, `metadata.product` oraz `unmapped.certyx_schema_version`, `unmapped.certyx_category`, `unmapped.certyx_action`. Gdy zdarzenie nie ma wymaganych atrybutów swojej klasy — na przykład anonimowe żądanie bez `actor.user` albo żądanie bez adresu źródłowego — jest zapisywane jako Base Event, a przyczyny są wymienione w `unmapped.certyx_ocsf_fallback`. CERTYX nigdy nie deklaruje klasy bez weryfikacji; walidator sprawdza obecność i typ wymaganych atrybutów, a nie pełny schemat OCSF.

Dostarczanie. Transport `https` × `ndjson` × `ocsf` do Twojego kolektora, `splunk-hec` × `ndjson` × `ocsf`, `syslog-tls` × `rfc5424` × `ocsf` albo archiwum plikowe `file` × `ndjson` × `ocsf` (`certyx-events-YYYY-MM-DD.ndjson`).

Amazon Security Lake. Niestandardowe źródło Security Lake przyjmuje OCSF w formacie Apache Parquet, jedną klasę zdarzeń OCSF na niestandardowe źródło, zapisywane w lokalizacji S3 źródła. CERTYX dostarcza OCSF w JSON; konwersja należy do odbiorcy: uruchom kolektor (na przykład za webhookiem HTTPS albo odczytujący pobrane archiwum `ndjson`), który grupuje dokumenty według `class_uid`, konwertuje je do Parquet i zapisuje w niestandardowym źródle danej klasy. Zdarzenia zapisane jako Base Event (`class_uid` 0) potrzebują własnego niestandardowego źródła albo muszą zostać odfiltrowane przez Twój potok. Usuwaj duplikaty według `metadata.uid`.

17 Microsoft Sentinel

CERTYX zapisuje dane do niestandardowej tabeli Log Analytics przez Azure Monitor Logs Ingestion API: punkt zbierania danych (DCE) odbiera dane, reguła zbierania danych (DCR) mapuje strumień na tabelę, a aplikacja Microsoft Entra uwierzytelnia CERTYX.

17.1 Co otrzymuje tabela

Transport `azure-monitor`, format `sentinel`: jeden wiersz na zdarzenie z kolumnami z pierwszego wydania oraz `EventId` (string, `<installation id>:<journal sequence>`). Aby zapisywać `EventId`, zadeklaruj tę kolumnę w tabeli i w strumieniu; reguła bez niej nadal pozyskuje pozostałe kolumny. Lista kolumn: Kolumny Sentinel.

17.2 Strona odbiorcy (Azure)

1. **Obszar roboczy.** Obszar roboczy Log Analytics z włączonym Microsoft Sentinel.
2. **Punkt zbierania danych.** *Monitor → Data Collection Endpoints → Create*, w regionie obszaru roboczego. Skopiuj jego adres **Logs Ingestion**, na przykład `https://certyx-dce-a1b2.westeurope-1.ingest.monitor.azure.com`.
3. **Tabela i reguła.** W obszarze roboczym: *Tables → Create → New custom log (DCR-based)*: nazwa tabeli `CertyxSecurity` (Azure dodaje `_CL`), *Create a new data collection rule*, wybierz punkt końcowy z kroku 2, prześlij poniższą próbkę, pozostaw transformację `source`. Możesz też utworzyć je za pomocą Azure CLI (poniżej).
4. **Niezmienny identyfikator.** Otwórz regułę → *JSON View* → skopiuj `immutableId` (`dcr-`, a po nim 32 znaki szesnastkowe). Nazwa strumienia to `Custom-CertyxSecurity_CL`.
5. **Aplikacja.** *Microsoft Entra ID → App registrations → New registration*: nazwa `certyx-siem-export`, pojedyncza dzierżawa, bez identyfikatora URI przekierowania. Skopiuj **Directory (tenant) ID** i **Application (client) ID**. *Certificates & secrets → New client secret*: skopiuj **Value** klucza tajnego (nie jego Secret ID) i zanotuj datę wygaśnięcia.
6. **Uprawnienia.** Aplikacja nie potrzebuje uprawnień API ani zgody administratora. Nadaj jej rolę **Monitoring Metrics Publisher** na regule zbierania danych: reguła → *Access control (IAM) → Add role assignment* → Monitoring Metrics Publisher → aplikacja. Nowe przypisanie roli może zacząć działać dopiero po kilku minutach; do tego czasu API odpowiada kodem 403.
7. **Sieć.** Zezwól na wychodzący HTTPS z serwera CERTYX do `login.microsoftonline.com` i do hosta DCE.

Próbka dla kreatora tabeli (jeden rekord ze wszystkimi kolumnami):

```
[{"TimeGenerated":"2026-10-11T08:15:02.417Z","EventId":"<installation id>:48213","Sequence":48213,"Organization":"3f2c9a6e-8d1b-4c55-9a0e-2b7f1d4c8e90","OrganizationName":"Example Ltd","OrganizationKind":"organization","Actor":"anonymous","SourceIp":"203.0.113.24","AgentFingerprint":"","Method":"POST","Route":"/auth/customer/login","Status":401,"Outcome":"authentication","TraceId":"0HN7J3K2L1M0:00000003","ErrorType":"","Instance":"certyx-web-1","EventHash":"9C1F","Changes":[],"User":"jane.doe@example.com","UserVerified":true,"UserOrganization":"3f2c9a6e-8d1b-4c55-9a0e-2b7f1d4c8e90","AuthAction":"authentication.sign-in.failed","AuthMethod":"password","AuthResult":"failure","Reason":"invalid-credentials","UserAgent":"Mozilla/5.0"}]
```

Alternatywa z Azure CLI (zastąp wartości w nawiasach ostrych):

```
az monitor log-analytics workspace table create --resource-group <rg> --workspace-name <workspace> \
  --name CertyxSecurity_CL --columns TimeGenerated=datetime EventId=string Sequence=long Organization=string \
  OrganizationName=string OrganizationKind=string Actor=string SourceIp=string AgentFingerprint=string \
  Method=string Route=string Status=int Outcome=string TraceId=string ErrorType=string Instance=string \
  EventHash=string Changes=dynamic User=string UserVerified=boolean UserOrganization=string AuthAction=string \
  AuthMethod=string AuthResult=string Reason=string UserAgent=string

az monitor data-collection rule create --resource-group <rg> --location <region> \
  --name certyx-dcr --rule-file certyx-dcr.json

az role assignment create --assignee <application-client-id> --role "Monitoring Metrics Publisher" \
  --scope /subscriptions/<subscription>/resourceGroups/<rg>/providers/Microsoft.Insights/dataCollectionRules/certyx-dcr
```

`certyx-dcr.json` (strumień deklaruje te same kolumny co tabela):

```
{
  "location": "<region>",
  "properties": {
```

```
    "dataCollectionEndpointId":
"/subscriptions/<subscription>/resourceGroups/<rg>/providers/Microsoft.Insights/dataCollectionEndpoints/<dce>",
    "streamDeclarations": {
      "Custom-CertyxSecurity_CL": {
        "columns": [
          { "name": "TimeGenerated", "type": "datetime" }, { "name": "EventId", "type": "string" },
          { "name": "Sequence", "type": "long" }, { "name": "Organization", "type": "string" },
          { "name": "OrganizationName", "type": "string" }, { "name": "OrganizationKind", "type": "string" },
          { "name": "Actor", "type": "string" }, { "name": "SourceIp", "type": "string" },
          { "name": "AgentFingerprint", "type": "string" }, { "name": "Method", "type": "string" },
          { "name": "Route", "type": "string" }, { "name": "Status", "type": "int" },
          { "name": "Outcome", "type": "string" }, { "name": "TraceId", "type": "string" },
          { "name": "ErrorType", "type": "string" }, { "name": "Instance", "type": "string" },
          { "name": "EventHash", "type": "string" }, { "name": "Changes", "type": "dynamic" },
          { "name": "User", "type": "string" }, { "name": "UserVerified", "type": "boolean" },
          { "name": "UserOrganization", "type": "string" }, { "name": "AuthAction", "type": "string" },
          { "name": "AuthMethod", "type": "string" }, { "name": "AuthResult", "type": "string" },
          { "name": "Reason", "type": "string" }, { "name": "UserAgent", "type": "string" }
        ]
      }
    },
    "destinations": {
      "logAnalytics": [
        { "name": "workspace", "workspaceResourceId":
"/subscriptions/<subscription>/resourceGroups/<rg>/providers/Microsoft.OperationalInsights/workspaces/<workspace>" }
      ]
    },
    "dataFlows": [
      { "streams": ["Custom-CertyxSecurity_CL"], "destinations": ["workspace"], "transformKql": "source", "outputStream":
"Custom-CertyxSecurity_CL" }
    ]
  }
}
```

Reguła utworzona, zanim istniały `EventId`, `OrganizationName`, `OrganizationKind` lub kolumny logowania, nadal pozyskuje pozostałe kolumny; aby zapisywać brakujące kolumny, dodaj je do tabeli i do strumienia.

17.3 Strona CERTYX

1. Transport **Microsoft Sentinel** (`azure-monitor`), format `sentinel`.
2. **Adres HTTPS**: adres Logs Ingestion punktu zbierania danych.
3. **Reguła zbierania danych (niezmienny identyfikator)**: `dcr-…` z widoku JSON reguły.
4. **Strumień**: `Custom-CertyxSecurity_CL`.
5. **Identyfikator dzierżawy Microsoft Entra** i **Identyfikator aplikacji (klienta)**: identyfikatory GUID z rejestracji aplikacji.
6. **Klucz tajny klienta**: wartość Value klucza tajnego. Odnów go w Entra przed wygaśnięciem i wpisz tu nową wartość.
7. Zapisz, **Sprawdź połączenie**, **Wyślij zdarzenie testowe**.

CERTYX uzyskuje token w przepływie client credentials z `https://login.microsoftonline.com/<tenant>/oauth2/v2.0/token` (zakres `https://monitor.azure.com//.default`) i wysyła paczkę do `<endpoint>/dataCollectionRules/<immutable ID>/streams/<stream>?api-version=2023-01-01`. Tokeny są używane ponownie aż do chwili krótko przed ich wygaśnięciem. Chmury suwerenne używają hosta urzędu (authority host) ustawionego przez operatora w `Clm:Siem:SentinelAuthorityHost`.

Oznaki powodzenia: miejsce docelowe przyjęło zdarzenie testowe i wyświetlany jest jego identyfikator zdarzenia. Dane pojawiają się w tabeli po opóźnieniu pozyskiwania (zwykle kilka minut):

```
CertyxSecurity_CL
| where Actor == "siem-test"

CertyxSecurity_CL
| summarize arg_max(TimeGenerated, *) by EventId
| where Outcome == "authentication" and AuthResult == "failure"
| summarize Failures = count() by User, SourceIp, Reason, bin(TimeGenerated, 15m)
```

18 OpenTelemetry Logs (OTLP/HTTP)

CERTYX wysyła zdarzenie kanoniczne jako rekordy dziennika OpenTelemetry przez OTLP/HTTP do każdego odbiorcy, który implementuje punkt końcowy dzienników OTLP: OpenTelemetry Collector, Grafana Alloy, Grafana Loki albo własny punkt końcowy OTLP danego systemu. Użyj go, aby korelować zdarzenia bezpieczeństwa ze śladami i metrykami swoich aplikacji; klasyczne formaty SIEM pozostają dostępne obok.

18.1 Co otrzymuje odbiorca

Transport `otlp-http`, format `otlp-protobuf` (binarny protobuf, `Content-Type: application/x-protobuf`, domyślny dla OTLP/HTTP) albo `otlp-json` (OTLP/JSON, `Content-Type: application/json`), profil `native`. Każda partia to jeden `POST` z `ExportLogsServiceRequest` (opentelemetry-proto `collector/logs/v1`) pod adres dokładnie taki, jak wpisano — CERTYX nie dopisuje `/v1/logs` — opcjonalnie z `Content-Encoding: gzip`. Komunikat protobuf koduje sam CERTYX według numerów pól opentelemetry-proto v1 (bez biblioteki protobuf).

Żądanie zawiera jeden `ResourceLogs` na każdy odrębny zasób (w praktyce jeden na organizację w partii), jeden `ScopeLogs` (zakres `certyx.security-journal`, wersja = wersja produktu) i jeden `LogRecord` na zdarzenie:

OTLP	Ze zdarzenia kanonicznego
Zasób `service.name`	`certyx`
Zasób `service.version`, `deployment.environment.name`, `host.name`, `host.ip`	`version`, `environment`, `hostname`, `host_ip` (tablica)
Zasób `certyx.organization.id`, `certyx.organization.name`, `certyx.organization.kind`	`organization_id`, `organization_name`, `organization_kind`
`Timestamp`, `ObservedTimestamp`	`timestamp`, `observed_timestamp` (nanosekundy Unix)
`SeverityNumber`, `SeverityText`	`severity` 0–3 → 9 `INFO`, 4–6 → 13 `WARN`, 7–8 → 17 `ERROR`, 9–10 → 21 `FATAL`
`Body`	`message`; przy *Treść rekordu dziennika: Zdarzenie kanoniczne* cały dokument kanoniczny jako lista klucz-wartość
`TraceId`, `SpanId`	`trace_id`, `span_id` (identyfikatory W3C żądania, wzbogacenie); pomijane, gdy nieznane
`event.name`	`action`
`user.id`, `user.name`, `user.roles`, `session.id`, `user_agent.original`	`user_id`, `username`, `user_role` (tablica), `session_id`, `user_agent`
`client.address`, `client.port`, `server.address`, `server.port`	`src_ip`, `src_port`, `dst_ip`, `dst_port`
`http.request.method`, `http.route`, `http.response.status_code`, `network.protocol.name`, `error.type`	`http_method`, `http_route` (szablon trasy), `http_status`, `protocol`, `error_type`
`certyx.event.id`, `certyx.event.code`, `certyx.event.category`, `certyx.event.outcome`, `certyx.event.severity`, …	`event_id`, `event_code`, `category`, `outcome`, `severity`; każde inne pole kanoniczne jako `certyx.<pole>`; `certyx.changes` to zwarty tekst JSON zmian
Własne pola mapowania pól	Atrybuty pod własnymi nazwami

Nieznane wartości są pomijane. W OTLP/JSON 64-bitowe liczby całkowite i czasy są tekstami dziesiętnymi, a identyfikatory trace i span tekstami szesnastkowymi; w protobuf są to liczby i bajty. Usuwaj duplikaty według atrybutu `certyx.event.id`.

Odpowiedzi. 2xx bez `partial_success` oznacza dostarczenie partii. 2xx z `partial_success.rejected_log_records` większym od zera to częściowy sukces: zgodnie ze specyfikacją OTLP CERTYX **nie** wysyła żądania ponownie (odbiorca zachował przyjęte rekordy). Pozycja przesuwa się za partię, odrzucenie jest zapisywane w dzienniku jako `siem.event.rejected` (kod `INTEGRATION-013`) z miejscem docelowym, liczbą odrzuconych rekordów, identyfikatorami zdarzeń i sekwencjami dziennika żądania (OTLP nie mówi, które rekordy odrzucono, więc wymieniane są wszystkie z żądania; przy ponad 200 zdarzeniach pierwsze i ostatnie) oraz `error_message` odbiorcy (drukowalny, najwyżej 200 znaków), a incydent `siem-rejected` jest zgłaszany z liczbą; pozostaje otwarty, dopóki operator go nie zamknie. **Nic nie ginie bez śladu**: zdarzenia pozostają w dzienniku i w archiwach plików, a po naprawie odbiorcy Wyślij ponownie od pierwszej wymienionej sekwencji wysyła je jeszcze raz (odbiorca usuwa duplikaty przyjętych według `certyx.event.id`). HTTP 400, 413 i 422 dzielą partię aż do odrzuconego zdarzenia (Odrzucone zdarzenia); 401, 403, 404, 415, 429 i 5xx ponawiają całą partię z wycofaniem, a `Retry-After` przy 429 lub 503 jest respektowany (następna próba czeka co najmniej tyle, najwyżej najdłuższe opóźnienie miejsca docelowego).

18.2 Strona odbiorcy (OpenTelemetry Collector)

Odbiornik `otlp` w OpenTelemetry Collector (dystrybucja contrib ze względu na rozszerzenie `bearertokenauth`) z TLS na porcie 4318 i tokenem okaziciela:

```
extensions:
  bearertokenauth:
    token: ${env:CERTYX_OTLP_TOKEN}
receivers:
  otlp:
    protocols:
      http:
        endpoint: 0.0.0.0:4318
        tls:
          cert_file: /etc/otelcol/tls/server.crt
          key_file: /etc/otelcol/tls/server.key
          # client_ca_file: /etc/otelcol/tls/certyx-client-ca.pem
        auth:
          authenticator: bearertokenauth
processors:
  batch: {}
exporters:
  debug:
    verbosity: detailed
service:
  extensions: [bearertokenauth]
  pipelines:
    logs:
      receivers: [otlp]
      processors: [batch]
      exporters: [debug]
```

1. Daj odbiornikowi certyfikat, którego nazwy obejmują nazwę hosta wpisaną w CERTYX; prywatne CA wklej w CERTYX w polu *Zaufane certyfikaty główne*.
2. Dla wzajemnego TLS ustaw `client_ca_file` na CA certyfikatu klienta CERTYX i wpisz ten certyfikat z kluczem w CERTYX (mTLS); token okaziciela jest wtedy opcjonalny.
3. Zastąp eksporter `debug` eksporterem swojego systemu.
4. W CERTYX: adres `https://collector.example.com:4318/v1/logs`, nazwa nagłówka `Authorization` (domyślna), sekret `Bearer <token>`.

18.3 Grafana Alloy i Loki

Grafana Alloy odbiera OTLP przez `otelcol.receiver.otlp` i przekazuje do natywnego punktu końcowego OTLP w Loki (Loki 3, ścieżka `/otlp/v1/logs`; eksporter dopisuje `/v1/logs`):

```
otelcol.receiver.otlp "certyx" {
  http {
    endpoint = "0.0.0.0:4318"
    tls {
      cert_file = "/etc/alloy/tls/server.crt"
      key_file  = "/etc/alloy/tls/server.key"
    }
  }
  output {
    logs = [otelcol.exporter.otlphttp.loki.input]
  }
}

otelcol.exporter.otlphttp "loki" {
  client {
    endpoint = "http://loki:3100/otlp"
  }
}
```

Loki zachowuje niektóre atrybuty zasobu, takie jak `service.name`, jako etykiety indeksu, a pozostałe atrybuty jako metadane strukturalne, z kropkami zamienionymi na podkreślenia, na przykład `{service_name="certyx"} | certyx_event_code="AUTHN-002"`. CERTYX może też wysyłać bezpośrednio na `https://<loki>/otlp/v1/logs`, gdy Loki jest osiągalny przez TLS i wymaga najwyżej jednego nagłówka; wielodzierżawny Loki, który wymaga dodatkowo `X-Scope-OrgID`, musi stać za Alloy albo Collectorem.

18.4 Inne systemy OTLP

Datadog, Elastic i inni dostawcy dokumentują własne przyjmowanie OTLP. Ogólna, oparta na specyfikacji droga to OpenTelemetry Collector albo Alloy jak wyżej, z eksporterem opisanym przez dostawcę. System, który udostępnia punkt końcowy dzienników OTLP/HTTP przez HTTPS i uwierzytelnia jednym nagłówkiem, można użyć bezpośrednio: wpisz adres dzienników, nazwę i wartość nagłówka dokładnie tak, jak opisuje je dostawca. CERTYX wysyła dokładnie jeden nagłówek uwierzytelniania i żadnych innych nagłówków specyficznych dla dostawcy.

18.5 Strona CERTYX

1. **Transport** *OpenTelemetry Logs (OTLP/HTTP)*; **Format** *OTLP protobuf* (zalecany) albo *OTLP/JSON*; profil *native*.
2. **Adres HTTPS**: pełny adres dzienników odbiorcy, na przykład `https://collector.example.com:4318/v1/logs`.
3. **Treść (Body) rekordu dziennika**: *Komunikat* (komunikat zdarzenia) albo *Zdarzenie kanoniczne (lista klucz-wartość)*. W obu przypadkach wszystkie pola są atrybutami.
4. **Nazwa nagłówka uwierzytelniania** (opcjonalnie; puste oznacza `Authorization`) i **Wartość nagłówka uwierzytelniania** jako sekret (na przykład `Bearer <token>` albo klucz API). Wartość jest przechowywana w postaci zaszyfrowanej i nigdy ponownie niewyświetlana; bez wartości nagłówek nie jest wysyłany. Nagłówki `Host`, `Content-Type`, `Content-Length`, `Content-Encoding`, `Transfer-Encoding`, `Connection`, `Cookie` i `Proxy-` są odrzucane.
5. **Kompresuj żądania gzip** (zalecane dla odległych odbiorców).
6. Zaufane certyfikaty główne, certyfikat klienta i sprawdzanie odwołania (TLS), *Wysyłaj tylko*, mapowanie pól i wartości dostarczania działają jak w pozostałych transportach.
7. Zapisz, **Sprawdź połączenie** i **Wyślij zdarzenie testowe**: wynik `otlp-accepted` podaje identyfikator zdarzenia; wyszukaj w systemie `certyx.event.id` o tej wartości.

19 Sprawdzenie połączenia i zdarzenie testowe

Sprawdź połączenie wykonuje etapy transportu miejsca docelowego bez wysyłania czegokolwiek: DNS → TCP → TLS (z certyfikatem klienta i sprawdzaniem unieważnienia) dla każdego transportu sieciowego; dla archiwum plikowego etap *Archiwum* sprawdza, czy do katalogu archiwum można zapisywać. **Wyślij zdarzenie testowe** wykonuje te same etapy, a następnie dostarcza jedno syntetyczne zdarzenie bez przesuwania pozycji miejsca docelowego. Pierwszy nieudany etap kończy sprawdzanie. Każdy etap pokazuje swój wynik i ustalone fakty:

Etap	Poprawny	Pokazywane fakty
DNS	`dns-ok`, `dns-literal`	Adresy, na które host jest rozwiązywany na serwerze CERTYX
TCP	`tcp-ok`	Adres i port połączenia
TLS	`tls-ok`	Wersja TLS, podmiot, wystawca i data wygaśnięcia certyfikatu
Dostarczenie	`hec-accepted`, `syslog-written`, `http-accepted`, `otlp-accepted`	Indeks i sourcetype Splunk; ramkowanie syslog; identyfikator zdarzenia testowego
Archiwum	`archive-ok`	Liczba plików, zajmowane przez nie miejsce i wolne miejsce

Zdarzenie testowe. Jego `event_id` to nowy UUID (zdarzenie nie ma numeru sekwencyjnego w dzienniku), `event_code` `INTEGRATION-001`, `category` `integration`, `action` `siem.test`, `user_id` / `Actor` `siem-test`, wynik: zmiana biznesowa; w rekordzie JSON `Sequence` 0, `Method` `INTERNAL`, `Route` `business/siem.test`. Przechodzi przez format i profil miejsca docelowego tak jak każde inne zdarzenie, więc pokazuje dokładnie to, co otrzyma odbiorca. Wynik podaje identyfikator zdarzenia: wyszukaj go u odbiorcy.

W przypadku miejsc docelowych syslog udany test podaje też, co musi zrobić odbiorca przy wybranym ramkowaniu (zliczanie oktetów: wejście odbierające musi mieć włączone zliczanie oktetów; nowa linia: musi dzielić strumień na końcach wierszy). Gdy odbiorca przyjmuje TCP, ale nie kończy uzgadniania TLS — jego wejście ma wyłączony TLS — sprawdzenie zgłasza `tls-timeout` lub `tls-handshake-failed`, a eksport zamiast przekroczenia czasu zapisuje *Odbiorca przyjął połączenie TCP, ale nie zakończył uzgadniania TLS …*. Archiwum plikowe nie ma zdarzenia testowego.

Wynik ostatniego sprawdzenia pozostaje na karcie miejsca docelowego i jest zapisywany w dzienniku bezpieczeństwa (`siem.destination.checked`, `INTEGRATION-003`; `siem.destination.tested`, `INTEGRATION-002`). Tokeny, sekrety i treści odpowiedzi nigdy się w nim nie pojawiają.

20 Dostarczanie, ponowienia i zaległości

- **Trwała kolejka.** Kolejką jest dziennik bezpieczeństwa: każde miejsce docelowe ma w nim własną pozycję (kursor), która przesuwa się dopiero po przyjęciu paczki przez odbiorcę. Zdarzenia są wysyłane w kolejności dziennika. Gdy odbiorca jest nieosiągalny, nic nie zostaje pominięte.
- **Co najmniej jednokrotnie.** Po przekroczeniu czasu lub utracie połączenia odbiorca mógł już zapisać paczkę, którą CERTYX wysyła ponownie; ponownie wysłane zdarzenia mają ten sam `event_id`. Usuwaj duplikaty według niego (Usuwanie duplikatów).
- **Wycofywanie (backoff).** Po nieudanym dostarczeniu miejsce docelowe czeka przed kolejną próbą: **pierwsze opóźnienie ponowienia** (domyślnie 30 sekund, `Clm:Siem:Delivery:InitialDelay`) jest podwajane przy każdym kolejnym następującym po sobie niepowodzeniu aż do **najdłuższego opóźnienia ponowienia** (domyślnie 15 minut, `Clm:Siem:Delivery:MaxDelay`), a każde opóźnienie jest losowo rozrzucane o ±20 % (`Clm:Siem:Delivery:Jitter`), aby miejsca docelowe, które zawodzą jednocześnie, nie ponawiały prób jednocześnie. Pierwsze udane dostarczenie resetuje opóźnienie. Odbiorca, który odpowiada 429 lub 503 z `Retry-After` (Splunk HEC, HTTPS, Sentinel, OTLP), jest czekany co najmniej tyle, najwyżej najdłuższe opóźnienie ponowienia.
- **Incydent** `siem-delivery`**.** Niepowodzenie zgłasza ten incydent operatorowi platformy jako ostrzeżenie; po tylu następujących po sobie niepowodzeniach, ile wynosi **Próby przed alertem krytycznym** (domyślnie 10, `Clm:Siem:Delivery:MaxAttempts`), staje się krytyczny. Zamyka się po następnym udanym dostarczeniu.

- **Zaległości.** Gdy na miejsce docelowe czeka więcej zdarzeń, niż wynosi jego limit **Alert zaległości powyżej (zdarzenia)** (domyślnie 100 000, `Clm:Siem:Delivery:BacklogLimit`), zgłaszany jest incydent `siem-backlog`. Nic nie zostaje pominięte (zasada przepełnienia *zachowaj i alarmuj*): zdarzenia pozostają w dzienniku i są wysyłane, gdy miejsce docelowe znów je przyjmuje. Incydent zamyka się, gdy zaległości spadną poniżej limitu.
- **Rozmiar paczki.** Do 200 zdarzeń na miejsce docelowe i przebieg (`Clm:Siem:BatchSize`); miejsce docelowe z konsoli może ustawić własny **Rozmiar partii (zdarzenia)** (1–5000). W przypadku Splunk HEC utrzymuj paczkę poniżej wartości `max_content_length` odbiorcy (najmniejsze typowe ustawienie to 1 000 000 bajtów).
- **Dla każdego miejsca docelowego.** Liczbę prób, pierwsze opóźnienie ponowienia (1–3600 s), najdłuższe opóźnienie ponowienia (1–86400 s, nie krótsze niż pierwsze), rozmiar paczki, alarm zaległości (1–100 000 000) i *Pomiń zdarzenie, które odbiorca nadal odrzuca po powyższych próbach* można ustawić w formularzu miejsca docelowego; puste pola oznaczają wartości domyślne serwera. Nie dotyczą one archiwów plikowych.

20.1 Odrzucone zdarzenia

Niektóre odpowiedzi oznaczają, że odbiorca odrzuca same dane, niezależnie od ponowień: HTTP 400, 413 i 422 oraz kody Splunk HEC 5 (brak danych), 6 (nieprawidłowy format danych), 12 (pole event jest wymagane), 13 (pole event nie może być puste) i 15 (błąd obsługi pól indeksowanych). Wtedy CERTYX:

1. rekurencyjnie dzieli paczkę na połowy, aż znajdzie pojedyncze odrzucane zdarzenie;
2. dostarcza każde zdarzenie przed nim i zatrzymuje pozycję tuż przed nim;
3. podaje jego `event_id` w ostatnim błędzie i w incydencie `siem-delivery` (*Odbiorca odrzuca zdarzenie …*).

Domyślnie: odrzucane zdarzenie jest ponawiane z wycofywaniem, a incydent pozostaje otwarty, dopóki odbiorca go nie przyjmie (popraw odbiorcę — na przykład indeks, limity pól lub limit rozmiaru — a kolejna próba je dostarczy).

Opcja *Pomiń zdarzenie, które odbiorca nadal odrzuca po powyższych próbach* **(formularz miejsca docelowego albo `Clm:Siem:Delivery:SkipRejected` dla wszystkich miejsc docelowych): po tylu próbach, ile wynosi Próby przed alertem krytycznym**, odrzucane zdarzenie jest pomijane, pozycja przesuwa się za nie, a pominięcie jest zapisywane w dzienniku jako `siem.event.skipped` (kod `INTEGRATION-011`) z identyfikatorem zdarzenia, numerem sekwencyjnym, liczbą prób i przyczyną. Zdarzenie pozostaje w dzienniku i w archiwach plikowych; po naprawieniu odbiorcy można je wysłać ponownie funkcją Wyślij ponownie od.

Każdy inny błąd — nieosiągalny odbiorca, błąd TLS, HTTP 401, 403, 404, 429 lub 5xx, inne kody HEC — powoduje ponowienie całej paczki.

20.2 Limity

- **Tempo.** Jeden przebieg co 30 sekund (`Clm:Siem:Interval`), limit czasu 20 sekund na żądanie lub połączenie (`Clm:Siem:HttpTimeout`); miejsce docelowe w trakcie wycofywania jest pomijane, dopóki nie minie jego opóźnienie.
- **Niezależność.** Każde miejsce docelowe ma własną pozycję, wycofywanie i stan; miejsce docelowe z błędami nie opóźnia pozostałych.
- **Historia.** Nowe miejsce docelowe zaczyna od początku przechowywanego dziennika swojego zakresu.
- **Poza zasięgiem obserwacji.** Logowań zablokowanych przed CERTYX (uzgadnianie TLS, zapora, limity żądań na wejściu) nie można eksportować; za serwerem pośredniczącym źródłowym adresem IP jest adres tego serwera.
- **Miejsca docelowe z konfiguracji.** Miejsca docelowe zdefiniowane przez operatora w konfiguracji serwera są wyświetlane w trybie tylko do odczytu w widoku ich zakresu; używają domyślnych wartości dostarczania serwera. Archiwa plikowe można skonfigurować wyłącznie w konsoli.
- **Identyfikacja organizacji.** Każdy format przenosi identyfikator, nazwę i rodzaj organizacji oraz instancję (Wiele organizacji w jednym SIEM).

21 Ponowne wysyłanie od numeru sekwencyjnego lub czasu

Wyślij ponownie od na karcie miejsca docelowego wysyła zdarzenia ponownie od numeru sekwencyjnego w dzienniku lub od wskazanej chwili, na przykład po utracie danych przez odbiorcę albo po pominięciu odrzuconego zdarzenia.

1. Wybierz **Wyślij ponownie od** na karcie miejsca docelowego.
2. Wpisz albo **numer sekwencyjny** w dzienniku (1 lub więcej; część `event_id` po dwukropku), albo **czas** — nie oba naraz.
3. Potwierdź. Pozycja miejsca docelowego cofa się tuż przed ten punkt; kolejne przebiegi wysyłają ponownie, w kolejności, każde zdarzenie od tego miejsca. Stan wycofywania i odrzuconego zdarzenia zostaje wyczyszczony.

Zasady:

- Pozycja może się tylko cofać, nigdy przesuwać naprzód: punkt, do którego miejsce docelowe jeszcze nie dostarczyło zdarzeń, jest odrzucany (*miejsce docelowe nie dostarczyło jeszcze zdarzeń do tego punktu*).
- Archiwum plikowe nie może wysyłać ponownie: zachowuje każde zdarzenie; zamiast tego pobierz jego pliki.
- Każde ponowne wysłanie jest zapisywane w dzienniku jako `siem.destination.replayed` (kod `INTEGRATION-012`) z poprzednią i nową pozycją.
- Odbiorca otrzymuje zdarzenia po raz drugi z tym samym `event_id`; usuwaj duplikaty według niego.
- Filtry działają tak jak w każdym przebiegu: zdarzenia wykluczone przez *Wysyłaj tylko* miejsca docelowego nie są wysyłane.

Uprawnienia. Administrator (Admin) organizacji z sesją MFA wysyła ponownie zdarzenia do miejsc docelowych własnej organizacji. Operator platformy wysyła ponownie zdarzenia do miejsc docelowych zakresów *Operatorzy platformy* i *Wszystkie zdarzenia*; jest to zmiana w centrum sterowania (control room) i wymaga kodu podwyższenia uprawnień operatora (step-up). Sesje aplikacji mobilnej nie mogą wysyłać ponownie.

API: `POST /api/administration/siem/{id}/replay` (organizacja) lub `POST /platform/api/siem/{scope}/{id}/replay` (platforma, zakres `platform` lub `all`, kod podwyższenia uprawnień w `X-Step-Up-Code`) z `{"fromSequence": 48000}` lub `{"fromTime": "2026-10-18T06:00:00Z"}`; odpowiedź to `{"position": …}`.

22 Usuwanie duplikatów według event_id

Dostarczanie jest co najmniej jednokrotne: po przekroczeniu czasu, utracie połączenia, niepotwierdzonym potwierdzeniu indeksowania HEC lub ponownym wysłaniu odbiorca może otrzymać zdarzenie dwukrotnie. Obie kopie mają ten sam identyfikator zdarzenia, unikalny we wszystkich instalacjach (`<installation id>:<journal sequence>`; UUID dla zdarzeń testowych).

Odbiorca	Gdzie jest identyfikator zdarzenia	Jak usuwać duplikaty
Splunk	pole indeksowane `event_id` (każdy format HEC), `event_id` w zdarzeniu kanonicznym	`dedup event_id` w wyszukiwaniach; dla podsumowań `stats latest(*) by event_id`
Elastic	`event.id` (ECS), `event_id` (native)	użyj go jako `_id` dokumentu (`document_id => "%{[event][id]}"` lub filtr `fingerprint`); duplikaty są odrzucane z kodem 409
QRadar	atrybut LEEF `eventId`	niestandardowa właściwość zdarzenia `eventId`; QRadar sam nie usuwa duplikatów — używaj jej w wyszukiwaniach i regułach (na przykład *group by eventId*)
ArcSight	CEF `externalId` (`cef`), `certyxEventId` (`cef-compat`)	ArcSight sam nie odrzuca duplikatów; grupuj lub filtruj według External ID w regułach i raportach
Sentinel	kolumna `EventId`	`summarize arg_max(TimeGenerated, *) by EventId`
Odbiorcy OCSF	`metadata.uid`	użyj go jako klucza zapisanego rekordu
Webhook / własny kolektor	`EventId`, `event_id`, `event.id` lub `metadata.uid` zależnie od profilu	unikalny klucz w Twoim magazynie danych
Archiwum plikowe	kolumna `event_id` (`csv`), `event_id` / `event.id` / `metadata.uid` (`ndjson`); `Sequence` (`csv-compat`)	archiwa nigdy nie zawierają wiersza dwukrotnie, z wyjątkiem awarii przy zmianie dnia (Dostarczanie, ponowne uruchomienia i miejsce na dysku)

Część identyfikatora instalacji zmienia się tylko wtedy, gdy operator zmieni `Clm:Siem:InstallationId`; utrzymuj ją bez zmian, w przeciwnym razie odbiorcy przestaną rozpoznawać ponownie wysłane zdarzenia jako duplikaty.

23 Wysyłaj tylko: mniej danych do SIEM

Zewnętrzne usługi SIEM i usługi logów są często licencjonowane według ilości pozyskanych danych. *Wysyłaj tylko* ogranicza to, co otrzymuje jedno miejsce docelowe, a archiwum plikowe zachowuje pełny zapis w Twoim własnym magazynie danych.

- **Wyniki** (pola wyboru): miejsce docelowe otrzymuje zaznaczone wyniki; zaznaczone opcje są łączone przez *lub*. *Zmiany konfiguracji i biznesowe* dodaje każde zdarzenie zawierające zmianę konfiguracji lub zmianę biznesową (na przykład `siem.destination.updated`, zmiany użytkowników i ról, decyzje o odnowieniu, `agent.health.changed`), niezależnie od pola wyboru jego wyniku. Przykład kanału SIEM oszczędzającego licencję: *Odmowy dostępu*, *Błędy serwera*, *Zdarzenia logowania* i *Zmiany konfiguracji i biznesowe*.
- **Minimalna ważność** (lista): wysyłane są tylko zdarzenia o tej lub wyższej ważności. Ważność (0–10): odebrane (`attempt`) 2, powodzenie i zmiana biznesowa 3, odrzucenie 5, odmowa dostępu i nieudane logowanie 7, błąd serwera i blokada 8.
- **Wysyłaj tylko (kategorie)**: jedna lub więcej z dziesięciu kategorii.
- **Wysyłaj tylko (kody zdarzeń)**: kody z katalogu kodów zdarzeń, na przykład `AUTHN-002`, najwyżej 200.
- **Wysyłane pola** (w sekcji *Kształt i rozmiar*, zwinięte): każde pole wybranego formatu z polem wyboru. Miejsce docelowe otrzymuje dokładnie zaznaczone pola; niezaznaczone pole jest zapisywane w kształtowaniu jako `excludeFields`. Działa dla każdego transportu i formatu oprócz stałych układów `cef-compat` i `leef-compat` (tam ustaw `cef` lub `leef`). Zawsze zostają: w formatach kanonicznych pola wymagane przez schemat (`schema_version`, `event_id`, `event_code`, `category`, `action`, `outcome`, `outcome_original`, `severity`, `severity_label`, `message`, trzy znaczniki czasu, `application`, `service_name`, `organization_kind`), w Sentinelu `TimeGenerated`; w rekordzie `json` można usunąć każde pole. **Zaznacz wszystkie** i **Tylko wymagane** ustawiają wszystkie pola naraz. Wynik pokazuje *Podgląd zdarzenia testowego*.
- **Więcej filtrów** (zwinięte): **Wysyłaj tylko te trasy** i **Nigdy nie wysyłaj tych tras** (jedna w wierszu; trasa obejmuje każdą trasę, która od niej się zaczyna, np. `/agent/v1/discovery/telemetry` dla regularnych raportów agentów), **Nigdy nie wysyłaj zdarzeń tych aktorów** (np. `pending`, żądania przed uwierzytelnieniem), **Nigdy nie wysyłaj tych kategorii** i **Nigdy nie wysyłaj tych kodów zdarzeń**. Wykluczenie zawsze wygrywa.
- Sondy kondycji nigdy nie są wysyłane, chyba że włączono `Clm:Siem:ExportHealthProbes`.

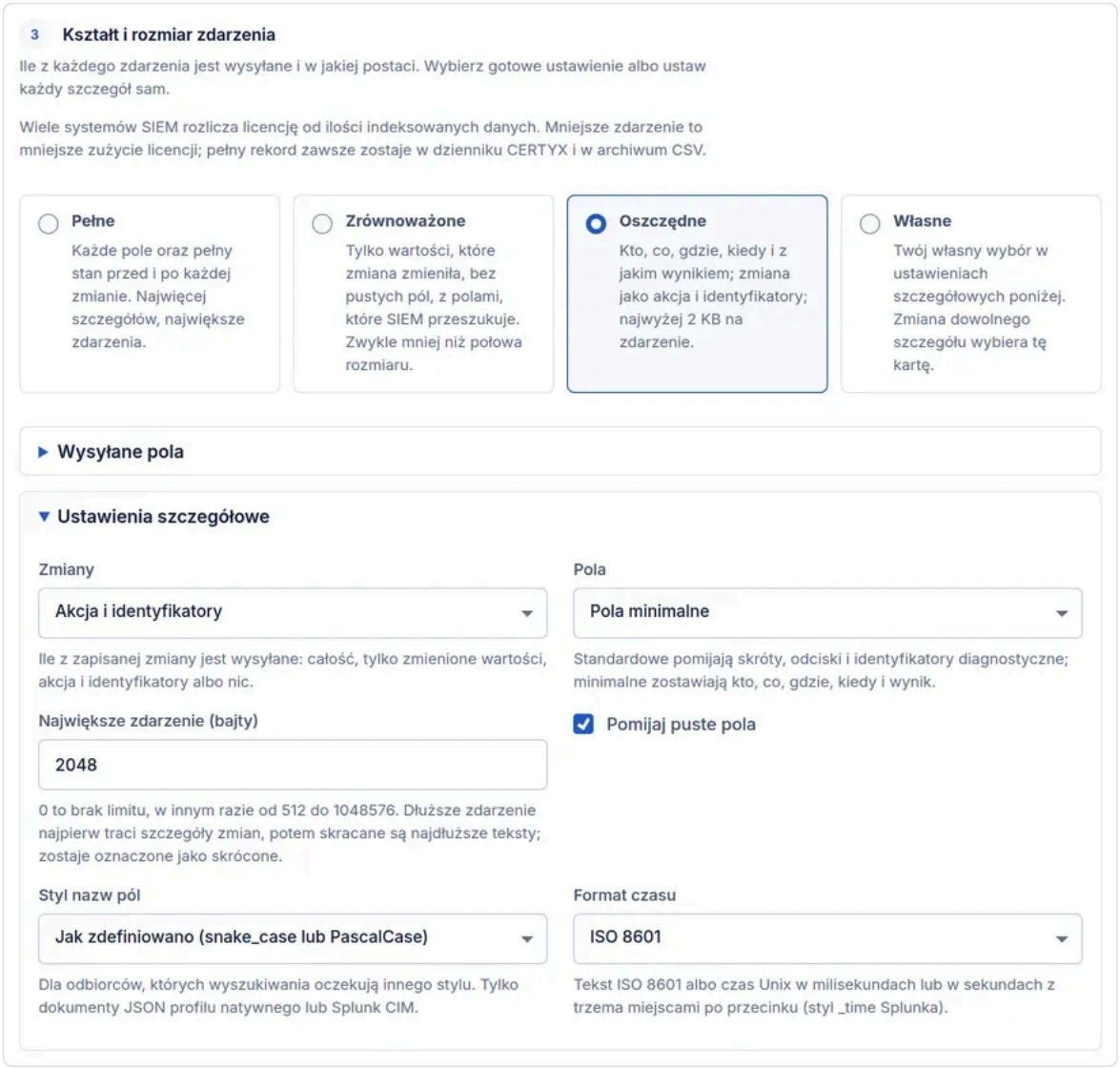
23.1 Łączenie filtrów

1. Sondy kondycji są usuwane (chyba że są eksportowane).
2. Wyniki (*lub* między zaznaczonymi) i minimalna ważność wybierają zdarzenia.
3. Kategorie i kody zdarzeń zawężają ten wynik: zdarzenie przechodzi, gdy na liście jest jego kategoria **lub** jego kod. Gdy żadna z list nie jest ustawiona, przechodzi każda kategoria i każdy kod.
4. *Więcej filtrów* usuwa resztę: trasy spoza *Wysyłaj tylko te trasy* oraz każdą wykluczoną trasę, aktora, kategorię i kod zdarzenia.

Przykład: wyniki puste (wszystkie), minimalna ważność 0, kategorie `authentication`, kody zdarzeń `CONFIG-008` → każde zdarzenie logowania i każda zmiana miejsca docelowego SIEM.

Pominięte zdarzenia nie giną: pozycja miejsca docelowego i tak przesuwa się za nie (dziennik je zachowuje), a archiwum plikowe o tym samym zakresie je przechowuje. Zmiana filtra dotyczy zdarzeń eksportowanych od tej chwili; już wyeksportowane zdarzenia nie są wysyłane ponownie, chyba że użyjesz ponownego wysyłania.

24 Kształtowanie zdarzeń: rozmiar i postać



Kształtowanie zdarzeń: karty gotowych ustawień i ustawienia szczegółowe miejsca docelowego (dane przykładowe)

Wiele usług SIEM i logów rozlicza licencję od ilości indeksowanych danych. *Wysyłaj tylko* decyduje, które zdarzenia trafiają do miejsca docelowego; **kształtowanie zdarzeń** decyduje, jak duże i w jakiej postaci każde z nich dociera. Każde miejsce docelowe ma własne kształtowanie, więc jeden SIEM może dostawać zwięzłe zdarzenia, a inny wszystko. Pełny rekord zawsze zostaje w dzienniku CERTYX i w archiwum plikowym; kształtowanie nigdy nie zmienia łańcucha skrótów.

Gotowe ustawienia (karty w sekcji 3 formularza):

Ustawienie	Zmiany	Pola	Puste pola	Największe zdarzenie
Pełne (jak przed kształtowaniem)	pełny stan przed i po	wszystkie	wysyłane	bez limitu
Zrównoważone	tylko zmienione wartości	standardowe	pomijane	bez limitu
Oszczędne	akcja i identyfikatory	minimalne	pomijane	2 KB
Własne	Twój wybór	Twój wybór	Twój wybór	Twój wybór

Wybór karty wypełnia **Ustawienia szczegółowe** jej wartościami; zmiana któregokolwiek z nich wybiera **Własne**. Zmierzone na obserwacji trzech certyfikatów przez agenta w formacie `json`: Pełne 4 578 bajtów, Zrównoważone 591 bajtów (−87%), Oszczędne 378 bajtów (−92%); zwykły raport agenta: 706, 462 i 390 bajtów. **Podgląd zdarzenia testowego** pokazuje rozmiar zdarzenia testowego z kształtowaniem i bez niego.

Ustawienia szczegółowe:

- **Zmiany** — *Pełny stan przed i po*; *Tylko zmienione wartości* (`before` i `after` zastępuje `changed`, np. `{"certificate.Owner":{"before":"Unassigned","after":"Team A"}}`; zagnieżdżone obiekty jako ścieżki z kropkami); *Akcja i identyfikatory* (proste wartości zmiany, bez obiektów i list); *Bez zmian*.
- **Pola** — *Wszystkie pola*; *Pola standardowe* (pomijają skróty, odcisk agenta, identyfikatory span i żądania, IP hosta i dane eksportu); *Pola minimalne* (kto, co, gdzie, kiedy i z jakim wynikiem). Wymagane pola zdarzenia kanonicznego (`schema_version`, `event_id`, `event_code`, `category`, `action`, `outcome`, `outcome_original`, `severity`, `severity_label`, `message`, trzy czasy, `application`, `service_name`, `organization_kind`) oraz `hostname` (wskazuje instancję w kopercie Splunk HEC, nagłówku syslog i zasobie OTLP) są zawsze wysyłane, a pole, które mapowanie pól zachowuje lub dodaje, zostaje. W rekordzie `json` zestaw minimalny to `Sequence`, `At`, `Category`, `EventCode`, `Tenant`, `Actor`, `SourceIp`, `Method`, `Route`, `Status`, `Outcome`, `EventId` i `SignIn`; standardowy dodaje `OrganizationName`, `Instance`, `TraceId`, `ErrorType` i `Changes`.
- **Pomijaj puste pola** — pola bez wartości (null, pusty tekst, pusta lista lub obiekt) nie są zapisywane.
- **Największe zdarzenie (bajty)** — 0 to brak limitu, w innym razie od 512 do 1 048 576. Dłuższe zdarzenie najpierw zachowuje tylko akcję i identyfikatory swoich zmian, potem traci zmiany, potem skracane są jego najdłuższe teksty (zakończone …); niesie wtedy `truncated: true` (`Truncated` w rekordzie `json`). Rozmiar jest mierzony na dokumencie zdarzenia; formaty liniowe są nieco krótsze lub dłuższe.
- **Styl nazw pól** — *Jak zdefiniowano*, `snake_case`, `camelCase` lub `PascalCase` dla pól najwyższego poziomu (wartości wewnątrz zmian i szczegółów logowania zachowują swoje nazwy). **Format czasu** — ISO 8601, czas Unix w milisekundach albo w sekundach z trzema miejscami po przecinku (styl `_time` Splunka). Oba działają tylko tam, gdzie zapisywany jest dokument JSON profilu natywnego lub Splunk CIM (`json`, `ndjson`, `rfc5424`); ECS, OCSF i formaty liniowe zachowują własne nazwy i czasy.
- **MSGID syslog** — *Kategoria zdarzenia* (domyślnie), *Kod zdarzenia*, *Własny tekst* (1–32 drukowalne znaki bez spacji, np. `security-journal`, aby zachować wyszukiwania sprzed 1.2.19) albo *Brak* (`-`); **APP-NAME syslog** — puste wysyła `clm`. Mają je tylko miejsca docelowe syslog.

Kształtowanie dotyczy każdego sieciowego miejsca docelowego i każdego formatu; archiwum plikowe zawsze zachowuje pełny rekord. Zmiana kształtowania dotyczy zdarzeń eksportowanych od tej chwili. Karta zapisanego miejsca docelowego podaje kształtowanie, np. *Oszczędne · wykluczenia: 1 · MSGID Kod zdarzenia*.

25 Mapowanie pól

Sieciowe miejsce docelowe z formatem kanonicznym (`ndjson`, `rfc5424`, `cef`, `leef-1.0`, `leef-2.0`, `kv`, `otlp-protobuf`, `otlp-json`) może mapować pola zdarzenia kanonicznego, zanim zapisze je którykolwiek format. Reguły są częścią miejsca docelowego: zapisywane razem z nim, wersjonowane razem z nim (zapis z nieaktualną wersją jest odrzucany) i rejestrowane w dzienniku z miejscem docelowym przed zmianą i po niej (`siem.destination.updated`).

Reguła	Działanie
Zmień nazwę (`rename`)	Przenosi pole kanoniczne pod nową nazwę (pole własne)
Usuń (`drop`)	Usuwa pole kanoniczne (lista zabronionych)
Zachowaj (`keep`)	Lista dozwolonych: przy co najmniej jednej regule Zachowaj każde pole opcjonalne, które nie jest zachowane ani przemianowane, jest usuwane
Dodaj stałą (`add`)	Dodaje pole własne ze stałym tekstem o długości najwyżej 256 znaków

Najpierw działają reguły Zachowaj, potem zmiana nazwy, usunięcie i dodanie w swojej kolejności. Pól `schema_version`, `event_id`, `event_code`, `category`, `action`, `outcome`, `outcome_original`, `severity`, `severity_label`, `message`, `timestamp`, `observed_timestamp`, `export_timestamp`, `application`, `service_name` i `organization_kind` nigdy nie można usunąć ani przemianować, więc identyfikacja, czas, kategoria i wynik pozostają w każdym zdarzeniu. Nowa nazwa ma 1–64 znaki, zaczyna się literą i zawiera litery, cyfry, podkreślenia i kropki (CEF: tylko litery i cyfry; ECS i OCSF: bez kropek); nie może zaczynać się od `certyx`, powtarzać innej nowej nazwy ani być równa polu kanonicznemu lub kluczowi zapisywanemu przez sam format (na przykład `dst` w CEF albo `server.address` w OTLP). Najwyżej 32 reguły; każde pole występuje w najwyżej jednej regule zmiany nazwy lub usunięcia.

Gdzie pojawia się wynik: usunięte pola znikają z każdego formatu (KV pomija ich klucze); pola własne następują po polach formatu — w dokumencie JSON (NDJSON, MSG RFC 5424, `event` HEC), pod `labels` w ECS (jako tekst), pod `unmapped` w OCSF, jako rozszerzenia w CEF i atrybuty w LEEF, jako klucze w KV i jako atrybuty rekordu dziennika w OTLP. Pola indeksowane HEC i pola Splunk CIM zachowują swoje standardowe nazwy. Rekord JSON, wiersze Sentinel, układy pierwszego wydania i archiwa plików (które przechowują pełne zdarzenie) nie mają mapowania pól.

Podgląd. Podgląd zdarzenia testowego wysyła formularz w obecnym, jeszcze niezapisanym stanie do serwera, który tworzy zdarzenie testowe zakresu po regułach w wybranym transporcie, formacie i kodowaniu: treść webhooka, kopertę HEC, komunikat syslog, wiersz Sentinel, żądanie OTLP (protobuf pokazany w kodowaniu OTLP/JSON, z rozmiarem binarnej treści) albo wiersz archiwum. Nic nie jest wysyłane do odbiorcy ani zapisywane. Nieprawidłowa reguła jest odrzucana z podaniem przyczyny.

API: treść zapisu niesie reguły w `fieldMapping`, na przykład

```
"fieldMapping": [
  {"op": "rename", "field": "user_id", "to": "account"},
  {"op": "drop", "field": "host_ip"},
  {"op": "add", "to": "region", "value": "eu-central"}
]
```

a `POST /api/administration/siem/preview` (organizacja) lub `POST /platform/api/siem/{scope}/preview` (platforma; bez kodu step-up, nic nie zmienia) przyjmuje tę samą treść co zapis i odpowiada `{transport, format, profile, eventId, contentType, payload, bytes, canonical}`.

Format `kv` z powyższymi regułami (user_id przemianowane na `account`, `host_ip` usunięte, `region` dodane), zdarzenie testowe:

```
<86>1 2026-10-19T04:20:37.893Z certyx-node-1 clm 1 integration [timeQuality tzKnown="1"][origin software="CERTYX CLM"
swVersion="1.0.0"] schema_version=certyx.event/1.0 event_id=f4293b79-ca2c-4fd2-a9d5-6490b28aee56 event_code=INTEGRATION-001
category=integration action=siem.test outcome=success outcome_original=business severity=3 severity_label=low
message="siem.test by siem-test" timestamp=2026-10-19T04:20:37.893Z observed_timestamp=2026-10-19T04:20:37.893Z
export_timestamp=2026-10-19T04:20:37.893Z application="CERTYX CLM" version=1.0.0 environment=production hostname=certyx-node-1
service_name=clm component=siem organization_id=platform organization_name=- organization_kind=platform username=- user_role=-
session_id=- authentication_method=- user_verified=- user_agent=- src_ip=- src_port=- http_method=- http_route=- http_status=-
protocol=- correlation_id=f4293b79-ca2c-4fd2-a9d5-6490b28aee56 request_id=f4293b79-ca2c-4fd2-a9d5-6490b28aee56 trace_id=-
resource_type=- resource_id=- change_type=- reason=- error_type=- sequence=- event_hash=- agent_fingerprint=- changes="
[{\"action\":\"siem.test\",\"requestedBy\":\"admin\"}]" changes_redacted=- dst_ip=- dst_port=- span_id=- account=siem-test
region=eu-central
```

26 Pola wzbogacenia

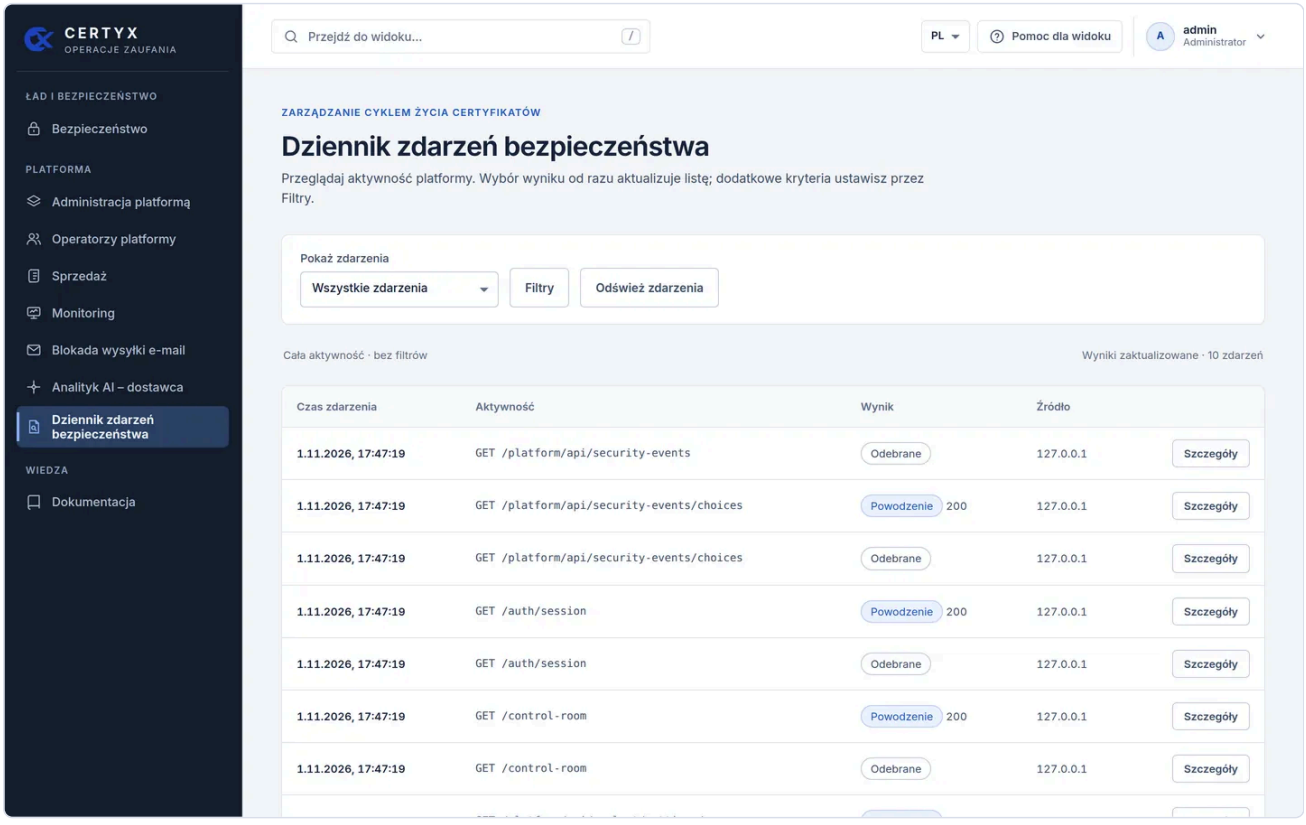
Od tego wydania CERTYX zapisuje obok wpisu dziennika te informacje o każdym żądaniu (w osobnej tabeli z kluczem w postaci numeru sekwencyjnego, poza łańcuchem skrótów, dzięki czemu skrót dziennika nadal można zweryfikować):

Pole	Zawartość	Uwagi
`trace_id`	Identyfikator śledzenia W3C aktywności żądania	Przychodzący nagłówek `traceparent` jest kontynuowany, więc identyfikator pasuje do śladu wywołującego
`src_port`	Port źródłowy klienta	Za serwerem pośredniczącym — port tego serwera
`host_ip`	Adres serwera, który przyjął połączenie	Za serwerem pośredniczącym lub w sieci kontenerów — adres lokalnego interfejsu; `origin ip` w RFC 5424

Pole	Zawartość	Uwagi
`dst_port`	Port serwera, który przyjął połączenie	`dst_ip` to ten sam adres co `host_ip`; za odwrotnym proxy lub w sieci kontenerów — lokalny port nasłuchu (na przykład 8080), a nie port publiczny
`span_id`	Identyfikator span W3C aktywności żądania	Razem z `trace_id` daje TraceId i SpanId rekordu dziennika OTLP
`user_role`	Rola (claim) zalogowanego podmiotu	
`session_id`	Identyfikator korelacji sesji: dla sesji po stronie serwera (konsola lub aplikacja mobilna) pierwsze 32 znaki szesnastkowe skrótu SHA-256 z `clm-session` i skrótu SHA-256 identyfikatora sesji; dla starszej sesji przeglądarki skrótu SHA-256 z `clm-session`, podmiotu i czasu logowania	Taki sam dla każdego żądania jednej sesji; nigdy nie jest plikiem cookie sesji, identyfikatorem sesji ani zapisanym kluczem sesji

Dostępność. Wpisy zapisane przed tym wydaniem, wpisy biznesowe (zmiany poza żądaniem) i zdarzenia testowe nie mają wzbogacenia; ich pola są nieznane (pomijane w JSON, puste w CSV, `-` w KV). Żądania agentów i kluczy API oraz sesje aplikacji mobilnej rozpoczęte przed tym wydaniem mają tylko część tych pól (bez `session_id`). `dst_port` i `span_id` są zapisywane od wydania z OpenTelemetry. Przekazywany nagłówek hosta nigdy nie jest używany jako cel, bo może go ustawić klient. Zdarzenia agentów i punktów końcowych, które wskazują obserwowany cel (alert wykrywania podaje swój punkt końcowy `host:port`), biorą `dst_ip` i `dst_port` z tego celu; nazwa hosta nie daje `dst_ip`. Te pola występują tylko w formatach i profilach kanonicznych; układy z pierwszego wydania pozostają bez zmian.

27 Wiele organizacji w jednym SIEM



Dziennik zdarzeń bezpieczeństwa w panelu operatora, w którym zarządza się miejscami docelowymi SIEM całej platformy (dane przykładowe)

Każde eksportowane zdarzenie identyfikuje swoją organizację, więc kilka organizacji — albo zakres operatora *Wszystkie zdarzenia* — może współdzielić jeden indeks SIEM. Pola są dodawane podczas eksportu; sam rekord dziennika powiązany łańcuchem skrótów nie jest zmieniany, więc skrót nadal można zweryfikować.

Znaczenie	Kanoniczne	Rekord JSON / HEC (`json`)	CEF (`cef`)	LEEF	Sentinel	CSV (`csv`, `compat`)
Identyfikator organizacji	`organization_id`	`Tenant`	`cs1`	`organization`	`Organization`	`OrganizationId`
Nazwa organizacji	`organization_name`	`OrganizationName`	`cs2`	`organizationName`	`OrganizationName`	`OrganizationName`
Rodzaj: `organization`, `platform`, `unattributed`	`organization_kind`	`OrganizationKind`	—	`organizationKind`	`OrganizationKind`	`OrganizationKind`
Instancja CERTYX	`hostname`	`Instance` (HEC także `host`)	`dvchost`	`instance`	`Instance`	`Instance`

W `cef-compat` organizacją jest `cs1`, a jej nazwą i rodzajem są `certyxOrganizationName` i `certyxOrganizationKind`. `platform` oznacza zdarzenia operatorów i nieudane logowania do platformy; `unattributed` oznacza żądania bez zalogowanej organizacji (przed zalogowaniem, wywołania anonimowe, sondy kondycji). Nazwa to nazwa organizacji na liście klientów platformy; jest pusta (nieznana), gdy instalacja nie ma administracji platformą. Do reguł dostępu i usuwania duplikatów używaj identyfikatora, a nie nazwy — nazwa może się zmienić.

Splunk:

```
index=clm sourcetype=certyx:event organization_kind=organization
| stats count by organization_name, organization_id, category
```

Cribl, aby kierować organizacje do osobnych indeksów: funkcja *Eval* z `index = 'clm_' + organization_id.substring(0, 8)` (albo tabela wyszukiwania (lookup) z identyfikatora organizacji na indeks), umieszczona po funkcji JSON *Parser*. Kontrola dostępu Splunk oparta na rolach może wtedy ograniczyć użytkowników każdej organizacji do jej indeksu.

28 Archiwa plikowe

Transport `file` zapisuje każde zdarzenie swojego zakresu do plików dziennych na serwerze CERTYX zamiast wysyłać je przez sieć. Używaj go, aby przechowywać pełny zapis bezpieczeństwa przez wymagany okres poza SIEM, a do SIEM wysyłać tylko to, czego potrzebuje (Wysyłaj tylko).

Format × profil	Nazwa pliku	Zawartość
`csv-compat`	`certyx-security-YYYY-MM-DD.csv`	Kolumny z pierwszego wydania (poniżej)
`csv`	`certyx-events-YYYY-MM-DD.csv`	Kolumny kanoniczne w stałej kolejności wersji schematu, `schema_version` jako pierwsza, `event_id` jako druga
`ndjson` × `native` / `ecs` / `ocsf`	`certyx-events-YYYY-MM-DD.ndjson`	Jeden dokument profilu na wiersz

28.1 Konfiguracja

1. **Organizacja:** administrator (Admin) zalogowany z MFA otwiera **Eksport do SIEM**. **Platforma:** operator otwiera **Dziennik zdarzeń bezpieczeństwa** → **Eksport do SIEM** i wybiera zakres *Operatorzy platformy* lub *Wszystkie zdarzenia*.
2. Nazwa miejsca docelowego i identyfikator (na przykład `csv-archive`), Transport **Archiwum plikowe**, Format `csv-compat`, `csv` lub `ndjson` (z jego profilem).
3. **Okres przechowywania (dni)**: 1–3650. Starsze pliki dzienne są usuwane automatycznie.
4. Opcjonalnie **Kompresuj zamknięte dni gzip** (`.csv.gz`, `.ndjson.gz`).
5. Zapisz, a następnie **Sprawdź połączenie**: sprawdza, czy do katalogu archiwum można zapisywać, i pokazuje liczbę plików, zajmowane przez nie miejsce oraz wolne miejsce na woluminie.

Archiwum zachowuje każde zdarzenie: nie ma filtra wyników, ważności, kategorii ani kodów, nie ma wartości dostarczania, certyfikatu klienta ani zdarzenia testowego. Każde archiwum wlicza się do limitu miejsc docelowych swojego zakresu.

Lokalizacja. Organizacja nie może wybrać ścieżki: jej pliki znajdują się w katalogu konfigurowanym przez operatora platformy, `<Clm:Siem:ArchiveRoot>/organizations/<organization ID>/<archive identifier>/` (domyślny `ArchiveRoot`: `siem-archive` w katalogu danych CERTYX). Archiwa obejmujące całą platformę znajdują się w `<Clm:Siem:PlatformArchiveDirectory>/<platform|all>/<archive identifier>/` (domyślnie `<ArchiveRoot>/platform`). Katalogi i pliki są tworzone z prawem odczytu wyłącznie dla konta usługi CERTYX; ścieżka zawierająca dowiązanie symboliczne jest odrzucana.

28.2 Pliki

- Jeden plik na każdy dzień UTC, w którym zapisano zdarzenia. Pierwszy plik nowego archiwum zawiera przechowywaną historię dziennika, a kolejne — zdarzenia z danego dnia.
- **CSV (`csv-compat`, `csv`)**: RFC 4180, UTF-8 bez znacznika kolejności bajtów (BOM), wiersz nagłówka, przecinek jako separator, końce wierszy CRLF, cudzysłowy podwojone. Znaki sterujące wewnątrz wartości są zamieniane na spacje (`csv-compat`) albo pozostają wewnątrz cudzysłowów (`csv`), więc każdy rekord jest jednym rekordem CSV. `csv-compat` ujmuje w cudzysłowy każdą komórkę. `csv` odróżnia wartość nieznaną od pustej: wartość nieznana to puste pole bez cudzysłowów, a znana pusta wartość to `""`.
- **Ochrona przed wstrzykiwaniem formuł:** komórka zaczynająca się od `=`, `+`, `-`, `@` (także po spacjach), tabulatora lub znaku powrotu karetki jest poprzedzana znakiem `'`, dzięki czemu arkusze kalkulacyjne pokazują ją jako tekst.
- Kolumny `csv-compat`: `Sequence`, `At` (UTC), `OrganizationId`, `OrganizationName`, `OrganizationKind`, `Instance`, `Actor`, `SourceIp`, `AgentFingerprint`, `Method`, `Route`, `Status`, `Outcome`, `Severity`, `TraceId`, `ErrorType`, `SignInAction`, `SignInUser`, `SignInMethod`, `SignInResult`, `SignInReason`, `Changes` (tablica JSON), `PreviousHash`, `Hash`.
- Kolumny `csv`: pola kanoniczne w kolejności z sekcji Opis pól; nowe pole jest dopisywane wyłącznie na końcu, wraz z nową wersją schematu.
- **NDJSON (`ndjson`)**: UTF-8 bez znacznika kolejności bajtów, jeden dokument JSON na wiersz zakończony znakiem LF, bez nagłówka.
- **Pieczętowanie i integralność.** Po zakończeniu dnia UTC plik tego dnia jest pieczętowany w następnym przebiegu eksportu: kompresowany gzip, gdy kompresja jest włączona, a jego SHA-256 jest dopisywany do manifestu `SHA256SUMS` w tym samym katalogu. Pobrane archiwum sprawdzisz poleceniem `sha256sum -c SHA256SUMS` (pliku bieżącego dnia nie ma w manifeście, dopóki nie zostanie zapieczętowany). W `csv-compat` kolumny `Hash` i `PreviousHash` łączą każdy wiersz z łańcuchem dziennika weryfikowanym w **Dziennik zdarzeń bezpieczeństwa → Sprawdź integralność dziennika**; formaty kanoniczne zawierają `event_hash`.
- **Okres przechowywania.** W każdym przebiegu eksportu pliki z dni starszych niż okres przechowywania są usuwane wraz z ich wierszami manifestu; każde usunięcie jest zapisywane w dzienniku jako `siem.archive.expired` (kod `INTEGRATION-009`) z nazwami plików (wykonawca `system:siem-archive`).

28.3 Pobieranie

Na karcie archiwum **Pliki archiwum** wyświetla każdy plik z jego rozmiarem, informacją, czy jest zapieczętowany, oraz jego SHA-256. **Pobierz** pobiera jeden plik, **Pobierz wszystkie (zip)** — wszystkie pliki wraz z manifestem. Pobieranie wymaga sesji zalogowanej z MFA (tak jak zmiany) i jest odrzucane dla sesji aplikacji mobilnej; każde pobranie jest zapisywane w dzienniku jako `siem.archive.downloaded` (kod `DATA-003`) z nazwami plików. Do wyświetlenia listy plików wystarcza rola Admin (organizacja) lub administracja platformą (operator). Operator może też skopiować pliki bezpośrednio z woluminu archiwum.

28.4 Dostarczanie, ponowne uruchomienia i miejsce na dysku

- Archiwum używa tej samej trwałej pozycji co sieciowe miejsca docelowe: wiersze są zapisywane i zrzucane na dysk, a dopiero potem pozycja się przesuwa (co najmniej jednokrotnie, nic nie jest pomijane). Po awarii między tymi krokami następny przebieg najpierw odczytuje ostatni kompletny wiersz otwartego pliku (jego numer sekwencyjny, z `Sequence` lub z identyfikatora zdarzenia), usuwa wiersz ucięty przez awarię i kontynuuje za nim, więc plik nigdy nie zawiera wiersza dwukrotnie. Wiersz może pojawić się w dwóch plikach tylko wtedy, gdy podczas takiej awarii zmienił się dzień.
- Do `Clm:Siem:BatchSize` zdarzeń (domyślnie 200) na przebieg, jeden przebieg co `Clm:Siem:Interval` (domyślnie 30 sekund); nowe archiwum nadrabia historię w tym tempie.

- **Do katalogu archiwum CSV nie można zapisywać (...)** zaplanuj około 0,5–1 KB na zdarzenie bez kompresji dla `csv-compat`, więcej dla `csv` i `ndjson` (więcej pól); gzip zwykle zmniejsza to do jednej dziesiątej. Monitoruj wolumin — pełny dysk lub brak woluminu powoduje błąd archiwum *Do katalogu archiwum CSV nie można zapisywać (...)*, zgłasza incydent `siem-delivery` i zatrzymuje pozycję, więc archiwum kontynuuje po zwolnieniu miejsca.
- W instalacji z wieloma instancjami każda instancja musi montować ten sam katalog archiwum (eksport działa naraz tylko na jednej instancji, ale nie zawsze na tej samej).
- Usunięcie miejsca docelowego archiwum zatrzymuje zapis i kasuje jego pozycję; pliki pozostają w katalogu, dopóki operator ich nie usunie. Ponowne dodanie z tym samym identyfikatorem kontynuuje w tym samym katalogu.

29 Uprawnienia

Działanie	Miejsca docelowe organizacji	Zakresy platformy (*Operatorzy platformy*, *Wszystkie zdarzenia*)
Wyświetlanie miejsc docelowych, stanu, listy plików archiwum	Rola Admin	Administracja platformą
Sprawdzenie połączenia, wysłanie zdarzenia testowego	Admin z sesją MFA	Operator platformy z sesją MFA
Zapisywanie, edycja, usuwanie, nowy sekret	Admin z sesją MFA	Operator platformy z sesją MFA i kodem podwyższenia uprawnień operatora
Ponowne wysyłanie od numeru sekwencyjnego lub czasu	Admin z sesją MFA	Operator platformy z sesją MFA i kodem podwyższenia uprawnień operatora
Pobieranie plików archiwum	Admin z sesją MFA	Operator platformy z sesją MFA

Sesje aplikacji mobilnej nie mogą zmieniać, testować, wysyłać ponownie ani pobierać. Każda zmiana, sprawdzenie, test, ponowne wysłanie, pominięcie i pobranie jest zapisywane w dzienniku bezpieczeństwa (kody `CONFIG-008`, `INTEGRATION-002`, `INTEGRATION-003`, `INTEGRATION-012`, `INTEGRATION-011`, `DATA-003`).

30 Rozwiązywanie problemów

30.1 Incydenty

Incydent	Ważność	Znaczenie	Co zrobić
`siem-delivery`	ostrzeżenie; krytyczny po tylu następujących po sobie niepowodzeniach, ile wynosi *Próby przed alertem krytycznym*	Ostatnie dostarczenie do miejsca docelowego nie powiodło się; przyczyna jest na karcie (a w przypadku odrzuconego zdarzenia podaje identyfikator zdarzenia)	Uruchom *Sprawdź połączenie*; napraw odbiorcę; w przypadku odrzuconego zdarzenia zob. Odrzucone zdarzenia
`siem-backlog`	ostrzeżenie	Czeka więcej zdarzeń, niż wynosi limit alarmu zaległości miejsca docelowego; nic nie zostaje pominięte	Usuń przyczynę błędu dostarczania albo zwiększ rozmiar paczki lub limit, gdy odbiorca jest jedynie wolny

Oba incydenty zamykają się samoczynnie: `siem-delivery` po następnym udanym dostarczeniu, `siem-backlog`, gdy zaległości spadną poniżej limitu.

30.2 Wyniki sprawdzenia i zdarzenia testowego

Kod	Znaczenie	Co zrobić
`dns-failed`	Serwer CERTYX nie może rozwiązać nazwy hosta	Popraw nazwę albo dodaj ją do DNS używanego przez serwer CERTYX; nazwy wewnętrzne muszą być rozwiązywane na serwerze, nie tylko na Twoim komputerze

Kod	Znaczenie	Co zrobić
`dns-private`	Host wskazuje na adres prywatny, pętli zwrotnej lub link-local, a operator ograniczył miejsca docelowe organizacji do adresów publicznych	Użyj adresu publicznego albo poproś operatora o zezwolenie na prywatne miejsca docelowe (`Clm:Siem:AllowPrivateDestinations`)
`tcp-refused`	Nic nie nasłuchuje na porcie albo zapora odrzuca połączenie	Włącz wejście odbierające na tym porcie; sprawdź numer portu
`tcp-unreachable`	Brak trasy sieciowej z serwera CERTYX do adresu	Sprawdź routing i zapory między serwerem a odbiorcą
`tcp-timeout`	Brak odpowiedzi w limicie czasu (domyślnie 10 sekund)	Prawdopodobnie zapora porzuca połączenie; zezwól na TCP z serwera CERTYX
`tls-timeout`	Połączenie TCP nawiązane, ale bez uzgadniania TLS	Wejście jest zwykłym TCP; włącz na nim TLS (Cribl: ustawienia TLS źródła; Splunk: `[tcp-ssl:<port>]` lub HEC z Enable SSL)
`tls-handshake-failed`	Odbiorca zamknął połączenie podczas uzgadniania	Włącz TLS na wejściu; oferuj TLS 1.2 lub 1.3; gdy odbiorca wymaga certyfikatu klienta, dodaj go (mTLS) albo sprawdź, czy wystawiło go CA, któremu ufa odbiorca
`tls-name-mismatch`	Certyfikat nie zawiera wpisanego hosta	Wpisz nazwę hosta zawartą w certyfikacie albo zainstaluj certyfikat dla tej nazwy (`SplunkServerDefaultCert` Splunk nigdy nie pasuje)
`tls-expired`	Certyfikat odbiorcy jest poza okresem ważności	Odnów certyfikat odbiorcy
`tls-untrusted`	Certyfikat nie prowadzi do systemowego magazynu zaufanych certyfikatów albo jest unieważniony (w trybie hard-fail: jego status unieważnienia jest nieznany)	Wklej certyfikat głównego CA (PEM) w polu Zaufane certyfikaty główne; wymień unieważniony certyfikat; w trybie hard-fail zapewnij osiągalność adresu CRL/OCSP albo wybierz soft-fail
`tls-untrusted-roots`	Certyfikat nie prowadzi do certyfikatów głównych wklejonych dla tego miejsca docelowego albo nie przechodzi sprawdzania unieważnienia	Wklej certyfikat główny, który faktycznie wystawił certyfikat odbiorcy; w sprawie unieważnienia — jak wyżej
`hec-refused`	Splunk odrzucił zdarzenie z kodem HEC	Zob. tabelę kodów HEC poniżej
`hec-status`	Splunk odpowiedział błędem HTTP bez kodu HEC (często serwer pośredniczący lub błędna ścieżka)	Użyj `/services/collector/event` ; sprawdź serwery pośredniczące po drodze
`hec-not-acknowledged`	Splunk przyjął paczkę, ale nie potwierdził indeksowania w ciągu 30 sekund	Sprawdź kondycję indeksera i potwierdzanie indeksowania dla tokenu; paczka zostanie wysłana ponownie
`entra-refused`	Microsoft Entra odrzucił poświadczenia aplikacji	Sprawdź identyfikator dzierżawy, identyfikator aplikacji (klienta) i wartość Value klucza tajnego (nie jego identyfikator); odnów wygasły klucz tajny
`http-status`	Odbiorca odpowiedział błędem HTTP	400/422: odbiorca odrzuca dane (zob. Odrzucone zdarzenia); 401/403: wpisz ponownie token lub sekret, a w przypadku Sentinel sprawdź przypisanie roli; 404: błędna ścieżka, niezmienny identyfikator DCR lub strumień; 413: paczka jest za duża dla odbiorcy — zmniejsz rozmiar paczki; 429/503: odbiorca przeciążony, ponowienie z wycofywaniem; 5xx: sprawdź dzienniki odbiorcy
`delivery-failed`	Połączenie lub zapis nie powiódł się po etapie TLS	Zob. pokazaną przyczynę (na przykład *Miejsce docelowe nie odpowiedziało na czas.*)
`archive-unwritable`	Do katalogu archiwum nie można zapisywać	Poproś operatora o sprawdzenie woluminu archiwum, jego uprawnień i wolnego miejsca (`Clm:Siem:ArchiveRoot`)
`archive-link`	Ścieżka archiwum zawiera dowiązanie symboliczne	Operator musi skonfigurować ścieżkę archiwum bez dowiązań symbolicznych

30.3 Odbiorca pokazuje fragmenty lub dane binarne

Co widać w SIEM (`raw`)	Przyczyna	Co zrobić
Rekordy zaczynające się od liczby i spacji (`412 <84>1 2026-…`), liczba doklejona do końca rekordu (`… }4`), rekordy ucięte w połowie (`<86>1 2026-10-11T1`)	CERTYX używa zliczania oktetów, a odbiorca dzieli strumień na znakach nowego wiersza (źródło syslog Cribl z *Octet count framing* No, ustawieniem domyślnym)	Ustaw na źródle *Octet count framing* Yes albo wybierz w CERTYX ramkowanie *Nowa linia* — tak samo po obu stronach
Zdarzenia binarne zaczynające się od `\x16\x03` (często pokazywane jako `\x16\x03\x01…`), zawierające nazwę hosta odbiorcy (na przykład `cribl-worker1…`)	Port odbierający ma wyłączony TLS; indeksuje komunikat TLS ClientHello wysłany przez CERTYX	Włącz TLS na źródle/wejściu (Cribl: *TLS Settings → Enabled*); CERTYX nigdy nie wysyła zwykłego TCP
`` , `ï»¿` lub `` przed JSON komunikatu `rfc5424`	Odbiorca pokazuje znacznik kolejności bajtów UTF-8 (RFC 5424 MSG-UTF8) jako tekst	Usuń go w parserze odbiorcy albo poproś operatora o ustawienie `Clm:Siem:Syslog:ByteOrderMark=false`
Zdarzenia z `/health/ready` z `Tenant unattributed` co kilka sekund	Load balancer sprawdza gotowość; wersje sprzed tego wydania eksportowały sondy	Bieżące wersje nie wysyłają sond (`Clm:Siem:ExportHealthProbes` , domyślnie wyłączone)
Każde żądanie pojawia się dwukrotnie (`attempt` , potem `success` / `denied` /…)	W *Wysyłaj tylko* zaznaczono *Odebrane żądania*	Odznacz je; gdy żadne pole nie jest zaznaczone, miejsce docelowe dostaje jeden rekord na żądanie
To samo zdarzenie pojawia się dwukrotnie z tym samym identyfikatorem zdarzenia	Dostarczanie co najmniej jednokrotne po przekroczeniu czasu lub ponownym wysłaniu	Usuwaj duplikaty według identyfikatora zdarzenia (Usuwanie duplikatów)
Wartości `host` lub `source` takie jak `http:clm` albo adres workera Cribl	Ustawione przez potok przekazujący (na przykład wyjście HEC w Cribl), a nie przez CERTYX	Użyj `hostname` / `Instance` i pól organizacji ze zdarzenia albo ustaw `host` funkcją Eval w Cribl
Pola Splunk z dwiema identycznymi wartościami (`event_id` , `action`)	Pole jest zarazem polem indeksowanym HEC i częścią zdarzenia JSON	Zob. props.conf i Splunk CIM

30.4 Kody Splunk HEC

Kod	Tekst Splunk	Co zrobić
1	Token disabled	Włącz token w *HTTP Event Collector*
2	Token is required	Wpisz token HEC
3	Invalid authorization	Wpisz wartość tokenu dokładnie tak, jak pokazuje ją Splunk
4	Invalid token	Zapisany token jest nieznany dla Splunk; wpisz prawidłowy token
5	No data	Traktowane jako odrzucenie danych (Odrzucone zdarzenia); sprawdź serwery pośredniczące, które mogłyby usuwać treść żądania
6	Invalid data format	Użyj `/services/collector/event` (nie `/raw`); traktowane jako odrzucenie danych
7	Incorrect index	Dodaj indeks do Allowed indexes tokenu albo popraw nazwę indeksu
8	Internal server error	Sprawdź kondycję indeksera Splunk
9	Server is busy	Splunk jest przeciążony; dostarczenie zostanie ponowione z wycofywaniem
10	Data channel is missing	Prawdopodobnie serwer pośredniczący usuwa nagłówek `X-Splunk-Request-Channel`
11	Invalid data channel	Wyłącz i ponownie włącz indexer acknowledgement dla tokenu
12, 13	Event field is required / cannot be blank	Użyj `/services/collector/event` ; traktowane jako odrzucenie danych
14	ACK is disabled	Nie wymaga działania; nie wpływa na dostarczanie
15	Error in handling indexed fields	Traktowane jako odrzucenie danych; sprawdź limity pól indeksowanych w Splunk
16	Query string authorization is not enabled	Nie wymaga działania; CERTYX używa uwierzytelniania w nagłówku

Kod	Tekst Splunk	Co zrobić
18, 19, 20	HEC is unhealthy	Kolejki są pełne lub potwierdzanie jest niedostępne; dostarczenie zostanie ponowione z wycofywaniem

30.5 Stan dostarczania na karcie miejsca docelowego

Ostatni błąd	Co zrobić
Nie udało się połączyć z miejscem docelowym.	Uruchom Sprawdź połączenie; wskaże ono nieudany etap
Weryfikacja TLS miejsca docelowego nie powiodła się.	Uruchom Sprawdź połączenie; zob. kody TLS powyżej
Miejsce docelowe nie odpowiedziało na czas.	Odbiorca nie odpowiedział w ciągu 20 sekund; sprawdź jego obciążenie lub sieć
HTTP <status>	Zob. `http-status` powyżej
Splunk HEC odpowiedział HTTP <status> z kodem <n> (...)	Zob. tabelę kodów HEC
Odbiorca odrzuca zdarzenie <event ID>: ...	Zob. Odrzucone zdarzenia
Microsoft Entra odrzucił poświadczenia aplikacji.	Zob. `entra-refused`
Zapisanego sekretu nie można odszyfrować; wpisz go ponownie.	Edytuj miejsce docelowe i wpisz ponownie sekret (zmienił się pierścień kluczy serwera)
Nie można odczytać certyfikatu klienta ani jego klucza prywatnego; wpisz oba ponownie.	Edytuj miejsce docelowe i wklej ponownie certyfikat klienta oraz jego klucz
Miejsce docelowe wskazuje na adres prywatny, pętli zwrotnej lub link-local; ...	Zob. `dns-private`
Odbiorca przyjął połączenie TCP, ale nie zakończył uzgadniania TLS ...	Wejście odbierające ma wyłączony TLS; zob. Odbiorca pokazuje fragmenty lub dane binarne
Do katalogu archiwum CSV nie można zapisywać (...)	Poproś operatora o sprawdzenie woluminu archiwum, jego uprawnień i wolnego miejsca (`Clm:Siem:ArchiveRoot`)
Ścieżka archiwum CSV zawiera dowiązanie symboliczne; ...	Operator musi skonfigurować ścieżkę archiwum bez dowiązań symbolicznych

Nieudana paczka jest ponawiana po upływie opóźnienia ponowienia i zgłasza incydent `siem-delivery` (Dostarczanie). Pozycja nie przesuwa się, dopóki odbiorca nie przyjmie paczki.

30.6 Komunikaty formularza i uprawnień

- Każde odrzucone pole podaje oczekiwany format, na przykład *Host syslog: wpisz tylko nazwę hosta, a port (na przykład 10514) wpisz w polu Port.*
- *Format, profil schematu i transport: wybierz transport, a następnie jeden z oferowanych dla niego formatów i profili.* — ta kombinacja nie jest dozwolona (Dozwolone kombinacje).
- *Separator LEEF: ...* — separator deklaruje tylko `leef-2.0`; tabulator lub znak interpunkcyjny inny niż `=`, kreska pionowa i ukośnik odwrotny, albo jego kod szesnastkowy.
- *Wysyłaj tylko (kategorie) | Wysyłaj tylko (kody zdarzeń)* — tylko kategorie z listy; kody z katalogu, najwyżej 200.
- *Próby przed alertem krytycznym*, *Pierwsze opóźnienie ponowienia (sekundy)*, *Najdłuższe opóźnienie ponowienia (sekundy)*, *Rozmiar partii (zdarzenia)*, *Alert zaległości powyżej (zdarzenia)* — liczby całkowite z zakresów podanych w sekcji Dostarczanie; najdłuższe opóźnienie nie może być krótsze niż pierwsze.
- *Certyfikat klienta: ...* — jeden certyfikat PEM z pasującym niezaszyfrowanym kluczem prywatnym PEM, każdy najwyżej 64 KiB; nowy certyfikat wymaga swojego klucza.
- *Archiwum plików zachowuje każde zdarzenie: ponawianie dostarczania, pomijanie odrzuconych zdarzeń i certyfikat klienta nie mają zastosowania.*
- *Wyślij ponownie od: ...* — numer sekwencyjny (1 lub więcej) albo czas, nie oba naraz, w pozycji miejsca docelowego lub przed nią; niedostępne dla archiwów plikowych.
- *Przy zmianie formatu podaj ponownie sekret.* — zapisany sekret należy do swojego transportu.

- *Miejsce docelowe zostało w międzyczasie zmienione, już istnieje lub osiągnięto limit.* — odśwież widok; po osiągnięciu limitu usuń nieużywane miejsce docelowe.
- *Podaj sekret przed wysłaniem zdarzenia testowego.* — webhook, Splunk HEC i Sentinel najpierw potrzebują swojego sekretu.
- Komunikat MFA podaje przyczynę: brak potwierdzonej aplikacji uwierzytelniającej, niepotwierdzona rejestracja, sesja rozpoczęta przed MFA, logowanie firmowe bez zgłoszonego MFA lub sesja tylko z hasłem. Wykonaj wyświetloną instrukcję, a następnie zaloguj się ponownie.

31 Przykładowe zdarzenia

Każdy przykład to zdarzenie testowe działającego serwera CERTYX w danym formacie i profilu (kod zdarzenia `INTEGRATION-001`); wartości zależne od instalacji będą w Twojej instalacji inne.

Przykłady zarejestrowano 19.10.2026 na serwerze CERTYX z domyślnymi ustawieniami syslog (facility authpriv, APP-NAME `clm`, bez numeru przedsiębiorstwa, więc bez elementu `certyx@…`) oraz `Clm:Siem:Environment=production`. Przykłady syslog pokazują jedną wiadomość bez prefiksu długości (octet counting); `<BOM>` oznacza znacznik kolejności bajtów UTF-8. Archiwum plikowe nie otrzymuje zdarzenia testowego, więc jego przykłady to pierwsze wpisy dziennika zapisane przez eksport.

31.1 Webhook HTTPS

Format `json` (tablica JSON rekordów):

```
[{"Sequence":0,"At":"2026-10-19T04:20:31.2998647+00:00","Category":"integration","EventCode":"INTEGRATION-001","Tenant":"platform","OrganizationName":"","OrganizationKind":"platform","Instance":"certyx-node-1","Actor":"siem-test","SourceIp":"system","AgentFingerprint":"","Method":"INTERNAL","Route":"business/siem.test","Status":200,"Outcome":"business","TraceId":"ecb63792-0af6-4902-b5c1-4a8b409b82ce","ErrorType":"","Changes":[{"action":"siem.test","requestedBy":"admin"}],"Hash":"","EventId":"ecb63792-0af6-4902-b5c1-4a8b409b82ce"}]
```

Format `ndjson`, profil `native`:

```
{"schema_version":"certyx.event/1.0","event_id":"c6030d2e-e437-4a96-a118-688cc908e6f9","event_code":"INTEGRATION-001","category":"integration","action":"siem.test","outcome":"success","outcome_original":"business","severity":3,"severity_label":"low","message":"siem.test by siem-test","timestamp":"2026-10-19T04:20:31.764Z","observed_timestamp":"2026-10-19T04:20:31.764Z","export_timestamp":"2026-10-19T04:20:31.764Z","application":"CERTYX CLM","version":"1.0.0","environment":"production","hostname":"certyx-node-1","service_name":"clm","component":"siem","organization_id":"platform","organization_kind":"platform","user_id":"siem-test","correlation_id":"c6030d2e-e437-4a96-a118-688cc908e6f9","request_id":"c6030d2e-e437-4a96-a118-688cc908e6f9","changes":[{"action":"siem.test","requestedBy":"admin"}]}
```

Format `ndjson`, profil `ecs`:

```
{"@timestamp":"2026-10-19T04:20:32.164Z","message":"siem.test by siem-test","ecs":{"version":"8.11.0"},"event":{"id":"81e697f9-214e-46c7-9b22-785f48e900a6","code":"INTEGRATION-001","kind":"event","category":["network"],"type":["connection"],"action":"siem.test","outcome":"success","severity":3,"created":"2026-10-19T04:20:32.164Z","dataset":"certyx.security","provider":"siem"},"user":{"id":"siem-test"},"host":{"hostname":"certyx-node-1"},"service":{"name":"clm","version":"1.0.0","environment":"production"},"organization":{"id":"platform"},"labels":{"schema_version":"certyx.event/1.0","certyx_category":"integration"}}
```

Format `ndjson`, profil `ocsf`:

```
{"class_uid":0,"category_uid":0,"activity_id":99,"type_uid":99,"severity_id":1,"status_id":1,"time":1792383632558,"message":"siem.test by siem-test","metadata":{"version":"1.1.0","uid":"d2bbe2f2-be7a-4963-903a-94a2c7790742","event_code":"INTEGRATION-
```

```
001","log_name":"security-journal","product":
{"name":"CLM","vendor_name":"CERTYX","version":"1.0.0"},"correlation_uid":"d2bbe2f2-be7a-4963-903a-94a2c7790742"},"unmapped":
{"certyx_schema_version":"certyx.event/1.0","certyx_category":"integration","certyx_action":"siem.test"}}
```


31.2 Splunk HEC

Format `json` (rekord z pierwszego wydania, pole indeksowane `event_id`):


```
{"time":1792383633.006,"host":"certyx-node-1","source":"certyx:security-journal","sourcetype":"certyx:security","event":
{"Sequence":0,"At":"2026-10-19T04:20:33.0060384+00:00","Category":"integration","EventCode":"INTEGRATION-
001","Tenant":"platform","OrganizationName":"","OrganizationKind":"platform","Instance":"certyx-node-1","Actor":"siem-
test","SourceIp":"system","AgentFingerprint":"","Method":"INTERNAL","Route":"business/siem.test","Status":200,"Outcome":"busin
ess","TraceId":"94ac6f46-f534-4fdc-95a5-ff0199cbc888","ErrorType":"","Changes":
[{"action":"siem.test","requestedBy":"admin"}],"Hash":"","EventId":"94ac6f46-f534-4fdc-95a5-ff0199cbc888"},"fields":
{"event_id":"94ac6f46-f534-4fdc-95a5-ff0199cbc888"}}
```


Format `ndjson`, profil `native`:


```
{"time":1792383633.454,"host":"certyx-node-1","source":"certyx:security-journal","sourcetype":"certyx:event","event":
{"schema_version":"certyx.event/1.0","event_id":"cbd516bc-2c12-497d-909d-66417ae5b605","event_code":"INTEGRATION-
001","category":"integration","action":"siem.test","outcome":"success","outcome_original":"business","severity":3,"severity_la
bel":"low","message":"siem.test by siem-test","timestamp":"2026-10-19T04:20:33.454Z","observed_timestamp":"2026-10-
19T04:20:33.454Z","export_timestamp":"2026-10-19T04:20:33.454Z","application":"CERTYX
CLM","version":"1.0.0","environment":"production","hostname":"certyx-node-
1","service_name":"clm","component":"siem","organization_id":"platform","organization_kind":"platform","user_id":"siem-
test","correlation_id":"cbd516bc-2c12-497d-909d-66417ae5b605","request_id":"cbd516bc-2c12-497d-909d-66417ae5b605","changes":
[{"action":"siem.test","requestedBy":"admin"}]},"fields":{"event_id":"cbd516bc-2c12-497d-909d-
66417ae5b605","event_code":"INTEGRATION-001","category":"integration"}}
```


Format `ndjson`, profil `ecs`:


```
{"time":1792383633.853,"host":"certyx-node-1","source":"certyx:security-journal","sourcetype":"certyx:event","event":
{"@timestamp":"2026-10-19T04:20:33.853Z","message":"siem.test by siem-test","ecs":{"version":"8.11.0"},"event":
{"id":"4bdad006-45f0-494e-a088-1857180b973c","code":"INTEGRATION-001","kind":"event","category":["network"],"type":
["connection"],"action":"siem.test","outcome":"success","severity":3,"created":"2026-10-
19T04:20:33.853Z","dataset":"certyx.security","provider":"siem"},"user":{"id":"siem-test"},"host":{"hostname":"certyx-node-
1"},"service":{"name":"clm","version":"1.0.0","environment":"production"},"organization":{"id":"platform"},"labels":
{"schema_version":"certyx.event/1.0","certyx_category":"integration"}},"fields":{"event_id":"4bdad006-45f0-494e-a088-
1857180b973c","event_code":"INTEGRATION-001","category":"integration"}}
```


Format `ndjson`, profil `ocsf`:


```
{"time":1792383634.227,"host":"certyx-node-1","source":"certyx:security-journal","sourcetype":"certyx:event","event":
{"class_uid":0,"category_uid":0,"activity_id":99,"type_uid":99,"severity_id":1,"status_id":1,"time":1792383634227,"message":"s
iem.test by siem-test","metadata":{"version":"1.1.0","uid":"05b4a4e8-c15b-439f-8051-d00980aca411","event_code":"INTEGRATION-
001","log_name":"security-journal","product":
{"name":"CLM","vendor_name":"CERTYX","version":"1.0.0"},"correlation_uid":"05b4a4e8-c15b-439f-8051-d00980aca411"},"unmapped":
{"certyx_schema_version":"certyx.event/1.0","certyx_category":"integration","certyx_action":"siem.test"}},"fields":
{"event_id":"05b4a4e8-c15b-439f-8051-d00980aca411","event_code":"INTEGRATION-001","category":"integration"}}
```


Format `ndjson`, profil `splunk-cim`:


```
{"time":1792383634.591,"host":"certyx-node-1","source":"certyx:security-journal","sourcetype":"certyx:event","event":
{"schema_version":"certyx.event/1.0","event_id":"38cd7f4b-5f1b-44c3-909c-695c0c9caf3c","event_code":"INTEGRATION-
```

```
001","category":"integration","action":"siem.test","outcome":"success","outcome_original":"business","severity":3,"severity_la
bel":"low","message":"siem.test by siem-test","timestamp":"2026-10-19T04:20:34.591Z","observed_timestamp":"2026-10-
19T04:20:34.591Z","export_timestamp":"2026-10-19T04:20:34.591Z","application":"CERTYX
CLM","version":"1.0.0","environment":"production","hostname":"certyx-node-
1","service_name":"clm","component":"siem","organization_id":"platform","organization_kind":"platform","user_id":"siem-
test","correlation_id":"38cd7f4b-5f1b-44c3-909c-695c0c9caf3c","request_id":"38cd7f4b-5f1b-44c3-909c-695c0c9caf3c","changes":
[{"action":"siem.test","requestedBy":"admin"}]},"fields":{"event_id":"38cd7f4b-5f1b-44c3-909c-
695c0c9caf3c","event_code":"INTEGRATION-001","category":"integration","vendor_product":"CERTYX
CLM","app":"clm","signature":"siem.test by siem-test","signature_id":"INTEGRATION-
001","severity":"informational","severity_id":"3","dest":"certyx-node-1","user":"siem-test","user_id":"siem-
test","action":"siem.test"}}
```


31.3 Syslog przez TLS

Format `json` (pierwsze wydanie, stały nagłówek):


```
<86>1 2026-10-19T04:20:34.960Z certyx-node-1 clm 1 integration [timeQuality tzKnown="1"] {"Sequence":0,"At":"2026-10-
19T04:20:34.9600107+00:00","Category":"integration","EventCode":"INTEGRATION-
001","Tenant":"platform","OrganizationName":"","OrganizationKind":"platform","Instance":"certyx-node-1","Actor":"siem-
test","SourceIp":"system","AgentFingerprint":"","Method":"INTERNAL","Route":"business/siem.test","Status":200,"Outcome":"busin
ess","TraceId":"e4828ba9-d4aa-46ef-bff7-82465c8f9598","ErrorType":"","Changes":
[{"action":"siem.test","requestedBy":"admin"}],"Hash":"","EventId":"e4828ba9-d4aa-46ef-bff7-82465c8f9598"}
```


Format `rfc5424`, profil `native`:


```
<86>1 2026-10-19T04:20:35.330Z certyx-node-1 clm 1 integration [timeQuality tzKnown="1"][origin software="CERTYX CLM"
swVersion="1.0.0"] <BOM>{"schema_version":"certyx.event/1.0","event_id":"75620e9f-9fe1-4f59-84d4-
5c1263f6c1fe","event_code":"INTEGRATION-
001","category":"integration","action":"siem.test","outcome":"success","outcome_original":"business","severity":3,"severity_la
bel":"low","message":"siem.test by siem-test","timestamp":"2026-10-19T04:20:35.330Z","observed_timestamp":"2026-10-
19T04:20:35.330Z","export_timestamp":"2026-10-19T04:20:35.330Z","application":"CERTYX
CLM","version":"1.0.0","environment":"production","hostname":"certyx-node-
1","service_name":"clm","component":"siem","organization_id":"platform","organization_kind":"platform","user_id":"siem-
test","correlation_id":"75620e9f-9fe1-4f59-84d4-5c1263f6c1fe","request_id":"75620e9f-9fe1-4f59-84d4-5c1263f6c1fe","changes":
[{"action":"siem.test","requestedBy":"admin"}]}
```


Format `rfc5424`, profil `ecs`:


```
<86>1 2026-10-19T04:20:35.699Z certyx-node-1 clm 1 integration [timeQuality tzKnown="1"][origin software="CERTYX CLM"
swVersion="1.0.0"] <BOM>{"@timestamp":"2026-10-19T04:20:35.699Z","message":"siem.test by siem-test","ecs":
{"version":"8.11.0"},"event":{"id":"ae9bc3c0-bc81-4d1e-9540-11fc3940029b","code":"INTEGRATION-001","kind":"event","category":
["network"],"type":["connection"],"action":"siem.test","outcome":"success","severity":3,"created":"2026-10-
19T04:20:35.699Z","dataset":"certyx.security","provider":"siem"},"user":{"id":"siem-test"},"host":{"hostname":"certyx-node-
1"},"service":{"name":"clm","version":"1.0.0","environment":"production"},"organization":{"id":"platform"},"labels":
{"schema_version":"certyx.event/1.0","certyx_category":"integration"}}
```


Format `rfc5424`, profil `ocsf`:


```
<86>1 2026-10-19T04:20:36.066Z certyx-node-1 clm 1 integration [timeQuality tzKnown="1"][origin software="CERTYX CLM"
swVersion="1.0.0"] <BOM>
{"class_uid":0,"category_uid":0,"activity_id":99,"type_uid":99,"severity_id":1,"status_id":1,"time":1792383636066,"message":"s
iem.test by siem-test","metadata":{"version":"1.1.0","uid":"f4dbd1be-ac9d-49b1-b952-07226fedb56e","event_code":"INTEGRATION-
001","log_name":"security-journal","product":
```

{"name":"CLM","vendor_name":"CERTYX","version":"1.0.0"},"correlation_uid":"f4dbd1be-ac9d-49b1-b952-07226fedb56e"},"unmapped":{"certyx_schema_version":"certyx.event/1.0","certyx_category":"integration","certyx_action":"siem.test"}}

Format `cef`:

<86>1 2026-10-19T04:20:36.426Z certyx-node-1 clm 1 integration [timeQuality tzKnown="1"][origin software="CERTYX CLM" swVersion="1.0.0"] CEF:0|CERTYX|CLM|1.0.0|INTEGRATION-001|siem.test by siem-test|3|rt=1792383636426 externalId=1ff31932-0574-411b-ae54-e5198a04aea0 act=siem.test cat=integration outcome=success msg=siem.test by siem-test suser=siem-test suid=siem-test dvchost=certyx-node-1 cs1Label=organizationId cs1=platform cs3Label=correlationId cs3=1ff31932-0574-411b-ae54-e5198a04aea0 cs6Label=schemaVersion cs6=certyx.event/1.0

Format `leef-1.0`:

<86>1 2026-10-19T04:20:36.792Z certyx-node-1 clm 1 integration [timeQuality tzKnown="1"][origin software="CERTYX CLM" swVersion="1.0.0"] LEEF:1.0|CERTYX|CLM|1.0.0|INTEGRATION-001|devTime=2026-10-19T04:20:36.792+0000 devTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSSZ cat=integration sev=3 usrName=siem-test eventId=cc2733fd-b537-4cec-98f2-80c0acf4e3c6 schemaVersion=certyx.event/1.0 action=siem.test outcome=success message=siem.test by siem-test userId=siem-test organization=platform organizationKind=platform correlationId=cc2733fd-b537-4cec-98f2-80c0acf4e3c6 instance=certyx-node-1

Format `leef-2.0` z separatorem miejsca docelowego `^` (bez separatora używany jest tabulator, deklarowany jako `x09`):

<86>1 2026-10-19T04:20:37.152Z certyx-node-1 clm 1 integration [timeQuality tzKnown="1"][origin software="CERTYX CLM" swVersion="1.0.0"] LEEF:2.0|CERTYX|CLM|1.0.0|INTEGRATION-001|^|devTime=2026-10-19T04:20:37.152+0000^devTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSSZ^cat=integration^sev=3^usrName=siem-test^eventId=4ead979d-6b67-496c-931a-d0c0ff1fc02a^schemaVersion=certyx.event/1.0^action=siem.test^outcome=success^message=siem.test by siem-test^userId=siem-test^organization=platform^organizationKind=platform^correlationId=4ead979d-6b67-496c-931a-d0c0ff1fc02a^instance=certyx-node-1

Format `kv` (`certyx-kv/1.0`):

<86>1 2026-10-19T04:20:37.523Z certyx-node-1 clm 1 integration [timeQuality tzKnown="1"][origin software="CERTYX CLM" swVersion="1.0.0"] schema_version=certyx.event/1.0 event_id=acbe1e97-a048-43f7-b350-ae2dba0f2dfb event_code=INTEGRATION-001 category=integration action=siem.test outcome=success outcome_original=business severity=3 severity_label=low message="siem.test by siem-test" timestamp=2026-10-19T04:20:37.523Z observed_timestamp=2026-10-19T04:20:37.523Z export_timestamp=2026-10-19T04:20:37.523Z application="CERTYX CLM" version=1.0.0 environment=production hostname=certyx-node-1 host_ip=- service_name=clm component=siem organization_id=platform organization_name=- organization_kind=platform user_id=siem-test username=- user_role=- session_id=- authentication_method=- user_verified=- user_agent=- src_ip=- src_port=- http_method=- http_route=- http_status=- protocol=- correlation_id=acbe1e97-a048-43f7-b350-ae2dba0f2dfb request_id=acbe1e97-a048-43f7-b350-ae2dba0f2dfb trace_id=- resource_type=- resource_id=- change_type=- reason=- error_type=- sequence=- event_hash=- agent_fingerprint=- changes="[{\"action\":\"siem.test\",\"requestedBy\":\"admin\"}]" changes_redacted=- dst_ip=- dst_port=- span_id=-

Format `cef-compat` (pierwsze wydanie):

<86>1 2026-10-19T04:20:38.263Z certyx-node-1 clm 1 integration [timeQuality tzKnown="1"] CEF:0|CERTYX|CLM|1.0.0|certyx:business|business INTERNAL business/siem.test|3|rt=1792383638263 suser=siem-test requestMethod=INTERNAL request=business/siem.test outcome=business externalId=0 dvchost=certyx-node-1 cn1Label=httpStatus cn1=200 cs1Label=organization cs1=platform certyxOrganizationName= certyxOrganizationKind=platform cs2Label=traceId cs2=0d0b9f13-888d-4f45-bca4-ec48d749f919 cs3Label=eventHash cs3= cs4Label=agentFingerprint cs4= cs5Label=errorType cs5= cs6Label=changes cs6=[{"action":"siem.test","requestedBy":"admin"}] certyxEventId=0d0b9f13-888d-4f45-bca4-ec48d749f919

Format `leef-compat` (pierwsze wydanie):

```
<86>1 2026-10-19T04:20:38.733Z certyx-node-1 clm 1 integration [timeQuality tzKnown="1"]
LEEF:2.0|CERTYX|CLM|1.0.0|certyx:business|^|devTime=2026-10-19T04:20:38.733+0000^devTimeFormat=yyyy-MM-
dd'T'HH:mm:ss.SSSZ^usrName=siem-
test^cat=business^sev=3^method=INTERNAL^resource=business/siem.test^httpStatus=200^organization=platform^organizationName=^org
anizationKind=platform^traceId=2938c9ab-5183-4e4f-81fa-
deab9119266a^sequence=0^eventHash=^agentFingerprint=^errorType=^instance=certyx-node-1^changes=
[{"action":"siem.test","requestedBy":"admin"}]^eventId=2938c9ab-5183-4e4f-81fa-deab9119266a
```

31.4 Microsoft Sentinel

Format `sentinel` (wiersz Logs Ingestion):

```
[{"TimeGenerated":"2026-10-
19T04:20:39.0967775Z","Sequence":0,"Organization":"platform","OrganizationName":"","OrganizationKind":"platform","Actor":"siem
-
test","SourceIp":"system","AgentFingerprint":"","Method":"INTERNAL","Route":"business/siem.test","Status":200,"Outcome":"busin
ess","TraceId":"70b73efa-1bea-4dfe-9e68-d72ba95b82a7","ErrorType":"","Instance":"certyx-node-1","EventHash":"","Changes":
[{"action":"siem.test","requestedBy":"admin"}],"User":"","UserVerified":false,"UserOrganization":"","AuthAction":"","AuthMetho
d":"","AuthResult":"","Reason":"","UserAgent":"","EventId":"70b73efa-1bea-4dfe-9e68-d72ba95b82a7"}]
```

31.5 OpenTelemetry Logs

Format `otlp-json`, treść rekordu dziennika *Komunikat* (zdarzenie testowe):

```
{"resourceLogs":[{"resource":{"attributes":[{"key":"service.name","value":{"stringValue":"certyx"}},
{"key":"service.version","value":{"stringValue":"1.0.0"}},{"key":"deployment.environment.name","value":
{"stringValue":"production"}},{"key":"host.name","value":{"stringValue":"certyx-node-1"}},
{"key":"certyx.organization.id","value":{"stringValue":"platform"}},{"key":"certyx.organization.kind","value":
{"stringValue":"platform"}}]},"scopeLogs":[{"scope":{"name":"certyx.security-journal","version":"1.0.0"},"logRecords":
[{"timeUnixNano":"1792838639470357800","observedTimeUnixNano":"1792838639470357800","severityNumber":9,"severityText":"INFO","
body":{"stringValue":"siem.test by siem-test"},"attributes":[{"key":"certyx.schema_version","value":
{"stringValue":"certyx.event/1.0"}},{"key":"certyx.event.id","value":{"stringValue":"eaf0e504-9ff5-4214-8758-5eebb3e5b907"}},
{"key":"certyx.event.code","value":{"stringValue":"INTEGRATION-001"}},{"key":"certyx.event.category","value":
{"stringValue":"integration"}},{"key":"event.name","value":{"stringValue":"siem.test"}},{"key":"certyx.event.outcome","value":
{"stringValue":"success"}},{"key":"certyx.event.outcome_original","value":{"stringValue":"business"}},
{"key":"certyx.event.severity","value":{"intValue":"3"}},{"key":"certyx.event.severity_label","value":{"stringValue":"low"}},
{"key":"certyx.export_timestamp","value":{"stringValue":"2026-10-19T04:20:39.470Z"}},{"key":"certyx.application","value":
{"stringValue":"CERTYX CLM"}},{"key":"certyx.service_name","value":{"stringValue":"clm"}},{"key":"certyx.component","value":
{"stringValue":"siem"}},{"key":"user.id","value":{"stringValue":"siem-test"}},{"key":"certyx.correlation_id","value":
{"stringValue":"eaf0e504-9ff5-4214-8758-5eebb3e5b907"}},{"key":"certyx.request_id","value":{"stringValue":"eaf0e504-9ff5-4214-
8758-5eebb3e5b907"}},{"key":"certyx.changes","value":{"stringValue":"
[{\"action\":\"siem.test\",\"requestedBy\":\"admin\"}]"}}]}]}]}]}
```

Wpis żądania z dziennika (`POST` testu, z identyfikatorem trace i span, adresem klienta i serwera), wyeksportowany przez przebieg eksportu w `otlp-json`:

```
{"resourceLogs":[{"resource":{"attributes":[{"key":"service.name","value":{"stringValue":"certyx"}},
{"key":"service.version","value":{"stringValue":"1.0.0"}},{"key":"deployment.environment.name","value":
{"stringValue":"production"}},{"key":"host.name","value":{"stringValue":"certyx-node-1"}},{"key":"host.ip","value":
{"arrayValue":{"values":[{"stringValue":"127.0.0.1"}]}}},{"key":"certyx.organization.id","value":{"stringValue":"default"}},
{"key":"certyx.organization.kind","value":{"stringValue":"organization"}}]},"scopeLogs":[{"scope":{"name":"certyx.security-
journal","version":"1.0.0"},"logRecords":
[{"timeUnixNano":"1792838631369104500","observedTimeUnixNano":"1792838631369104500","severityNumber":9,"severityText":"INFO","
body":{"stringValue":"POST /platform/api/siem/{scope}/{id}/test 200 success"},"attributes":
```

```
[{"key":"certyx.schema_version","value":{"stringValue":"certyx.event/1.0"}},{"key":"certyx.event.id","value":
{"stringValue":"e828c2f0-1089-48fe-838a-9c5267fb560b:31"}},{"key":"certyx.event.code","value":{"stringValue":"INTEGRATION-
002"}},{"key":"certyx.event.category","value":{"stringValue":"integration"}},{"key":"event.name","value":
{"stringValue":"siem.destination.tested"}},{"key":"certyx.event.outcome","value":{"stringValue":"success"}},
{"key":"certyx.event.outcome_original","value":{"stringValue":"success"}},{"key":"certyx.event.severity","value":
{"intValue":"3"}},{"key":"certyx.event.severity_label","value":{"stringValue":"low"}},
{"key":"certyx.export_timestamp","value":{"stringValue":"2026-10-19T04:20:41.828Z"}},{"key":"certyx.application","value":
{"stringValue":"CERTYX CLM"}},{"key":"certyx.service_name","value":{"stringValue":"clm"}},{"key":"certyx.component","value":
{"stringValue":"platform"}},{"key":"user.id","value":{"stringValue":"7e636f39d1f54da2a7b53c583a2c16ab"}},
{"key":"user.roles","value":{"arrayValue":{"values":[{"stringValue":"Admin"}]}}},{"key":"session.id","value":
{"stringValue":"2387475c1fe53858e83262b02ab8c789"}},{"key":"client.address","value":{"stringValue":"127.0.0.1"}},
{"key":"client.port","value":{"intValue":"38350"}},{"key":"server.address","value":{"stringValue":"127.0.0.1"}},
{"key":"server.port","value":{"intValue":"5291"}},{"key":"http.request.method","value":{"stringValue":"POST"}},
{"key":"http.route","value":{"stringValue":"/platform/api/siem/{scope}/{id}/test"}},
{"key":"http.response.status_code","value":{"intValue":"200"}},{"key":"network.protocol.name","value":{"stringValue":"http"}},
{"key":"certyx.correlation_id","value":{"stringValue":"0HNPDJ0V49OUH:00000002"}},{"key":"certyx.request_id","value":
{"stringValue":"0HNPDJ0V49OUH:00000002"}},{"key":"certyx.sequence","value":{"intValue":"31"}},
{"key":"certyx.event_hash","value":{"stringValue":"3C7261A625BABD9DCFC9918736DBE1825E73B63BCAF264DAF54D419EE4C6FECC"}},
{"key":"certyx.changes","value":{"stringValue":"[{\"action\":\"siem.destination.tested\",\"before\":
{\"scope\":\"platform\",\"id\":\"https-json\"},\"after\":{\"scope\":\"platform\",\"id\":\"https-
json\",\"Ok\":true,\"Error\":null,\"steps\":[{\"Step\":\"dns\",\"Ok\":true,\"Code\":\"dns-literal\"},
{\"Step\":\"tcp\",\"Ok\":true,\"Code\":\"tcp-ok\"},{\"Step\":\"tls\",\"Ok\":true,\"Code\":\"tls-ok\"},
{\"Step\":\"delivery\",\"Ok\":true,\"Code\":\"http-accepted\"}]}},{\"action\":\"request.resource\",\"values\":
{\"scope\":\"platform\",\"id\":\"https-
json\"}}]"}}],"traceId":"5484ed97229f3acd5acff7a0bce7b454","spanId":"ae1a1295fae542f9"}]}]}]}
```


Format `otlp-protobuf` wysyła to samo żądanie w binarnym protobuf; powyższe zdarzenie testowe miało 1030 bajtów.

31.6 Archiwum plikowe

Zdarzenie testowe nie jest zapisywane w archiwach; poniżej znajdują się wiersze zdarzeń z dziennika. Format `csv` (nagłówek i jeden wiersz):


```
"schema_version","event_id","event_code","category","action","outcome","outcome_original","severity","severity_label","message
","timestamp","observed_timestamp","export_timestamp","application","version","environment","hostname","host_ip","service_name
","component","organization_id","organization_name","organization_kind","user_id","username","user_role","session_id","authent
ication_method","user_verified","user_agent","src_ip","src_port","http_method","http_route","http_status","protocol","correlat
ion_id","request_id","trace_id","resource_type","resource_id","change_type","reason","error_type","sequence","event_hash","age
nt_fingerprint","changes","changes_redacted","dst_ip","dst_port","span_id"
"certyx.event/1.0","e828c2f0-1089-48fe-838a-9c5267fb560b:1","CONFIG-028","configuration-
change","sales.mail.seeded","success","business","3","low","sales.mail.seeded mail by system:configuration","2026-10-
19T04:19:41.297Z","2026-10-19T04:19:41.297Z","2026-10-19T04:20:43.904Z","CERTYX CLM","1.0.0","production","certyx-node-
1",,"clm","sales","platform",,"platform","system:configuration",,,,,,,,,,,,"9cf31c6f3be3445ba7e988dc7146cfd4","9cf31c6f3be344
5ba7e988dc7146cfd4",,"sales.mail","mail","create",,,"1","C6E68A3969E5557A0CD49A6969FE6824130603A162AB84DDD0B9D4B1E03FE932",,"
[{""action"":""sales.mail.seeded"",""resource"":""mail"",""before"":{},""after"":
{""Enabled"":false,""Host"":""",""Port"":587,""From"":""",""Username"":null,""OperatorCopy"":null,""InquiryRecipient"":null}
}]","true",,,
```


Format `csv-compat` (nagłówek i jeden wiersz):


```
"Sequence","At","OrganizationId","OrganizationName","OrganizationKind","Instance","Actor","SourceIp","AgentFingerprint","Metho
d","Route","Status","Outcome","Severity","TraceId","ErrorType","SignInAction","SignInUser","SignInMethod","SignInResult","Sign
InReason","Changes","PreviousHash","Hash"
"1","2026-10-19T04:19:41.2973423Z","platform","","platform","certyx-node-
1","system:configuration","system","","INTERNAL","business/sales.mail.seeded","200","business","3","9cf31c6f3be3445ba7e988dc71
46cfd4","","","","","","","[{""action"":""sales.mail.seeded"",""resource"":""mail"",""before"":{},""after"":
```

{""Enabled"":false,""Host"":"""",""Port"":587,""From"":"""",""Username"":null,""password"":{""Set"":false,""Reference"":null},""OperatorCopy"":null,""InquiryRecipient"":null}}]","","C6E68A3969E5557A0CD49A6969FE6824130603A162AB84DDD0B9D4B1E03FE932"

Format `ndjson`, profil `native` (jeden wiersz):

{"schema_version":"certyx.event/1.0","event_id":"e828c2f0-1089-48fe-838a-9c5267fb560b:1","event_code":"CONFIG-028","category":"configuration-change","action":"sales.mail.seeded","outcome":"success","outcome_original":"business","severity":3,"severity_label":"low","message":"sales.mail.seeded mail by system:configuration","timestamp":"2026-10-19T04:19:41.297Z","observed_timestamp":"2026-10-19T04:19:41.297Z","export_timestamp":"2026-10-19T04:20:43.904Z","application":"CERTYX CLM","version":"1.0.0","environment":"production","hostname":"certyx-node-1","service_name":"clm","component":"sales","organization_id":"platform","organization_kind":"platform","user_id":"system:configuration","correlation_id":"9cf31c6f3be3445ba7e988dc7146cfd4","request_id":"9cf31c6f3be3445ba7e988dc7146cfd4","resource_type":"sales.mail","resource_id":"mail","change_type":"create","sequence":1,"event_hash":"C6E68A3969E5557A0CD49A6969FE6824130603A162AB84DDD0B9D4B1E03FE932","changes":[{"action":"sales.mail.seeded","resource":"mail","before":{},"after":{"Enabled":false,"Host":"","Port":587,"From":"","Username":null,"OperatorCopy":null,"InquiryRecipient":null}}],"changes_redacted":true}

32 Opis pól

Pełny opis — każde pole kanoniczne z jego źródłem i mapowaniem na CEF, LEEF, KV, RFC 5424, ECS, OCSF i Splunk CIM — zawiera dokument opisu pól `docs/SIEM-EXPORT-FIELDS.md` w dokumentacji CERTYX. Ta sekcja go podsumowuje.

Wartość nieznana a pusta. Pole, którego dziennik nie zna lub które nie ma zastosowania (na przykład `http_status` zmiany biznesowej), jest *nieznane*. Formaty JSON (NDJSON, MSG RFC 5424, ECS, OCSF, HEC) pomijają nieznane pola; CSV zapisuje wartość nieznaną jako puste pole bez cudzysłowów, a znaną pustą wartość jako `""`; KV zapisuje wartość nieznaną jako samo `-`, a znaną pustą wartość jako `""`; CEF i LEEF pomijają wartości nieznane i puste. Wszystkie czasy są w formacie ISO 8601 UTC z milisekundami i `Z` (CEF `rt`, OCSF `time` i `time` w HEC to ta sama chwila zapisana jako wartości epoki).

32.1 Zdarzenie kanoniczne

Wersja schematu `certyx.event/1.0`. Kolejność odpowiada stałej kolejności kolumn `csv` i `kv`.

Pole	Zawartość
`schema_version`	`certyx.event/1.0`
`event_id`	`<installation id>:<journal sequence>`; UUID dla zdarzeń testowych
`event_code`, `category`	Z katalogu kodów zdarzeń
`action`	Nazwa zdarzenia logowania, pierwsza zmiana biznesowa albo pseudoakcja wyniku (`http.read`, `http.write`, `http.denied`, …)
`outcome`, `outcome_original`	`success`, `failure` lub `unknown`; wynik z dziennika
`severity`, `severity_label`	0–10 (próba 2, powodzenie/zmiana biznesowa 3, odrzucenie 5, odmowa dostępu 7, błąd 8; udane logowanie 3, nieudane 7, blokada 8); low, medium, high, very-high
`message`	Krótkie zdanie w języku angielskim
`timestamp`, `observed_timestamp`, `export_timestamp`	Kiedy zdarzenie wystąpiło, zostało zaobserwowane (ta sama chwila) i zostało zserializowane do eksportu
`application`, `version`, `environment`	`CERTYX CLM`, wersja produktu, środowisko (`Clm:Siem:Environment`, w przeciwnym razie środowisko hostingu)
`hostname`, `host_ip`	Instancja, która zapisała zdarzenie; adres serwera (wzbogacenie)
`service_name`, `component`	`clm`; pierwszy segment trasy po `api` lub pierwszy segment akcji biznesowej

Pole	Zawartość
`organization_id`, `organization_name`, `organization_kind`	Zob. Wiele organizacji
`user_id`, `username`, `user_role`, `session_id`	Wykonawca; użytkownik logowania; rola i identyfikator korelacji sesji (wzbogacenie)
`authentication_method`, `user_verified`, `user_agent`	Zdarzenia logowania
`src_ip`, `src_port`	Adres źródłowy (tylko prawidłowy adres); port źródłowy (wzbogacenie)
`dst_ip`, `dst_port`	Cel: adres i port serwera, które przyjęły żądanie (wzbogacenie), albo obserwowany cel zdarzenia wykrywania
`span_id`	Identyfikator span W3C aktywności żądania (wzbogacenie)
`http_method`, `http_route`, `http_status`, `protocol`	Wpisy żądań; szablon trasy, nigdy surowa ścieżka; `http`
`correlation_id`, `request_id`, `trace_id`	Łączy próbę i wynik; identyfikator żądania ASP.NET; identyfikator śledzenia W3C (wzbogacenie)
`resource_type`, `resource_id`, `change_type`	Zmieniony zasób; `create`, `update`, `delete`
`reason`, `error_type`	Kod przyczyny logowania lub typ błędu; nazwa typu wyjątku
`sequence`, `event_hash`, `agent_fingerprint`	Numer sekwencyjny w dzienniku (nieznany dla zdarzeń testowych); skrót łańcucha dziennika; odcisk certyfikatu agenta
`changes`, `changes_redacted`	Zapisane zmiany po redakcji (tablica JSON; zwarty tekst JSON w CSV i KV); `true`, gdy coś usunięto

32.2 Rekord JSON

Używany przez format `json` w webhooku (tablica rekordów), syslogu (jeden rekord na komunikat) i Splunk HEC (`event`).

Pole	Typ	Zawartość
`Sequence`	liczba	Pozycja w dzienniku CERTYX; 0 dla zdarzenia testowego
`EventId`	ciąg	Identyfikator zdarzenia `<installation id>:<journal sequence>` (klucz usuwania duplikatów); UUID dla zdarzenia testowego
`At`	ciąg	Czas zdarzenia, ISO 8601 z przesunięciem strefy
`Tenant`	ciąg	Identyfikator organizacji, `platform` dla zdarzeń operatorów, `unattributed` dla żądań bez zalogowanej organizacji
`OrganizationName`	ciąg	Nazwa organizacji, jeśli platforma ją zna; pusta dla `platform`, `unattributed` i instalacji bez administracji platformą (dodawana przy eksporcie)
`OrganizationKind`	ciąg	`organization`, `platform` lub `unattributed` (dodawany przy eksporcie)
`Instance`	ciąg	Identyfikator instancji CERTYX, która zapisała zdarzenie (`Clm:Instance:Id`)
`Actor`	ciąg	Konto, tożsamość logowania firmowego, agent lub wykonawca systemowy; `anonymous` przed zalogowaniem
`SourceIp`	ciąg	Adres drugiej strony gniazda (`system` dla zdarzeń w tle)
`AgentFingerprint`	ciąg	Odcisk SHA-256 certyfikatu klienta agenta (żądania agentów)
`Method`	ciąg	Metoda HTTP, `INTERNAL` dla zdarzeń w tle
`Route`	ciąg	Szablon trasy (nigdy surowa ścieżka), `business/<action>` dla zmian w tle
`Status`	liczba	Status HTTP (200 lub 401 dla zdarzeń logowania)
`Outcome`	ciąg	`attempt`, `success`, `rejected`, `denied`, `error`, `business`, `authentication`
`TraceId`	ciąg	Identyfikator korelacji żądania
`ErrorType`	ciąg	Typ wyjątku dla błędów serwera

Pole	Typ	Zawartość
`Changes`	tablica obiektów	Każdy element to obiekt JSON `{action, before, after}` (zagnieżdżony, bez cudzysłowów poprzedzonych ukośnikiem; od wydania 1.2.12, wcześniej każdy element był ciągiem zawierającym obiekt); zmiany poza żądaniem i zdarzenia logowania dodają `resource`
`Hash`	ciąg	SHA-256 wpisu w łańcuchu dziennika CERTYX (szesnastkowo, wielkimi literami)
`SignIn`	obiekt	Tylko zdarzenia logowania: `Action`, `User`, `UserVerified`, `Organization`, `Method`, `Result`, `Reason`, `UserAgent`

32.3 Pola CEF (pierwsze wydanie)

Format `cef-compat`. Kanoniczny format `cef` opisano w sekcji ArcSight.

Klucz CEF	Zawartość
Signature ID	`certyx:<outcome>`; zdarzenia logowania `certyx:<event name>`
Name	`<outcome> <method> <route>`; zdarzenia logowania `<event name> <method>`
`rt`	Czas zdarzenia, milisekundy epoki
`suser`	Wykonawca; zdarzenia logowania: adres e-mail użytkownika
`suid`	Zdarzenia logowania: wykonawca
`src`	Źródłowy adres IP (tylko prawidłowy adres)
`requestMethod`, `request`	Metoda HTTP, szablon trasy
`outcome`	Wynik; zdarzenia logowania `success` lub `failure`
`externalId`	Numer sekwencyjny w dzienniku
`certyxEventId`	Identyfikator zdarzenia `<installation id>:<journal sequence>`
`dvchost`	Instancja CERTYX
`cn1` (`httpStatus`)	Status HTTP
`cs1` … `cs6`	`organization`, `traceId`, `eventHash`, `agentFingerprint`, `errorType`, `changes` (JSON)
`certyxOrganizationName`, `certyxOrganizationKind`	Nazwa i rodzaj organizacji (klucze rozszerzeń producenta; ArcSight pokazuje je jako dane dodatkowe)
`cat`, `act`, `reason`	Zdarzenia logowania: `authentication`, nazwa zdarzenia, kod przyczyny
`requestClientApplication`	Zdarzenia logowania: agent użytkownika
`flexString1` (`authMethod`), `flexString2` (`userVerified`)	Zdarzenia logowania: metoda, zweryfikowana tożsamość

Pola nagłówka mają zmaskowane znaki `\` i kreskę pionową; wartości rozszerzeń mają zmaskowane znaki `\`, `=` i końce wierszy (`\n`, `\r`).

32.4 Pola LEEF (pierwsze wydanie)

Format `leef-compat` (LEEF 2.0, separator `^`). Kanoniczne formaty `leef-1.0` i `leef-2.0` opisano w sekcji QRadar.

Atrybut LEEF	Zawartość
Event ID	`certyx:<outcome>`; zdarzenia logowania `certyx:<event name>`
`devTime`, `devTimeFormat`	Czas zdarzenia (`yyyy-MM-dd'T'HH:mm:ss.SSSZ`)
`usrName`	Wykonawca; zdarzenia logowania: adres e-mail użytkownika
`src`	Źródłowy adres IP (tylko prawidłowy adres)

Atrybut LEEF	Zawartość
`cat`, `sev`	Wynik, ważność 1–10
`method`, `resource`, `httpStatus`	Metoda HTTP, szablon trasy, status
`organization`, `organizationName`, `organizationKind`, `traceId`, `sequence`, `eventHash`, `agentFingerprint`, `errorType`, `instance`, `changes`	Jak w rekordzie JSON (`organization` = `Tenant`)
`eventId`	Identyfikator zdarzenia `<installation id>:<journal sequence>`
`actor`, `action`, `authMethod`, `result`, `reason`, `userAgent`, `userVerified`	Tylko zdarzenia logowania

Wartości mają zmaskowane znaki `\` i `^`; końce wierszy i tabulatory są zamieniane na spacje.

32.5 Kolumny Sentinel

Kolumna	Typ
`TimeGenerated`	datetime
`EventId`	string (`<installation id>:<journal sequence>`)
`Sequence`	long
`Organization`, `OrganizationName`, `OrganizationKind`, `Actor`, `SourceIp`, `AgentFingerprint`, `Method`, `Route`, `Outcome`, `TraceId`, `ErrorType`, `Instance`, `EventHash`	string
`Status`	int
`Changes`	dynamic (tablica obiektów)
`User`, `UserOrganization`, `AuthAction`, `AuthMethod`, `AuthResult`, `Reason`, `UserAgent`	string (puste dla zdarzeń innych niż zdarzenia logowania)
`UserVerified`	boolean

Reguła utworzona, zanim istniały `EventId`, `OrganizationName` i `OrganizationKind`, nadal pozyskuje pozostałe kolumny; aby je zapisywać, dodaj je (string) do tabeli i do deklaracji strumienia.

33 Katalog kodów zdarzeń

Każda akcja dziennika ma stały kod zdarzenia; wpis dokładny ma pierwszeństwo przed rodziną, a spośród rodzin wygrywa najdłuższy prefiks. Wiersz rodziny (prefiksu) obejmuje nazwy akcji tworzone w czasie działania, takie jak `renewal.profile.<decision>`. Kody nigdy nie są przenumerowywane; nowe akcje otrzymują nowe kody.

Kategoria	Prefiks kodu	Znaczenie
`authentication`	AUTHN	logowanie, wylogowanie, blokada, kroki MFA
`authorization`	AUTHZ	odrzucone żądania (401/403) i odrzucone sieci logowania
`user-management`	USER	konta, użytkownicy i grupy SCIM, urządzenia, resety MFA
`configuration-change`	CONFIG	ustawienia SSO, sieci, powiadomień, SIEM, agentów, wykrywania, odnawiania i monitorowania
`data-access`	DATA	eksporty, pobrania archiwów, ujawnione hasła dokumentów, odczyty
`administrative`	ADMIN	działania operatora platformy, klienci, rekordy sprzedaży, zatwierdzenia i decyzje operacyjne
`security`	SECURITY	unieważnienie i tożsamość agentów, przedstawione certyfikaty, alerty certyfikatów i wykrywania
`application-error`	ERROR	nieudane i odrzucone żądania, błędy aprowizacji
`system`	SYSTEM	kondycja, skanowania, zadania, wdrożenia, próby żądań i adnotacje

Kategoria	Prefiks kodu	Znaczenie
`integration`	INTEGRATION	sprawdzenia połączeń i wiadomości testowe połączeń SIEM, powiadomień, alertów i analityka, importy, pominięte i ponownie wysłane zdarzenia SIEM

Kategoria jest także wartością MSGID w RFC 5424.

33.1 Wybierane według wyniku

Wpisy bez akcji biznesowej otrzymują pseudoakcję i kod swojego wyniku. Udane żądanie używa `http.read` dla GET i HEAD, a w pozostałych przypadkach `http.write`; akcja biznesowa spoza katalogu zachowuje swoją nazwę i otrzymuje SYSTEM-001.

Kod	Kategoria	Akcja	Rodzaj
AUTHN-000	authentication	`authentication`	wpis logowania bez czytelnych szczegółów
AUTHZ-000	authorization	`http.denied`	wynik denied
DATA-000	data-access	`http.read`	wynik success, GET/HEAD
ADMIN-000	administrative	`http.write`	wynik success, pozostałe metody
ERROR-000	application-error	`http.error`	wynik error
ERROR-001	application-error	`http.rejected`	wynik rejected
SYSTEM-000	system	`http.attempt`	wpis próby
SYSTEM-001	system	`business`	wpis biznesowy z akcją spoza katalogu

33.2 Akcje dziennika

Kod	Kategoria	Akcja	Rodzaj
AUTHN-001	authentication	`authentication.sign-in.succeeded`	dokładne
AUTHN-002	authentication	`authentication.sign-in.failed`	dokładne
AUTHN-003	authentication	`authentication.sign-out`	dokładne
AUTHN-004	authentication	`authentication.locked`	dokładne
AUTHN-005	authentication	`authentication.repeated-failures`	dokładne
AUTHN-006	authentication	`authentication.mfa.enrolled`	dokładne
AUTHN-007	authentication	`authentication.mfa.confirmed`	dokładne
AUTHN-008	authentication	`authentication.mfa.recovery-codes-regenerated`	dokładne
AUTHN-009	authentication	`authentication.claimed-identity`	dokładne
AUTHN-010	authentication	`mobile.signin.failed`	dokładne
AUTHN-011	authentication	`mobile.session.created`	dokładne
AUTHN-012	authentication	`account.locked`	dokładne
AUTHN-013	authentication	`account.mfa.recovery-code-used`	dokładne
AUTHN-014	authentication	`account.passkey.used`	dokładne
AUTHN-015	authentication	`session.revoked`	dokładne
AUTHZ-001	authorization	`identity.signin-networks.refused`	dokładne
USER-001	user-management	`identity.scim.user-created`	dokładne
USER-002	user-management	`identity.scim.user-replaced`	dokładne
USER-003	user-management	`identity.scim.user-updated`	dokładne
USER-004	user-management	`identity.scim.user-deactivated`	dokładne

Kod	Kategoria	Akcja	Rodzaj
USER-005	user-management	`identity.scim.user-deleted`	dokładne
USER-006	user-management	`identity.scim.group-created`	dokładne
USER-007	user-management	`identity.scim.group-replaced`	dokładne
USER-008	user-management	`identity.scim.group-updated`	dokładne
USER-009	user-management	`identity.scim.group-deleted`	dokładne
USER-010	user-management	`identity.scim.role-changed`	dokładne
USER-011	user-management	`account.created`	dokładne
USER-012	user-management	`account.updated`	dokładne
USER-013	user-management	`account.mfa.reset`	dokładne
USER-014	user-management	`account.mfa.recovery-codes-regenerated`	dokładne
USER-015	user-management	`authentication.mfa.reset`	dokładne
USER-016	user-management	`mfa-setup.mail.`	rodzina (prefiks)
USER-017	user-management	`customer.account.`	rodzina (prefiks)
USER-018	user-management	`mobile.device.`	rodzina (prefiks)
USER-019	user-management	`mobile.enrollment.`	rodzina (prefiks)
USER-020	user-management	`account.passkey.registered`	dokładne
USER-021	user-management	`account.passkey.removed`	dokładne
USER-022	user-management	`account.second-factor.changed`	dokładne
USER-023	user-management	`identity.scim.role-raised`	dokładne
USER-024	user-management	`account.create-refused`	dokładne
USER-025	user-management	`account.email-refused`	dokładne
CONFIG-001	configuration-change	`identity.sso.`	rodzina (prefiks)
CONFIG-002	configuration-change	`identity.signin-networks.changed`	dokładne
CONFIG-003	configuration-change	`identity.signin-networks.cleared-by-operator`	dokładne
CONFIG-004	configuration-change	`platform.signin-networks.changed`	dokładne
CONFIG-005	configuration-change	`customer.signin-networks.cleared`	dokładne
CONFIG-006	configuration-change	`notification.channel.`	rodzina (prefiks)
CONFIG-007	configuration-change	`notification.smtp.`	rodzina (prefiks)
CONFIG-008	configuration-change	`siem.destination.`	rodzina (prefiks)
CONFIG-009	configuration-change	`agent.configuration.`	rodzina (prefiks)
CONFIG-010	configuration-change	`agent.capabilities.updated`	dokładne
CONFIG-011	configuration-change	`agent.discovery.profile.updated`	dokładne
CONFIG-012	configuration-change	`discovery.scope.`	rodzina (prefiks)
CONFIG-013	configuration-change	`renewal.automatic.`	rodzina (prefiks)
CONFIG-014	configuration-change	`auto-renewal.`	rodzina (prefiks)
CONFIG-015	configuration-change	`platform.cloud-source.`	rodzina (prefiks)
CONFIG-016	configuration-change	`cloud-sources.seeded`	dokładne
CONFIG-017	configuration-change	`monitoring.alert-channel.`	rodzina (prefiks)

Kod	Kategoria	Akcja	Rodzaj
CONFIG-018	configuration-change	`monitoring.alert-relay.`	rodzina (prefiks)
CONFIG-019	configuration-change	`monitoring.database-log-source.`	rodzina (prefiks)
CONFIG-020	configuration-change	`monitoring.settings.`	rodzina (prefiks)
CONFIG-021	configuration-change	`analyst.settings.`	rodzina (prefiks)
CONFIG-022	configuration-change	`analyst.organization.`	rodzina (prefiks)
CONFIG-023	configuration-change	`remediation.policy.`	rodzina (prefiks)
CONFIG-024	configuration-change	`recipient-group.updated`	dokładne
CONFIG-025	configuration-change	`policy.update.v`	rodzina (prefiks)
CONFIG-026	configuration-change	`mail.suppression.`	rodzina (prefiks)
CONFIG-027	configuration-change	`mail.events.subscription-confirmed`	dokładne
CONFIG-028	configuration-change	`sales.mail.`	rodzina (prefiks)
CONFIG-029	configuration-change	`execution.private-verification.`	rodzina (prefiks)
CONFIG-030	configuration-change	`execution.target.`	rodzina (prefiks)
CONFIG-031	configuration-change	`family.`	rodzina (prefiks)
CONFIG-032	configuration-change	`certificate.metadata.update`	dokładne
CONFIG-033	configuration-change	`ssh.metadata.updated`	dokładne
CONFIG-034	configuration-change	`trust-graph.updated`	dokładne
CONFIG-035	configuration-change	`endpoint-health.monitor.`	rodzina (prefiks)
DATA-001	data-access	`audit.exported`	dokładne
DATA-002	data-access	`security-events.exported`	dokładne
DATA-003	data-access	`siem.archive.downloaded`	dokładne
DATA-004	data-access	`sales.document.password-revealed`	dokładne
DATA-005	data-access	`analyst.request`	dokładne
DATA-006	data-access	`analyst.conversation.deleted`	dokładne
ADMIN-001	administrative	`platform.operator.`	rodzina (prefiks)
ADMIN-002	administrative	`platform.customer.changed`	dokładne
ADMIN-003	administrative	`platform.license.contract-override`	dokładne
ADMIN-004	administrative	`platform.subscription.contract-override`	dokładne
ADMIN-005	administrative	`customer.`	rodzina (prefiks)
ADMIN-006	administrative	`sales.`	rodzina (prefiks)
ADMIN-007	administrative	`certificate.import`	dokładne
ADMIN-008	administrative	`renewal.approved`	dokładne
ADMIN-009	administrative	`renewal.cancelled`	dokładne
ADMIN-010	administrative	`renewal.plan`	dokładne
ADMIN-011	administrative	`renewal.profile.`	rodzina (prefiks)
ADMIN-012	administrative	`alert.acknowledged`	dokładne
ADMIN-013	administrative	`monitoring.incident.`	rodzina (prefiks)
ADMIN-014	administrative	`agent.enrollment.ticket.created`	dokładne

Kod	Kategoria	Akcja	Rodzaj
ADMIN-015	administrative	`agent.discovery.warning.acknowledged`	dokładne
ADMIN-016	administrative	`remediation.decision`	dokładne
ADMIN-017	administrative	`remediation.notice`	dokładne
ADMIN-018	administrative	`ssh.profile.`	rodzina (prefiks)
ADMIN-019	administrative	`ssh.revocation.`	rodzina (prefiks)
ADMIN-020	administrative	`ssh.certificate.imported`	dokładne
ADMIN-021	administrative	`profile.`	rodzina (prefiks)
SECURITY-001	security	`agent.revoked`	dokładne
SECURITY-002	security	`agent.enrolled`	dokładne
SECURITY-003	security	`agent.identity.`	rodzina (prefiks)
SECURITY-004	security	`agent.presented-certificate`	dokładne
SECURITY-005	security	`certificate.alert`	dokładne
SECURITY-006	security	`certificate.alert.escalated`	dokładne
SECURITY-007	security	`discovery.alert.raised`	dokładne
SECURITY-008	security	`data-protection.secret-purpose-migrated`	dokładne
ERROR-002	application-error	`customer.provisioning.step-failed`	dokładne
ERROR-003	application-error	`sales.customer.provisioning-failed`	dokładne
SYSTEM-002	system	`agent.health.changed`	dokładne
SYSTEM-003	system	`agent.discovery.baseline.completed`	dokładne
SYSTEM-004	system	`agent.discovery.networks.reported`	dokładne
SYSTEM-005	system	`discovery.scan.`	rodzina (prefiks)
SYSTEM-006	system	`discovery.started`	dokładne
SYSTEM-007	system	`discovery.resumed`	dokładne
SYSTEM-008	system	`endpoint.observe`	dokładne
SYSTEM-009	system	`ssh.job.`	rodzina (prefiks)
SYSTEM-010	system	`ssh.deployment.`	rodzina (prefiks)
SYSTEM-011	system	`relay.deployment.`	rodzina (prefiks)
SYSTEM-012	system	`lease.expired`	dokładne
SYSTEM-013	system	`inventory.projected`	dokładne
SYSTEM-014	system	`execution.result.imported`	dokładne
SYSTEM-015	system	`request.resource`	dokładne
SYSTEM-016	system	`unmatched.path`	dokładne
SYSTEM-017	system	`certificate.expiry`	dokładne
SYSTEM-018	system	`certificate.renewed`	dokładne
INTEGRATION-001	integration	`siem.test`	dokładne
INTEGRATION-002	integration	`siem.destination.tested`	dokładne
INTEGRATION-003	integration	`siem.destination.checked`	dokładne
INTEGRATION-004	integration	`notification.channel.tested`	dokładne

Kod	Kategoria	Akcja	Rodzaj
INTEGRATION-005	integration	`notification.smtp.tested`	dokładne
INTEGRATION-006	integration	`monitoring.alert-channel.tested`	dokładne
INTEGRATION-007	integration	`analyst.connection.tested`	dokładne
INTEGRATION-008	integration	`sales.mail.tested`	dokładne
INTEGRATION-009	integration	`siem.archive.expired`	dokładne
INTEGRATION-010	integration	`cloud.snapshot.imported`	dokładne
INTEGRATION-011	integration	`siem.event.skipped`	dokładne
INTEGRATION-012	integration	`siem.destination.replayed`	dokładne
INTEGRATION-013	integration	`siem.event.rejected`	dokładne