



Podstawowe wymagania cyberbezpieczeństwa dla systemów automatyki ICS-OT

Standard Cyberbezpieczeństwa OT

Zał. 1.1.3 Procedura Zarządzania Logami Cyberbezpieczeństwa OT

Zatwierdził	Data	Podpis
Robert Oleński Dyrektor Biura Cyberbezpieczeństwa	15.06.2026	<i>Dokument podpisany elektronicznie dnia 2026.06.16. Oryginał dostępny w Dziale Cyberbezpieczeństwa OT.</i>
Zaakceptował	Data	Podpis
Artur Sidorko Kierownik Działu Cyberbezpieczeństwa OT	21.01.2025	<i>Dokument podpisany elektronicznie dnia 2026.06.16. Oryginał dostępny w Dziale Cyberbezpieczeństwa OT.</i>

	Standard Cyberbezpieczeństwa OT Procedura Zarządzania Logami Cyberbezpieczeństwa OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	2 / 8

Historia zmian dokumentu

Wersja	Data	Osoba	Opis zmian
1.0	21.01.2019 r.	Dział Cyberbezpieczeństwa OT	Utworzenie dokumentu
2.0	15.03.2021 r.	Dział Cyberbezpieczeństwa OT	Aktualizacja dokumentu
3.0	06.02.2023 r.	Dział Cyberbezpieczeństwa OT	Aktualizacja dokumentu
4.0	20.01.2025 r.	Dział Cyberbezpieczeństwa OT	Aktualizacja dokumentu

	Standard Cyberbezpieczeństwa OT Procedura Zarządzania Logami Cyberbezpieczeństwa OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	3 / 8

Spis treści

1.	Cel dokumentu	4
2.	Definicje	4
3.	Zakres stosowania	5
4.	Wymagania ogólne	6
4.1	Źródło danych.....	6
4.2	Źródła syslog	6
4.2.1	Ogólny schemat – Syslog.....	6
4.3	Źródła Windows – Windows Event Forwarding.....	7
4.3.1	Ogólny schemat – Windows Event Forwarding	7
5.	Postanowienia końcowe.....	8

	Standard Cyberbezpieczeństwa OT Procedura Zarządzania Logami Cyberbezpieczeństwa OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	4 / 8

1. Cel dokumentu

Spełnienie wymagań ustawy o krajowym systemie cyberbezpieczeństwa (KSC) w zakresie umożliwiającym wykrywania incydentów bezpieczeństwa z systemów ICS.

Zapewnienie spójnego procesu generowania, przesyłania, przechowywania, analizowania i retencji danych logów bezpieczeństwa z systemów ICS.

Korelacja zebranych logów w centralnym systemie monitorowania.

2. Definicje

KSC – Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa implementująca do polskiego porządku prawnego dyrektywę Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa 2016/1148), tzw. Dyrektywa NIS.

ORLEN S.A. – ORLEN Spółka Akcyjna

Log- zapis zdarzeń zachodzących w systemach i sieciach w organizacji.

Zarządzanie Logami – Proces generowania, przesyłania, przechowywania i analizowania danych z logów.

Log Parsing – Wyodrębnienie danych z dziennika tak, aby sparsowane wartości mogły być użyte jako dane wejściowe dla innego systemu.

SIEM - Security Information and Event Management Software – Program, który służy do gromadzenia, monitorowania i analizowania danych związanych z bezpieczeństwem. Zapewnia korelację informacji pochodzących z wielu źródeł.

Syslog – Protokół określający ogólny format wpisu do dziennika oraz mechanizm transportu.

Rsyslog – Narzędzie typu open source używane w systemach komputerowych typu UNIX i podobne do przekazywania dziennika w sieci IP.

Event Viewer – Składowik systemu operacyjnego Microsoft Windows, który pozwala przeglądać dziennik zdarzeń lokalnie lub zdalnie.

Windows Security Log – Dziennik zabezpieczeń w systemie Microsoft Windows zawierający zapisy dotyczące zdarzeń związanych z bezpieczeństwem określone przez systemowe zasady audytu.

PKI – służy do zarządzania cyfrowymi certyfikatami i kluczami szyfrującymi dla osób, programów i systemów.

Intrusion Detection and Prevention System (IDPS) – Oprogramowanie automatyzujące proces monitorowania zdarzeń zachodzących w systemie komputerowym lub sieci i analizujące je pod kątem oznak możliwych incydentów oraz podejmujące próby powstrzymania wykrytych możliwych incydentów.

	Standard Cyberbezpieczeństwa OT Procedura Zarządzania Logami Cyberbezpieczeństwa OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	5 / 8

Transport Layer Security (TLS) – protokół oparty o szyfrowanie asymetryczne zapewniający poufność i integralność transmisji danych.

WEC – usługa Windows Event Collector, która zarządza subskrypcjami zdarzeń ze zdalnych źródeł, które obsługują protokół WS Management.

Infrastruktura klucza Publicznego (PKI) – zbiór osób, polityk, procedur i systemów komputerowych niezbędnych do świadczenia usług uwierzytelniania, szyfrowania, integralności i niezaprzeczalności za pośrednictwem kryptografii klucza publicznego i prywatnego i certyfikatów elektronicznych.

WinRM (Windows Remote Management) – jest implementacją WS-Management firmy Microsoft w systemie Windows, która pozwala systemem na dostęp lub wymianę informacji o zarządzaniu poprzez wspólną sieć.

Active Directory (AD) – jest usług katalogową opracowaną przez firmę Microsoft dla sieci domenowych Windows. Jest ona zawarta w większości systemów operacyjnych Windows Server jako zestaw procesów i usług.

Group Policy Object (GPO) - która kontroluje środowisko pracy kont użytkowników i kont komputerów. Zasady grupy zapewniają scentralizowane zarządzanie i konfigurację systemów operacyjnych, aplikacji i ustawień użytkowników w środowisku Active Directory.

Grupa robocza – logiczny zespół [komputerów](#) połączonych ze sobą siecią

Industrial Control System (ICS) – oznacza przemysłowe systemy sterowania min. systemy monitorowania, zabezpieczania i kontroli przemysłowej) należy interpretować w rozumieniu systemów monitorowania, sterowania i bezpieczeństwa infrastruktury przemysłowej (wszystkie stacje PC, serwery, sterowniki PLC, kontrolery, urządzenia sieciowe, specjalistyczne oprogramowanie urządzeń).

3. Zakres stosowania

Procedura zarządzania logami w ORLEN ORLEN S.A. zwana dalej procedurą reguluje sposób zbierania informacji o zdarzeniach z wielu źródeł systemów ICS, w tym oprogramowania zabezpieczającego, takiego jak: oprogramowanie antywirusowe, zapory sieciowe, systemy wykrywania i zapobiegania włamaniom (IDPS), systemy operacyjne na serwerach, stacjach roboczych i urządzeniach sieciowych, aplikacjach oraz innych źródłach zapewniających wymagany analizą ryzyka poziom akceptacji ryzyka.

Niniejsza procedura ma za zadanie:

- ujednolicenie sposobu zbierania i zarządzania logami bezpieczeństwa w kontekście liczby, objętości i różnorodności,
- zapewnienie spójnego podejścia do analizy logów dla identyfikacji incydentów bezpieczeństwa z systemów ICS w ORLEN S.A.

	Standard Cyberbezpieczeństwa OT Procedura Zarządzania Logami Cyberbezpieczeństwa OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	6 / 8

4. Wymagania ogólne

4.1 Źródło danych

Podstawowym źródłem danych są logi generowane przez systemy, urządzenia i aplikacje.

Standardowymi typami logów, które gromadzone są w ORLEN S.A. to:

4.2 Źródła syslog

System Logging Protocol ułatwia przesyłanie informacji z wielu różnych typów urządzeń i aplikacji do centralnego serwera, zwanego jako serwer logów w określonym formacie wiadomości.

Ten protokół rejestrowania jest kluczową częścią monitorowania infrastruktury (urządzeń sieciowych, aplikacji) i pozwala śledzić ogólny stan urządzeń poprzez uproszczone zarządzanie komunikatami dziennika.

Poniżej przykładowa architektura sieciowa stosowana w ORLEN S.A. dla zbierania zdarzeń typu syslog.

4.2.1 Ogólny schemat – Syslog

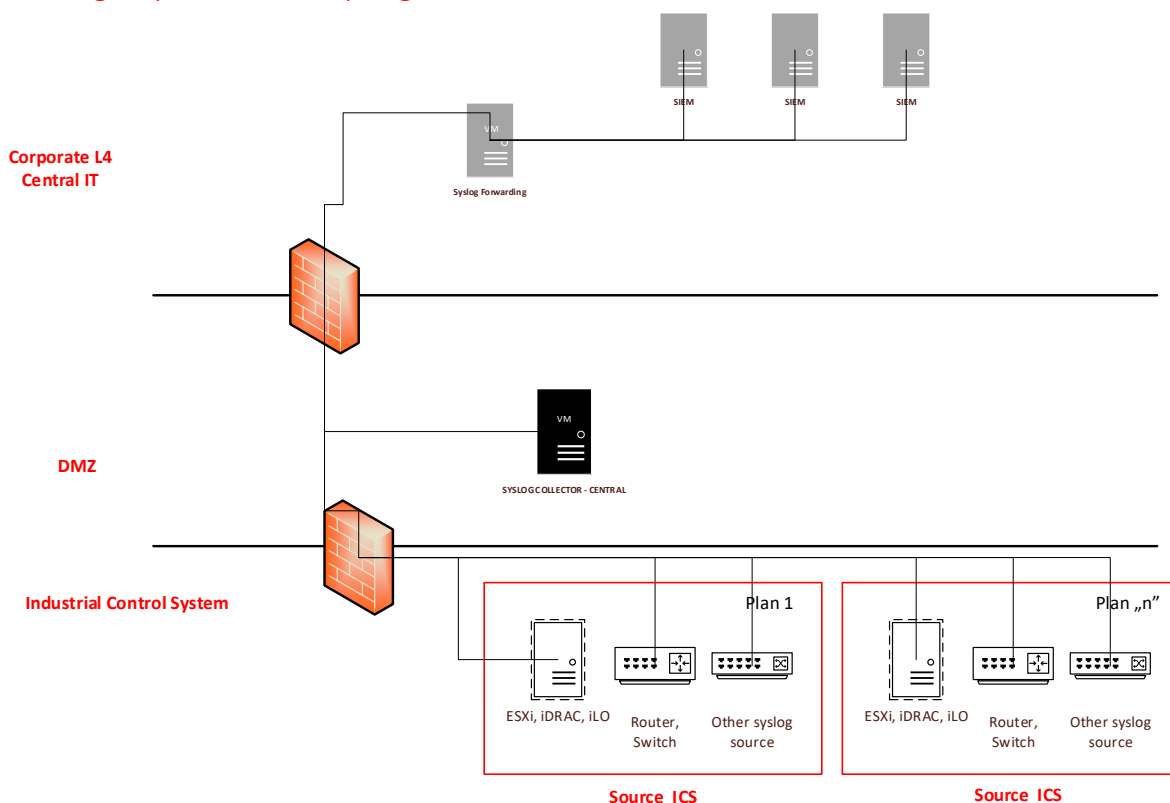


Figure 2 Syslog- diagram sieciowy

	Standard Cyberbezpieczeństwa OT Procedura Zarządzania Logami Cyberbezpieczeństwa OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	7 / 8

4.3 Źródła Windows – Windows Event Forwarding

Dziennik zdarzeń systemu Windows to szczegółowy zapis zdarzeń związanych z systemem, zabezpieczeniami i aplikacjami przechowywanymi w systemie operacyjnych Windows.

Zbieranie zdarzeń z systemów Windows (Windows Event Log) powinno odbywać się zgodnie z przedstawioną architekturą sieciową stosowaną w ORLEN S.A. bazującą na subskrypcji funkcjonalności Windows Event Forwarding.

4.3.1 Ogólny schemat – Windows Event Forwarding

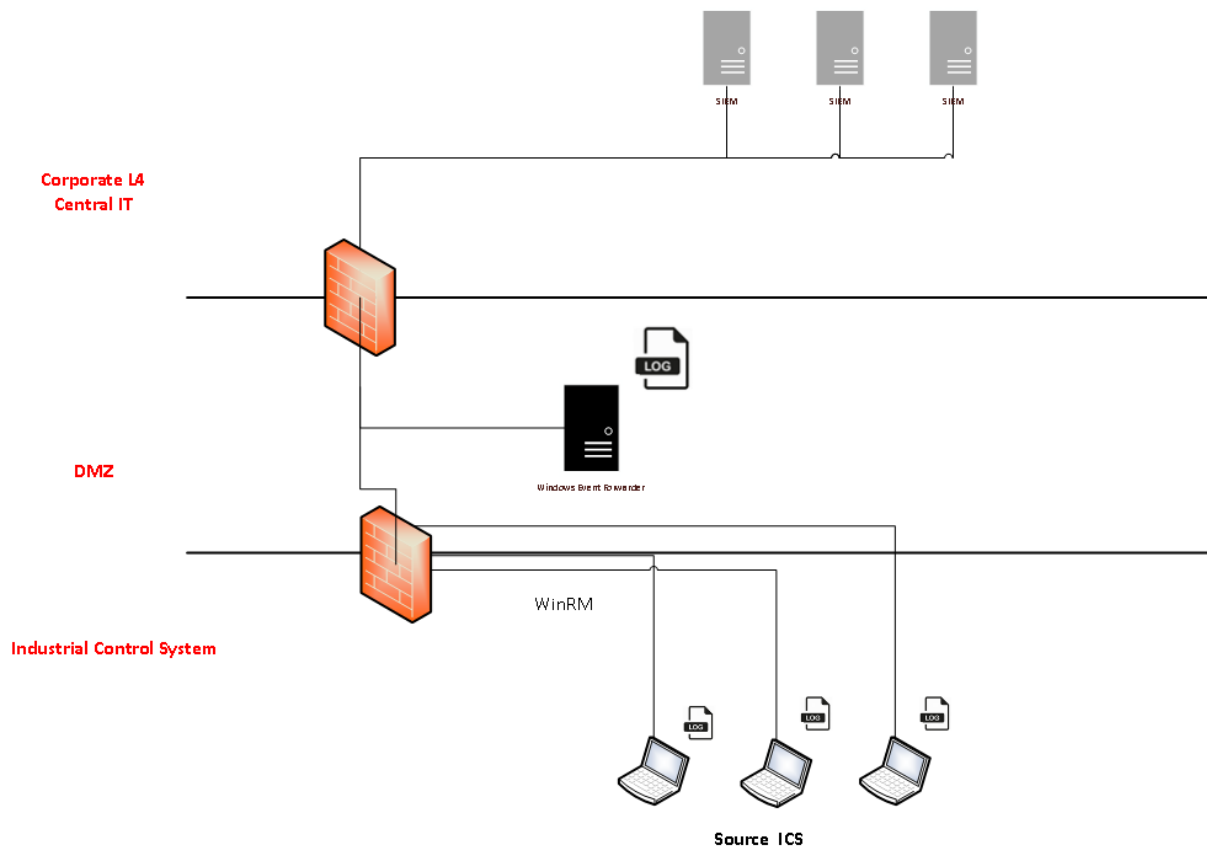


Figure 3 Windows Event - diagram sieciowy

Szczegółowe informacje odnośnie konfiguracji poszczególnych rozwiązań zostaną przekazane na prośbę oferenta po podpisaniu umowy.

Dopuszcza się wdrożenia innego rozwiązania po akceptacji Obszaru Cyberbezpieczeństwa OT ORLEN S.A.

	Standard Cyberbezpieczeństwa OT Procedura Zarządzania Logami Cyberbezpieczeństwa OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	8 / 8

5. Postanowienia końcowe

Właścicielem niniejszego standardu jest Obszar Cyberbezpieczeństwa OT ORLEN S.A. Jakikolwiek zmiany lub aktualizacje w dokumencie muszą być realizowane za zgodą i przez Obszar Cyberbezpieczeństwa OT ORLEN S.A. Każda aktualizacja dokumentu musi być zaakceptowana przez osobę kierownika Obszar Cyberbezpieczeństwa OT ORLEN S.A.