
	Standard Cyberbezpieczeństwa OT <hr/> Załącznik nr 3 do Standardu Cyberbezpieczeństwa OT - Procedura Zarządzania Logami Security	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	1 z 6




Standard Cyberbezpieczeństwa OT

Załącznik nr 3 do Standardu Cyberbezpieczeństwa OT **Procedura Zarządzania Logami Security**

	Standard Cyberbezpieczeństwa OT Załącznik nr 3 do Standardu Cyberbezpieczeństwa OT - Procedura Zarządzania Logami Security	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	2 z 6

Spis treści

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

	Standard Cyberbezpieczeństwa OT Załącznik nr 3 do Standardu Cyberbezpieczeństwa OT - Procedura Zarządzania Logami Security	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	3 z 6

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.

GK ORLEN – Grupa Kapitałowa ORLEN

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

	Standard Cyberbezpieczeństwa OT Załącznik nr 3 do Standardu Cyberbezpieczeństwa OT - Procedura Zarządzania Logami Security	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	4 z 6

oznak możliwych incydentów oraz podejmujące próby powstrzymania wykrytych możliwych incydentów.

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 PKN 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 PKN ORLEN S.A.

	Standard Cyberbezpieczeństwa OT Załącznik nr 3 do Standardu Cyberbezpieczeństwa OT - Procedura Zarządzania Logami Security	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	5 z 6

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 GK ORLEN 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 GK ORLEN dla zbierania zdarzeń typu syslog.

4.2.1 Ogólny schemat – Syslog

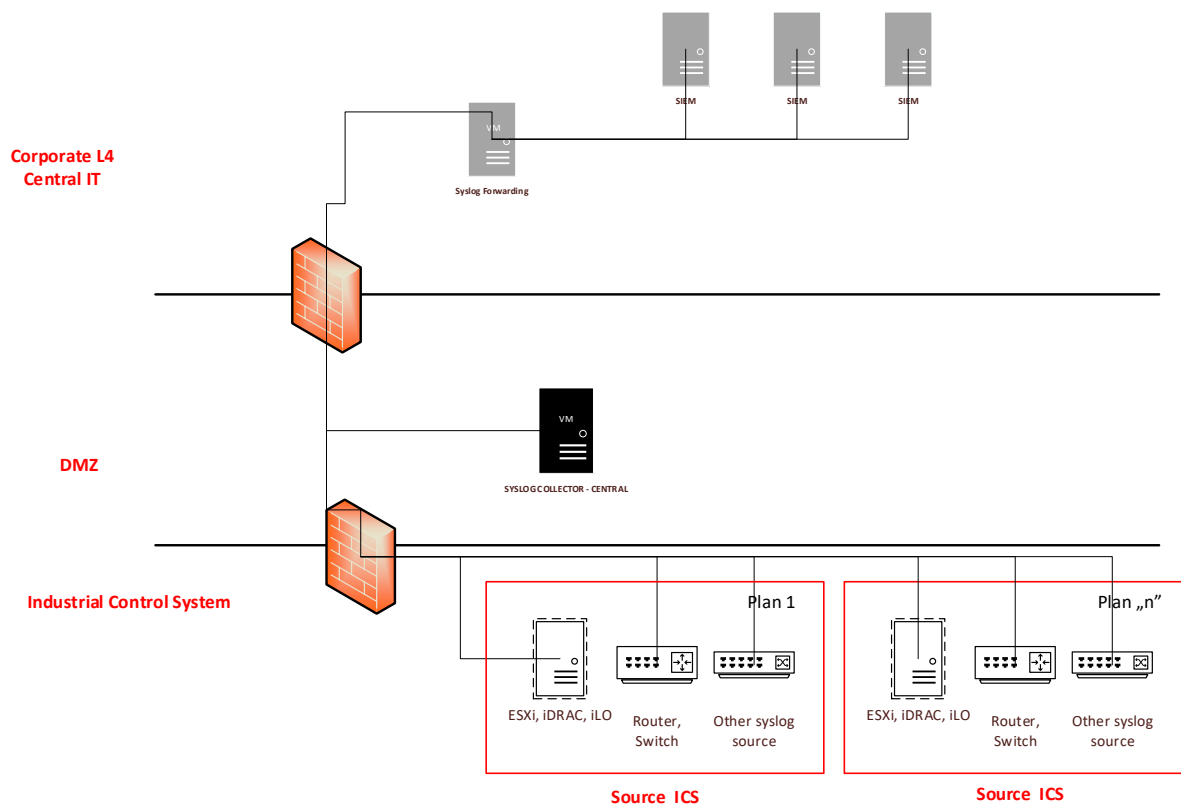



Figure 2 Syslog- diagram sieciowy

	Standard Cyberbezpieczeństwa OT Załącznik nr 3 do Standardu Cyberbezpieczeństwa OT - Procedura Zarządzania Logami Security	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	6 z 6

4.3 Źródła Windows Event Log

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

Poniżej przykładowa architektura sieciowa stosowana w GK ORLEN dla zbierania zdarzeń typu Windows Event Log.

4.3.1 Ogólny schemat – Windows Event Log

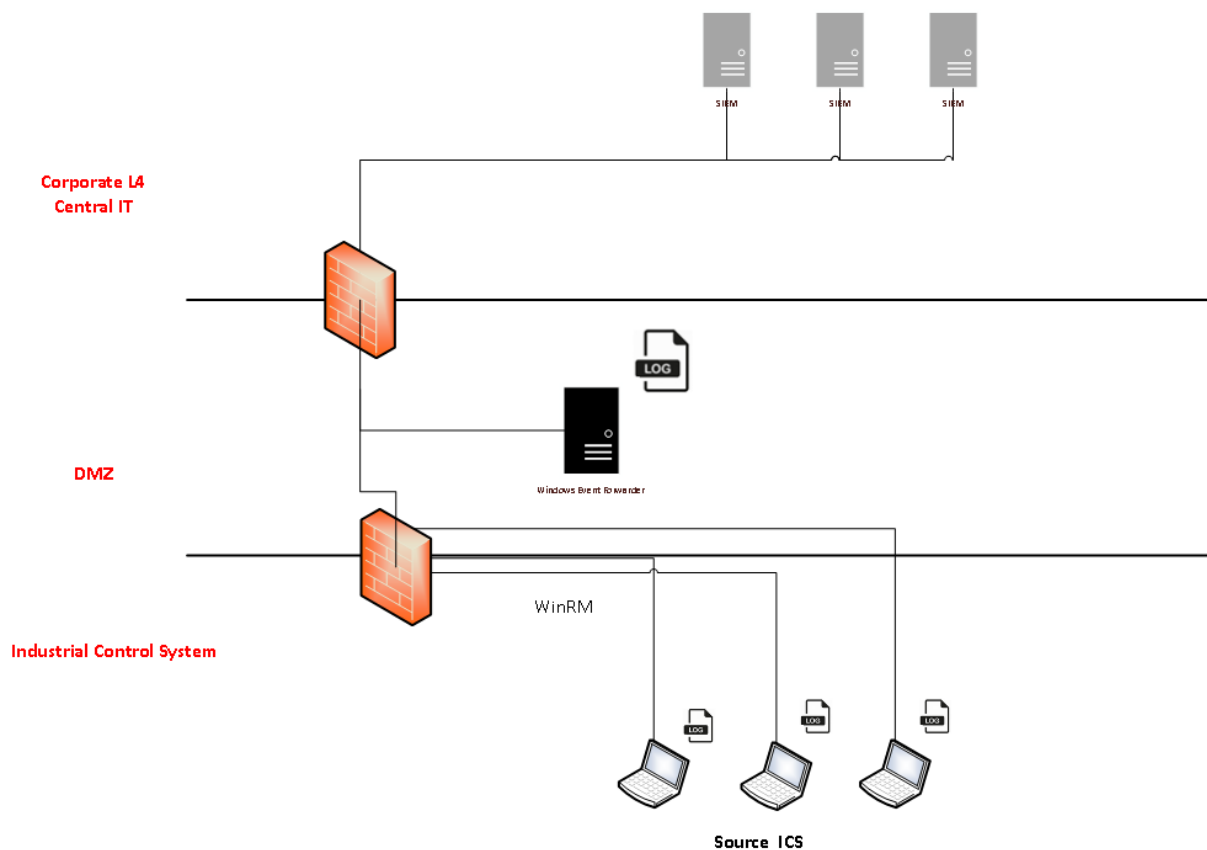


Figure 3 Windows Event - diagram sieciowy

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

Dopuszcza się wdrożenia innego rozwiązania po akceptacji działu Cyberbezpieczeństwa OT w PKN ORLEN