

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa i wdrożenie systemu klasy
Endpoint Detection and Response (EDR)
dla środowiska OT/ICS/SCADA

**Część nr 4 zamówienia – Zadanie nr 3 obszaru technicznego OT wniosku o
dofinansowanie**

1. Informacje ogólne

Niniejszy Opis Przedmiotu Zamówienia (OPZ) określa minimalne wymagania techniczne i funkcjonalne dotyczące dostawy, wdrożenia i licencjonowania systemu klasy Endpoint Detection and Response (EDR) przeznaczonego do ochrony stacji roboczych w środowisku OT (stacje operatorskie SCADA, stacje inżynierskie, stacje terminalowe).

System musi być zaprojektowany z uwzględnieniem specyfiki środowisk przemysłowych: wsparcia dla starszych systemów operacyjnych, pracy w trybie offline (bez połączenia z Internetem), braku wpływu na ciągłość procesów produkcyjnych oraz natywnej ochrony aplikacji klasy OT.

Parametr	Wartość
Przedmiot zamówienia	System EDR klasy OT – agenci endpoint + konsola zarządzająca
Środowisko docelowe	OT/ICS/SCADA: stacje operatorskie, stacje inżynierskie, stacje terminalowe
Architektura	Agent na stacji roboczej + konsola zarządzająca w serwerowni OT
Tryb pracy agenta	Online (z konsolą) lub standalone (bez konsoli)
Tryb sieciowy	Praca bez połączenia z Internetem (air-gap)
Maks. zużycie RAM przez agenta	≤ 600 MB (przy uruchomionych wszystkich usługach, w tym AV Real-Time)
Licencja	Subskrypcja ważna co najmniej do 31.12.2026 r. albo licencja wieczysta – 10 agentów + konsola zarządzająca
Gwarancja	5 lat
Wsparcie systemów Windows	Min. 3 lata od daty odbioru: Windows 2000, XP, 7 i nowsze
Wsparcie systemów Linux	RHEL/CentOS 6/7/8/9, Rocky Linux 8.4/9/10, Ubuntu 18/20/22, Debian 10/11
Certyfikacja producenta	IEC 62443-4-1

2. Zakres przedmiotu zamówienia

Przedmiotem zamówienia jest:

- Dostawa oprogramowania agentów EDR klasy OT wraz z licencjami subskrypcyjnymi lub wieczystymi na 10 agentów chroniących stacje robocze wskazane przez Zamawiającego w środowisku OT.
- Dostawa i wdrożenie konsoli zarządzającej w serwerowni OT Zamawiającego wraz z licencjami dołączonymi do licencji agentów.
- Instalacja i konfiguracja agentów na stacjach roboczych OT (stacje operatorskie SCADA, stacje inżynierskie, stacje terminalowe).

- Konfiguracja polityk bezpieczeństwa, białych list aplikacji, ochrony USB i ochrony plików.
- Przeprowadzenie szkoleń dla administratorów systemu.
- Dostarczenie dokumentacji powykonawczej w terminie do 14 dni od zakończenia wdrożenia.

3. Minimalne wymagania – obsługiwane systemy operacyjne

3.1. Systemy Windows

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Wsparcie dla starszych systemów Windows	Agent musi obsługiwać co najmniej następujące systemy operacyjne Windows: – Windows 2000 – Windows XP – Windows 7 – Windows 8 / 8.1 – Windows 10 – Windows 11 – Windows Server 2008 / 2012 / 2016 / 2019 / 2022 Wsparcie musi być zapewnione przez co najmniej 3 lata od daty odbioru.
2	Krytyczność wsparcia starszych wersji	Wsparcie dla systemów Windows XP i Windows 7 jest wymaganiem bezwzględnym, ze względu na obecność tych systemów na stacjach operatorskich SCADA Zamawiającego, których modernizacja nie jest możliwa w bieżącym postępowaniu.

3.2. Systemy Linux

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	RHEL / CentOS	Agent musi obsługiwać: RHEL / CentOS 6, 7, 8, 9.
2	Rocky Linux	Agent musi obsługiwać: Rocky Linux 8.4, 9, 10.
3	Ubuntu	Agent musi obsługiwać: Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS.
4	Debian	Agent musi obsługiwać: Debian 10 (Buster), Debian 11 (Bullseye).

4. Minimalne wymagania funkcjonalne – agent EDR

4.1. Ochrona aplikacji OT i plików

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Wbudowana ochrona aplikacji OT	Agent musi posiadać wbudowaną, natywną ochronę aplikacji klasy OT, w tym co najmniej: Siemens TIA

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
		Portal, CODESYS – bez konieczności ręcznej konfiguracji przez administratora.
2	Natywne rozpoznawanie certyfikatów i plików wykonywalnych	Agent musi natywnie rozpoznawać certyfikaty cyfrowe oraz pliki wykonywalne i na tej podstawie automatycznie budować ochronę.
3	Automatyczna ochrona plików wykonywalnych	Agent musi automatycznie chronić pliki wykonywalne bez konieczności samodzielnego ich dodawania do listy plików chronionych przez administratora.
4	Ręczne wskazanie ścieżek chronionych	Administrator musi mieć możliwość ręcznego wskazania ścieżek i folderów zawierających pliki objęte ochroną (np. pliki diagramów systemu SCADA).
5	Ochrona integralności plików	Agent musi zapewniać brak możliwości usunięcia oraz wprowadzenia nieautoryzowanych zmian w plikach znajdujących się w chronionych folderach (np. foldery z plikami diagramów SCADA). Wszelkie próby modyfikacji lub usunięcia muszą być blokowane i rejestrowane.

4.2. Biała lista zaufanych aplikacji (Application Whitelisting)

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Automatyczne skanowanie przy instalacji	Przy instalacji agenta system musi automatycznie skanować system operacyjny w poszukiwaniu zainstalowanych aplikacji, ustawień rejestrów systemowych i bibliotek DLL w celu zbudowania bazowej listy zaufanych aplikacji.
2	Blokowanie niezaufanych aplikacji	Agent musi ograniczać stację komputerową wyłącznie do uruchamiania aplikacji z zaufanej listy (whitelist). Uruchomienie aplikacji spoza listy musi być automatycznie blokowane i rejestrowane w logach.
3	Tryb serwisowy (Service Mode)	Agent musi posiadać dedykowany tryb serwisowy przeznaczony do wprowadzania zmian na stacjach podczas okien serwisowych lub w sytuacjach awaryjnych: – W trybie serwisowym dozwolone jest instalowanie nowych aplikacji i aktualizacji – Poza trybem serwisowym instalowanie aplikacji spoza whitelist musi być automatycznie blokowane
4	Analiza behawioralna skryptów	Mechanizm uczenia i analizy behawioralnej musi obejmować zachowania skryptów. W odpowiednim trybie system musi wymagać pełnej zgodności nie tylko nazwy skryptu, ale również całego łańcucha wywołań procesu macierzystego (parent process chain).

4.3. Ochrona antywirusowa

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Ochrona antywirusowa Real-Time	Agent musi posiadać wbudowaną ochronę antywirusową w czasie rzeczywistym (Real-Time Protection / On-Access Scanning).
2	Limit zużycia zasobów	Maksymalne zużycie pamięci RAM przez agenta przy uruchomionych wszystkich usługach (w tym ochrony antywirusowej Real-Time) nie może przekraczać 600 MB.
3	Praca bez połączenia z Internetem	Ochrona antywirusowa musi działać poprawnie bez stałego połączenia z Internetem. Aktualizacje sygnatur muszą być możliwe w trybie offline (np. przez konsolę zarządzającą lub nośnik).

4.4. Ochrona portów USB i nośników zewnętrznych

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Ochrona portów USB	Agent musi posiadać mechanizm kontroli portów USB umożliwiający blokowanie nieautoryzowanych urządzeń USB.
2	Biała lista nośników USB – metatagi	System musi obsługiwać białą listę dopuszczonych nośników USB budowaną na podstawie metatagów (identyfikatorów urządzenia, np. VID/PID/numer seryjny), a nie wyłącznie na podstawie klasy urządzenia.
3	Jednorazowe dopuszczenie urządzenia	System musi umożliwiać jednorazowe dopuszczenie urządzenia USB spoza białej listy (np. przez administratora lub z użyciem kodu jednorazowego) bez trwałego dodawania go do listy zaufanych.

4.5. Analiza behawioralna i mechanizm uczenia

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Wbudowany mechanizm uczenia behawioralnego	Agent musi posiadać wbudowany mechanizm automatycznego uczenia się i monitorowania zachowań operacyjnych stacji roboczej. Mechanizm musi analizować bieżący ruch aplikacyjny i budować bazowy profil normalnego zachowania.
2	Analiza łańcucha wywołań procesów (process chain)	Analiza behawioralna musi obejmować weryfikację pełnego łańcucha wywołań procesów macierzystych (parent process chain), nie tylko samych nazw plików wykonywalnych.
3	Kontrola argumentów skryptów	W odpowiednim trybie system musi wymagać pełnej zgodności nie tylko nazwy skryptu, ale również

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
		argumentów wywołania i łańcucha procesów macierzystych.

4.6. Tryby pracy agenta

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Tryb standalone (bez konsoli)	Agent musi obsługiwać tryb standalone – pełna ochrona stacji roboczej bez konieczności komunikacji z konsolą zarządzającą. Tryb ten jest wymagany dla stacji w segmentach sieciowych odizolowanych od serwerowni OT.
2	Tryb online (z konsolą zarządzającą)	Agent musi obsługiwać tryb online z pełną komunikacją z konsolą zarządzającą – centralne zarządzanie politykami, aktualizacjami i raportowaniem.
3	Praca offline (bez Internetu)	Agent oraz konsola zarządzająca muszą działać poprawnie bez połączenia z Internetem (środowisko air-gap / izolowane).

5. Minimalne wymagania – konsola zarządzająca

5.1. Architektura i wdrożenie

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Lokalna instalacja w serwerowni OT	Konsola zarządzająca musi być instalowana lokalnie w serwerowni środowiska OT Zamawiającego – nie dopuszcza się wyłącznie rozwiązań SaaS/chmurowych jako jedynej opcji zarządzania.
2	Licencje agentów dołączone do konsoli	Konsola zarządzająca musi być dostarczana wraz z licencjami agentów w ramach jednej transakcji licencyjnej.
3	Aktualizacja agentów bez restartu stacji	Konsola musi umożliwiać aktualizację agentów oraz polityk bezpieczeństwa bez konieczności restartowania stacji komputerowych.

5.2. Zarządzanie grupami i lokalizacjami

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Tworzenie grup urządzeń wg lokalizacji	Konsola musi umożliwiać tworzenie osobnych grup urządzeń dla poszczególnych lokalizacji (np. stacja uzdatniania wody A, oczyszczalnia B, ujęcie C).

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
2	Gradacja uprawnień i RBAC	System musi obsługiwać gradację uprawnień – różne poziomy dostępu dla różnych administratorów. Uprawnienia administracyjne muszą umożliwiać tworzenie indywidualnych polityk dla wskazanej lokalizacji.
3	Polityki globalne z wyjątkami lokalnymi	System musi umożliwiać wymuszenie polityk globalnych z możliwością definiowania wyjątków dla poszczególnych lokalizacji w zakresie: – Listy dopuszczonych nośników USB – Listy wyjątków dotyczących aplikacji objętych skanowaniem antywirusowym Real-Time – Haseł dostępu administracyjnego do agentów – Procesów autoryzowanych do wprowadzania zmian w chronionych plikach lub aplikacjach

6. Licencjonowanie

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Licencja subskrypcyjna lub wieczysta – 10 agentów	System musi być dostarczony z licencją subskrypcyjną ważną co najmniej do 31.12.2026 r. lub wieczystą dla 10 agentów oraz konsoli zarządzającej. Licencja obejmuje 10 stanowisk (stacji roboczych OT) chronionych przez agentów EDR. .
2	Aktualizacje i wsparcie	Licencja musi obejmować dostęp do aktualizacji oprogramowania agentów i konsoli oraz aktualizacji sygnatur bezpieczeństwa przez cały okres aktywnej subskrypcji.
3	Gwarancja	Gwarancja producenta na oprogramowanie (poprawność działania, błędy krytyczne): 5 lat od daty odbioru.

7. Certyfikacja producenta

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	IEC 62443-4-1 (wymagane)	Producent dostarczanego oprogramowania EDR musi posiadać certyfikat IEC 62443-4-1 potwierdzający bezpieczny proces tworzenia oprogramowania dla systemów bezpieczeństwa przemysłowego. Wykonawca zobowiązany jest przedstawić kopię certyfikatu lub link do rejestru organu certyfikującego.
2	Dodatkowe certyfikacje (mile widziane)	Mile widziane dodatkowe certyfikacje: IEC 62443-4-2, Common Criteria (CC), certyfikaty branżowe dla sektora wodno-kanalizacyjnego.

8. Wymagania dotyczące wdrożenia i szkoleń

- Wykonawca przeprowadzi instalację i konfigurację konsoli zarządzającej w serwerowni OT Zamawiającego.
- Wykonawca przeprowadzi instalację agentów na wszystkich wskazanych stacjach roboczych środowiska OT.
- Wykonawca skonfiguruje bazowe polityki bezpieczeństwa: białą listę aplikacji (na podstawie automatycznego skanowania przy instalacji), ochronę USB, ochronę plików, grupy urządzeń wg lokalizacji.
- Wykonawca przeprowadzi fazę uczenia behawioralnego agentów i zaprezentuje wygenerowane reguły administratorom Zamawiającego.
- Wykonawca przeprowadzi szkolenie dla minimum 2 administratorów systemu z zakresu obsługi konsoli zarządzającej, zarządzania politykami i procedur serwisowych (tryb serwisowy).
- Wykonawca dostarczy dokumentację powykonawczą (opis konfiguracji, procedury operacyjne, instrukcja trybu serwisowego) w terminie do 14 dni od zakończenia wdrożenia.