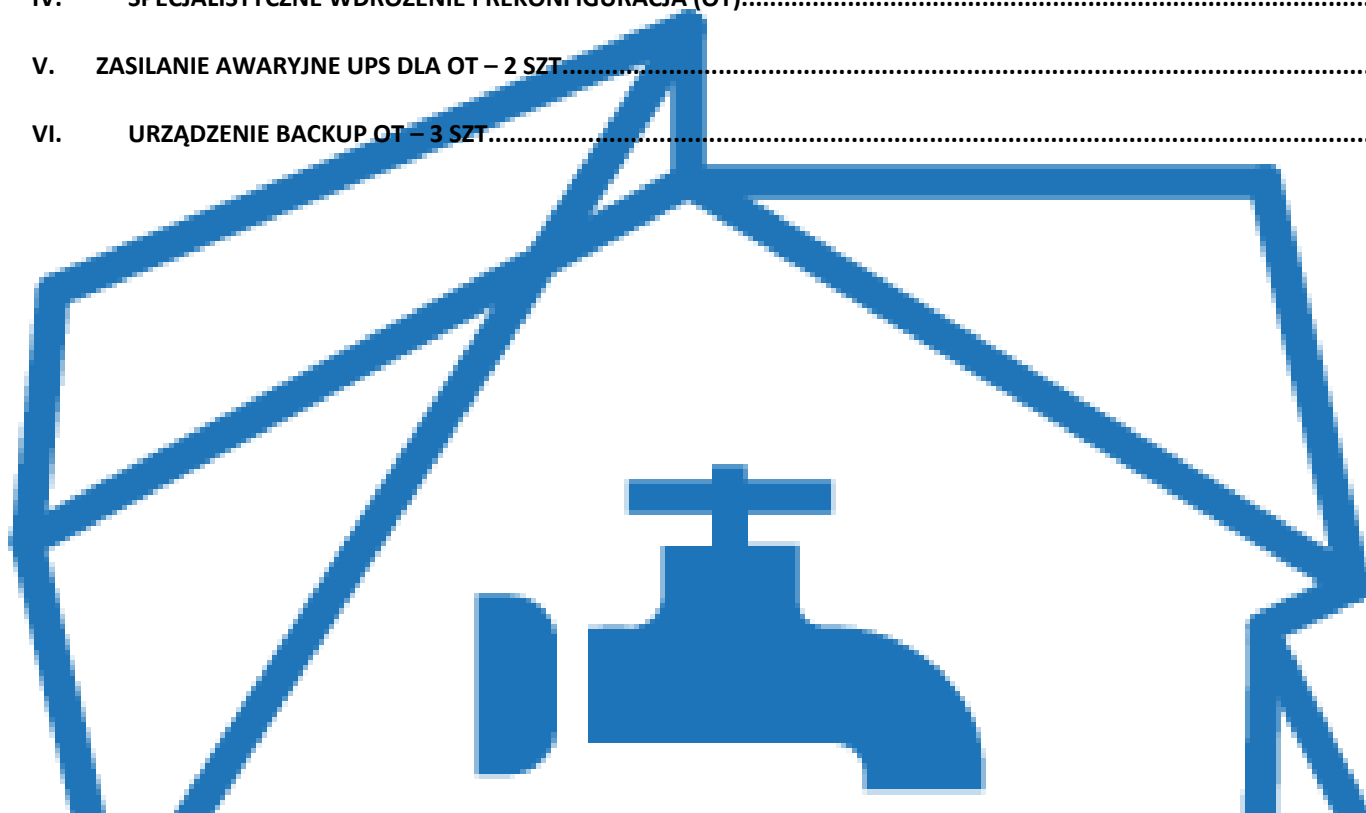


Załącznik Nr 1 do SWZ SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

Na potrzeby postępowania zakupowego pn.: „...Dostawa sprzętu i oprogramowania w ramach projektu grantowego Cyberbezpieczne Wodociągi - Obszar techniczny OT” w ramach projektu “Cyberbezpieczne Wodociągi” Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo: “Cyberbezpieczeństwo – Cyberbezpieczne Wodociągi”. Krajowy Plan Odbudowy i Zwiększania Odporności finansowany ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności.

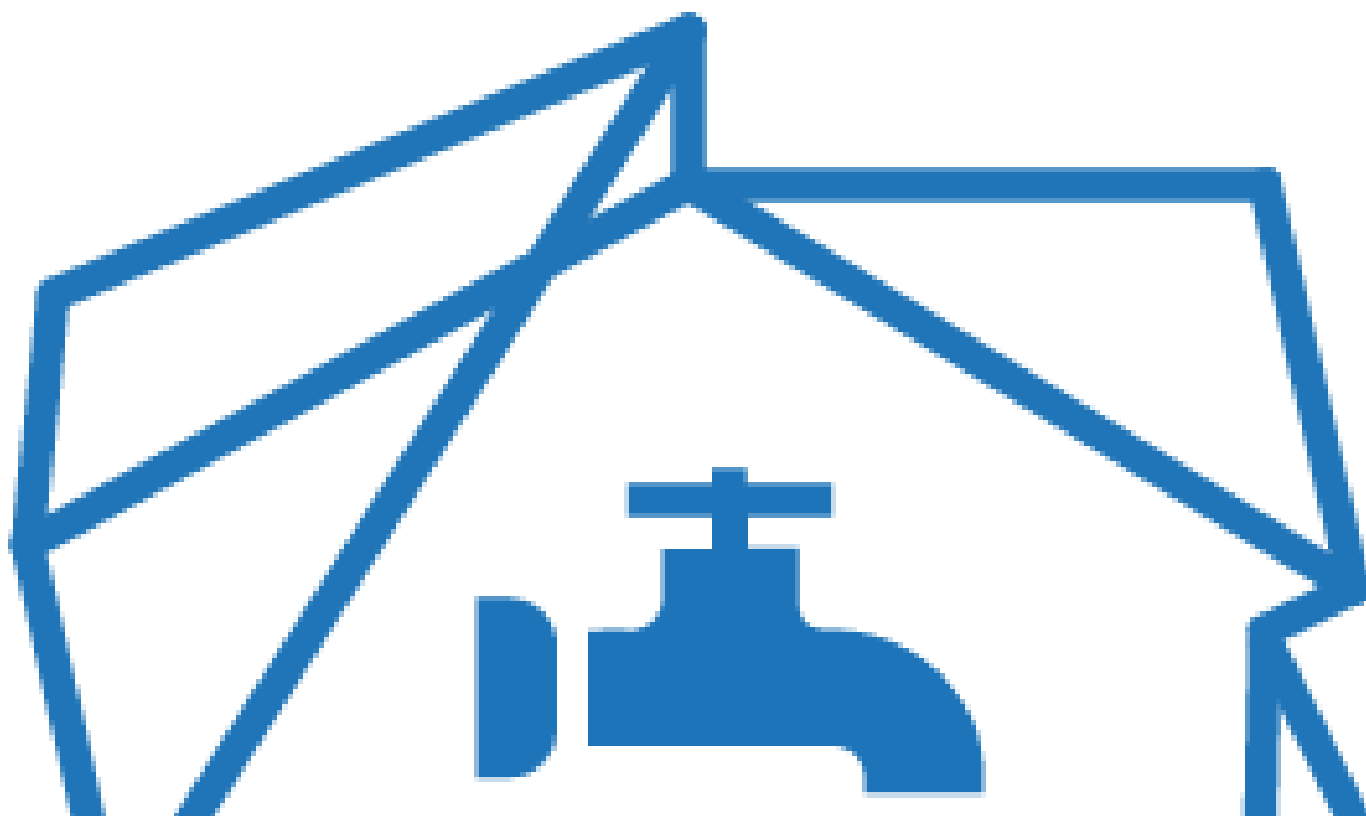
Spis treści

WYMAGANIA OGÓLNE.....	2
I. SYSTEM IDS DLA OT - MONITORING SIECI – 1 ZEST.....	3
II. ZESTAW SPRZĘTOWYCH SOND DO MONITOROWANIA SIECI OT – 1 ZEST.....	15
III. SWITCHE ZARZĄDZALNE OT – 2 SZT.....	19
IV. SPECJALISTYCZNE WDROŻENIE I REKONFIGURACJA (OT).....	23
V. ZASILANIE AWARYJNE UPS DLA OT – 2 SZT.....	25
VI. URZĄDZENIE BACKUP OT – 3 SZT.....	29



Wymagania ogólne

W przypadkach, kiedy w szczegółowym opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”. Dostarczany sprzęt musi być nowy, nieużywany, nieregenerowany, kompletny, wyprodukowany nie wcześniej niż w 2025 r., wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie, pochodzić z oficjalnego kanału dystrybucyjnego. Przez "wadę fizyczną" należy rozumieć również jakąkolwiek niezgodność ze szczegółowym opisem przedmiotu zamówienia. Sprzęt musi być wyposażony we wszystkie niezbędne do jego działania i zapewnienia wymaganych funkcjonalności Sprzętu standardowe rozwiązania softwarowe wraz z prawem do bezterminowego korzystania przez Zamawiającego z tych rozwiązań w takiej funkcji, jednakże w każdym przypadku nie krócej, niż przez czas, w jakim będzie technicznie możliwe używanie Sprzętu. O ile inaczej nie zaznaczono, wszelkie zapisy SOPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.



I. System IDS dla OT - monitoring sieci – 1 zest.

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa 1 sztuki oprogramowania dedykowanego do detekcji zagrożeń i monitorowania bezpieczeństwa sieci OT, wraz z kompletem licencji niezbędnych do jego pełnego uruchomienia, konfiguracji oraz eksploatacji, zgodnie z wymaganiami technicznymi i funkcjonalnymi określonymi przez Zamawiającego.

2. Wymagania dotyczące rozwiązania

2.1. Centralny system bezpieczeństwa

- Preferuje się system zintegrowany z jedną konsolą zarządzającą dla poniższych grup funkcyjnych.
- Dopuszcza się stosowanie wielu rozwiązań, pod warunkiem integracji umożliwiającej wizualizację danych na centralnych pulpitych bezpieczeństwa, bez konieczności uruchamiania dedykowanych konsol dla pozostałych systemów wchodzących w skład architektury.
- Wymaga się, aby wszystkie zastosowane grupy programowe nie miały ograniczeń licencyjnych na ilość przetwarzanych danych, ilość adresów IP czy MAC.

2.2. System SIEM/IDS/

PARAMETR	OPIS / WARTOŚĆ PARAMETRU	ILOŚĆ
Ilość użytkowników	Ilość jednoczesnych logowań Ilość licencjonowanych użytkowników	Bez ograniczeń licencyjnych
Okres objęty licencją	Licencja bezterminowa czasowo	n/d
Dostęp dla użytkownika	Przez przeglądarkę internetową	n/d
Projektowanie widoczności danych	Poprzez interfejs GUI	n/d
Pulpity operacyjne	Ilość możliwych pulpitych do	Bez ograniczeń

PARAMETR	OPIS / WARTOŚĆ PARAMETRU	ILOŚĆ
	wprowadzenia	
Ilość instancji	Ilość wymaganych instalacji przez Zamawiającego	1
Miejsce instalacji	Lokalna u Zamawiającego	n/d
Instalacja chmurowa	Nie dopuszczalna	n/d
Wymagana integracja	XDR	n/d
Wsparcie AI	TAK	Zdalnie u producenta / niedopuszczalna jest komunikacja z chmurą lub systemami zlokalizowanymi poza Polską.

2.3. Opis ogólny

- Wymagany system powinien stanowić centralny panel wizualizacji stanu bezpieczeństwa OT i aktywności systemu cyberbezpieczeństwa. Musi umożliwiać operatorowi SOC (Security Operations Center) lub administratorowi OT szybki wgląd w sytuację bezpieczeństwa, liczbę zdarzeń, alarmów oraz aktywność urządzeń w sieci.
- Zamawiający oczekuje zintegrowanego systemu klasy SIEM/IDS/Asset/NSPM dla środowisk przemysłowych, łączącym funkcje bezpieczeństwa, inwentaryzacji i zarządzania politykami w jednym środowisku. System musi być zaprojektowany specjalnie dla infrastruktury OT/ICS i oferować pasywne monitorowanie, automatyczną analizę, raportowanie ryzyka i korelację zdarzeń bez domyślnej ingerencji w proces produkcyjny.

2.4. Wymagane minimalne funkcjonalności systemu IDS:

- Monitoring i korelacja zdarzeń (SIEM / IDS)
 - Centralna baza wszystkich zdarzeń z systemów IT, OT i IoT.
 - Korelacja logów z różnych źródeł (firewalle, routery, IDS, serwery, PLC).
 - Wykrywanie i grupowanie incydentów bezpieczeństwa.
 - Analiza w czasie rzeczywistym z klasyfikacją ryzyka (niski/średni/wysoki).
 - Automatyczna identyfikacja powiązanych zasobów i relacji między nimi.
 - Widok szczegółów alarmu: reguła, czas, źródło, typ, ryzyko, status.

- g) Integracja z silnikiem reguł alarmowych (Zasady alarmowe).
- h) Wsparcie dla korelacji według MITRE ATT&CK (np. T1040, T1071).
- i) Pełna historia i oś czasu zdarzeń (timeline).
- j) Możliwość filtrowania, eksportu i analizy porównawczej.
- System alarmowy (IDS/IPS/Anomalie sieciowe)
 - a) Wykrywanie anomalii sieciowych w oparciu o sygnatury i heurystykę.
 - b) Detekcja nieautoryzowanego ruchu, nietypowych portów i protokołów.
 - c) Identyfikacja potencjalnych prób eksfiltracji danych lub sniffingu.
 - d) Integracja z modułem Network Anomalies.
 - e) Wsparcie dla CVE i korelacja podatności (np. CVE-2020-0796).
 - f) Klasyfikacja alarmów wg typu i priorytetu ryzyka.
 - g) Mapowanie powiązanych zasobów i adresów IP/MAC.
 - h) Powiązanie alarmów z konkretnymi urządzeniami producenta systemu oraz innymi źródłami danych.
 - i) Możliwość ręcznego lub automatycznego zamykania alarmów.
 - j) Historia alarmów i statusów (aktywny, ponownie otwarty, zamknięty).
- Inwentarz zasobów (Asset)
 - a) Automatyczna identyfikacja zasobów w sieci (adres MAC, IP, model, OS).
 - b) Profilowanie urządzeń i przypisywanie ich do grup lub sieci.
 - c) Baza konfiguracji sprzętowych i programowych (CPU, RAM, porty, OS).
 - d) Klasyfikacja urządzeń: ICS Dev, Router, Switch, Serwer, Host, SCADA itp.
 - e) Przypisywanie wartości aktywa (1–10) oraz poziomu ryzyka.
 - f) Rejestr zdarzeń powiązanych z zasobem.
 - g) Historia zmian konfiguracji i aktualizacji.
 - h) Wbudowany edytor zasobu i przypisanie do sieci/peryferii.
 - i) Możliwość dodania notatek technicznych lub operacyjnych.
 - j) Integracja z modułem *Diagram PERA* — wizualizacja topologii.
- Profile komunikacyjne (Network Behavior Profiling)
 - a) Tworzenie profili zachowań sieciowych dla każdego adresu MAC.
 - b) Rejestr interfejsów, ruchu i komunikacji między urządzeniami.
 - c) Analiza różnic w zachowaniu (detekcja odchyśleń od normy).
 - d) Automatyczne tworzenie i aktualizacja profili.
 - e) Eksport listy profili do raportów i porównań audytowych.
 - f) Wizualne odwzorowanie relacji z urządzeniami aktywnymi sieci tego samego producenta co system SIEM/IDS
- Analiza danych i ryzyka
 - a) Automatyczna analiza zidentyfikowanych anomalii.
 - b) Raporty o potencjalnych wektorach ataku (MITRE ATT&CK).
 - c) Wskazanie nieautoryzowanych portów i usług.
 - d) Analiza zgodności z IEC 62443 i ISO 27001.
 - e) Raport z zaleceniami: „Zagrożenia – Konsekwencje – Działania”.
 - f) Ocena ryzyka braku działań korygujących (np. w 90 dni).
 - g) Szacowanie wpływu incydentu na zasoby i infrastrukturę.
- Wizualizacja i topologia sieci (Diagram PERA)
 - a) Automatyczna mapa relacji między zasobami i segmentami sieci.

- b) Kolorystyczne oznaczenia poziomu ryzyka i statusu połączeń.
- c) Możliwość interakcji z elementami (kliknięcie → szczegóły zasobu).
- d) Integracja z danymi z modułów *Zdarzenia* i *Alarmy*.
- e) Widok struktury per strefy PERA (Enterprise / Control / Field / DMZ).
- Zasady alarmowe i polityki bezpieczeństwa (NSPM)
 - a) Definiowanie reguł alarmowych (np. porty, IP, usługi, typ zdarzenia).
 - b) Priorytetyzacja zasad i poziomy alarmowe.
 - c) Automatyczne uruchamianie alarmów po spełnieniu warunków.
 - d) Możliwość wyciszania określonych alarmów lub źródeł.
 - e) Integracja z tabelą interfejsów i reguł firewall dostarczonych urządzeń bezpieczeństwa OT
 - f) Pełna zgodność z architekturą Zone-Based Firewall.
- Raportowanie operacyjne i analityka wspierane AI
 - a) Generowanie raportów z analizy ryzyka i podatności.
 - b) Podsumowania incydentów i trendów zagrożeń.
 - c) Raporty dla audytów (IEC 62443, ISO 27001, ISO 22301).
 - d) Możliwość eksportu do PDF, CSV.
 - e) Raporty z przypisaniem do zasobów, sieci i alarmów.
- Integracja z urządzeniami aktywnymi sieci
 - a) System musi zapewniać natywną integrację z urządzeniami bezpieczeństwa tego samego producenta umożliwiającą synchronizację polityk bezpieczeństwa oraz jednocześnie umożliwiać integrację z urządzeniami innych producentów poprzez standardowe mechanizmy wymiany danych.
 - b) Odczyt metadanych sprzętowych (model, CPU, pamięć, porty, firmware).
 - c) Monitorowanie stanu portów, interfejsów i komunikacji L2/L3.
 - d) Wykorzystanie urządzeń aktywnych sieci tego samego producenta jako źródeł danych IDS i monitoringu sieciowego.
 - e) Wykorzystanie urządzeń aktywnych sieci dowolnego producenta który umożliwia wysyłanie zdarzeń, kopii ruchu (poprzez sondy danych tego samego producenta), logowań, danych z sflow/netflow jako źródeł danych dla SIEM/IDS
 - f) Synchronizacja polityk bezpieczeństwa między systemem a urządzeniami aktywnymi tego samego producenta
- Dodatkowe funkcje operacyjne
 - a) Historia działań administratora (logi operacyjne).
 - b) Panel użytkownika i uprawnienia administracyjne.
 - c) Przegląd wszystkich interfejsów sieciowych i tabeli firewall.
 - d) Możliwość wizualizacji alarmów w czasie rzeczywistym (Alarmy live).
 - e) Panel wydajności systemu (monitor CPU, pamięci, dysków).
 - f) Integracja z modułem raportów dziennych / tygodniowych.
 - g) Mechanizmy wykluczeń i filtrów do analizy danych.
- Normy, zgodność i audyt
 - a) Zgodność z normami IEC 62443, ISO 27001, ISO 22301.
 - b) Analiza niezgodności i rekomendacje działań korygujących.
 - c) Mapowanie do wymagań bezpieczeństwa OT i IT.
- Architektura i integracja

- a) Działanie w środowisku Linux / Vmware / HyperV / KVM / Proxmox lub na dedykowanym Appliance sprzętowym – certyfikowanym IEC 62443 4-2 SL4
- b) Baza danych typu SQL
- c) Możliwość pracy w środowiskach mieszanych (OT, IT)
- d) API do integracji z zewnętrznymi systemami.
- e) Zdalna administracja i aktualizacje systemu.
- Wyróżniki unikalne
 - a) Dedykowane dla środowisk OT / ICS / SCADA.
 - b) Brak komponentów wymagających dodatkowych licencji.
 - c) Pełna integracja z fizycznymi urządzeniami aktywnymi sieci tego samego producenta.
 - d) Wysoka czytelność interfejsu – jeden panel łączący SIEM, Asset i NSPM.
 - e) Polski interfejs
 - f) Polskie komunikaty w szczególności dane analityczne
- Analiza anomalii ruchu sieciowego
 - a. System musi umożliwiać wykrywanie anomalii w ruchu sieciowym na podstawie:
 - i. analizy statystycznej
 - ii. profili komunikacyjnych urządzeń
 - iii. relacji komunikacyjnych pomiędzy zasobami
 - b. System musi umożliwiać identyfikację:
 - i. nietypowych źródeł ruchu
 - ii. nietypowych usług
 - iii. nietypowych portów komunikacyjnych
 - iv. anomalii wolumetrycznych
 - c. System musi prezentować wyniki w postaci:
 - i. rankingów
 - ii. statystyk
 - iii. wizualizacji rozkładu ruchu
- Analityka rozptyłu ruchu
- Detekcja i kontrola zmian w aktywności komponentów sieciowych
- Podgląd z kamer przypisanych do poszczególnych zasobów
- Dynamiczne mapy zależności komunikacyjnych. System musi umożliwiać generowanie dynamicznych map komunikacji pomiędzy zasobami w sieci.
 - Mapa musi umożliwiać:
 - wizualizację relacji pomiędzy adresami IP
 - wizualizację relacji pomiędzy adresami MAC
 - identyfikację centralnych węzłów komunikacyjnych
 - analizę kierunków przepływu danych
 - System musi umożliwiać analizę grafową obejmującą:
 - powiązania pomiędzy zasobami
 - intensywność komunikacji
 - topologię relacji
- Automatyczne modelowanie topologii sieci
 - System musi automatycznie tworzyć i aktualizować:
 - diagramy fizycznej topologii sieci

- relacje pomiędzy urządzeniami
 - powiązania interfejsów sieciowych
- System musi umożliwiać:
 - wizualizację urządzeń sieciowych
 - identyfikację interfejsów
 - identyfikację połączeń fizycznych
 - identyfikację połączeń logicznych
- Diagram musi być:
 - dynamiczny
 - aktualizowany automatycznie
 - powiązany z rzeczywistymi zdarzeniami sieciowymi.
- Inwentaryzacja zasobów OT i IT
 - System musi zapewniać automatyczną inwentaryzację zasobów obejmującą:
 - adres IP
 - adres MAC
 - nazwę hosta
 - producenta urządzenia
 - model urządzenia
 - typ urządzenia
 - rolę w sieci
 - System musi umożliwiać klasyfikację zasobów co najmniej jako:
 - urządzenia OT
 - urządzenia IT
 - urządzenia sieciowe
 - stacje robocze
 - serwery
 - urządzenia przemysłowe.
- Profile komunikacyjne zasobów
 - System musi umożliwiać tworzenie profili komunikacyjnych urządzeń.
 - Profil musi obejmować co najmniej:
 - typowe kierunki komunikacji
 - wykorzystywane porty
 - wykorzystywane protokoły
 - wolumen komunikacji
 - System musi umożliwiać wykrywanie odchyłań od profilu.
- Analiza zdarzeń powiązanych z zasobami
 - System musi umożliwiać analizę zdarzeń w kontekście konkretnego zasobu obejmującą:
 - historię zdarzeń
 - powiązane zasoby
 - zdarzenia sieciowe
 - zdarzenia bezpieczeństwa
 - Analiza musi być dostępna z poziomu:
 - widoku zasobu

- widoku zdarzeń
 - widoku analitycznego.
- Korelacja zdarzeń bezpieczeństwa
 - System musi zapewniać możliwość budowania mechanizmów korelacji zdarzeń w oparciu o:
 - sekwencje zdarzeń
 - liczbę wystąpień zdarzeń
 - zależności pomiędzy zdarzeniami
 - zależności czasowe.
 - Mechanizm korelacji musi umożliwiać:
 - budowę scenariuszy detekcji
 - budowę playbooków
 - definiowanie progów zdarzeń.
- Graficzny edytor playbooków bezpieczeństwa
 - System musi umożliwiać tworzenie procedur detekcji i reakcji w postaci graficznych diagramów logicznych.
 - Edytor musi umożliwiać:
 - definiowanie filtrów zdarzeń
 - tworzenie liczników zdarzeń
 - definiowanie progów alarmowych
 - budowę scenariuszy korelacji
- Alarmowanie i zarządzanie incydentami
 - System musi umożliwiać generowanie alarmów bezpieczeństwa na podstawie:
 - reguł korelacyjnych
 - wykrytych anomalii
 - zdarzeń bezpieczeństwa
 - Alarm musi zawierać:
 - poziom wiarygodności
 - liczbę zdarzeń powiązanych
 - listę zasobów powiązanych
- Analiza wolumenów zdarzeń
 - System musi umożliwiać analizę wolumenów zdarzeń obejmującą:
 - zdarzenia na sekundę
 - zdarzenia na urządzenie
 - zdarzenia na typ zdarzenia
 - System musi umożliwiać wizualizację trendów zdarzeń w czasie.
- Wizualizacja przepływów zdarzeń
 - System musi umożliwiać wizualizację przepływu zdarzeń pomiędzy:
 - źródłami danych
 - modułami analitycznymi
 - mechanizmami korelacyjnymi
 - systemem alarmowym.
- Model hierarchiczny infrastruktury (rozszerzony model PERA)

- System musi umożliwiać modelowanie infrastruktury w oparciu o hierarchiczny model architektury przemysłowej, obejmujący co najmniej:
 - poziomy modelu Purdue (PERA)
 - strefy logiczne systemów OT/IT
 - lokalizacje fizyczne
 - jednostki organizacyjne.
- System musi umożliwiać zagnieżdżanie kontenerów infrastruktury, pozwalające na grupowanie zasobów według:
 - lokalizacji geograficznych
 - budynków
 - pomieszczeń
 - stref technologicznych
 - poziomów architektury przemysłowej.
- Kontenery muszą umożliwiać tworzenie hierarchicznych struktur wielopoziomowych
- Telemetria infrastruktury
 - System musi umożliwiać zbieranie oraz wizualizację parametrów telemetrycznych infrastruktury obejmujących co najmniej:
 - obciążenie CPU
 - wykorzystanie pamięci RAM
 - wykorzystanie przestrzeni dyskowej
 - średnie obciążenie systemu.
 - System musi umożliwiać analizę telemetryczną w czasie rzeczywistym oraz historyczną.
 - System musi umożliwiać wizualizację parametrów w postaci:
 - wykresów czasowych
 - rankingów zasobów
 - map obciążenia infrastruktury.
- Centralne zarządzanie polityką bezpieczeństwa sieci
 - System musi umożliwiać centralne zarządzanie polityką bezpieczeństwa sieci obejmującą urządzenia filtrujące ruch sieciowy.
 - System musi umożliwiać:
 - przegląd reguł bezpieczeństwa
 - analizę relacji pomiędzy regułami
 - analizę wykorzystania reguł
 - identyfikację reguł nieużywanych.
 - System musi umożliwiać analizę reguł bezpieczeństwa w kontekście:
 - źródeł komunikacji
 - celu komunikacji
 - portów
 - protokołów.
- Przetwarzanie ruchu sieciowego

- System musi umożliwiać analizę ruchu sieciowego w sposób rozproszony, z wykorzystaniem urządzeń bezpieczeństwa sieciowego działających w warstwie infrastruktury OT.
- Analiza ruchu sieciowego musi być realizowana lokalnie na urządzeniach bezpieczeństwa sieciowego poprzez:
 - analizę pakietów,
 - analizę protokołów przemysłowych,
 - analizę anomalii komunikacyjnych.
- Do centralnego systemu bezpieczeństwa muszą być przekazywane dane przetworzone, obejmujące co najmniej:
 - zdarzenia bezpieczeństwa,
 - metadane komunikacyjne,
 - profile komunikacyjne zasobów,
 - informacje o wykrytych anomaliach.
- System nie może wymagać przesyłania pełnej kopii ruchu sieciowego do centralnej platformy analitycznej.
- Integracja z urządzeniami sieciowymi i systemami bezpieczeństwa
 - System musi umożliwiać integrację z urządzeniami bezpieczeństwa sieciowego oraz systemami monitoringu infrastruktury zarówno tego samego producenta, jak i innych producentów.
 - System musi umożliwiać:
 - natywną integrację z urządzeniami bezpieczeństwa tego samego producenta, umożliwiającą wymianę danych telemetrycznych, zdarzeń bezpieczeństwa oraz synchronizację polityk bezpieczeństwa,
 - integrację z urządzeniami innych producentów poprzez standardowe mechanizmy wymiany danych, w szczególności:
- Moduł automatycznej analizy incydentów bezpieczeństwa
 - System musi posiadać mechanizm analizy zdarzeń bezpieczeństwa wspierający operatora SOC w procesie klasyfikacji, triage oraz oceny ryzyka incydentów bezpieczeństwa.
 - Mechanizm analityczny musi umożliwiać generowanie raportu analitycznego dla zdarzenia bezpieczeństwa obejmującego co najmniej:
 - syntetyczne podsumowanie zdarzenia (Executive Summary),
 - analizę techniczną zdarzenia,
 - ocenę charakteru zdarzenia (atak, anomalia, zdarzenie informacyjne, brak danych),
 - ocenę poziomu ryzyka i poziomu wiarygodności analizy,
 - identyfikację powiązanych systemów, usług oraz zasobów infrastruktury,
 - mapowanie zdarzeń do technik MITRE ATT&CK dla środowisk Enterprise oraz ICS,
 - analizę potencjalnych podatności powiązanych ze zdarzeniem w oparciu o bazę CVE,
 - ocenę zgodności zdarzenia z wymaganiami regulacyjnymi i normatywnymi (np. IEC 62443, ISO 27001, NIS2, KSC),
 - rekomendacje działań operacyjnych dla zespołów SOC,
 - analizę konsekwencji braku reakcji na zdarzenie,
 - końcową klasyfikację zdarzenia.
- Analiza incydentów bezpieczeństwa

- System musi posiadać mechanizm automatycznej analizy zdarzeń bezpieczeństwa umożliwiający generowanie raportu analitycznego dla wskazanego zasobu (asset) na podstawie zestawu powiązanych zdarzeń.
- Mechanizm analityczny musi umożliwiać:
 - korelację zdarzeń pochodzących z jednego zasobu lub powiązanych zasobów,
 - analizę kontekstu komunikacji sieciowej,
 - ocenę charakteru zdarzeń (atak / anomalia / zdarzenie informacyjne / działanie polityki bezpieczeństwa),
 - analizę zachowania zasobu w odniesieniu do jego profilu komunikacyjnego,
 - identyfikację usług sieciowych, protokołów oraz typów komunikacji,
 - identyfikację usług publicznych lub znanych dostawców infrastruktury
- Raportowanie analityczne
 - System musi umożliwiać automatyczne generowanie raportu analitycznego obejmującego co najmniej:
 - ocenę poziomu pilności zdarzenia (SOC triage),
 - syntetyczne podsumowanie analizy (Executive Summary),
 - analizę techniczną zdarzeń,
 - ocenę charakteru zdarzenia,
 - mapowanie zdarzeń do MITRE ATT&CK,
 - analizę potencjalnych podatności (CVE),
 - analizę wpływu na zgodność regulacyjną (IEC 62443, ISO 27001, NIS2, KSC),
 - rekomendacje działań dla zespołu SOC,
 - ocenę konsekwencji braku reakcji,
 - końcową klasyfikację zdarzenia.

2.5. System / moduł korelacji

- System musi stanowić platformę korelacji umożliwiającą:
 - orkiestrację procesów reagowania na incydenty,
 - automatyzację działań operacyjnych,
 - korelację zdarzeń z wielu źródeł,
 - realizację reakcji w środowisku IT i OT.
- System musi posiadać:
 - centralny silnik korelacyjny (event processing engine),
 - graficzny silnik playbooków (workflow engine),
 - moduł zarządzania alarmami (incident lifecycle),
 - warstwę integracyjną z urządzeniami bezpieczeństwa dostarczonymi w ramach Zamówienia.
- System musi umożliwiać:
 - Tworzenie graficznych playbooków reakcji incydentowej w modelu:
 - event-driven,
 - stateful (utrzymywanie stanu),
 - warunkowym (IF/AND/OR).
 - Budowę wieloetapowych scenariuszy zawierających:
 - filtry zdarzeń,
 - agregację progową (threshold),

- korelację czasową (time window),
 - warunki logiczne,
 - akcje reakcyjne.
- Łączenie zdarzeń pochodzących z różnych źródeł (np. IDS, firewall, NDR, monitoring OT).
- Obsługę sygnałów wejścia/wyjścia między węzłami (signal-based workflow).
- System musi umożliwiać automatyczne:
 - Generowanie alarmów na podstawie warunków korelacyjnych.
 - Agregowanie zdarzeń w jeden incydent.
 - Resetowanie i czyszczenie kontekstu po zakończeniu scenariusza.
 - Dynamiczne przypisywanie poziomu wiarygodności (reliability).
 - Wykonywanie akcji na podstawie:
 - przekroczenia progu zdarzeń,
 - przekroczenia limitu czasowego,
 - spełnienia warunków logicznych.
- System musi realizować:
 - Korelację progową (N zdarzeń w czasie T).
 - Korelację czasową (timeout-based).
 - Korelację wieloźródłową (cross-source).
 - Korelację kontekstową (asset-aware correlation).
 - Grupowanie zdarzeń w ramach jednego incydentu.
 - Mechanizm resetu stanu po spełnieniu warunków.
- System musi zapewniać:
 - Pełny lifecycle alarmu:
 - utworzenie,
 - aktualizacja,
 - rozwiązanie,
 - wyciszenie,
 - zamknięcie.
 - Rejestr linii czasu (timeline).
 - Powiązanie alarmu z zasobem i zdarzeniami.
 - Klasyfikację poziomu ryzyka.
 - Możliwość raportowania i eksportu danych.
- Licencja nie może ograniczać ilości IP, MAC, scenariuszy reakcyjnych

2.6. System typu EDR/XDR

- Architektura systemu
 - System musi bezpośrednio współpracować z zintegrowanym systemem klasy EDR (Endpoint Detection and Response) umożliwiającym:
 - monitorowanie zdarzeń bezpieczeństwa na stacjach roboczych i serwerach,
 - detekcję zagrożeń w czasie rzeczywistym,
 - korelację zdarzeń,
 - reakcję na incydenty.
 - System musi składać się z:
 - agentów instalowanych na chronionych hostach,

- centralnego serwera zarządzającego,
 - silnika analityczno-korelacyjnego,
 - repozytorium logów,
 - interfejsu webowego (GUI).
- System musi umożliwiać instalację:
 - w środowisku lokalnym (on-premise),
 - w środowisku wirtualnym,
- Obsługiwane systemy operacyjne
 - Agent musi obsługiwać co najmniej:
 - Windows (Server i Workstation),
 - Linux (różne dystrybucje).
 - System musi umożliwiać centralne zarządzanie konfiguracją agentów.
- Funkcjonalności EDR – detekcja
 - System musi zapewniać:
 - Monitoring integralności plików (FIM – File Integrity Monitoring):
 - wykrywanie zmian w plikach systemowych i konfiguracyjnych,
 - wykrywanie zmian w rejestrze Windows,
 - generowanie alertów przy nieautoryzowanych modyfikacjach.
 - Monitoring procesów:
 - rejestrowanie uruchamianych procesów,
 - analiza linii poleceń (command line),
 - wykrywanie podejrzanych procesów (np. PowerShell, WMI, LOLBins).
 - Monitoring aktywności użytkowników:
 - logowania lokalne i zdalne,
 - próby eskalacji uprawnień,
 - zmiany w grupach uprzywilejowanych.
 - Detekcję malware i rootkitów:
 - wbudowany mechanizm rootkit detection,
 - integrację z zewnętrznymi silnikami AV (np. ClamAV).
 - Detekcję anomalii i ataków zgodnie z MITRE ATT&CK:
 - mapowanie zdarzeń do technik ATT&CK,
 - możliwość generowania raportów według taksonomii MITRE.
 - Wykrywanie podatności (Vulnerability Detection):
 - identyfikację zainstalowanego oprogramowania,
 - korelację z bazami CVE,
 - raportowanie podatności.
- Korelacja i analiza
 - System musi posiadać:
 - silnik reguł (rule-based detection),
 - możliwość tworzenia własnych reguł detekcyjnych,
 - możliwość korelacji wielu zdarzeń w jeden incydent.
 - System musi:
 - wspierać analizę logów z różnych źródeł (systemowe, aplikacyjne, sieciowe),

- umożliwiać integrację z Syslog,
 - umożliwiać integrację z urządzeniami sieciowymi.
- Funkcjonalności Response
 - System musi umożliwiać:
 - Zdalne wykonywanie komend na hoście.
 - Blokowanie adresów IP (np. poprzez integrację z firewall).
 - Automatyczne reakcje (active response) na podstawie zdefiniowanych reguł.
 - Izolację hosta (logicznie – poprzez blokowanie komunikacji).
 - System musi umożliwiać wywoływanie reakcji z poziomu SOAR zintegrowanego z główną konsolą.
- Zarządzanie i raportowanie
 - System musi posiadać:
 - interfejs webowy (dashboard),
 - wyszukiwarkę zdarzeń,
 - możliwość filtrowania po hostach, użytkownikach, czasie, typie zagrożenia.
 - System musi umożliwiać:
 - generowanie raportów PDF/CSV,
 - raporty zgodności (np. PCI-DSS, CIS, ISO 27001),
 - raporty podatności.
 - System musi umożliwiać wielopoziomowe role użytkowników (RBAC).
- Integracje
 - System musi umożliwiać integrację z:
 - SIEM,
 - systemami SOC,
 - systemami zarządzania podatnościami,
 - bazami threat intelligence.

Bezpieczeństwo systemu

1. Komunikacja agent–serwer musi być szyfrowana (TLS).
2. System musi posiadać:
 - mechanizmy uwierzytelniania,
 - role i uprawnienia,
 - logowanie działań administratorów.

II. Zestaw sprzętowych sond do monitorowania sieci OT – 1 zest.

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa 1 zestaw dedykowanego urządzenia sprzętowego w postaci sondy/sensora do monitorowania sieci OT (Operational Technology), umożliwiającego analizę komunikacji oraz identyfikację zdarzeń w zakresie protokołów przemysłowych, zgodnych z wymaganiami technicznymi określonymi w dokumentacji postępowania.

2. Wymagania dotyczące rozwiązania

2.1. Wymagania ogólne dla sprzętu:

- musi być nowy i pochodzić z polskiego kanału dystrybucji
- musi posiadać gwarancję i wsparcie producenta na okres nie krótszy niż do 31.12.2026
- producent musi zapewnić czas życia produktu do końca roku 2032 roku. Nie dopuszcza się rozwiązań będących w okresie zakończenia życia (end-of-life) lub zakończenia wsparcia (end-of-support) lub zakończenia sprzedaży (end-of-sale).

2.2. Wymagania ogólne dla urządzeń aktywnych sieci

Urządzenia montowane na szynę DIN35mm muszą:

- Być dostarczone z dwoma zasilaczami 230 V / DC 24 V dostosowane mocowo do dostarczanych urządzeń działające w układzie nadmiarowym i uzupełniającym
- Posiadać aktualny certyfikat IEC 62443 4-2 SL4
- Urządzenia muszą stanowić platformę bezpieczeństwa obok standardowych funkcjonalności urządzeń aktywnych sieci takich jak przełączanie czy routing L3.
- Być montowane na szynach wysuwanych umożliwiając łatwy dostęp do górnej części urządzenia
- Muszą posiadać certyfikat FCC Class A, CE, UL

PARAMETR	OPIS / WARTOŚĆ PARAMETRU	ILOŚĆ
Pamięć RAM	Min. 8 GB	1
Storage	Min. 480 GB	1
Interfejs Szeregowy	Konsola RS232	1
Zasilacze	230 V 5 A – 24 V DC	2
Interfejs 1 Gb/s	Min RJ45 Ethernet 2 porty bypass Min RJ45 Ethernet 2 porty pracujące bez bypass	Minimum 2 pracujące w trybie bypass (utrzymanie łączności w przypadku braku zasilania)
Interfejs 1 Gb/s	SFP 1 Gb/s	Minimum 2 x SFP 1 Gb/s.
Wkładki 1 Gb/s	SFP 1 Gb/s	2 sztuki – parametry: 10 KM 1310 nm

PARAMETR	OPIS / WARTOŚĆ PARAMETRU	ILOŚĆ
		SM
Uchwyty montażowe	1 komplet dla DIN35	1
Kable zasilające	Min 0,5 m	2
Typ montażu	Szyna DIN35	n/d
Patch cordy	Miedziane CAT6, 1,5 M RJ45	2
Patch cordy	Światłowodowe SC/LC 1,5 m SM PC/APC LC-LC	2
Konsola centralna	Zarządzanie Firewall z poziomu konsoli centralnej zintegrowanej z centralnym systemem SIEM/IDS, pochodząca od tego samego producenta co urządzenie aktywne	n/d
Certyfikaty wymagane	CE, FCC Class A, UL, IEC 62443 4-2 SL4, IEC 62443 4-2 SL4	n/d
Temperatura pracy	Od minus 40 stopni Celsjusza do plus 70 stopni Celsjusza	

2.3. Wymagania dla funkcjonalności systemu pracującego na urządzeniu:

- Routing i przełączanie (L2 / L3)
 - a) Pełny routing IPv4 i IPv6 (statyczny, dynamiczny, policy-based, VRF).
 - b) Obsługa protokołów routingu: OSPFv2/v3, BGP, RIP, RIPng, Babel, IS-IS.
 - c) VRRP – redundancja bramy sieciowej (High Availability).
 - d) MPLS / VPLS / LDP / RSVP – wsparcie dla sieci operatorskich i segmentacji.
 - e) Policy-Based Routing (PBR) – wybór trasy na podstawie źródła, portu, typu ruchu.
 - f) Ethernet bridging (L2) – możliwość pracy jako przełącznik (bridge, VLAN, trunk).
 - g) STP / RSTP – obsługa protokołów zapobiegających pętlom w sieci.
 - h) 802.1Q VLAN / QinQ – pełne wsparcie dla VLAN i tunelowania VLAN w VLAN.
 - i) LACP / Bonding / Port-channel – łączenie interfejsów dla redundancji i wydajności.

- j) VRF / Route Tables – separacja ruchu i izolacja sieci logicznych.
- Firewall i bezpieczeństwo
 - a) Stateful Firewall (ZBFW – Zone-Based Firewall) – inspekcja stanu połączeń i przypisanie reguł do stref logicznych.
 - b) NAT (Source, Destination, Static, Masquerade) – pełna translacja adresów.
 - c) Policy NAT i Hairpin NAT – elastyczne mapowanie adresów w zależności od kierunku.
 - d) IPv6 Firewall – osobne polityki bezpieczeństwa dla IPv6.
 - e) Traffic Filtering na poziomie L2–L4 – filtrowanie pakietów, portów, protokołów.
 - f) Time-based Rules – polityki bezpieczeństwa zależne od czasu.
 - g) Conntrack / Helper modules – śledzenie sesji i stanów połączeń.
 - h) Rate-limiting / DoS protection – ograniczanie przepustowości, ochrona przed floodem.
 - i) MAC Firewall / ARP Inspection / Static ARP tables – kontrola komunikacji warstwy drugiej.
- VPN i tunelowanie
 - a) IPsec IKEv1 / IKEv2 – szyfrowane tunele site-to-site i remote access.
 - b) L2TP, PPTP, OpenVPN, WireGuard – elastyczne protokoły VPN dla użytkowników i urządzeń.
 - c) GRE / mGRE / VTI / VXLAN / IP-in-IP – tunelowanie ruchu między sieciami (np. SCADA ↔ DMZ).
 - d) Dynamiczny routing przez VPN (BGP over IPsec) – skalowalność w dużych sieciach.
 - e) DMVPN V3 – automatyka zestawiania topologii HUB Spoke z zabezpieczaniem IPsec i protokołami routingu wraz z protokołem NHRP
 - f) SSL VPN / Remote Access – wsparcie dla zdalnego dostępu użytkowników.
- QoS i kontrola ruchu
 - a) Traffic Shaping / Policing / Queueing (HTB, CBQ, HFSC) – kontrola pasma.
 - b) Hierarchical QoS (HQoS) – wielopoziomowe kolejkowanie.
 - c) Traffic Classification (DSCP / CoS / ACL match) – klasyfikacja ruchu na podstawie atrybutów.
 - d) Bandwidth Management per interface / per VLAN – kontrola przepustowości per-port lub per-sieć.
- Monitoring, logowanie i diagnostyka
 - a) SNMP v1/v2c/v3 – monitorowanie zewnętrzne.
 - b) Syslog (lokalny i zdalny) – pełna integracja logów z systemami SIEM/IDS.
 - c) NetFlow / sFlow / IPFIX – eksport statystyk ruchu do systemów analitycznych.
 - d) Ping / Traceroute / MTR / Packet Capture (tcpdump) – diagnostyka sieciowa.
 - e) BFD – szybkie wykrywanie awarii tras routingu.
 - f) Interface Counters / Flow statistics – bieżące statystyki ruchu.
 - g) Monitorowanie w trybie inline – analityka DPI oraz IDS realizowana pasywnie w trybie ciągłym na każdym interfejsie aktywnym,
 - h) Mirror Port – możliwość skopiowania ramek z interfejsów źródłowych na interfejs wyjściowy
 - i) Przekierowanie wewnętrzne do systemów analityki – funkcja zautomatyzowana przekierowania ruchu przez wewnętrzny system IPS (w trybie IPS) dla analityki z automatyzacją ochrony inline
 - j) Analityka anomalii komunikacji sieciowej pomiędzy komponentami
 - k) Behavioral monitoring,
 - l) Profilowanie obiektów logicznych i fizycznych sieci
 - m) Identyfikacja komponentów w danych z ruchu sieciowego
 - n) Analityka czasów transmisji dla komunikacji sesyjnej i niesesyjnej
 - o) Traceability dla podanych parametrów zidentyfikowanych w ruchu sieciowym
 - p) Tryb maintenance dla wyciszenia alertów z profili zgłoszonych do zmiany w środowisku sieciowym

- q) Thread Detection
- r) Analityka głęboka protokołów IT i OT w tym Modbus TCP, Goose, Profinet, Ethernet/IP, EtherCat, S-BUS, Step7, IEC 60870-5-104
- s) Diagnostyka protokołów OT
- t) Diagnostyka protokołów IT
- u) Wbudowany system traceability dla monitorowania głębokich danych do poziomu nastaw i wartości np. rejestrów
- Zarządzanie i automatyzacja
 - a) CLI / SSH / API / RESTCONF / NETCONF – wielowarstwowe zarządzanie.
 - b) Konfiguracja CLI w stylu Cisco / Juniper – logiczne drzewo konfiguracji.
 - c) Atomic commits / rollback / diff – bezpieczne zmiany i cofanie konfiguracji.
 - d) Scheduled tasks / cron / event-driven scripts – automatyzacja procesów.
 - e) Ansible / Salt / Terraform ready – zgodność z narzędziami DevOps.
 - f) Zarządzanie użytkownikami / RADIUS / TACACS+ / LDAP – kontrola dostępu administracyjnego.
 - g) Backup / restore / config versioning – bezpieczeństwo konfiguracji.
 - h) Zarządzanie Firewall – wymagane jest również zarządzanie z poziomu konsoli centralnej

2.4. IDS/IPS - Detekcja, analiza i blokowanie zagrożeń sieciowych w czasie rzeczywistym.

- Analiza i inspekcja ruchu sieciowego (Deep Packet Inspection – DPI)
 - a) Pełna inspekcja pakietów na poziomie L2–L7 w czasie rzeczywistym.
 - b) Analiza protokołów przemysłowych (Modbus, DNP3, IEC 60870-5-104, PROFINET, BACnet, OPC UA itp.).
 - c) Wykrywanie anomalii w komunikacji sterowników PLC, HMI i urządzeń przemysłowych.
 - d) Rozpoznawanie struktur poleceń, zmiennych procesowych i komunikacji SCADA.
- Detekcja zagrożeń (Intrusion Detection System – IDS)
 - a) Wykrywanie prób włamań, skanowania portów, exploitów, ataków DoS/DDoS i naruszeń polityk sieciowych.
 - b) Identyfikacja złośliwego oprogramowania, beaconingu i nieautoryzowanych połączeń C2 (Command & Control).
 - c) Korelacja zdarzeń z regułami IDS Rules oraz regułami zespołu MDR i CTI.
 - d) Generowanie alertów i przekazywanie ich do systemu SIEM/IDS.
- Blokowanie zagrożeń (Intrusion Prevention System – IPS)
 - a) Dynamiczne blokowanie pakietów i sesji zgodnie z regułami bezpieczeństwa.
 - b) Automatyczne odcinanie źródeł ataków, modyfikacja polityk firewallowych w czasie rzeczywistym.
 - c) Współpraca z modułem firewall (ZBFW) i komponentami SIEM/IDS w celu natychmiastowej reakcji.
 - d) Minimalny wpływ na opóźnienia i przepustowość ruchu sieciowego (low-latency design).
- Analiza sygnatur i anomalii
 - a) Wykorzystanie sygnatur znanych ataków oraz mechanizmów heurystycznych i statystycznych.
 - b) Wykrywanie anomalii w zachowaniach urządzeń i użytkowników (np. nagłe wzrosty ruchu, zmiana portów, niezgodność protokołów).
 - c) Wsparcie dla analizy behawioralnej w połączeniu z modułami CTI i MDR.
 - d) Aktualizacje baz reguł bezpieczeństwa w sposób automatyczny i kontrolowany.
- Integracja z systemami analitycznymi i korelacyjnymi
 - a) Wysyłanie logów i alertów do systemów SIEM, SOC, MDR.
 - b) Normalizacja danych i mapowanie zdarzeń do frameworków MITRE ATT&CK i IEC 62443.

- c) Współpraca z bazami danych CTI w celu identyfikacji źródeł zagrożeń i kampanii APT.
- d) Eksport danych w formatach EVE JSON, Syslog, PCAP i NetFlow.
- Wsparcie inspekcji w sieciach OT
 - a) Zoptymalizowane reguły detekcji dla środowisk przemysłowych.
 - b) Tryb „passive monitoring” bez ingerencji w ruch procesowy (dla systemów krytycznych).
 - c) Tryb „inline” z prewencyjnym blokowaniem ataków przy zachowaniu zgodności z IEC 62443-3-3.
 - d) Pełna widoczność komunikacji pomiędzy segmentami IT a OT.
- Mechanizmy automatyzacji i korelacji
 - a) Automatyczne przekazywanie alertów do modułów reakcji MDR.
 - b) Aktywacja polityk obronnych w firewallu .
 - c) Dynamiczne uczenie się ruchu sieciowego (profilowanie).
 - d) Możliwość tworzenia własnych reguł i skryptów reakcji w środowisku SIEM/IDS.
- Raportowanie i wizualizacja
 - a) Raporty incydentów bezpieczeństwa, trendów i statystyk detekcji.
 - b) Graficzne przedstawienie ruchu sieciowego i źródeł zagrożeń w panelu SIEM/IDS.
 - c) Eksport alertów i logów do systemów zewnętrznych w formacie JSON, CSV, Syslog.
 - d) Możliwość integracji z pulpitemi centralnego SIEM/IDS .

2.5. Dodatkowe moduły

- DHCP server/relay/client, DNS server/forwarder, NTP, HTTP proxy, NetBIOS relay.
- Dynamic DNS, Static Hosts, Name-resolution cache.
- Multicast routing (PIM/IGMP).
- IPv6 autoconfiguration / router advertisement (RA).
- System High Availability (VRRP, Sync) – redundancja i przełączenie awaryjne.
- Zarządzanie certyfikatami SSL / PKI – obsługa CA, klucze i certyfikatów.

2.6. Dodatkowe cechy

- Rolling Release – aktualizacje bezpieczeństwa w cyklu ciągłym.
- Integracja z Docker / LXC / KVM – uruchamianie usług w kontenerach

III. Switche zarządzalne OT – 2 szt.

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa 2 sztuk dedykowanych urządzeń sieciowych, umożliwiających dodatkowo analizę komunikacji oraz identyfikację zdarzeń w zakresie protokołów przemysłowych, zgodnych z wymaganiami technicznymi określonymi w dokumentacji postępowania.

2. Wymagania dotyczące rozwiązania

2.1. Przeznaczenie i kontekst regulacyjny

- Oferowane urządzenie stanowi kluczowy element ochrony sieci IT/OT, przeznaczony do pracy w środowisku infrastruktury krytycznej, w szczególności w systemach sterowania procesami technologicznymi (ICS/SCADA).

- Urządzenie musi wspierać realizację obowiązków Zamawiającego wynikających z:
 - nowelizacji Ustawy o Krajowym Systemie Cyberbezpieczeństwa (UKSC),
 - dyrektywy NIS2,
 - norm IEC 62443,
- w zakresie:
 - ciągłego monitorowania sieci OT,
 - wykrywania anomalii i zagrożeń,
 - odporności na zaawansowane, ukierunkowane ataki (APT),
 - zapewnienia ciągłości i bezpieczeństwa procesów technologicznych.

2.2. Charakter rozwiązania

- Zamawiający wymaga sprzętowej, zintegrowanej platformy komunikacyjnej i diagnostycznej, która w jednym urządzeniu realizuje łącznie funkcje:
 - przełączania i routingu ruchu OT,
 - aktywnej ochrony sieci OT,
 - analizy i korelacji ruchu przemysłowego,
 - detekcji i prewencji zagrożeń.
- Nie dopuszcza się:
 - wyłącznie pasywnych sond monitorujących,
 - rozwiązań wymagających stałego mirrorowania ruchu do zewnętrznych systemów,
 - rozwiązań, w których funkcje bezpieczeństwa realizowane są poza oferowanym urządzeniem.
- Urządzenie musi być zdolne do pracy zarówno w trybie pasywnym, jak i inline, w zależności od wymagań danego segmentu OT.

2.3. Platforma sprzętowa i instalacja

- Urządzenie sprzętowe klasy przemysłowej, przystosowane do pracy ciągłej 24/7.
- Montaż w szafie RACK 19"
- Redundantne zasilanie (zewnętrzne zasilacze) – 2 zasilacze 230V – moc dostosowana do wymagań sprzętu i pełnego obciążenia analityki
- Urządzenie musi posiadać dwa niezależne tory zasilające akceptujące napięcie 230 V
- Zasoby sprzętowe umożliwiające jednoczesną realizację:
 - analizy DPI,
 - IDS/IPS,
 - analityki behawioralnej,
 - korelacji zdarzeń.

2.4. Funkcje bezpieczeństwa

- Urządzenie musi zapewniać aktywne mechanizmy bezpieczeństwa OT, w tym:
 - Detekcja i prewencja
 - IDS / IPS dla sieci OT:
 - analiza ruchu w czasie rzeczywistym,
 - możliwość dynamicznego blokowania zagrożeń,
 - niski narzut na opóźnienia (low-latency design).
 - Ochrona przed:
 - atakami DoS / DDoS,

- kampaniami APT,
- nieautoryzowaną komunikacją między segmentami OT.
- Anomaly Detection i behavioral monitoring
 - Detekcja anomalii komunikacyjnych w sieciach przemysłowych.
 - Profilowanie zachowań:
 - sterowników PLC,
 - HMI,
 - serwerów SCADA,
 - urządzeń pomiarowych i wykonawczych.
 - Identyfikacja zmian w topologii i wzorcach komunikacji.

2.5. Analiza protokołów przemysłowych

- Urządzenie musi realizować głęboką analizę protokołów przemysłowych (DPI OT), co najmniej dla:
 - Modbus TCP,
 - IEC 60870-5-104,
 - PROFINET,
 - EtherNet/IP,
 - EtherCAT,
 - GOOSE,
 - STEP7 / S7,
 - oraz innych protokołów przemysłowych równoważnych funkcjonalnie.
- Analiza musi obejmować:
 - rozpoznawanie poleceń i funkcji protokołów,
 - analizę zmiennych procesowych,
 - identyfikację nieautoryzowanych operacji sterujących,
 - diagnostykę komunikacji OT.

2.6. Tryby pracy i ciągłość działania

- Urządzenie musi umożliwiać:
 - tryb pasywny – bez ingerencji w ruch procesowy,
 - tryb inline – z aktywną ochroną i blokowaniem zagrożeń,
- Dla trybu inline wymagane są mechanizmy minimalizujące ryzyko zakłócenia pracy systemów OT (fail-safe, bypass lub równoważne).

2.7. Monitoring, traceability i integracja

- Urządzenie musi zapewniać:
 - pełną traceability zdarzeń i parametrów komunikacji,
 - rejestrowanie i eksport logów bezpieczeństwa,
 - integrację z:
 - SIEM,
 - SOC,
 - Usługami MDR,
 - normalizację danych i możliwość mapowania zdarzeń do:
 - MITRE ATT&CK (ICS),
 - IEC 62443.

2.8. Zarządzanie i automatyzacja

- Zarządzanie lokalne i zdalne:
 - Pełne CLI / API,
- Nie dopuszcza się rozwiązań z konsolą Web na urządzeniu
- Możliwość integracji z centralną platformą zarządzania bezpieczeństwem.
- Obsługa polityk bezpieczeństwa i reguł reagowania.
- Możliwość aktualizacji reguł detekcji i mechanizmów analitycznych.

2.9. Zgodność normatywna i odporność

- Oferowane urządzenie musi być przeznaczone do pracy w środowiskach OT i spełniać wymagania:
 - IEC 62443-4-2- SL4
 - odporności na zaawansowane, celowane ataki (APT),
 - wymagań wynikających z nowelizacji UKSC / NIS2.
- Rozwiązania oparte wyłącznie na pasywnym monitoringu, bez możliwości aktywnej ochrony, nie spełniają założeń projektu.

2.10. Uwagi dodatkowe

- Zamawiający oczekuje sprzętowej platformy OT Security, łączącej funkcje komunikacyjne, diagnostyczne i ochronne, przeznaczonej do realnej ochrony procesów technologicznych.
- Rozwiązania będące jedynie:
 - pasywną sondą,
 - narzędziem IT przeniesionym do OT,
 - systemem wymagającym dodatkowych appliance'ów,
- nie będą uznane za równoważne.

Wymaganie pracy w trybie inline

- Tryb pracy i egzekwowanie bezpieczeństwa
- Oferowane urządzenie musi umożliwiać pracę w trybie inline, tj. jako aktywny element toru komunikacyjnego sieci OT, z bezpośrednią możliwością blokowania, modyfikowania lub przerywania ruchu sieciowego w czasie rzeczywistym, zgodnie z politykami bezpieczeństwa.
- Funkcja blokowania ruchu w trybie inline musi być realizowana bezpośrednio na oferowanym urządzeniu, bez konieczności:
 - przekazywania decyzji do zewnętrznych systemów (np. SOAR),
 - stosowania dodatkowych firewalli lub urządzeń pośredniczących,
 - rekonfiguracji topologii sieci w momencie detekcji incydentu.

Bezpieczeństwo procesu i ciągłość działania (fail-safe)

- Praca w trybie inline musi być zaprojektowana zgodnie z zasadami bezpieczeństwa procesowego OT, w tym:
 - fail-safe / fail-open lub bypass w przypadku awarii urządzenia,
 - brak pojedynczego punktu awarii (SPOF),
 - minimalny i deterministyczny wpływ na opóźnienia transmisji
 - wymagane jest dostarczenie minimum 1 pary portów RJ45 działających w trybie by-pass, które przepuszczą ruch nawet po pełnej utracie zasilania na urządzeniu.
- Urządzenie musi umożliwiać kontrolowane przełączanie pomiędzy trybem pasywnym a inline, bez zakłócania pracy procesu technologicznego.

- Zamawiający nie dopuszcza rozwiązań, w których funkcja blokowania ruchu realizowana jest:
 - wyłącznie poprzez pasywną sondę i zewnętrzny firewall,
 - poprzez systemy SOAR/MDR działające poza oferowanym urządzeniem,
 - poprzez reakcję opóźnioną (out-of-band),
 - poprzez zestaw kilku odrębnych urządzeń zamiast jednej, zintegrowanej platformy.
- Rozwiązania takie nie spełniają wymagań aktywnej ochrony sieci OT wynikających z nowelizacji UKSC oraz IEC 62443.

Jednoczesna praca aktywna i analityczna

- Role urządzenia w topologii sieci OT
- Oferowane urządzenie musi być zdolne do jednoczesnej pracy jako pełnoprawny, aktywny element infrastruktury sieciowej OT oraz jako platforma analityczna monitorująca ruch sieciowy, bez ograniczeń funkcjonalnych wynikających z wyboru trybu pracy.
- Urządzenie nie może wymagać przełączania pomiędzy trybem „aktywnym” a „analitycznym” – obie funkcje muszą być realizowane równolegle i w sposób ciągły.

Analiza ruchu z wielu portów jednocześnie

- Urządzenie musi umożliwiać jednoczesne przyjmowanie i analizę kopii ruchu sieciowego z wielu interfejsów Ethernet, bez ograniczenia do jednego portu obserwacyjnego w danym czasie.
- Analiza ruchu musi być możliwa zarówno:
 - dla ruchu przechodzącego przez urządzenie (inline),
 - jak i dla ruchu kopiowanego (SPAN / mirror / TAP) z innych elementów sieci.
- Rozwiązania umożliwiające analizę ruchu wyłącznie z jednego portu w danym czasie nie spełniają wymagań projektu.

Funkcje przełączania, routingu, analizy ruchu oraz egzekwowania polityk bezpieczeństwa muszą być realizowane przez jedno, spójne urządzenie sprzętowe, bez rozdzielania ich pomiędzy osobne sondy, sensory lub appliance'y.

- Zamawiający nie dopuszcza rozwiązań, w których:
 - urządzenie analityczne nie pełni żadnej aktywnej roli w topologii sieci,
 - analiza ruchu realizowana jest wyłącznie na dedykowanym, pojedynczym interfejsie obserwacyjnym.

2.11. Wymagania sprzętowe

- Minimalna ilość portów
 - Minimum 16 x 1 Gb/s z czego minimum 14 portów pracujące w trybie bypass
 - Minimum 2 porty 10 Gb/s SFP +
 - Minimum 8 portów RJ45 bez trybu bypass
 - Dedykowany port MGMT RS232 – RJ45

Wszystkie porty Ethernet muszą być wyposażone w funkcje IEEE 1588V2

- Ilość storage: min 1000 GB
- Ilość RAM min: 32 GB

2.12. Wymagania certyfikacyjne - Wymagane jest posiadanie certyfikatów na urządzenie :

- FCC Class A
- CE
- UL

- IEC 62443-4-2 SL4

Certyfikacja IEC 62443-4-2 SL4 musi dotyczyć całego urządzenia jako całości, obejmując platformę sprzętową oraz system operacyjny, a nie wyłącznie wybranych

IV. Specjalistyczne wdrożenie i rekonfiguracja (OT)

1. Przedmiot zamówienia

Przedmiotem zamówienia jest wdrożenie urządzeń, oprogramowania oraz rozwiązań z zakresu bezpieczeństwa w środowiskach OT, ICS oraz IIoT, a także przeprowadzenie czynności odbiorowych, zgodnie z wymaganiami Zamawiającego. Wdrożenie musi zostać zrealizowane na podstawie uprzednio zaakceptowanego Projektu Wykonawczego.

2. Wymagania dotyczące usługi wdrożenia

2.1. WYMAGANIA WSTĘPNE

- Realizacja prac projektowych będzie bazowała m.in. na: Prince 2, ISO/IEC 27001, ISO/IEC 27002, Ustawie o ochronie danych osobowych, IEC 62443, Ustawie o Krajowym Systemie Cyberbezpieczeństwa.
- Metodyki dostarczenia produktów specjalistycznych są dobierane w zależności od skali i zakresu merytorycznego.
- Przebieg realizacji całości zamówienia musi być zakończony przekazaniem dokumentacji powykonawczej dla rozwiązań bezpieczeństwa i monitorowania systemów OT
 - Wymaganiem Zamawiającego jest wizualizacja zdarzeń i możliwość reakcji na zagrożenie z jednego, centralnego systemu zarządzania widocznością i bezpieczeństwem.
 - Dane źródłowe: ruch sieci, logi i inne podłączane źródła być kolekcjonowane przez system centralny, normalizowany, wizualizowany i musi zapewnić pełną widoczność.
 - Dopuszcza się stosowanie niezależnych dostępu i interfejsów celem zarządzania i wprowadzania zmian w systemie i zarządzanych komponentach podłączonych do danego systemu. Tym samym, szczegółowe zarządzanie może odbywać się na poziomie poszczególnych komponentów całości rozwiązania.
 - Wymaganiem jest aby urządzenia OT oraz system centralny pochodziły od tego samego producenta i posiadały Certyfikat IEC 62443 4-2 na poziomie SL4 akredytowany przez PCA lub ISA.
 - Urządzenia aktywne sieci zarówno na szynę DIN jak i Rack 9" muszą minimum posiadać certyfikaty CE, FCC Class A, UL lub równoważne, celem upewnienia się, że nadają się do zastosowań w Automatyce Przemysłowej i systemach AKPiA.
- Systemy i produkty podlegające wdrożeniu w środowisku Zamawiającego.
 - Komplementarny system komunikacyjny i cyberbezpieczeństwa OT oparty o dostarczone urządzenia przez Wykonawcę

- Urządzenie będące jednocześnie (przełącznikiem, routerem, FW i urządzeniem diagnostycznym) –z pełną ochroną i monitorowaniem na platformie sprzętowej rack 19” z systemem bezpieczeństwa IPS/IDS, OT Anomaly Detection, threat detection, data traceability controll, SDN, anti DDOS, anti APT (Advanced Persistent Threat)
- Urządzenia będące jednocześnie (przełącznikami, routerami, FW i urządzeniami diagnostycznymi) –z pełną ochroną i monitorowaniem na platformie sprzętowej DIN35 czy RACK 19” z systemem bezpieczeństwa IPS/IDS, OT Anomaly Detection, threat detection, data traceability controll, SDN, anti DDOS, anti APT (Advanced Persistent Threat)
- Oprogramowanie platformowe - Zintegrowany System bezpieczeństwa IPS/IDS, OT Anomaly Detection, threat detection, data traceability controll, SDN, anti DDOS, anti APT (Advanced Persistent Threat), SIEM, , AKPiA , XDR, NDR, Active Daschboards, Central FW MGMT, Alarm Risk MGMT
- Platforma sprzętowa DIN35 - System bezpieczeństwa IPS/IDS, OT Anomaly Detection, threat detection, data traceability controll, SDN, anti DDOS, anti APT (Advanced Persistent Threat) , AI MGMT, ZBFW

● **Wdrożenie:**

- 1) Wdrożenie ma być wykonane zgodnie z obowiązującymi przepisami BHP. W szczególności wymaga się od Wykonawcy zapewnienia osób wykonujących pracę w miejscach wymagających odpowiednich dopuszczeń z odpowiednimi uprawnieniami np. D1 i/lub E1.
- 2) Prace montażowe i uruchomieniowe muszą być uzgodnione z Zamawiającym.
- 3) Każde prace modyfikujące jakiegokolwiek obszary w strefach OT muszą być odrębnie zatwierdzone przez Zamawiającego
- 4) Wszelkie zatrzymania lub odstawienia procesu muszą być poprzedzone wydaniem zgody Zamawiającego.
- 5) Samowolne działania Wykonawcy, które spowodują zatrzymanie, lub odstawienie procesu technologicznego będą podstawą do wniesienia roszczeń za uczynione szkody.
- 6) Zachowanie na terenie Zamawiającego niezgodnie z zasadami BHP spowoduje natychmiastowe usunięcie przedstawicieli Wykonawcy co nie będzie skutkowało przesunięciem terminu realizacji Zamówienia.
- 7) Wdrożenie musi zakończyć się wytworzeniem dokumentacji Powykonawczej uwzględniającej
 - Instrukcje dla wdrażanych urządzeń i systemów
 - Schematy połączeń
 - Adresacja IP
 - Dostęp do wdrażanych urządzeń i systemów umożliwiających swobodną zmianę konfiguracji czy wykonywania aktualizacji bez udziału Wykonawcy, Producenta czy innych osób trzecich.
 - Pliki z konfiguracją wdrażanych urządzeń

V. Zasilanie awaryjne UPS dla OT – 2 szt.

LP.	OPIS WYMAGAŃ TECHNICZNO-FUNKCYJONALNYCH	KONFIGURACJA MINIMALNA ZAMAWIAJĄCEGO
1.	Technologia	VFI (true on-line, podwójne przetwarzanie energii)
2.	Budowa	Rack 19" 2U
3.	Moc znamionowa	1 kVA / 1 kW
4.	Wyjściowy współczynnik mocy (PF)	1
5.	Napięcie wejściowe	230 Vac
6.	Sposób zasilania	Plug&Play Gniazdo w standardzie IEC 320 W komplecie powinien znajdować się przewód zasilający.
7.	Tolerancja napięcia wejściowego przy obciążeniu 100%; bez przechodzenia na baterie	161 – 299 Vac
8.	Regulowany zakres napięcia wejściowego zależnie od poziomu obciążenia UPS bez przechodzenia na baterie	110 – 299 Vac
9.	Częstotliwość wejściowa	40-70 Hz
10.	Sprawność AC-AC w trybie pracy	nie mniejsza niż 93%

	on-line z obciążeniem 100%	
11.	Sprawność AC-AC w trybie pracy Oszczędzania energii Eco Mode	nie mniejsza niż 99%
12.	Przeciążalność falownika	110% - bez limitu, 130% - 5 min, 140% - 30 sek., >140% - 1,5 sek.
13.	Tryb pracy z konwersją częstotliwości	Wymagana praca ze stałą częstotliwością wyjściową 50Hz, przy zasilaniu 60Hz lub odwrotnie.
14.	Napięcie wyjściowe	230 Vac W komplecie powinny znajdować się przynajmniej 2 przewody odbiorcze.
15.	Częstotliwość wyjściowa	50/60Hz (programowalna) z funkcją autosensing
16.	Zintegrowane bezprzerwowe przełączniki obejściowe (by-pass)	Statyczny przełącznik (SCR) z możliwością ręcznego przełączenia UPSa do trybu Bypass elektroniczny – wymuszanie opcji Bypass z poziomu panelu LCD
17.	Automatyczny układ doładowywania baterii i ciągłego sprawdzania stanu naładowania oraz zabezpieczenie chroniące baterie przed głębokim rozładowaniem	Wymagane
18.	Wbudowany charger o regulowanym prądzie ładowania	Wymagana regulacja ładowania w zakresie 1A – 12A, pozwalająca na szybkie ładowanie baterii o dużej pojemności.
19.	Regulacja prądu chargera	Regulacja powinna być możliwa z poziomu użytkownika na panelu LCD

20.	Baterie wewnętrzne	Minimum 3 x 9Ah/12V
21.	Autonomia	Minimum 7minut dla obciążenia 1000W
22.	Gniazdo baterii zewnętrznych	Wymagane, umożliwia podłączenie dodatkowych pakietów baterii w celu wydłużenia czasu autonomii.
23.	Baterie	Szczelne, bezobsługowe, w technologii AGM, o projektowanej żywotności min. 10-12 lat, <u>umieszczone wewnątrz</u> zasilacza UPS
24.	Możliwość rozbudowy pojemności baterii do min. 120Ah	Tak
25.	Stabilizacja napięcia wyjściowego w stanie ustalonym	$\pm 1\%$
26.	Stabilizacja napięcia wyjściowego w stanie nieustalonym	$\pm 3\%$
27.	Stabilność częstotliwości wyjściowej:	bez synchronizacji: $\pm 0,05$ Hz
28.	Współczynnik szczytu	3:1
29.	Panel sterujący z wyświetlaczem ciekłokrystalicznym LCD oraz sygnalizacją akustyczną	Wymagane ze wskazaniem parametrów napięcia wejściowego i wyjściowego, częstotliwości a także napięcia i pozostałej autonomii pracy z baterii podczas gdy UPS pracuje w trybie bateryjnym.
30.	Złącze interfejsów	RS232, USB, programowane złącze REPO do zdalnego wyłącznika pożarowego

		NO lub NC. Port zabezpieczający transmisję danych TVSS, slot karty SNMP.
31.	Gniazda wyjściowe IEC320 na zasilaczu UPS z możliwością zarządzania	Wymagane minimum gniazd – 2 grupy gniazd, w każdej przynajmniej 4 gniazda w standardzie IEC 320-C13. Możliwość programowania czasu obecności napięcia na gniazdach w pracy z baterii w zakresie 0-999 minut.
32.	Karta sieciowa SNMP	Wymagana SNMP z protokołem IP v. 4 i 6, obsługą VM oraz ModBus TCP.
33.	Zdalny panel LCD	UPS powinien posiadać możliwość podłączenia wyniesionego panelu LCD ze wskazaniem parametrów pracy i czasu autonomii.
34.	Interfejs EPO (do wyłącznika ppoż.)	Wymagane – styk programowany NO lub NC z poziomu wyświetlacza LCD.
35.	Diagnostyka parametrów urządzenia UPS i baterii	Automatyczna diagnostyka parametrów urządzenia UPS i baterii na panelu UPS-a i z wykorzystaniem oprogramowania do zarządzania i monitorowania UPS
36.	Oprogramowanie zapewniające pełny monitoring, zarządzanie i automatyczny shut-down systemu operacyjnego	Wymagane
37.	Poziom hałasu w odległości 1m,	< 48 dBA Wentylatory o regulowanej prędkości obrotowej w zależności od obciążenia i temperatury
38.	Funkcja oszczędzania energii	UPS powinien automatycznie wyłączyć się podczas pracy baterijnej, gdy obciążenie UPS spadnie <5% wartości mocy nominalnej.

39.	Możliwość regulacji z poziomu LCD tolerancji napięcia wejściowego i częstotliwości wejściowej w linii bypassu	Wymagane
40.	Zasilacz musi posiadać możliwość upgrade'u wersji oprogramowania sterującego pracą zasilacza.	Wymagane
41.	Spełnienie wszystkich obowiązujących norm w zakresie bezpieczeństwa, kompatybilności elektromagnetycznej potwierdzone deklaracją zgodności CE	Wymagane
42.	Producent zasilacza UPS z siedzibą w Polsce, posiadający biuro dystrybucji i serwisu na terenie kraju.	Wymagane
43.	Wymiary zasilacza UPS w szafie rack	Maks 2U
44.	Maksymalne wymiary urządzenia	Szerokość: 440 mm Głębokość: 410 mm Wysokość: 2U (88mm)
45.	Komplet szyn montażowych Rack	Wymagane
46.	Instrukcja w języku polskim	Wymagane
47.	Gwarancja	24 miesiące na UPS i baterie

VI. Urządzenie backup OT – 3 szt.

PROCESOR	PROCESOR OSIĄGAJĄCY WYNIK MIN. 4,5 TYSIĄCA PUNKTÓW W TEŚCIE PASSMARK.
Obudowa	Typu tower (wolnostojąca)
Pamięć RAM	Minimum 8GB typu DDR4 lub DDR5
Ilość obsługiwanych dysków	Minimum 4 dyski o rozmiarze 3.5" i maksymalnej pojemności nie mniejszej niż 22TB każdy.
Zainstalowane dyski	2 dyski o pojemności 8TB każdy zgodne z listą kompatybilności oferowanego serwera oraz charakteryzujące się następującymi parametrami: - prędkość obrotowa: minimum 7200 RPM, - pamięć cache: minimum 256MB, - gwarancja: minimum 60 miesięcy, - MTBF: minimum 2 miliony.
Interfejsy sieciowe	Minimum 2 porty 2.5GbE RJ-45. Możliwość zamontowania minimum dwóch dodatkowych karty sieciowych z portami 10GbE SFP+ lub 10GbE RJ-45. Obsługa VLAN i Jumbo Frame.
Wskaźniki LED	Minimum status, USB, LAN, dyski 1-4
Obsługa RAID	RAID 0, 1, 5, 6, 10, 50, 60, Tripple Mirror, Tripple Parity, RAID 5, 6, 10 + dysk zapasowy.
Funkcje RAID	Dodanie grupy RAID do puli magazynu, wymiana wszystkich dysków w danej grupie RAID na większe,

PROCESOR	PROCESOR OSIĄGAJĄCY WYNIK MIN. 4,5 TYSIĄCA PUNKTÓW W TEŚCIE PASSMARK.
	podłączanie jednostek rozszerzających JBOD.
Szyfrowanie	256-bitowe szyfrowanie AES folderów oraz szyfrowanie dysków zewnętrznych.
System Operacyjny	Apple Mac OS 10.10 lub nowszy Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 lub nowszy Linux IBM AIX 7, Solaris 10 lub nowszy UNIX Microsoft Windows 7, 8, 10, 11 Microsoft Windows Server 2008 R2, 2012, 2012 R2 oraz 2016, 2019, 2022
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Usługi	Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer WWW, Serwer plików, Manager plików przez WWW, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog.
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów.
Język GUI	Polski
Gwarancja i serwis	Minimum 36 miesięcy gwarancji Next Business Day zapewniającej dostawę serwera zastępczego na następny dzień roboczy po wystąpieniu awarii sprzętowej.
System plików	Dyski wewnętrzne ZFS lub EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+
Funkcje ZFS	Liniowa deduplikacja, kompresja i kompakcja, Cache odczytu & ZIL
iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation
Zasilanie	Zewnętrzny (adapter) lub wewnętrzny o mocy minimum 90W.
UPS	Obsługa sieciowych awaryjnych zasilaczy UPS.
Procesor	Procesor osiągający wynik min. 4,5 tysiąca punktów w teście PassMark.
Obudowa	Typu tower (wolnostojąca)
Pamięć RAM	Minimum 8GB typu DDR4 lub DDR5

PROCESOR	PROCESOR OSIĄGAJĄCY WYNIK MIN. 4,5 TYSIĄCA PUNKTÓW W TEŚCIE PASSMARK.
Ilość obsługiwanych dysków	Minimum 4 dyski o rozmiarze 3.5" i maksymalnej pojemności nie mniejszej niż 22TB każdy.
Zainstalowane dyski	2 dyski o pojemności 8TB każdy zgodne z listą kompatybilności oferowanego serwera oraz charakteryzujące się następującymi parametrami: - prędkość obrotowa: minimum 7200 RPM, - pamięć cache: minimum 256MB, - gwarancja: minimum 60 miesięcy, - MTBF: minimum 1 milion
Interfejsy sieciowe	Minimum 2 porty 2.5GbE RJ-45. Możliwość zamontowania minimum dwóch dodatkowych karty sieciowych z portami 10GbE SFP+ lub 10GbE RJ-45. Obsługa VLAN i Jumbo Frame.
Wskaźniki LED	Minimum status, USB, LAN, dyski 1-4
Obsługa RAID	RAID 0, 1, 5, 6, 10, 50, 60, Tripple Mirror, Tripple Parity, RAID 5, 6, 10 + dysk zapasowy.
Funkcje RAID	Dodanie grupy RAID do puli magazynu, wymiana wszystkich dysków w danej grupie RAID na większe, podłączanie jednostek rozszerzających JBOD.
Szyfrowanie	256-bitowe szyfrowanie AES folderów oraz szyfrowanie dysków zewnętrznych.
System Operacyjny	Apple Mac OS 10.10 lub nowszy Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 lub nowszy Linux IBM AIX 7, Solaris 10 lub nowszy UNIX Microsoft Windows 7, 8, 10, 11 Microsoft Windows Server 2008 R2, 2012, 2012 R2 oraz 2016, 2019, 2022
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP

PROCESOR	PROCESOR OSIĄGAJĄCY WYNIK MIN. 4,5 TYSIĄCA PUNKTÓW W TEŚCIE PASSMARK.
Usługi	Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer WWW, Serwer plików, Manager plików przez WWW, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog.
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów.
Język GUI	Polski
Gwarancja i serwis	Minimum 36 miesięcy gwarancji Next Business Day zapewniającej dostawę serwera zastępczego na następny dzień roboczy po wystąpieniu awarii sprzętowej.
System plików	Dyski wewnętrzne ZFS lub EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+
Funkcje ZFS	Liniowa deduplikacja, kompresja i kompakcja, Cache odczytu & ZIL
iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation
Zasilanie	Zewnętrzny (adapter) lub wewnętrzny o mocy minimum 90W.
UPS	Obsługa sieciowych awaryjnych zasilaczy UPS.

