

Załącznik nr 4
do IWZ 1/NI/2026

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

na

**Zwiększenie cyberodporności i ciągłości działania Przedsiębiorstwa
Wodociągów i Kanalizacji Sp. z o.o. w Olkuszu poprzez wdrożenie
nowoczesnych rozwiązań, modernizację infrastruktury oraz podniesienie
kompetencji personelu**

Spis treści

1.	HARMONOGRAM RZECZOWO-FINANSOWY	4
1.1.	Obszar IT/OT Usługi	4
1.2.	Obszar Organizacyjny	4
1.3.	Obszar IT Dostawy	4
1.4.	Obszar OT dostawy	5
1.5.	Obszar IT - Usługi	6
1.6.	Obszar OT Usługi	6
1.7.	Obszar IT - Usługi	6
1.8.	Obszar kompetencyjny	6
1.9.	Usługa asysty i wsparcia	7
1.10.	Prace dodatkowe	7
2.	INWENTARYZACJA I PROJEKTOWANIE	7
2.1.	Wymagania wstępne	7
2.2.	Harmonogram ogólny	7
2.2.1	Faza I – Analiza dokumentacji i przygotowanie produktów wstępnych do procesu inwentaryzacji i projektowania	7
2.2.2.	Faza II – Realizacja procesu projektowania	8
2.2.3.	Faza III - Administracja końca faz inwentaryzacji i projektowania – przygotowanie dokumentacji końcowej i rozliczenie merytoryczne ZAMÓWIENIA - Czas trwania – do 3 dni od dnia zakończenia Fazy II.	8
2.3.	Szczegółowy opis faz	8
2.3.1.	Faza I - Analiza dokumentacji i przygotowanie produktów wstępnych do procesu inwentaryzacji i projektowania	8
2.3.2.	Faza II Realizacja procesu inwentaryzacji i projektowania	9
2.3.2.1.	Inwentaryzacja obiektów fizycznych w formie Audytu	9
2.3.2.2.	Projektowanie koncepcyjne – przygotowanie projektu koncepcyjnego (zwanego dalej KONCEPCJĄ) - realizacja zatwierdzonego Planu Projektowania	15
2.3.2.3.	Realizacja procesu projektowania wykonawczego – Wytworzenie projektu Wykonawczego	18
2.3.3.	Faza III - Administracja końca projektu	19
3.	DOSTAWY	20
3.1.	Wymagania ogólne dla sprzętu:	20
3.2.	Wymagania ogólne dla urządzeń aktywnych sieci	20
3.3.	Urządzenia montowane na szynę DIN 35 mm muszą:	21
3.4.	Szczegółowy opis wymagań dla dostaw sprzętu	21
3.4.1.	Serwer do wykonywania kopii zapasowych typu NAS z deduplikacją	21
3.4.2.	Serwer cyberbezpieczeństwa	23
3.4.3.	Zarządzalne urządzenie sieciowe z obsługą VLAN, MACsec, standardu 802.1X	25
3.4.4.	Platforma kontroli i nagrywania sesji	30
3.4.5.	System MFA	32
3.4.6.	Klucze U2F	32
3.4.7.	Przełącznik i Sonda Danych z funkcjonalnościami DPI dla OT – do szafy Rack 19” Ilość: 1 szt.	32
3.4.8.	Przełącznik i Sonda Danych z funkcjonalnościami DPI dla OT – na szynę DIN 35 Ilość 12 szt.	37
3.4.9.	UTM OT z montażem na szynę DIN35	42
3.5.	Centralny system bezpieczeństwa	47
3.5.1.	System typu EDR/XDR z ochroną ransomware	47
3.5.2.	System typu ITSM/CMDB	49

3.5.3.	System zarządzania urządzeniami mobilnymi (MDM)	50
3.5.4.	System typu DLP	52
3.5.5.	System SIEM/IDS	54
3.5.6.	System SOAR	58
4.	USŁUGI	59
4.1.	Szkolenia	60
4.2.	Prace projektowe i wdrożeniowe zgodnie z rekomendacjami audytu Systemu Zarządzania Bezpieczeństwem Informacji	62
4.3.	Testy bezpieczeństwa infrastruktury sieciowej, serwisów internetowych, IT/OT/ICS/IIoT	62
4.4.	Audyt cyberbezpieczeństwa sieci	63
4.5.	Usługi MDR, MIDS, CTI	65
4.6.	Usługa APN	71
4.7.	Usługi SOC	71
5.	WDROŻENIE, SEGMENTACJA SIECI, ODBIORY	73
5.1.	Wdrożenie	73
5.2.	Usługi hardeningu systemów i urządzeń	73
5.3.	Segmentacja sieci	73
5.4.	Odbiory	73
6.	PRACE DODATKOWE	75

1. HARMONOGRAM RZECZOWO-FINANSOWY

Całość prac związanych z ZAMÓWIENIEM w obszarach od 1.1 do 1.8 musi zakończyć się do dnia 30 czerwca 2026r, natomiast w obszarach 1,9 i 1.10 w terminie 36 miesięcy od podpisania protokołu odbioru końcowego.

Ustala się następujący harmonogram rzeczowo finansowy

1.1. Obszar IT/OT Usługi

ID	Opis	Odniesienie do szczegółowych opisów OPZ	Zależność od poprzednich zadań (ID zadania)	Ilość
1.1	Usługa inwentaryzacji aktywów teleinformatycznych IT/OT/ICS/IIoT	2	Brak zależności	1
1.2	Zaprojektowanie rozwiązania z zakresu bezpieczeństwa z doborem urządzeń, oprogramowania i usług wdrożenia i eksploatacji IT	2	1.1	1
1.3	Zaprojektowanie rozwiązania z zakresu bezpieczeństwa z doborem urządzeń, oprogramowania i usług wdrożenia i eksploatacji OT/ICS/IIoT	2	1.1	1

1.2. Obszar Organizacyjny

ID	Opis	Odniesienie do szczegółowych opisów OPZ	Zależność od poprzednich zadań (ID zadania)	Ilość
2.1	Prace projektowe i wdrożeniowe w sposób zapewniający zgodność z rekomendacjami wynikającymi z audytu cyberbezpieczeństwa oraz obowiązującymi wymaganiami bezpieczeństwa systemów OT	4.2.	1.1.	1

1.3. Obszar IT Dostawy

ID	Opis	Odniesienie do szczegółowych opisów OPZ	Zależność od poprzednich zadań (ID zadania)	Ilość
3.1	Oprogramowanie do badania podatności - licencje	3.5.5.	Bez zależności	1
3.2	Oprogramowanie do ochrony przed ransomware - licencje	3.5.1.	Bez zależności	1
3.3	System typu EDR - licencje	3.5.1.	Bez zależności	1
3.4	Serwer typu NAS z oprogramowaniem do wykonywania kopii zapasowych z obsługą deduplikacji	3.4.1.	Bez zależności	1

3.5	Serwer pod system wirtualizacji – niezbędny do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa	3.4.2.	Bez zależności	1
3.6	Zarządzalne urządzenie sieciowe z obsługą VLAN, MACsec, standardu 802.1X	3.4.3.	Bez zależności	1
3.7	System typu ITSM – licencje	3.5.2.	Bez zależności	1
3.8	System zarządzania urządzeniami mobilnymi (MDM) – licencje	3.5.3.	Bez zależności	1
3.9	System typu DLP – licencje	3.5.4.	Bez zależności	20
3.10	Oprogramowanie do zarządzania tożsamością i dostępem – licencje	3.4.4.	Bez zależności	1
3.11	System typu MFA – licencje	3.4.5.	Bez zależności	20
3.12	Klucze U2F - urządzenia	3.4.6.	Bez zależności	20

1.4. Obszar OT dostawy

ID	Opis	Odniesienie do szczegółowych opisów OPZ	Zależność od poprzednich zadań (ID zadania)	Ilość
4.1	Sprzętowa Sonda OT. Komplementarny system komunikacyjny (switch, router, FW) i diagnostyczny z pełną ochroną i monitorowaniem na platformie sprzętowej rack 19”: System bezpieczeństwa IPS/IDS, OT Anomaly Detection, threat detection, data traceability controll, SDN, anti DDOS, anti APT (Advanced Persistent Threat)	3.4.7.	Bez zależności	1
4.2	Sprzętowa Sonda OT. Komplementarny system komunikacyjny (switch, router, FW) i diagnostyczny z pełną ochroną i monitorowaniem na platformie sprzętowej DIN35: System bezpieczeństwa IPS/IDS, OT Anomaly Detection, threat detection, data traceability controll, SDN, anti DDOS, anti APT (Advanced Persistent Threat)	3.4.8.	Bez zależności	12
4.3	Oprogramowanie platformowe - Zintegrowany System bezpieczeństwa IPS/IDS, OT Anomaly Detection, threat detection, data traceability controll, SDN, anti DDOS, anti APT (Advanced Persistent Threat), SIEM, ITSM, AKPiA RSDT, SOAR, XDR, NDR, Active Dashboards, Central FW MGMT, Alarm Risk MGMT	3.5.5.	Bez zależności	1
4.4	UTM (Unified Threat Management) Platforma sprzętowa DIN35 - System bezpieczeństwa IPS/IDS, OT Anomaly Detection, threat detection, data traceability controll, SDN, anti	3.4.9.	Bez zależności	1

	DDOS, anti APT (Advanced Persistent Threat) , AI Sanitization, AI MGMT, ZBFW			
--	--	--	--	--

1.5. Obszar IT - Usługi

ID	Opis	Odniesienie do szczegółowych opisów OPZ	Zależność od poprzednich zadań (ID zadania)	Ilość
5.1	Usługa wdrożenia	5.1.	Obszar IT Dostawy	1
5.2	Usługi konfiguracji i hardeningu systemów/urządzeń	5.2.	5.1	1
5.3	Usługa segmentacji sieci	5.3.	5.1	1

1.6. Obszar OT Usługi

ID	Opis	Odniesienie do szczegółowych opisów OPZ	Zależność od poprzednich zadań (ID zadania)	Ilość
6.1	Usługa Private APN	4.6.	5.3	14
6.2	Wdrożenie urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa. Dotyczy to również rozwiązań typu open source IT/OT/ICS/IIoT	5.1.	Obszar OT Dostawy	1
6.3	Testy bezpieczeństwa infrastruktury sieciowej, serwisów internetowych, IT/OT/ICS/IIoT	4.3.	6.3, 5.3	1

1.7. Obszar IT - Usługi

ID	Opis	Odniesienie do szczegółowych opisów OPZ	Zależność od poprzednich zadań (ID zadania)	Ilość
7.1	Audyt cyberbezpieczeństwa sieci	4.4.	6.3	1
7.2	Usługa typu MDR (Managed Detection and Response)	4.5.	7.1	360

1.8. Obszar kompetencyjny

ID	Opis	Odniesienie do szczegółowych opisów OPZ	Zależność od poprzednich zadań (ID zadania)	Ilość
8.1	Podstawowe szkolenia (lub dostęp do platform szkoleniowych) budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników	4.1.	Bez zależności	1
8.2	Szkolenia z zakresu cyberbezpieczeństwa kadry, istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji	4.1.	7.1	1

8.3	Szkolenia specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych środków bezpieczeństwa w ramach zamówienia	4.1.	7.2	1
-----	--	------	-----	---

1.9. Usługa asysty i wsparcia

ID	Opis	Odniesienie do szczegółowych opisów OPZ	Zależność od poprzednich zadań (ID zadania)	Ilość
9.1	Asysta i wsparcie	4.7.	Po podpisaniu protokołu odbioru końcowego	36 m-cy

1.10. Prace dodatkowe

ID	Opis	Odniesienie do szczegółowych opisów OPZ	Zależność od poprzednich zadań (ID zadania)	Ilość
10.1.	Prace dodatkowe	6.	Bez zależności	Czas trwania umowy

2. INWENTARYZACJA I PROJEKTOWANIE

2.1. Wymagania wstępne

- Projekt, jako dokument i faza realizacji prac, stanowiący przedmiot niniejszego OPZ , ale nie obejmuje rekonfiguracji istniejącego środowiska teleinformatycznego czy automatyki przemysłowej, dostaw sprzętu, oprogramowania czy usług z tymi dostawami związanych.
- Realizacja prac projektowych będzie bazowała m.in. na: Prince 2, ISO/IEC 27001, ISO/IEC 27002, C-HAZOP, Ustawie o ochronie danych osobowych, ISO/IEC TR 27002, CPwE, IEC 62443, Ustawie o Krajowym Systemie Cyberbezpieczeństwa
- Metodyki dostarczenia produktów specjalistycznych są dobierane w zależności od skali i zakresu merytorycznego. Notacja dla dokumentacji procesowej – Archimate 3.0 lub BPMN 2.0 lub w systemie standardu CAD
- Przebieg realizacji całości zamówienia zakończony przekazaniem dokumentacji projektu wykonawczego dla rozwiązań bezpieczeństwa i monitorowania systemów OT, została ujęta i przedstawiona w Harmonogramie ogólnym poniżej .

2.2. Harmonogram ogólny

Wymaga się realizacji zadania zgodnie z poniższym planem harmonogramu kamieni milowych.

2.2.1 Faza I – Analiza dokumentacji i przygotowanie produktów wstępnych do procesu inwentaryzacji i projektowania.

- Analiza istniejącej dokumentacji oraz ryzyk projektowych zgodnie z metoda FMEA i analizą wpływu C-HAZOP, celem przygotowania produktów wstępnych. Realizacja pierwszych etapów kwalifikacji - Czas trwania – do 6 dni roboczych od dnia podpisania umowy

2.2.2. Faza II – Realizacja procesu projektowania

- Inwentaryzacja obiektów fizycznych i logicznych w formie Audytu - Czas trwania – maksymalnie do 3 dni od dnia zakończenia Fazy I.
- Projektowanie koncepcyjne – przygotowanie projektu koncepcyjnego (zwanego dalej KONCEPCJA) - realizacja zatwierdzonego Planu Projektowania - Czas trwania – do 5 dni od dnia zakończenia zadania Inwentaryzacji
- Projektowanie wykonawcze – przygotowanie projektu wykonawczego w ustalonych ramach opisanych w KONCEPCJI, realizacja i zamknięcie procesu projektowania - Czas trwania – do 5 dni od dnia zakończenia zadania projektowania koncepcyjnego

2.2.3. Faza III - Administracja końca faz inwentaryzacji i projektowania – przygotowanie dokumentacji końcowej i rozliczenie merytoryczne ZAMÓWIENIA - Czas trwania – do 3 dni od dnia zakończenia Fazy II.

2.3. Szczegółowy opis faz

2.3.1. Faza I - Analiza dokumentacji i przygotowanie produktów wstępnych do procesu inwentaryzacji i projektowania

Analiza istniejącej dokumentacji, celem przygotowania produktów wstępnych. Realizacja pierwszych etapów projektowania.

Zakres ogólny

Cel: Uzyskanie wspólnej wizji realizacji prac fazy wraz z ustaleniem wytycznych i zakresu merytorycznego prac. Przekazanie dokumentacji. Omówienie dokumentacji i jej zakresu merytorycznego.

Zamawiający udostępni niezbędne dokumenty i informacje, jeżeli będzie w ich posiadaniu.

Efektem fazy ma być dokument określający zakres oraz plan realizacji Fazy II.

Zamawiający dostarczy istniejącą dokumentację

Oczekuje się od Wykonawcy przygotowanie zestawień dokumentacji i jej analizy pod kątem przygotowania do realizacji Fazy II.

Analiza ma być przeprowadzona zgodnie z zasadami realizacji kwalifikacji dokumentacji.

Produkt fazy

- Przygotowanie dokumentacji i rejestrów niezbędnych do przeprowadzenia procesu kwalifikacji dla poniższych zakresów

Format

- Pisemny, drukowany oraz w edytowalnej formie elektronicznej (format pliku do wyboru docx, odt, vpp).

Sposób dostarczenia produktu fazy

- Osobiście przez członka zespołu wykonawczego ze strony WYKONAWCY.

- Podczas procesu dostarczenia produktu odbywa się transfer wiedzy w postaci prezentacji wyników analiz i dyskusji z członkami zespołu wykonawczego

Miejsce realizacji prac fazy

- Miejsce eksploatacji systemów u ZAMAWIAJĄCEGO lub
- Biuro WYKONAWCY

2.3.2. Faza II Realizacja procesu inwentaryzacji i projektowania**2.3.2.1. Inwentaryzacja obiektów fizycznych w formie Audytu****Zakres ogólny**

- Wprowadzenie i wstępne spotkanie robocze
 - Cel: Ustalenie wytycznych i zakresu merytorycznego prac. Akceptacja planu audytu fizycznego na obiekcie.
 - Zmapowanie zapisów dokumentacji ze środowiskiem fizycznym
 - Przegląd procesów głównych i wspomagających, zadań jednostki, czynności stanowiskowych, rodzajów informacji (pod kątem cyberbezpieczeństwa), u Zamawiającego.
 - Przegląd infrastruktury OT i IT (również środowiska teleinformatycznego) w stopniu wymaganym do przeprowadzenia analiz.
 - Wywiady z pracownikami zakładu
 - Konsultacje z kadrami zarządzającą obszarami merytorycznymi
- Miejsce realizacji prac fazy
 - Miejsce eksploatacji systemów u ZAMAWIAJĄCEGO lub
 - Biuro WYKONAWCY

Celem przeprowadzenia analizy środowiska teleinformatycznego eksploatowanego na użytek systemów OT i IT wymaga się przeprowadzenia inwentaryzacji (zwana dalej INWENTARYZACJĄ) zasobów zgodnie z poniższym opisem:

Zakres czynności inwentaryzacji

Celem zadania jest dostarczenie informacji, na podstawie przeprowadzonych analiz i wywiadów poszczególnych obszarów i procesów.

Zakres merytoryczny oferty jest skupiony na środowisku OT wskazanym podczas pierwszego etapu INWENTARYZACJI przez ZAMAWIAJĄCEGO oraz, w części, na środowisku teleinformatycznym, w obrębie produktu podlegającego inwentaryzacji.

Zakres merytoryczny inwentaryzacji ujęty w dokumentacji poinwentaryzacyjnej

Proces inwentaryzacji dopuszcza się z wykorzystaniem systemów monitorowania i detekcji podłączonych do środowiska w oparciu o uzgodnienia z Zamawiającym na etapie Fazy I lub II.

Dopuszcza się wykonanie inwentaryzacji w formie elektronicznej w postaci uruchomionego systemu cyberbezpieczeństwa jeżeli system dostarczany w ramach Zamówienia jest systemem docelowym, dostarczany przez Wykonawcę.

Poniżej wymieniono obszary merytoryczne podlegające inwentaryzacji:

Ustalenie elementów środowiska IT dla OT

Elementy wchodzące w skład powyższej architektury:

- a) Obiekty fizyczne
 - hosty dostępne
 - serwery bazodanowy
 - serwery funkcyjne
 - urządzenia aktywne
 - elementy pasywne (media)
- b) Obiekty logiczne
 - serwery metadanych
 - serwery baz danych
 - platformy Systemów Operacyjnych
 - platformy aplikacyjne
 - systemy operacyjne

Inwentaryzacja IT:

- 1. Warstwa 1
 - a. Topologia fizyczna Numeracja segmentów fizycznych sieci
 - b. Rodzaje sygnalizacji technologii transmisji danych
 - c. Rodzaje medium Opis sprzętu
 - d. Opis wyposażenia pasywnego (z pominięciem okablowania wymienionego w pkt. d)
- 2. Warstwa 2
 - a. Topologia logiczna (strefy/segmenty STP – CST, PVST, MST, H-RING, ...)
 - b. Adresacja – fizyczna (rodzaje adresów i wartości)
 - c. Protokoły użytkowników (enkapsulacja)
 - d. Protokoły obszaru komunikacji sterowania
 - e. Protokoły typu maintenance (VTP, CDP, STP, itp.)
- 3. Warstwa 3
 - a. Topologia logiczna

- b. Routing
 - c. Adresacja użytkowników
 - d. Adresacja WAN
 - e. Adresacja Aplikacji serwerowych
 - f. Adresacja zewnętrznych AS-ów (Autonomous System)
 - g. Określanie ścieżek transmisji pakietów w stosunku do topologii logicznej warstw 1 – 3
4. Warstwa 4
- a. Protokoły warstwy dla ruchu użytkowników
 - b. Protokoły warstwy dla ruchu maintenance
 - c. Protokoły warstwy dla ruchu WAN
 - d. Protokoły warstwy dla ruchu niechcianego (w miarę możliwości skanowania)
5. Warstwa 5
- a. Rodzaje sesji
 - b. Opisy lokalizacyjne dla interfejsów terminujących sesje
 - c. Rodzaje wykorzystywanych protokołów
6. Warstwa 6
- a. Rodzaje kompresji protokołów
 - b. Protokoły reprezentacji danych transmisyjnych
 - c. Protokoły reprezentacji danych składowanych (na nośnikach danych)
7. Warstwa 7
- a. Inwentaryzacja aplikacji korzystających wprost z zasobów sieci
 - b. Inwentaryzacja aplikacji korzystających pośrednio z zasobów sieci
8. Opis sprzętu aktywnego
- a. Warstwy 1 – lokalizacja fizyczna w stosunku do topologii fizycznej
 - b. Warstwy 2 – lokalizacja fizyczna w stosunku do topologii fizycznej i logicznej (warstwy 1 – 3)
 - c. Warstwy 3 - lokalizacja fizyczna w stosunku do topologii fizycznej i logicznej (warstwy 1 – 3)
 - d. Spis rodzaju, modelu, producenta i systemu operacyjnego sprzętu
9. Opis serwerów
- a. Platforma sprzętowa

- b. Platforma systemu operacyjnego
- c. Adresacja w odniesieniu do topologii warstwy 2 i 3 oraz udostępnionych zasobów
- d. Opis platformy systemowej (systemu operacyjnego)
- e. Opis procesów systemowych (elementy maintenance)
- f. Opis sposobu zarządzania platformą sprzętową i systemową
- g. Opis wykorzystywanej funkcjonalności systemu operacyjnego
- h. Opis zależności w strukturze współdzielenia zasobów z innymi serwerami w sieci.

10. Opis aplikacji i systemów

- a. Lokalizacja fizyczna aplikacji (serwer, interfejs, segment sieci fizycznej)
- b. Lokalizacja logiczna aplikacji (serwer logiczny, segment warstwy 2 i 3, adresacja warstwy 2 i 3, segmenty dostępowe z warstw 1 – 3)
- c. Lista i opis funkcjonalny aplikacji użytkowych
- d. Lista i opis funkcjonalny aplikacji maintenance

11. Konfiguracje sprzętu aktywnego

- a. Konfiguracje urządzeń aktywnych sieci

Wymogi bezpieczeństwa systemów

1. Bezpieczeństwo pasywne systemu

- 1. Zasilanie środowiska IT
- 2. Ochrona dostępu fizycznego
- 3. Redundancja sprzętowa (elementów pasywnych i aktywnych środowiska IT)

2. Bezpieczeństwo aktywne systemu

- System archiwizacji i przywracania danych
- Rodzaje szyfrowania
 - a. Transmisje danych użytkowników
 - b. Transmisje sesji logowania (uwierzytelnianie)
 - c. Transmisje sesji zarządzających siecią
 - d. Ścieżki transmisji danych szyfrowanych w odniesieniu do topologii warstw 1 – 3
- Redundancja logiczna

- Opis systemów logowania w odniesieniu do topologii warstwy 1 – 3 i aplikacji (bazy LDAP – Windows, Unix, Linux, itp)
- Opis grup roboczych w zakresie obszarów domen logowania
- Opis domen logowania
- Opis struktur baz danych zasobów Active Directory i innych tym podobnych
- Opis funkcji wykorzystywany przy autentykacji i autoryzacji użytkowników i innych zasobów

W odniesieniu do poprzednich punktów wymagane jest określenie poziomu szczegółowości opisów pod kątem ewentualnej integracji systemów i aplikacji.

Administracja

Obszary podlegające przygotowaniu

1. utrzymanie ruchu
2. zarządzanie dostępem
3. zarządzanie zmianą – modyfikacje systemowe
4. dokumentacja operacyjna

Przyjęte w przedsiębiorstwie procedury implementacji środowiska IT/OT

Opis przyjętych metodyk, norm, wytycznych, dyrektyw niezbędne do właściwego postępowania na obiekcie i przygotowywania właściwej dokumentacji projektowej i użytkowej.

Inwentaryzacja OT

Inwentaryzacja ma być wykonana do poziomu urządzeń aktywnych systemów AKPiA

Dokumentacja inwentaryzacyjna ma zawierać:

- a) Topologię fizyczną sieci Ethernet
 - Forma graficzna w dowolnym narzędziu pod warunkiem dostarczenie narzędzia do odczytu
 - Eksport do wektorowego PDF
 - Topologia ma zawierać informację o połączeniach logicznych wraz z ujęciem patchpaneli, przełącznic światłowodowych gniazd RJ45, gniazd światłowodowych
 - Urządzeń podłączonych do infrastruktury kablowej
 - Topologia ma być ograniczona do punk tu styku z operatorami zewnętrznymi
- b) Topologię logiczną sieci warstwy 2
 - Forma graficzna w dowolnym narzędziu pod warunkiem dostarczenie narzędzia do odczytu
 - Eksport do wektorowego PDF
 - Topologia ma zawierać urządzenia ze źródłowymi adresami MAC i wskazaniem portu fizycznego urządzeń sąsiedzkich (np. komputer <-> przełącznik)
 - Topologia ma być ograniczona do punk tu styku z operatorami zewnętrznymi
- c) Topologię logiczną sieci warstwy 3

- Forma graficzna w dowolnym narzędziu pod warunkiem dostarczenie narzędzia do odczytu
- Eksport do wektorowego PDF
- Topologia ma zawierać urządzenia ze źródłowymi adresami IP
- Topologia ma być ograniczona do punktu styku z operatorami zewnętrznymi
- d) Mapę komunikacji – oznaczenie obiektów, które wymieniają między sobą dane
 - Forma tabelaryczna z oznaczeniem MAC oraz IPv4 źródła i przeznaczenia. W przypadku routingu oznaczyć MAC interfejsu wyjściowego routera jako adres przypisany do IP źródłowego. Wykazać w tabeli powiązanie IP do wielu adresów MAC (jeden sprzętowy źródła oraz wszystkie adresy MAC interfejsów wyjściowych routerów w całej ścieżce komunikacyjnej do miejsca docelowego.
- e) Ustawienia reguł Firewalli
 - Forma tabelaryczna w formacie xlsx lub zgodnym
 - Ujęcie urządzenia, wirtualizacji jeśli istnieje, zapisu reguły, status (aktywna lub nie aktywna) efekt działania,
- f) Listy komponentów
 - Forma tabelaryczna w formacie xlsx lub zgodnym
- g) Zestawienie musi zawierać minimum, model, lokalizacja, miejsce montażu, numer seryjny lub numer inwentarzowy (jeżeli urządzenie wymaga demontażu – nie dokonujemy tej czynności a numery seryjne lub model pozostawiamy niewypełniony) adres MAC, adres IP, przypisanie do systemu dziedzicznego, właściciel systemu (osoba lub osoby odpowiedzialne za działanie komponentu)
- h) Ustawienia zasad dostępu do zasobów do poziomu stacji roboczych i użytkowników
 - Forma tabelaryczna w formacie xlsx lub zgodnym
 - Wylistowanie użytkowników oraz zasobów sieciowych wraz z przypisaniem do komponentu (jeśli dotyczy) oraz systemu docelowego do poziomu adresu IPv4

Dopuszczalna jest dokumentacja zdjęciowa jako uzupełnienie technicznej dokumentacji opisowej

Całość dokumentacji musi być przekazana na nośniku elektronicznym, z uruchomionym szyfrowaniem sprzętowym posiadającym certyfikat bezpieczeństwa NATO np. NATO Restricted, w ilość 1 szt.

Produkt fazy

Dokumentacja inwentaryzacyjna i analityczna.

Raport rozbieżności

Format

Pisemny, drukowany oraz w edytowalnej formie elektronicznej (format pliku docx, odt, vpp).

Sposób dostarczenia produktu fazy

Osobiście przez członka zespołu wykonawczego ze strony WYKONAWCY.

Podczas procesu dostarczenia produktu odbywa się transfer wiedzy w postaci prezentacji wyników analiz i dyskusji z członkami Państwa zespołu wykonawczego

Miejsce realizacji prac fazy

Miejsce eksploatacji systemów u ZAMAWIAJĄCEGO

Biuro WYKONAWCY

2.3.2.2. Projektowanie koncepcyjne – przygotowanie projektu koncepcyjnego (zwanego dalej KONCEPCJĄ) - realizacja zatwierdzonego Planu Projektowania

Zakres ogólny

Przygotowanie projektu koncepcyjnego, celem wykazania poziomu zgodności z założeniami i wymaganiami przez ZAMAWIAJĄCEGO. (porównanie wyników inwentaryzacji i koncepcji wstępnej, uzyskanie informacji o potencjalnych rozbieżnościach celem ich uzupełnienia lub modyfikacji koncepcji)

Realizacja planu projektowania ze szczególnym uwzględnieniem cyklu życia i analiz ryzyk zgodnie z FMEA i analizą wpływu C-HAZOP

Obszary podlegające opracowaniu:

- Systemy skomputeryzowane
- Warstwa sterowania i automatyki
- Warstwa manufacturing (zgodne z IEC 62443)
- Komunikacja sieciowa
- Monitoring systemów i transmisji danych
- Interfejsy systemowe
- Zestaw wymiany danych z systemem nadrzędnym ICS
- Opis projektowanych systemów IT, OT
- Wytyczne i wymagania producentów poszczególnym komponentów głównych

Miejsce realizacji prac

- Miejsce eksploatacji systemów u ZAMAWIAJĄCEGO lub
- Biuro WYKONAWCY

Projekt koncepcyjny

Projekt koncepcyjny powinien opisywać wymagane przez ZAMAWIAJĄCEGO zakres i formułę działania systemu na poziomie opracowania topologii L1 do L3 w odniesieniu do modelu OSI, topologię logiczną aplikacji i powinny być oparte na udokumentowanej ocenie ryzyka i wpływu systemu komputerowego. Dokument KONCEPCJI musi zawierać scenariusz użycia danego rozwiązania ukazującego poglądowy sposób pracy operatorów w ramach danego rozwiązania. Wymagania użytkowników powinny być identyfikowalne w całym cyklu życia systemu komputerowego.

Scenariusz może być przedstawiony w formie szkolenia stanowiskowego

Systemy mogą być zaprojektowane w formie pojedynczego systemu lub struktury różnych rozwiązań zarówno komercyjnych jak i open source.

Wymaganiem Zamawiającego jest wizualizacja zdarzeń i możliwość reakcji na zagrożenie z jednego, centralnego systemu zarządzania widocznością i bezpieczeństwem.

Wszystkie dane źródłowe: ruch sieci, logi i inne podłączane źródła zarówno z systemów chmurowych czy lokalnych muszą być kolekcjonowane przez system centralny, normalizowany, wizualizowany i musi zapewnić pełną widoczność.

Wykonawca bierze odpowiedzialność za działanie systemu w formie zintegrowanej.

Nie dopuszcza się niezależnych systemów, które będą wymagały, dla uzyskania widoczności danych, logowania się na różne systemy i ich interfejsy.

Dopuszcza się stosowanie niezależnych dostępów 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 oraz system centralny pochodziły od tego samego producenta i posiadały Certyfikat IEC 62443 4-2 na poziomie SL4 akredytowany przez PCA. 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 zaprojektowaniu w środowisku Zamawiającego.

- Oprogramowanie do badania podatności
- Oprogramowanie do ochrony przed ransomware
- System typu EDR
- System typu NAS z oprogramowaniem do wykonywania kopii zapasowych z obsługą deduplikacji
- Serwer pod system wirtualizacji
- System typu ITSM
- System zarządzania urządzeniami mobilnymi (MDM)
- System typu DLP dla OT
- Oprogramowanie do zarządzania tożsamością i dostępem
- System typu MFA
- Klucze U2F
- Komplementarny system komunikacyjny oparty o dostarczone urządzenia przez Wykonawcę
 - Urządzenie będące jednocześnie (przełącznikiem, routerem, FW i urządzeniem diagnostycznym) – 1 szt 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) – 12 szt z pełną ochroną i monitorowaniem na platformie sprzętowej DIN35 z systemem bezpieczeństwa IPS/IDS, OT Anomaly Detection, threat detection, data traceability controll, SDN, anti DDOS, anti APT (Advanced Persistent Threat)
 - Zarządzalne urządzenie sieciowe z obsługą VLAN, MACsec, standardu 802.1X - Urządzenie będące jednocześnie (przełącznikiem, routerem, FW i urządzeniem diagnostycznym) – 1 szt 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)

- Oprogramowanie platformowe - Zintegrowany System bezpieczeństwa IPS/IDS, OT Anomaly Detection, threat detection, data traceability controll, SDN, anti DDOS, anti APT (Advanced Persistent Threat), SIEM, ITSM, AKPiA RSDT, SOAR, XDR, NDR, Active Dashboards, Central FW MGMT, Alarm Risk MGMT
- UTM (Unified Threat Management) - Platforma sprzętowa DIN35 - System bezpieczeństwa IPS/IDS, OT Anomaly Detection, threat detection, data traceability controll, SDN, anti DDOS, anti APT (Advanced Persistent Threat) , AI Sanitization, AI MGMT, ZBFW
- Usługa Private APN – 14 kart SIM - oparta o usługę dostarczoną przez Wykonawcę. Bezpieczeństwo transmisji musi być zapewniane przez Wykonawcę poprzez monitorowanie ruchu przez SOC i własne systemy cyberbezpieczeństwa zlokalizowane u Wykonawcy. SOC Wykonawcy musi legitymować się certyfikacją akredytowaną przez PCA w zakresie minimum ISO 27001 oraz ISO 9001. Dopuszcza się konsorcja lub podwykonawstwo w którym Wykonawca bierze odpowiedzialność za działanie usługi APN.

Wymagana zawartość dokumentu projektowego.

Wymaga się aby projekt koncepcyjny zawierał niewylącznie opracowanie poniższych obszarów:

- Wymogi operacyjne
- Wymagania funkcjonalne
- Wymagania dotyczące danych
- Wymagania techniczne
- Wymagania dotyczące interfejsu
- Wymagania środowiskowe
- Wymagania dostępności
- Wymagania w zakresie utrzymania
- Opis ograniczeń dla rozwiązania
- Wymagania dotyczące cyklu życia

Obszary podlegające opracowaniu

- Systemy skomputeryzowane
- Warstwa sterowania i automatyki
- Warstwa manufacturing
- Komunikacja
- Interfejsy systemowe
- Opis projektowanych systemów IT, OT
- Wytyczne i wymagania producentów poszczególnym komponentów głównych

Format

Pisemny, drukowany oraz w edytowalnej formie elektronicznej (format pliku docx, odt, vpp).

- Mapa połączeń wykonana zgodnie z notacją Archimate 2.0

Sposób dostarczenia produktu fazy

- Osobiście przez członka zespołu wykonawczego ze strony WYKONAWCY.
- Podczas procesu dostarczenia produktu odbywa się transfer wiedzy w postaci prezentacji wyników analiz i dyskusji z członkami zespołu wykonawczego ZAMAWIAJĄCEGO produktów projektu

Miejsce realizacji prac

- Miejsce eksploatacji systemów u ZAMAWIAJĄCEGO
- Biuro WYKONAWCY

WYKONANIE RAPORTU ROZBIEŻNOŚCI

Raport rozbieżności stanowi część projektu koncepcji jako proces urealnienia wykonania prac i osiągniętych efektów.

- Raport rozbieżności należy wykonać poprzez porównanie projektu koncepcyjnego oraz wyników przeprowadzonej inwentaryzacji.
- Forma raportu musi być pisemna i musi zawierać informację o różnicach pomiędzy zaakceptowaną przez ZAMAWIAJĄCEGO KONCEPCJĄ a istniejącymi zasobami, które można wykorzystać do realizacji i wdrożenia rozwiązań projektowanych w Fazie II.
- Raport musi obejmować analogiczny obszar merytoryczny jak projekt koncepcyjny.

2.3.2.3. Realizacja procesu projektowania wykonawczego – Wytworzenie projektu

Wykonawczego

Zakres ogólny

Przygotowanie projektu wykonawczego dla ustalonych w KONCEPCJI rozwiązań

Obszary podlegające fazie

- Specyfikacja funkcjonalna
- Specyfikacja projektowa
- System cyberbezpieczeństwa
- Instalacja
- Procesy eksploatacyjne

Miejsce realizacji prac

- Miejsce eksploatacji systemów u ZAMAWIAJĄCEGO
- Biuro WYKONAWCY

Produkty

Produktem jest dokument w formie pisemnej na nośniku elektronicznym.

Projekt Wykonawczy musi być zgodny z projektem koncepcyjnym i zaakceptowanym Raportem Rozbieżności

Projekt musi uwzględniać ewentualne zmiany uzgodnione na etapie analizy i zatwierdzania Projektu Koncepcyjnego i warunków montażowych i uruchomieniowych na obiekcie.

Dopuszcza się zatwierdzenie Projektu Koncepcyjnego jako Projektu Wykonawczego w przypadku braku rozbieżności z warunkami montażu i uruchomień oraz wystarczającej szczegółowości Projektu Koncepcyjnego

- Projekt wykonawczy musi opisywać wymagane przez użytkownika funkcje systemu/rozwiązania, bazując na zaakceptowanym projekcie koncepcyjnym i musi być oparty na udokumentowanej ocenie ryzyka i wpływu. Wymagania użytkowników powinny być identyfikowalne w całym cyklu życia systemu
- Projekt musi spełniać wymagania następujących norm i dobrych praktyk:
 - IEC 62443 w zakresie segmentacji i kontroli sieci
 - ISO 27001 – w zakresie bezpieczeństwa informacji

Format

- Pisemny, drukowany oraz w edytowalnej formie elektronicznej (format pliku docx, odt, vpp).
- Mapa połączeń wykonana zgodnie z notacją Archimate 2.0

Sposób dostarczenia produktu fazy

- Osobiście przez członka zespołu wykonawczego ze strony WYKONAWCY.
- Podczas procesu dostarczenia produktu odbywa się transfer wiedzy w postaci prezentacji wyników analiz i dyskusji z członkami zespołu wykonawczego ZAMAWIAJĄCEGO produktów projektu

Miejsce realizacji prac

- Miejsce eksploatacji systemów u ZAMAWIAJĄCEGO
- Biuro WYKONAWCY

2.3.3. Faza III - Administracja końca projektu

Faza AKP stanowi zakończenie i rozliczenie merytoryczne projektu. W tej fazie:

- przygotowywany jest końcowy raport z przebiegu całości prac
- konsolidowane są dokumenty w jednej zbior
- dokumenty są drukowane oraz nanoszone na nośnik nieulotny (zaszyfrowany pendrive) i przekazanie nośnika z zawartością, fizycznie do ZAMAWIAJĄCEGO
- zapisy elektroniczne są nanoszone na nośnik nieulotny i przekazany do ZAMAWIAJĄCEGO w formacie edytowalnym oraz w formacie PDF

Faza kończy się spotkaniem przekazującym, na którym przedstawiane są wyniki projektu i następuje akceptacja Fazy Realizacji.

Miejsce spotkania i zakończenia projektu

- Miejsce eksploatacji systemów u ZAMAWIAJĄCEGO lub

- Biuro WYKONAWCY

Produkty:

- Protokół z Fazy od I i II
- Komplet dokumentów z Faz I i II

Format

- Pisemny, drukowany oraz w edytowalnej formie elektronicznej (format pliku docx, odt, vpp).
- Mapa połączeń wykonana zgodnie z notacją Archimate 2.0

Sposób dostarczenia produktu fazy

- Osobiście przez członka zespołu wykonawczego ze strony WYKONAWCY.
- Podczas procesu dostarczenia produktu odbywa się transfer wiedzy w postaci prezentacji wyników analiz i dyskusji z członkami zespołu wykonawczego ZAMAWIAJĄCEGO produktów projektu

Miejsce realizacji prac

- Miejsce eksploatacji systemów u ZAMAWIAJĄCEGO

Biuro WYKONAWCY

3. DOSTAWY

3.1. Wymagania ogólne dla sprzętu:

- musi być nowy (nie starszy niż z 4 kwartału 2025 r) i pochodzić z polskiego kanału dystrybucji
- musi posiadać gwarancję i wsparcie producenta na okres nie krótszy niż do 30.06.2026
- 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).

3.2. Wymagania ogólne dla urządzeń aktywnych sieci

Urządzenia montowane do szaf rack 19” muszą:

- Posiadać dwa zasilacze 230 V działające w układzie nadmiarowym i uzupełniającym
- Posiadać strukturę modułarną (nie dopuszcza się sprzętu które nie posiada chociaż jednego modułu rozszerzeń do którego można dołożyć – po za projektem np. dodatkowy moduł komunikacyjny np. interfejsy Ethernet 8x 1 Gb/S SFP)
- Producent musi pochodzić z Państw należących do Unii Europejskiej
- Posiadać aktualny certyfikat IEC 62443 4-2 SL4 akredytowany przez PCA
- 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

3.3. Urządzenia montowane na szynę DIN 35 mm muszą:

- Być dostarczone z dwoma zasilaczami 230 V / DC 24 V dostosowane mocowo do dostarczanych urządzeń działające w układzie nadmiarowym i uzupełniającym
- Posiadać strukturę modułową (nie dopuszcza się sprzętu które posiada chociaż jednego modułu rozszerzeń do którego można dołożyć – po za projektem np. dodatkowy moduł komunikacyjny np. LTE lub WiFi
- Posiadać aktualny certyfikat IEC 62443 4-2 SL4 akredytowany przez PCA
- 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
- W przypadku montażu w podstacjach elektroenergetycznych wymagany jest certyfikat na sprzęt IEEE 1613, C1D2

3.4. Szczegółowy opis wymagań dla dostaw sprzętu

3.4.1. Serwer do wykonywania kopii zapasowych typu NAS z deduplikacją

Komplet wymieniony w ilości 1 szt

Parametr	Opis / wartość parametru	Ilość
Pamięć RAM	8 GB	1
Storage	24 TB SATA III, z ramkami	1
Kontroler RAID	Typy RAID 0, 1, 10, 01, 5, 6,	1
CPU	Intel	1
Zasilacze	230 V	2
Interfejs 10 Gb/s	SFP28 Ethernet	2
Wkładki	SFP28 10 Gb/s SM	2
Interfejs 1 Gb/s	RJ45 Ethernet	4
Szyny montażowe	Rail, teleskopowe, do szaf 19"	1
Kable zasilające	Min 1,5 m	2
Typ montażu	Do szafy 19", wysokość max 2 U	n/d
Zarządzanie	, interfejs GUI	1
Łańcuch dostaw	Nie dopuszcza się urządzeń z krajów uznanych za niebezpieczne, Nie dopuszcza się rozwiązań pochodzących z Federacji Rosyjskiej lub krajów bezpośrednio wspierających jej działania.	

Grupy funkcyjne systemu cyberbezpieczeństwa:

- Skaner antywirusowy

- System backupu i odtwarzania zainstalowany na NAS, wraz z deduplikacją

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja systemu pamięci masowej typu NAS (Network Attached Storage), przeznaczonego do realizacji kopii zapasowych danych w środowiskach IT oraz OT, wyposażonego w dedykowane oprogramowanie do zarządzania backupem, replikacją oraz deduplikacją danych.

Wymagania funkcjonalne:

Funkcjonalność systemu backupowego:

- wykonywanie kopii zapasowych danych z systemów:
 - Windows, Linux,
 - środowisk wirtualnych (np. VMware, Hyper-V),
 - serwerów plików i baz danych,
- obsługa backupów:
 - pełnych, przyrostowych i różnicowych,
 - harmonogramowanych oraz uruchamianych na żądanie,
- możliwość tworzenia polityk backupowych,
- obsługa wersjonowania danych oraz retencji.

Deduplikacja i optymalizacja danych:

- deduplikacja danych na poziomie bloków, realizowana na poziomie systemu backupowego lub systemu plików
- kompresja danych,
- możliwość redukcji wykorzystania przestrzeni dyskowej,
- deduplikacja lokalna oraz (opcjonalnie) po stronie źródła.

Replikacja i odzyskiwanie danych:

- możliwość replikacji danych:
 - lokalnej,
 - zdalnej (do drugiego systemu NAS lub chmury),
- wsparcie dla replikacji w czasie rzeczywistym lub harmonogramowanej,
- funkcje Disaster Recovery,
- możliwość szybkiego odtwarzania danych (granular restore, bare-metal restore).

Obsługa protokołów i integracja:

- wsparcie dla protokołów:
 - SMB/CIFS, NFS, FTP/SFTP,
 - iSCSI (target),
- integracja z usługami katalogowymi (np. Active Directory, LDAP),
- możliwość pracy jako centralne repozytorium backupów.

Zarządzanie i bezpieczeństwo:

- dostęp do systemu przez interfejs webowy,
- zarządzanie użytkownikami i uprawnieniami,
- szyfrowanie danych:
 - w spoczynku (at-rest),
 - w transmisji (in-transit),
- obsługa mechanizmów snapshot,
- ochrona przed ransomware (np. immutable snapshots, WORM),
- logowanie i audyt operacji.

Wymagania sprzętowe:

- system NAS oparty o architekturę x86 (procesor klasy Intel lub równoważny),
- minimum:
 - procesor wielordzeniowy,
 - pamięć RAM: min. 8 GB (rozszerzalna),
- możliwość instalacji wielu dysków
- obsługa RAID (min. RAID 1, 5, 6, 10),
- interfejsy sieciowe:
 - min. 2 × 1 Gb/s lub 10 Gb/s,
- możliwość rozbudowy (RAM, dyski, interfejsy sieciowe),
- redundantne lub zabezpieczone zasilanie (jeśli wymagane przez Zamawiającego)
- dostawa obejmuje dyski twarde zapewniające 24 TB przestrzeni fizycznej.

Wymagania dotyczące oprogramowania:

- zintegrowane lub dedykowane oprogramowanie do backupu i zarządzania kopiami zapasowymi,
- możliwość centralnego zarządzania zadaniami backupu,
- intuicyjny interfejs administracyjny,
- możliwość integracji z systemami zewnętrznymi,
- licencjonowanie umożliwiające wykorzystanie wszystkich wymaganych funkcji (w tym deduplikacji).

Wymagania eksploatacyjne:

- system musi być dostarczony jako rozwiązanie kompletne i gotowe do pracy,
- wykonawca zapewni:
 - instalację i konfigurację,
 - uruchomienie systemu backupowego,
 - testy poprawności działania (backup/restore),
 - dokumentację powykonawczą,
- przeprowadzenie szkolenia dla administratorów.

Dodatkowe wymagania (opcjonalne / premiowane):

- wsparcie dla backupu do chmury (np. S3, Azure, inne),
- możliwość tworzenia maszyn wirtualnych bezpośrednio na NAS,
- integracja z systemami SIEM/SOC,

3.4.2. Serwer cyberbezpieczeństwa

Komplet wymieniony poniżej w ilości: 1 szt

Parametr	Opis / wartość parametru	Ilość
Pamięć RAM	256 GB	1
Storage	4 TB w dyskach SAS lub SSD lub lepszych wydajnościowo, z ramkami	1
Kontroler RAID	Typy RAID 0, 1, 10, 01, 5, 6, 50, 51, 60, 61	1
CPU	minimum 16 core	2

Zasilacze	230 V	2
Interfejs 10 Gb/s	SFP28 Ethernet	2
Wkładki	SFP28 10 Gb/s SM	2
Interfejs 1 Gb/s	RJ45 Ethernet	4
Szyny montażowe	Rail, teleskopowe, do szaf 19"	1
Kable zasilające	Min 1,5 m	2
Typ montażu	Do szafy 19", wysokość max 2 U	n/d
Łańcuch dostaw	Dopuszczalne są jedynie produkty pochodzące z Unii Europejskiej Nie dopuszcza się urządzeń z krajów uznanych za niebezpieczne	

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja serwera przeznaczonego do pracy jako platforma wirtualizacyjna dla środowisk IT oraz (opcjonalnie) OT, zapewniającego wysoką wydajność, niezawodność oraz możliwość dalszej rozbudowy.

Wymagania sprzętowe:

Procesory:

- minimum 2 × procesor klasy x86_64
- każdy procesor wielordzeniowy (min. 16 rdzeni na CPU),
- wsparcie dla technologii wirtualizacyjnych

Pamięć operacyjna:

- minimum 256 GB RAM,
- możliwość rozbudowy do co najmniej 512 GB.
- pamięć przystosowana do pracy ciągłej 24/7 w środowiskach serwerowych,
- moduły pamięci muszą być kompatybilne z oferowaną platformą sprzętową i znajdować się na liście kompatybilności producenta (QVL – Qualified Vendor List),
- pamięć musi być dostarczona przez producenta serwera lub autoryzowanego partnera producenta,
- niedopuszczalne jest stosowanie komponentów niecertyfikowanych przez producenta platformy serwerowej.

Przestrzeń dyskowa:

- minimum 4 × dysk fizyczny,
- łączna przestrzeń użytkowa (po konfiguracji RAID) min. 6 TB,
- wsparcie dla konfiguracji RAID (min. RAID 1, 5, 6, 10),
- kontroler RAID sprzętowy z pamięcią cache i podtrzymaniem bateryjnym kontrolera RAID,
- możliwość rozbudowy przestrzeni dyskowej.

Interfejsy sieciowe:

- minimum:
 - 4 × 1 Gb/s RJ45,
 - 2 × 10 Gb/s SFP+,
- możliwość agregacji łączy (LACP)
- serwer będzie dostarczony z 2 sztukami wkładek 10 Gb/s SFP+ 1310 nm, 10 KM,

- o wsparcie dla VLAN.

Obudowa i zasilanie:

- o obudowa rack (19") przystosowana do montażu w szafie serwerowej max 2 U,
- o redundantne zasilacze (hot-swap) – minimum 2 zasilacze,
- o redundantne wentylatory (hot-swap).

Zarządzanie:

- o dedykowany port zarządzający (out-of-band management),
- o możliwość zdalnego zarządzania (KVM over IP, monitoring, aktualizacja firmware),

Wymagania funkcjonalne:
Przeznaczenie:

- o serwer przeznaczony do uruchomienia platformy wirtualizacyjnej (np. VMware, Hyper-V, Proxmox lub równoważnej), dla systemów cyberbezpieczeństwa.
- o System ma zostać dostarczony z preinstalowanym najnowszym systemem Proxmox
- o możliwość uruchamiania wielu maszyn wirtualnych jednocześnie.

Wydajność i skalowalność:

- o architektura umożliwiająca rozbudowę:
 - pamięci RAM,
 - przestrzeni dyskowej,
 - interfejsów sieciowych,

Bezpieczeństwo:

- o wsparcie dla mechanizmów szyfrowania (np. TPM, Secure Boot),
- o możliwość integracji z systemami backupu i Disaster Recovery,
- o izolacja zasobów pomiędzy maszynami wirtualnymi.

Kompatybilność:

- o kompatybilność z popularnymi platformami wirtualizacyjnymi,
- o wsparcie dla systemów operacyjnych serwerowych (Windows Server, Linux).

Wymagania eksploatacyjne:

- dostarczenie urządzenia fabrycznie nowego, nieużywanego,
- instalacja i konfiguracja sprzętu,
- przygotowanie środowiska pod wirtualizację (instalacja hypervisora)

3.4.3. Zarządzalne urządzenie sieciowe z obsługą VLAN, MACsec, standardu 802.1X

Komplet wymieniony poniżej w ilości: 1 szt

Parametr	Opis / wartość parametru	Ilość
Pamięć RAM	Min. 32 GB	1
Storage	Min. 500 GB w dyskach SSD	2
Interfejs MGMT	RJ45	1
Interfejs Szeregowy	Konsola RS232	1

Zasilacze	230 V	2
Interfejs 10 Gb/s	SFP+ Ethernet	4
Wkładki	SFP28 10 Gb/s SM	2
Interfejs 1 Gb/s	RJ45 Ethernet with bypass	8
Interfejs 1 Gb/s	SFP 1 Gb/s	16
Wkładki 1 Gb/s	SFP 1 Gb/s SM	16
Szyny montażowe	Rail, teleskopowe, do szaf 19"	1
Kable zasilające	Min 1,5 m	2
Typ montażu	Do szafy 19", wysokość max 2 U	n/d
Patch cordy	Miedziane CAT6, 1,5 M RJ45	24
Patch cordy	Światłowodowe SC/LC 1,5 m SM	4
Montaż	Do szafy Rack 19", szyny rail, teleskopowe	n/d
Kable zasilające	Min 1,5 m	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

Wymagania dla funkcjonalności systemu pracującego na urządzeniu:

Routing i przełączanie (L2 / L3)

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

Firewall i bezpieczeństwo

- **Stateful Firewall (ZBFW – Zone-Based Firewall)** – inspekcja stanu połączeń i przypisanie reguł do stref logicznych.
- **NAT (Source, Destination, Static, Masquerade)** – pełna translacja adresów.
- **Policy NAT i Hairpin NAT** – elastyczne mapowanie adresów w zależności od kierunku.
- **IPv6 Firewall** – osobne polityki bezpieczeństwa dla IPv6.

- **Traffic Filtering na poziomie L2–L4** – filtrowanie pakietów, portów, protokołów.
- **Time-based Rules** – polityki bezpieczeństwa zależne od czasu.
- **Conntrack / Helper modules** – śledzenie sesji i stanów połączeń.
- **Rate-limiting / DoS protection** – ograniczanie przepustowości, ochrona przed floodem.
- **MAC Firewall / ARP Inspection / Static ARP tables** – kontrola komunikacji warstwy drugiej.

VPN i tunelowanie

- **IPsec IKEv1 / IKEv2** – szyfrowane tunele site-to-site i remote access.
- **L2TP, PPTP, OpenVPN, WireGuard** – elastyczne protokoły VPN dla użytkowników i urządzeń.
- **GRE / mGRE / VTI / VXLAN / IP-in-IP** – tunelowanie ruchu między sieciami (np. SCADA ↔ DMZ).
- **Dynamiczny routing przez VPN (BGP over IPsec)** – skalowalność w dużych sieciach.
- **DMVPN V3** – automatyka zestawiania topologii HUB Spoke z zabezpieczeniem IPsec i protokołami routingu wraz z protokołem NHRP
- **SSL VPN / Remote Access** – wsparcie dla zdalnego dostępu użytkowników.

QoS i kontrola ruchu

- **Traffic Shaping / Policing / Queueing (HTB, CBQ, HFSC)** – kontrola pasma.
- **Hierarchical QoS (HQoS)** – wielopoziomowe kolejkovanie.
- **Traffic Classification (DSCP / CoS / ACL match)** – klasyfikacja ruchu na podstawie atrybutów.
- **Bandwidth Management per interface / per VLAN** – kontrola przepustowości per-port lub per-sieć.

Monitoring, logowanie i diagnostyka

- **SNMP v1/v2c/v3** – monitorowanie zewnętrzne.
- **Syslog (lokalny i zdalny)** – pełna integracja logów z systemami SIEM/IDS.
- **NetFlow / sFlow / IPFIX** – eksport statystyk ruchu do systemów analitycznych.
- **Ping / Traceroute / MTR / Packet Capture (tcpdump)** – diagnostyka sieciowa.
- **BFD** – szybkie wykrywanie awarii tras routingu.
- **Interface Counters / Flow statistics** – bieżące statystyki ruchu.

- **Monitorowanie w trybie inline** – analityka DPI oraz IDS realizowana pasywnie w trybie ciągłym na każdym interfejsie aktywnym,
- **Mirror Port** – możliwość skopiowania ramek z interfejsów źródłowych na interfejs wyjściowy
- **Przekierowanie wewnętrzne do systemów analityki** – funkcja zautomatyzowana przekierowania ruchu przez wewnętrzny system IPS (w trybie IPS) dla analityki z automatyka ochrony inline
- Analityka anomalii komunikacji sieciowej pomiędzy komponentami
- Behavioral monitoring,
- Profilowanie obiektów logicznych i fizycznych sieci
- Identyfikacja komponentów w danych z ruchu sieciowego
- Analityka czasów transmisji dla komunikacji sesyjnej i niesesyjnej
- Traceability dla podanych parametrów zidentyfikowanych w ruchu sieciowym
- Tryb maintenance dla wyciszenia alertów z profili zgłoszonych do zmiany w środowisku sieciowym
- Thread Detection
- Analityka głęboka protokołów IT i OT w tym Modbus TCP, Goose, Profinet, Ethernet/IP, EtherCat, S-BUS, Step7, IEC 60870-5-104
- Diagnostyka protokołów OT
- Diagnostyka protokołów IT

Zarządzanie i automatyzacja

- **CLI / SSH / API / RESTCONF / NETCONF** – wielowarstwowe zarządzanie.
- **Konfiguracja CLI w stylu Cisco / Juniper** – logiczne drzewo konfiguracji.
- **Atomic commits / rollback / diff** – bezpieczne zmiany i cofanie konfiguracji.
- **Scheduled tasks / cron / event-driven scripts** – automatyzacja procesów.
- **Ansible / Salt / Terraform ready** – zgodność z narzędziami DevOps.
- **Zarządzanie użytkownikami / RADIUS / TACACS+ / LDAP** – kontrola dostępu administracyjnego.
- **Backup / restore / config versioning** – bezpieczeństwo konfiguracji.
- **Zarządzanie Firewall** – wymagane jest również zarządzanie z poziomu konsoli centralnej

IDS/IPS

Detekcja, analiza i blokowanie zagrożeń sieciowych w czasie rzeczywistym.

- Analiza i inspekcja ruchu sieciowego (Deep Packet Inspection – DPI)

- Pełna inspekcja pakietów na poziomie L2–L7 w czasie rzeczywistym.
 - Analiza protokołów przemysłowych (Modbus, DNP3, IEC 60870-5-104, PROFINET, BACnet, OPC UA itp.).
 - Wykrywanie anomalii w komunikacji sterowników PLC, HMI i urządzeń przemysłowych.
 - Rozpoznawanie struktur poleceń, zmiennych procesowych i komunikacji SCADA.
- Detekcja zagrożeń (Intrusion Detection System – IDS)
 - Wykrywanie prób włamań, skanowania portów, exploitów, ataków DoS/DDoS i naruszeń polityk sieciowych.
 - Identyfikacja złośliwego oprogramowania, beaconingu i nieautoryzowanych połączeń C2 (Command & Control).
 - Korelacja zdarzeń z regułami IDS Rules oraz regułami zespołu MDR i CTI.
 - Generowanie alertów i przekazywanie ich do systemu SIEM/IDS.
- Blokowanie zagrożeń (Intrusion Prevention System – IPS)
 - Dynamiczne blokowanie pakietów i sesji zgodnie z regułami bezpieczeństwa.
 - Automatyczne odcinanie źródeł ataków, modyfikacja polityk firewallowych w czasie rzeczywistym.
 - Współpraca z modułem firewall (ZBFW) i komponentami SIEM/IDS w celu natychmiastowej reakcji.
 - Minimalny wpływ na opóźnienia i przepustowość ruchu sieciowego (low-latency design).
- Analiza sygnatur i anomalii
 - Wykorzystanie sygnatur znanych ataków oraz mechanizmów heurystycznych i statystycznych.
 - Wykrywanie anomalii w zachowaniach urządzeń i użytkowników (np. nagłe wzrosty ruchu, zmiana portów, niezgodność protokołów).
 - Wsparcie dla analizy behawioralnej w połączeniu z modułami CTI i MDR.
 - Aktualizacje baz reguł bezpieczeństwa w sposób automatyczny i kontrolowany.
- Integracja z systemami analitycznymi i korelacyjnymi
 - Wysyłanie logów i alertów do systemów, SIEM, SOC, MDR.
 - Normalizacja danych i mapowanie zdarzeń do frameworków MITRE ATT&CK i IEC 62443.
 - Współpraca z bazami danych CTI w celu identyfikacji źródeł zagrożeń i kampanii APT.
 - Eksport danych w formatach EVE JSON, Syslog, PCAP i NetFlow.
- Wsparcie inspekcji w sieciach OT
 - Zoptymalizowane reguły detekcji dla środowisk przemysłowych.
 - Tryb „passive monitoring” bez ingerencji w ruch procesowy (dla systemów krytycznych).
 - Tryb „inline” z prewencyjnym blokowaniem ataków przy zachowaniu zgodności z IEC 62443-3-3.
 - Pełna widoczność komunikacji pomiędzy segmentami IT a OT.
- Mechanizmy automatyzacji i korelacji
 - Automatyczne przekazywanie alertów do modułów reakcji MDR.
 - Aktywacja polityk obronnych w firewallu .
 - Dynamiczne uczenie się ruchu sieciowego (profilowanie).

- Możliwość tworzenia własnych reguł i skryptów reakcji w środowisku SIEM/IDS.
- Raportowanie i wizualizacja
 - Raporty incydentów bezpieczeństwa, trendów i statystyk detekcji.
 - Graficzne przedstawienie ruchu sieciowego i źródeł zagrożeń w panelu SIEM IDS.
 - Eksport alertów i logów do systemów zewnętrznych w formacie JSON, CSV, Syslog.
 - Możliwość integracji z pulpitemi centralnego SIEM/IDS .

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, kluczy i certyfikatów.**

Dodatkowe cechy

- **Rolling Release – aktualizacje bezpieczeństwa w cyklu ciągłym.**
- **Integracja z Docker / LXC / KVM – uruchamianie usług w kontenerach.**
- **Obsługa Netfilter nftables / eBPF – nowoczesne mechanizmy filtrowania.**

3.4.4. Platforma kontroli i nagrywania sesji

Zamawiający wymaga dostawy systemu PAM w formie dedykowanego Appliance 1 U jako centralny system zarządzania i kontroli dostępu do infrastruktury IT oraz OT, umożliwiający **bezpieczne, audytowane i izolowane połączenia z systemami krytycznymi**, bez konieczności bezpośredniego dostępu użytkowników do sieci wewnętrznej.

Parametr	Opis / wartość parametru	Ilość
Pamięć RAM	Min. 32 GB	1
Storage	Min. 4 TB w dyskach SSD	2
Interfejs MGMT	RJ45	1
Interfejs Szeregowy	Konsola RS232	1
Zasilacze	230 V	2
Interfejs 10 Gb/s	SFP+ Ethernet	2
Wkładki	SFP 10 Gb/s SM	2
Interfejs 1 Gb/s	RJ45 Ethernet	15

Szyny montażowe	Rail, teleskopowe, do szaf 19"	1
Kable zasilające	Min 1,5 m	2
Typ montażu	Do szafy 19", wysokość max 2 U	n/d
Patch cordy	Miedziane CAT6, 1,5 M RJ45	15
Patch cordy	Światłowodowe SC/LC 1,5 m SM	2
Montaż	Do szafy Rack 19", szyny rail, teleskopowe	n/d
Kable zasilające	Min 1,5 m	2
Zarządzanie	GUI	1

Wymagania funkcjonalne

1. Centralne zarządzanie dostępem uprzywilejowanym

- Umożliwia bezpieczne połączenia do systemów i urządzeń przez przeglądarkę (HTML5 – bez agentów).
- Musi obsługiwać protokoły minimum: **RDP, SSH, VNC**,
- Granularne przydzielanie dostępów zgodnie z zasadą „**least privilege**” (najmniejszych uprawnień).

2. Izolacja i bezpieczeństwo sesji

- Użytkownicy nie łączą się bezpośrednio z urządzeniami
- Sesje użytkowników są **izolowane** i monitorowane w czasie rzeczywistym.
- Pełne nagrywanie sesji administracyjnych (RDP, SSH, VNC)
- Możliwość natychmiastowego rozłączenia użytkownika przez operatora SOC/MDR.

3. Kontrola tożsamości i autoryzacja

- Integracja z mechanizmami uwierzytelniania minimum: **LDAP**.
- Obsługa **MFA (Multi-Factor Authentication)** – w tym tokeny sprzętowe, aplikacje TOTP,.
- Rejestracja operacji logowania, autoryzacji i zakończenia sesji.

4. Audyt i rejestrowanie działań użytkowników

- Nagrania sesji wideo
- Raporty audytowe zgodne z wymaganiami
- Szybkie wyszukiwanie sesji po użytkowniku, dacie, adresie IP lub nazwie urządzenia.
- Możliwość eksportu nagrań i logów do systemów SIEM / SOC /

5. Wsparcie dla środowisk IT i OT

- Tryb **Jump Host / Bastion**, umożliwiający dostęp do sieci przemysłowych przez bezpieczną bramę.

6. Automatyzacja i zarządzanie poświadczeniami

- Automatyczne logowanie użytkownika bez znajomości poświadczeń docelowych.
- Bezpieczne API do integracji z innymi systemami (np. ticketing, SIEM, CMDB).

3.4.5. System MFA

MFA ma być dostarczone w postaci systemu kontroli poświadczeń w oparciu o dopuszczalne dwa rozwiązania technologiczne opisane poniżej pod warunkiem obsługi minimum 20 użytkowników w tym samym czasie.

Rozwiązanie będzie wykorzystywane dla zdalnego dostępu do infrastruktury Zamawiającego

Rozwiązanie 1 – w postaci urządzeń i oprogramowania wydanego dla każdego z 20 użytkowników
lub

Rozwiązanie 2 – w postaci oprogramowania które można zainstalować na telefonie komórkowym z systemem Android lub IOS

Rozwiązanie musi zostać zintegrowane z usługą VPN uruchomioną na dostarczonym rozwiązaniu sprzętowym w ramach pozostałych obszarów.

Poświadczenia, klucze i pozostałe elementy nie mogą być przechowywane po za środowiskiem Zamawiającego. Jedynie urządzenie lub oprogramowanie dla generowania dodatkowego czynnika poświadczeń powinno być przy użytkowniku ale z zastrzeżeniem braku możliwości komunikacji ze środowiskiem Zamawiającego celem wymiany jakichkolwiek danych

Zarządzanie MFA musi odbywać się w ramach dostarczonego rozwiązania. Nie dopuszcza się rozwiązań chmurowych.

3.4.6. Klucze U2F

Rozwiązanie w postaci kluczy fizycznych wraz z oprogramowaniem wydawane użytkownikom celem podawania drugiego składnika uwierzytelniania. Klucze muszą być kompatybilne z systemami Windows 10 i 11. Klucze dla poprawnego działania muszą być umieszczane fizycznie w porcie USB i za pomocą dedykowanego oprogramowania uczestniczyć w wydaniu dodatkowego składnika poświadczeń.

Nie dopuszcza się rozwiązań chmurowych.

3.4.7. Przełącznik i Sonda Danych z funkcjonalnościami DPI dla OT – do szafy Rack 19” Ilość: 1 szt.

Komplet wymieniony poniżej w ilości: 1 szt

Parametr	Opis / wartość parametru	Ilość
Pamięć RAM	Min. 32 GB	1
Storage	Min. 500 GB w dyskach SSD	2
Interfejs MGMT	RJ45	1
Interfejs Szeregowy	Konsola RS232	1

Zasilacze	230 V	2
Interfejs 10 Gb/s	SFP+ Ethernet	4
Wkładki	SFP28 10 Gb/s SM	2
Interfejs 1 Gb/s	RJ45 Ethernet with bypass	8
Interfejs 1 Gb/s	SFP 1 Gb/s	16
Wkładki 1 Gb/s	SFP 1 Gb/s SM	16
Szyny montażowe	Rail, teleskopowe, do szaf 19"	1
Kable zasilające	Min 1,5 m	2
Typ montażu	Do szafy 19", wysokość max 2 U	n/d
Patch cordy	Miedziane CAT6, 1,5 M RJ45	24
Patch cordy	Światłowodowe SC/LC 1,5 m SM	4
Montaż	Do szafy Rack 19", szyny rail, teleskopowe	n/d
Kable zasilające	Min 1,5 m	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

Wymagania dla funkcjonalności systemu pracującego na urządzeniu:

Routing i przełączanie (L2 / L3)

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

Firewall i bezpieczeństwo

- **Stateful Firewall (ZBFW – Zone-Based Firewall)** – inspekcja stanu połączeń i przypisanie reguł do stref logicznych.
- **NAT (Source, Destination, Static, Masquerade)** – pełna translacja adresów.
- **Policy NAT i Hairpin NAT** – elastyczne mapowanie adresów w zależności od kierunku.
- **IPv6 Firewall** – osobne polityki bezpieczeństwa dla IPv6.

- **Traffic Filtering na poziomie L2–L4** – filtrowanie pakietów, portów, protokołów.
- **Time-based Rules** – polityki bezpieczeństwa zależne od czasu.
- **Conntrack / Helper modules** – śledzenie sesji i stanów połączeń.
- **Rate-limiting / DoS protection** – ograniczanie przepustowości, ochrona przed floodem.
- **MAC Firewall / ARP Inspection / Static ARP tables** – kontrola komunikacji warstwy drugiej.

VPN i tunelowanie

- **IPsec IKEv1 / IKEv2** – szyfrowane tunele site-to-site i remote access.
- **L2TP, PPTP, OpenVPN, WireGuard** – elastyczne protokoły VPN dla użytkowników i urządzeń.
- **GRE / mGRE / VTI / VXLAN / IP-in-IP** – tunelowanie ruchu między sieciami (np. SCADA ↔ DMZ).
- **Dynamiczny routing przez VPN (BGP over IPsec)** – skalowalność w dużych sieciach.
- **DMVPN V3** – automatyka zestawiania topologii HUB Spoke z zabezpieczeniem IPsec i protokołami routingu wraz z protokołem NHRP
- **SSL VPN / Remote Access** – wsparcie dla zdalnego dostępu użytkowników.

QoS i kontrola ruchu

- **Traffic Shaping / Policing / Queueing (HTB, CBQ, HFSC)** – kontrola pasma.
- **Hierarchical QoS (HQoS)** – wielopoziomowe kolejkovanie.
- **Traffic Classification (DSCP / CoS / ACL match)** – klasyfikacja ruchu na podstawie atrybutów.
- **Bandwidth Management per interface / per VLAN** – kontrola przepustowości per-port lub per-sieć.

Monitoring, logowanie i diagnostyka

- **SNMP v1/v2c/v3** – monitorowanie zewnętrzne.
- **Syslog (lokalny i zdalny)** – pełna integracja logów z systemami SIEM/IDS.
- **NetFlow / sFlow / IPFIX** – eksport statystyk ruchu do systemów analitycznych.
- **Ping / Traceroute / MTR / Packet Capture (tcpdump)** – diagnostyka sieciowa.
- **BFD** – szybkie wykrywanie awarii tras routingu.
- **Interface Counters / Flow statistics** – bieżące statystyki ruchu.

- **Monitorowanie w trybie inline** – analityka DPI oraz IDS realizowana pasywnie w trybie ciągłym na każdym interfejsie aktywnym,
- **Mirror Port** – możliwość skopiowania ramek z interfejsów źródłowych na interfejs wyjściowy
- **Przekierowanie wewnętrzne do systemów analityki** – funkcja zautomatyzowana przekierowania ruchu przez wewnętrzny system IPS (w trybie IPS) dla analityki z automatyka ochrony inline
- Analityka anomalii komunikacji sieciowej pomiędzy komponentami
- Behavioral monitoring,
- Profilowanie obiektów logicznych i fizycznych sieci
- Identyfikacja komponentów w danych z ruchu sieciowego
- Analityka czasów transmisji dla komunikacji sesyjnej i niesesyjnej
- Traceability dla podanych parametrów zidentyfikowanych w ruchu sieciowym
- Tryb maintenance dla wyciszenia alertów z profili zgłoszonych do zmiany w środowisku sieciowym
- Thread Detection
- Analityka głęboka protokołów IT i OT w tym Modbus TCP, Goose, Profinet, Ethernet/IP, EtherCat, S-BUS, Step7, IEC 60870-5-104
- Diagnostyka protokołów OT
- Diagnostyka protokołów IT

Zarządzanie i automatyzacja

- **CLI / SSH / API / RESTCONF / NETCONF** – wielowarstwowe zarządzanie.
- **Konfiguracja CLI w stylu Cisco / Juniper** – logiczne drzewo konfiguracji.
- **Atomic commits / rollback / diff** – bezpieczne zmiany i cofanie konfiguracji.
- **Scheduled tasks / cron / event-driven scripts** – automatyzacja procesów.
- **Ansible / Salt / Terraform ready** – zgodność z narzędziami DevOps.
- **Zarządzanie użytkownikami / RADIUS / TACACS+ / LDAP** – kontrola dostępu administracyjnego.
- **Backup / restore / config versioning** – bezpieczeństwo konfiguracji.
- **Zarządzanie Firewall** – wymagane jest również zarządzanie z poziomu konsoli centralnej

IDS/IPS

Detekcja, analiza i blokowanie zagrożeń sieciowych w czasie rzeczywistym.

- Analiza i inspekcja ruchu sieciowego (Deep Packet Inspection – DPI)

- Pełna inspekcja pakietów na poziomie L2–L7 w czasie rzeczywistym.
 - Analiza protokołów przemysłowych (Modbus, DNP3, IEC 60870-5-104, PROFINET, BACnet, OPC UA itp.).
 - Wykrywanie anomalii w komunikacji sterowników PLC, HMI i urządzeń przemysłowych.
 - Rozpoznawanie struktur poleceń, zmiennych procesowych i komunikacji SCADA.
- Detekcja zagrożeń (Intrusion Detection System – IDS)
 - Wykrywanie prób włamań, skanowania portów, exploitów, ataków DoS/DDoS i naruszeń polityk sieciowych.
 - Identyfikacja złośliwego oprogramowania, beaconingu i nieautoryzowanych połączeń C2 (Command & Control).
 - Korelacja zdarzeń z regułami IDS Rules oraz regułami zespołu MDR i CTI.
 - Generowanie alertów i przekazywanie ich do systemu SIEM/IDS.
- Blokowanie zagrożeń (Intrusion Prevention System – IPS)
 - Dynamiczne blokowanie pakietów i sesji zgodnie z regułami bezpieczeństwa.
 - Automatyczne odcinanie źródeł ataków, modyfikacja polityk firewallowych w czasie rzeczywistym.
 - Współpraca z modułem firewall (ZBFW) i komponentami SIEM/IDS w celu natychmiastowej reakcji.
 - Minimalny wpływ na opóźnienia i przepustowość ruchu sieciowego (low-latency design).
- Analiza sygnatur i anomalii
 - Wykorzystanie sygnatur znanych ataków oraz mechanizmów heurystycznych i statystycznych.
 - Wykrywanie anomalii w zachowaniach urządzeń i użytkowników (np. nagłe wzrosty ruchu, zmiana portów, niezgodność protokołów).
 - Wsparcie dla analizy behawioralnej w połączeniu z modułami CTI i MDR.
 - Aktualizacje baz reguł bezpieczeństwa w sposób automatyczny i kontrolowany.
- Integracja z systemami analitycznymi i korelacyjnymi
 - Wysyłanie logów i alertów do systemów, SIEM, SOC, MDR.
 - Normalizacja danych i mapowanie zdarzeń do frameworków MITRE ATT&CK i IEC 62443.
 - Współpraca z bazami danych CTI w celu identyfikacji źródeł zagrożeń i kampanii APT.
 - Eksport danych w formatach EVE JSON, Syslog, PCAP i NetFlow.
- Wsparcie inspekcji w sieciach OT
 - Zoptymalizowane reguły detekcji dla środowisk przemysłowych.
 - Tryb „passive monitoring” bez ingerencji w ruch procesowy (dla systemów krytycznych).
 - Tryb „inline” z prewencyjnym blokowaniem ataków przy zachowaniu zgodności z IEC 62443-3-3.
 - Pełna widoczność komunikacji pomiędzy segmentami IT a OT.
- Mechanizmy automatyzacji i korelacji
 - Automatyczne przekazywanie alertów do modułów reakcji MDR.
 - Aktywacja polityk obronnych w firewallu .
 - Dynamiczne uczenie się ruchu sieciowego (profilowanie).

- Możliwość tworzenia własnych reguł i skryptów reakcji w środowisku SIEM/IDS.
- Raportowanie i wizualizacja
 - Raporty incydentów bezpieczeństwa, trendów i statystyk detekcji.
 - Graficzne przedstawienie ruchu sieciowego i źródeł zagrożeń w panelu SIEM IDS.
 - Eksport alertów i logów do systemów zewnętrznych w formacie JSON, CSV, Syslog.
 - Możliwość integracji z pulpitemi centralnego SIEM/IDS .

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, kluczy i certyfikatów.

Dodatkowe cechy

- **Rolling Release** – aktualizacje bezpieczeństwa w cyklu ciągłym.
- **Integracja z Docker / LXC / KVM** – uruchamianie usług w kontenerach.
- **Obsługa Netfilter nftables / eBPF** – nowoczesne mechanizmy filtrowania.

3.4.8. Przełącznik i Sonda Danych z funkcjonalnościami DPI dla OT – na szynę DIN 35 Ilość 12 szt.

Komplet wymieniony poniżej w ilości: 12 szt

Parametr	Opis / wartość parametru	Ilość
Pamięć RAM	Min. 8 GB	1
Storage	Min. 480 GB w dyskach SSD	1
Interfejs Szeregowy	Konsola RS232	1
Zasilacze	230 V 5 A – 24 V DC	2
Interfejs 1 Gb/s	RJ45 Ethernet with 2 porty 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 SM

Moduł GSM	LTE wraz z aktywną kartą SIM 1 szt., 2 x kabel antenowy, antena x 2	1
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	24
Patch cordy	Światłowodowe SC/LC 1,5 m SM	4
Montaż	Do szafy Rack 19", szyny rail, teleskopowe	n/d
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,	n/d
Temperatura pracy	Od minus 40 stopni Celsjusza do plus 70 stopni Celsjusza	

Wymagania dla funkcjonalności systemu pracującego na urządzeniu:

Routing i przełączanie (L2 / L3)

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

Firewall i bezpieczeństwo

- **Stateful Firewall (ZBFW – Zone-Based Firewall)** – inspekcja stanu połączeń i przypisanie reguł do stref logicznych.
- **NAT (Source, Destination, Static, Masquerade)** – pełna translacja adresów.

- **Policy NAT i Hairpin NAT** – elastyczne mapowanie adresów w zależności od kierunku.
- **IPv6 Firewall** – osobne polityki bezpieczeństwa dla IPv6.
- **Traffic Filtering na poziomie L2–L4** – filtrowanie pakietów, portów, protokołów.
- **Time-based Rules** – polityki bezpieczeństwa zależne od czasu.
- **Conntrack / Helper modules** – śledzenie sesji i stanów połączeń.
- **Rate-limiting / DoS protection** – ograniczanie przepustowości, ochrona przed floodem.
- **MAC Firewall / ARP Inspection / Static ARP tables** – kontrola komunikacji warstwy drugiej.

VPN i tunelowanie

- **IPsec IKEv1 / IKEv2** – szyfrowane tunele site-to-site i remote access.
- **L2TP, PPTP, OpenVPN, WireGuard** – elastyczne protokoły VPN dla użytkowników i urządzeń.
- **GRE / mGRE / VTI / VXLAN / IP-in-IP** – tunelowanie ruchu między sieciami (np. SCADA ↔ DMZ).
- **Dynamiczny routing przez VPN (BGP over IPsec)** – skalowalność w dużych sieciach.
- **DMVPN V3** – automatyka zestawiania topologii HUB Spoke z zabezpieczeniem IPsec i protokołami routingu wraz z protokołem NHRP
- **SSL VPN / Remote Access** – wsparcie dla zdalnego dostępu użytkowników.

QoS i kontrola ruchu

- **Traffic Shaping / Policing / Queueing (HTB, CBQ, HFSC)** – kontrola pasma.
- **Hierarchical QoS (HQoS)** – wielopoziomowe kolejkovanie.
- **Traffic Classification (DSCP / CoS / ACL match)** – klasyfikacja ruchu na podstawie atrybutów.
- **Bandwidth Management per interface / per VLAN** – kontrola przepustowości per-port lub per-sieć.

Monitoring, logowanie i diagnostyka

- **SNMP v1/v2c/v3** – monitorowanie zewnętrzne.
- **Syslog (lokalny i zdalny)** – pełna integracja logów z systemami SIEM/IDS.
- **NetFlow / sFlow / IPFIX** – eksport statystyk ruchu do systemów analitycznych.
- **Ping / Traceroute / MTR / Packet Capture (tcpdump)** – diagnostyka sieciowa.

- **BFD** – szybkie wykrywanie awarii tras routingu.
- **Interface Counters / Flow statistics** – bieżące statystyki ruchu.
- **Monitorowanie w trybie inline** – analityka DPI oraz IDS realizowana pasywnie w trybie ciągłym na każdym interfejsie aktywnym,
- **Mirror Port** – możliwość skopiowania ramek z interfejsów źródłowych na interfejs wyjściowy
- **Przekierowanie wewnętrzne do systemów analityki** – funkcja zautomatyzowana przekierowania ruchu przez wewnętrzny system IPS (w trybie IPS) dla analityki z automatyka ochrony inline
- Analityka anomalii komunikacji sieciowej pomiędzy komponentami
- Behavioral monitoring,
- Profilowanie obiektów logicznych i fizycznych sieci
- Identyfikacja komponentów w danych z ruchu sieciowego
- Analityka czasów transmisji dla komunikacji sesyjnej i niesesyjnej
- Traceability dla podanych parametrów zidentyfikowanych w ruchu sieciowym
- Tryb maintenance dla wyciszenia alertów z profili zgłoszonych do zmiany w środowisku sieciowym
- Thread Detection
- Analityka głęboka protokołów IT i OT w tym Modbus TCP, Goose, Profinet, Ethernet/IP, EtherCat, S-BUS, Step7, IEC 60870-5-104
- Diagnostyka protokołów OT
- Diagnostyka protokołów IT

Zarządzanie i automatyzacja

- **CLI / SSH / API / RESTCONF / NETCONF** – wielowarstwowe zarządzanie.
- **Konfiguracja CLI w stylu Cisco / Juniper** – logiczne drzewo konfiguracji.
- **Atomic commits / rollback / diff** – bezpieczne zmiany i cofanie konfiguracji.
- **Scheduled tasks / cron / event-driven scripts** – automatyzacja procesów.
- **Ansible / Salt / Terraform ready** – zgodność z narzędziami DevOps.
- **Zarządzanie użytkownikami / RADIUS / TACACS+ / LDAP** – kontrola dostępu administracyjnego.
- **Backup / restore / config versioning** – bezpieczeństwo konfiguracji.
- **Zarządzanie Firewall** – wymagane jest również zarządzanie z poziomu konsoli centralnej

IDS/IPS

Detekcja, analiza i blokowanie zagrożeń sieciowych w czasie rzeczywistym.

- Analiza i inspekcja ruchu sieciowego (Deep Packet Inspection – DPI)
 - Pełna inspekcja pakietów na poziomie L2–L7 w czasie rzeczywistym.
 - Analiza protokołów przemysłowych (Modbus, DNP3, IEC 60870-5-104, PROFINET, BACnet, OPC UA itp.).
 - Wykrywanie anomalii w komunikacji sterowników PLC, HMI i urządzeń przemysłowych.
 - Rozpoznawanie struktur poleceń, zmiennych procesowych i komunikacji SCADA.
- Detekcja zagrożeń (Intrusion Detection System – IDS)
 - Wykrywanie prób włamań, skanowania portów, exploitów, ataków DoS/DDoS i naruszeń polityk sieciowych.
 - Identyfikacja złośliwego oprogramowania, beaconingu i nieautoryzowanych połączeń C2 (Command & Control).
 - Korelacja zdarzeń z regułami IDS Rules oraz regułami zespołu MDR i CTI.
 - Generowanie alertów i przekazywanie ich do systemu SIEM/IDS.
- Blokowanie zagrożeń (Intrusion Prevention System – IPS)
 - Dynamiczne blokowanie pakietów i sesji zgodnie z regułami bezpieczeństwa.
 - Automatyczne odcinanie źródeł ataków, modyfikacja polityk firewallowych w czasie rzeczywistym.
 - Współpraca z modułem firewall (ZBFW) i komponentami SIEM/IDS w celu natychmiastowej reakcji.
 - Minimalny wpływ na opóźnienia i przepustowość ruchu sieciowego (low-latency design).
- Analiza sygnatur i anomalii
 - Wykorzystanie sygnatur znanych ataków oraz mechanizmów heurystycznych i statystycznych.
 - Wykrywanie anomalii w zachowaniach urządzeń i użytkowników (np. nagłe wzrosty ruchu, zmiana portów, niezgodność protokołów).
 - Wsparcie dla analizy behawioralnej w połączeniu z modułami CTI i MDR.
 - Aktualizacje baz reguł bezpieczeństwa w sposób automatyczny i kontrolowany.
- Integracja z systemami analitycznymi i korelacyjnymi
 - Wysyłanie logów i alertów do systemów SIEM, SOC, MDR.
 - Normalizacja danych i mapowanie zdarzeń do frameworków MITRE ATT&CK i IEC 62443.
 - Współpraca z bazami danych CTI w celu identyfikacji źródeł zagrożeń i kampanii APT.
 - Eksport danych w formatach EVE JSON, Syslog, PCAP i NetFlow.
- Wsparcie inspekcji w sieciach OT
 - Zoptymalizowane reguły detekcji dla środowisk przemysłowych.
 - Tryb „passive monitoring” bez ingerencji w ruch procesowy (dla systemów krytycznych).
 - Tryb „inline” z prewencyjnym blokowaniem ataków przy zachowaniu zgodności z IEC 62443-3-3.
 - Pełna widoczność komunikacji pomiędzy segmentami IT a OT.
- Mechanizmy automatyzacji i korelacji

- Automatyczne przekazywanie alertów do modułów reakcji MDR.
- Aktywacja polityk obronnych w firewallu .
- Dynamiczne uczenie się ruchu sieciowego (profilowanie).
- Możliwość tworzenia własnych reguł i skryptów reakcji w środowisku SIEM/IDS.
- Raportowanie i wizualizacja
 - Raporty incydentów bezpieczeństwa, trendów i statystyk detekcji.
 - Graficzne przedstawienie ruchu sieciowego i źródeł zagrożeń w panelu SIEM/IDS.
 - Eksport alertów i logów do systemów zewnętrznych w formacie JSON, CSV, Syslog.
 - Możliwość integracji z pulpitemi centralnego SIEM/IDS .

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, kluczy i certyfikatów.

Dodatkowe cechy

- **Rolling Release** – aktualizacje bezpieczeństwa w cyklu ciągłym.
- **Integracja z Docker / LXC / KVM** – uruchamianie usług w kontenerach.
- **Obsługa Netfilter nftables / eBPF** – nowoczesne mechanizmy filtrowania.

3.4.9. UTM OT z montażem na szynę DIN35

Komplet wymieniony poniżej w ilości: 1 szt

Parametr	Opis / wartość parametru	Ilość
Pamięć RAM	Min. 8 GB	1
Storage	Min. 480 GB w dyskach SSD	1
Interfejs Szeregowy	Konsola RS232	1
Interfejs Szeregowy cd	RS 232/422/485	2
Zasilacze	230 V 5 A – 24 V DC - synchroniczne	2
Interfejs 1 Gb/s	RJ45 Ethernet with bypass	2
Interfejs 1 Gb/s	SFP 1 Gb/s	2
Wkładki 1 Gb/s	SFP 1 Gb/s SM	2
Moduł GSM	LTE, 2 x kabel antenowy, antena x 2	1

Moduł WiFi	WiFi 6 + anteny 2 szt	1
Uchwyty montażowe	1 komplet dla DIN35	
Kable zasilające	Min 0,5 m	2
Typ montażu	Szyna DIN35	n/d
Patch cordy	Miedziane CAT6, 1,5 M RJ45	24
Patch cordy	Światłowodowe SC/LC 1,5 m SM	4
Montaż	Do szafy Rack 19", szyny rail, teleskopowe	n/d
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, RoHS	n/d
Temperatura pracy	Od minus 40 stopni Celsjusza do plus 70 stopni Celsjusza	

Wymagania dla funkcjonalności systemu pracującego na urządzeniu:

Routing i przełączanie (L2 / L3)

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

Firewall i bezpieczeństwo

- **Stateful Firewall (ZBFW – Zone-Based Firewall)** – inspekcja stanu połączeń i przypisanie reguł do stref logicznych.
- **NAT (Source, Destination, Static, Masquerade)** – pełna translacja adresów.
- **Policy NAT i Hairpin NAT** – elastyczne mapowanie adresów w zależności od kierunku.
- **IPv6 Firewall** – osobne polityki bezpieczeństwa dla IPv6.
- **Traffic Filtering na poziomie L2–L4** – filtrowanie pakietów, portów, protokołów.
- **Time-based Rules** – polityki bezpieczeństwa zależne od czasu.

- **Conntrack / Helper modules** – śledzenie sesji i stanów połączeń.
- **Rate-limiting / DoS protection** – ograniczanie przepustowości, ochrona przed floodem.
- **MAC Firewall / ARP Inspection / Static ARP tables** – kontrola komunikacji warstwy drugiej.

VPN i tunelowanie

- **IPsec IKEv1 / IKEv2** – szyfrowane tunele site-to-site i remote access.
- **L2TP, PPTP, OpenVPN, WireGuard** – elastyczne protokoły VPN dla użytkowników i urządzeń.
- **GRE / mGRE / VTI / VXLAN / IP-in-IP** – tunelowanie ruchu między sieciami (np. SCADA ↔ DMZ).
- **Dynamiczny routing przez VPN (BGP over IPsec)** – skalowalność w dużych sieciach.
- **DMVPN V3** – automatyka zestawiania topologii HUB Spoke z zabezpieczeniem IPsec i protokołami routingu wraz z protokołem NHRP
- **SSL VPN / Remote Access** – wsparcie dla zdalnego dostępu użytkowników.

QoS i kontrola ruchu

- **Traffic Shaping / Policing / Queueing (HTB, CBQ, HFSC)** – kontrola pasma.
- **Hierarchical QoS (HQoS)** – wielopoziomowe kolejkowanie.
- **Traffic Classification (DSCP / CoS / ACL match)** – klasyfikacja ruchu na podstawie atrybutów.
- **Bandwidth Management per interface / per VLAN** – kontrola przepustowości per-port lub per-sieć.

Monitoring, logowanie i diagnostyka

- **SNMP v1/v2c/v3** – monitorowanie zewnętrzne.
- **Syslog (lokalny i zdalny)** – pełna integracja logów z systemami SIEM/IDS.
- **NetFlow / sFlow / IPFIX** – eksport statystyk ruchu do systemów analitycznych.
- **Ping / Traceroute / MTR / Packet Capture (tcpdump)** – diagnostyka sieciowa.
- **BFD** – szybkie wykrywanie awarii tras routingu.
- **Interface Counters / Flow statistics** – bieżące statystyki ruchu.
- **Monitorowanie w trybie inline** – analityka DPI oraz IDS realizowana pasywnie w trybie ciągłym na każdym interfejsie aktywnym,
- **Mirror Port** – możliwość skopiowania ramek z interfejsów źródłowych na interfejs wyjściowy

- **Przekierowanie wewnętrzne do systemów analityki** – funkcja zautomatyzowana przekierowania ruchu przez wewnętrzny system IPS (w trybie IPS) dla analityki z automatyka ochrony inline
- Analityka anomalii komunikacji sieciowej pomiędzy komponentami
- Behavioral monitoring,
- Profilowanie obiektów logicznych i fizycznych sieci
- Identyfikacja komponentów w danych z ruchu sieciowego
- Analityka czasów transmisji dla komunikacji sesyjnej i niesesyjnej
- Traceability dla podanych parametrów zidentyfikowanych w ruchu sieciowym
- Tryb maintenance dla wyciszenia alertów z profili zgłoszonych do zmiany w środowisku sieciowym
- Thread Detection
- Analityka głęboka protokołów IT i OT w tym Modbus TCP, Goose, Profinet, Ethernet/IP, EtherCat, S-BUS, Step7, IEC 60870-5-104
- Diagnostyka protokołów OT
- Diagnostyka protokołów IT

Zarządzanie i automatyzacja

- **CLI / SSH / API / RESTCONF / NETCONF** – wielowarstwowe zarządzanie.
- **Konfiguracja CLI w stylu Cisco / Juniper** – logiczne drzewo konfiguracji.
- **Atomic commits / rollback / diff** – bezpieczne zmiany i cofanie konfiguracji.
- **Scheduled tasks / cron / event-driven scripts** – automatyzacja procesów.
- **Ansible / Salt / Terraform ready** – zgodność z narzędziami DevOps.
- **Zarządzanie użytkownikami / RADIUS / TACACS+ / LDAP** – kontrola dostępu administracyjnego.
- **Backup / restore / config versioning** – bezpieczeństwo konfiguracji.
- **Zarządzanie Firewall** – wymagane jest również zarządzanie z poziomu konsoli centralnej

IDS/IPS

Detekcja, analiza i blokowanie zagrożeń sieciowych w czasie rzeczywistym.

- Analiza i inspekcja ruchu sieciowego (Deep Packet Inspection – DPI)
 - Pełna inspekcja pakietów na poziomie L2–L7 w czasie rzeczywistym.
 - Analiza protokołów przemysłowych (Modbus, DNP3, IEC 60870-5-104, PROFINET, BACnet, OPC UA itp.).
 - Wykrywanie anomalii w komunikacji sterowników PLC, HMI i urządzeń przemysłowych.

- Rozpoznawanie struktur poleceń, zmiennych procesowych i komunikacji SCADA.
- Detekcja zagrożeń (Intrusion Detection System – IDS)
 - Wykrywanie prób włamań, skanowania portów, exploitów, ataków DoS/DDoS i naruszeń polityk sieciowych.
 - Identyfikacja złośliwego oprogramowania, beaconingu i nieautoryzowanych połączeń C2 (Command & Control).
 - Korelacja zdarzeń z regułami IDS Rules oraz regułami zespołu MDR i CTI.
 - Generowanie alertów i przekazywanie ich do systemu SIEM/IDS.
- Blokowanie zagrożeń (Intrusion Prevention System – IPS)
 - Dynamiczne blokowanie pakietów i sesji zgodnie z regułami bezpieczeństwa.
 - Automatyczne odcinanie źródeł ataków, modyfikacja polityk firewallowych w czasie rzeczywistym.
 - Współpraca z modułem firewall (ZBFW) i komponentami SIEM/IDS w celu natychmiastowej reakcji.
 - Minimalny wpływ na opóźnienia i przepustowość ruchu sieciowego (low-latency design).
- Analiza sygnatur i anomalii
 - Wykorzystanie sygnatur znanych ataków oraz mechanizmów heurystycznych i statystycznych.
 - Wykrywanie anomalii w zachowaniach urządzeń i użytkowników (np. nagle wzrosty ruchu, zmiana portów, niezgodność protokołów).
 - Wsparcie dla analizy behawioralnej w połączeniu z modułami CTI i MDR.
 - Aktualizacje baz reguł bezpieczeństwa w sposób automatyczny i kontrolowany.
- Integracja z systemami analitycznymi i korelacyjnymi
 - Wysyłanie logów i alertów do systemów SIEM, SOC, MDR.
 - Normalizacja danych i mapowanie zdarzeń do frameworków MITRE ATT&CK i IEC 62443.
 - Współpraca z bazami danych CTI w celu identyfikacji źródeł zagrożeń i kampanii APT.
 - Eksport danych w formatach EVE JSON, Syslog, PCAP i NetFlow.
- Wsparcie inspekcji w sieciach OT
 - Zoptymalizowane reguły detekcji dla środowisk przemysłowych.
 - Tryb „passive monitoring” bez ingerencji w ruch procesowy (dla systemów krytycznych).
 - Tryb „inline” z prewencyjnym blokowaniem ataków przy zachowaniu zgodności z IEC 62443-3-3.
 - Pełna widoczność komunikacji pomiędzy segmentami IT a OT.
- Mechanizmy automatyzacji i korelacji
 - Automatyczne przekazywanie alertów do modułów reakcji MDR.
 - Aktywacja polityk obronnych w firewallu .
 - Dynamiczne uczenie się ruchu sieciowego (profilowanie).
 - Możliwość tworzenia własnych reguł i skryptów reakcji w środowisku SIEM/IDS
- Raportowanie i wizualizacja
 - Raporty incydentów bezpieczeństwa, trendów i statystyk detekcji.

- Graficzne przedstawienie ruchu sieciowego i źródeł zagrożeń w panelu SIEM/IDS.
- Eksport alertów i logów do systemów zewnętrznych w formacie JSON, CSV, Syslog.
- Możliwość integracji z pulpitemi centralnego SIEM/IDS .

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, kluczy i certyfikatów.**

Dodatkowe cechy

- **Rolling Release** – aktualizacje bezpieczeństwa w cyklu ciągłym.
- **Integracja z Docker / LXC / KVM** – uruchamianie usług w kontenerach.
- **Obsługa Netfilter nftables / eBPF** – nowoczesne mechanizmy filtrowania.

3.5. Centralny system bezpieczeństwa

3.5.1. System typu EDR/XDR z ochroną ransomware

Architektura systemu

1. System musi być rozwiązaniem 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.
2. System musi składać się z:
 - agentów instalowanych na chronionych hostach,
 - centralnego serwera zarządzającego,
 - silnika analityczno-korelacyjnego,
 - repozytorium logów,
 - interfejsu webowego (GUI).
3. System musi umożliwiać instalację:
 - w środowisku lokalnym (on-premise),
 - w środowisku wirtualnym,

Obsługiwane systemy operacyjne

1. Agent musi obsługiwać co najmniej:

- Windows (Server i Workstation),
- Linux (różne dystrybucje).

2. System musi umożliwiać centralne zarządzanie konfiguracją agentów.

Funkcjonalności EDR – detekcja

System musi zapewniać:

1. **Monitoring integralności plików (FIM – File Integrity Monitoring):**
 - wykrywanie zmian w plikach systemowych i konfiguracyjnych,
 - wykrywanie zmian w rejestrze Windows,
 - generowanie alertów przy nieautoryzowanych modyfikacjach.
2. **Monitoring procesów:**
 - rejestrowanie uruchamianych procesów,
 - analiza linii poleceń (command line),
 - wykrywanie podejrzanych procesów (np. PowerShell, WMI, LOLBins).
3. **Monitoring aktywności użytkowników:**
 - logowania lokalne i zdalne,
 - próby eskalacji uprawnień,
 - zmiany w grupach uprzywilejowanych.
4. **Detekcję malware i rootkitów:**
 - wbudowany mechanizm rootkit detection,
 - integrację z zewnętrznymi silnikami AV (np. ClamAV).
5. **Detekcję anomalii i ataków zgodnie z MITRE ATT&CK:**
 - mapowanie zdarzeń do technik ATT&CK,
 - możliwość generowania raportów według taksonomii MITRE.
6. **Wykrywanie podatności (Vulnerability Detection):**
 - identyfikację zainstalowanego oprogramowania,
 - korelację z bazami CVE,
 - raportowanie podatności.

Korelacja i analiza

1. System musi posiadać:
 - silnik reguł (rule-based detection),
 - możliwość tworzenia własnych reguł detekcyjnych,
 - możliwość korelacji wielu zdarzeń w jeden incydent.
2. 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:

1. Zdalne wykonywanie komend na hoście.
2. Blokowanie adresów IP (np. poprzez integrację z firewall).
3. Automatyczne reakcje (active response) na podstawie zdefiniowanych reguł.
4. Izolację hosta (logicznie – poprzez blokowanie komunikacji).
5. Integrację z systemem ticketowym / SIEM / SOAR.

Zarządzanie i raportowanie

1. System musi posiadać:
 - interfejs webowy (dashboard),
 - wyszukiwarkę zdarzeń,
 - możliwość filtrowania po hostach, użytkownikach, czasie, typie zagrożenia.
2. System musi umożliwiać:
 - generowanie raportów PDF/CSV,
 - raporty zgodności (np. PCI-DSS, CIS, ISO 27001),
 - raporty podatności.
3. System musi umożliwiać wielopoziomowe role użytkowników (RBAC).

Skalowalność i wydajność

1. System musi umożliwiać obsługę co najmniej 100 agentów.

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.

3.5.2. System typu ITSM/CMDB

Konfiguracja zarządzania zasobami i relacjami („CMDB” — Configuration Management Database)

- Pełna baza danych CI (Configuration Items): sprzęt, oprogramowanie, usługi, lokalizacje, kontakt, zespoły.
- Wizualizacja zależności i wpływu („impact analysis”): jakie usługi lub komponenty zależą od danego elementu.
- Możliwość importu danych masowo (CSV, Excel) i synchronizacji zewnętrznych źródeł (np. Active Directory, monitoring) dla aktualizacji zasobów.

Zarządzanie incydentami i zgłoszeniami użytkowników (Incident & Request Management)

- Rejestracja incydentów i żądań użytkowników w jednym systemie.
- Powiązanie zgłoszenia z CI w CMDB — np. ten incydent dotyczy konkretnego serwera lub usługi.
- Automatyczne powiadomienia, eskalacje SLA, śledzenie statusu zgłoszenia.

Zarządzanie problemami (Problem Management)

- Identyfikacja i rejestracja problemów (ustalne przyczyny incydentów).
- Powiązanie znanych błędów (Known Errors) z CI oraz zgłoszeniami incydentów.

Zarządzanie zmianami (Change Management)

- Planowanie, zatwierdzanie i wdrożenie zmian w infrastrukturze IT zgodnie z procesem.
- Obsługa różnych typów zmian: rutynowe, awaryjne, normalne.
- Pełna historyczność zmian i powiązań z incydentami i CI — lepsza kontrola ryzyka.

Katalog usług i zarządzanie SLA (Service Catalog & SLA Management)

- Definiowanie usług IT świadczonych klientom/organizacji, wraz z ich opisem.
- Określanie i monitorowanie SLA (umów o poziomie usług) dla tych usług.
- Portal użytkownika (self-service) dla zgłaszania żądań / incydentów.

Zarządzanie zasobami, licencjami i kontraktami (Asset, License & Contract Management)

- Rejestracja sprzętu, oprogramowania, licencji, partnerów i działań serwisowych.
- Powiązanie zasobów z CI i usługami oraz rozliczanie kosztów/umów.

Automatyzacja, workflowy i integracje

- Możliwość konfiguracji workflowów automatyzujących procesy (np. przypisanie zgłoszenia, zatwierdzenie zmiany).
- REST API / Webhooks dla integracji z zewnętrznymi systemami (np. monitoring, automatyzacja, narzędzia SOAR).
- Możliwość rozbudowy modelu danych i UI bez głębokiego programowania („low-code” designer).

Raportowanie, dashboardy i analiza wpływu

- Dashboardy i raporty operacyjne: przegląd zgłoszeń, statusów, SLA, CI.
- Analiza zależności CI wpływu na usługi — umożliwia proaktywne działania.

Zarządzanie bezpieczeństwem i audyt

- Role-based Access Control (RBAC) – kontrola dostępu użytkowników do danych.
- Logowanie działań użytkowników, audyt zmian w systemie i danych CMDB.

Elastyczność wdrożenia i skalowalność

- Dostępna wersja on-premises (self-host) lub możliwość adaptacji.
- Modułowa architektura: możesz stopniować funkcje według potrzeb (np. najpierw CMDB + incydenty, potem zmiany, potem katalog usług).

3.5.3. System zarządzania urządzeniami mobilnymi (MDM)

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja systemu klasy MDM (Mobile Device Management) przeznaczonego do zarządzania i zabezpieczania urządzeń mobilnych w organizacji.

System musi obsługiwać minimum 20 urządzeń mobilnych.

Wymagania ogólne:

- system musi być dostarczony w formie rozwiązania instalowanego lokalnie (on-premise),
- niedopuszczalne są rozwiązania wymagające wyłącznie pracy w chmurze (SaaS),
- system musi umożliwiać licencjonowanie w modelu bezterminowym (perpetual), bez obowiązku utrzymywania subskrypcji,
- wszystkie dane muszą być przechowywane w infrastrukturze Zamawiającego,
- system musi zapewniać centralne zarządzanie urządzeniami z jednej konsoli administracyjnej.

Zakres funkcjonalny:**1. Obsługa urządzeń:**

- wsparcie dla systemów:
 - Android (wymagane),
 - iOS/iPadOS (wymagane),
- możliwość rejestracji i ewidencji urządzeń,
- przypisywanie urządzeń do użytkowników i grup,
- zarządzanie flotą urządzeń z poziomu centralnej konsoli.

2. Polityki bezpieczeństwa:

- wymuszanie polityk bezpieczeństwa, w tym:
 - blokady ekranu (PIN, hasło),
 - szyfrowania urządzenia,
- możliwość zdalnego:
 - blokowania urządzenia,
 - usuwania danych (remote wipe),
- kontrola zgodności urządzeń z politykami bezpieczeństwa (compliance).

3. Zarządzanie aplikacjami:

- zdalna instalacja i usuwanie aplikacji,
- możliwość definiowania list aplikacji dozwolonych i zabronionych,
- możliwość wdrażania aplikacji firmowych.

4. Zarządzanie konfiguracją:

- zdalna konfiguracja:
 - sieci Wi-Fi,
 - połączeń VPN,
 - kont pocztowych,
- możliwość tworzenia i przypisywania profili konfiguracyjnych.

5. Monitoring i raportowanie:

- monitorowanie stanu urządzeń,
- raportowanie zgodności z politykami bezpieczeństwa,
- generowanie raportów i alertów,
- rejestrowanie zdarzeń administracyjnych.

6. Funkcje dodatkowe:

- możliwość pracy w trybie ograniczonym (compliance-only), bez konieczności pełnego zarządzania urządzeniami,
- możliwość lokalizacji urządzeń (opcjonalnie),
- wsparcie dla trybu kiosk (opcjonalnie).

Wymagania techniczne:

- system musi być możliwy do uruchomienia w środowisku:
 - maszyny wirtualnej lub serwera fizycznego,
 - systemu operacyjnego klasy Linux lub Windows,
- dostęp do systemu przez przeglądarkę internetową,
- komunikacja z systemem musi być szyfrowana (HTTPS),
- system musi posiadać architekturę umożliwiającą rozbudowę.

Wymagania bezpieczeństwa:

- uwierzytelnianie użytkowników i administratorów,
- role i poziomy uprawnień,
- rejestrowanie i audyt operacji,
- możliwość integracji z usługami katalogowymi (LDAP/Active Directory),
- możliwość eksportu logów (np. do SIEM/SOC).

Wymagania wdrożeniowe:

- instalacja i konfiguracja systemu w infrastrukturze Zamawiającego,
- wdrożenie dla minimum 20 urządzeń,
- konfiguracja podstawowych polityk bezpieczeństwa,
- przeprowadzenie testów poprawności działania,
- dostarczenie dokumentacji powykonawczej,
- przeprowadzenie szkolenia dla administratorów.

Wymagania licencyjne:

- licencja musi obejmować minimum 20 urządzeń,
- licencja musi być **bezterminowa (perpetual)**,
- system musi działać bez konieczności odnawiania licencji,
- aktualizacje i wsparcie techniczne mogą być opcjonalne.

3.5.4. System typu DLP

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja systemu klasy **DLP (Data Loss Prevention)** przeznaczonego do monitorowania, wykrywania oraz kontrolowania przepływu danych w sieci Zamawiającego, ze szczególnym uwzględnieniem transmisji do sieci zewnętrznych.

Wymagania ogólne:

- system musi działać w modelu **on-premise**, bez konieczności korzystania z usług chmurowych,
- wszystkie dane przetwarzane przez system muszą pozostawać w infrastrukturze Zamawiającego,
- system musi umożliwiać działanie bez konieczności utrzymywania subskrypcji,

- rozwiązanie musi umożliwiać integrację z istniejącymi systemami bezpieczeństwa Zamawiającego.

Zakres funkcjonalny:**1. Kontrola ruchu sieciowego (Network DLP):**

- analiza ruchu sieciowego w czasie rzeczywistym,
- kontrola transmisji danych w szczególności dla protokołów:
 - HTTP/HTTPS,
 - FTP/SFTP,
- identyfikacja kierunków transmisji danych (wewnętrzne / zewnętrzne),

2. Analiza i klasyfikacja danych:

- możliwość identyfikacji danych wrażliwych w ruchu sieciowym na podstawie:
 - wzorców (regex),
 - typów plików,
 - nazw plików,
- możliwość analizy przesyłanych danych,
- możliwość definiowania własnych reguł detekcji.

3. Polityki bezpieczeństwa:

- możliwość definiowania polityk kontroli przepływu danych,
- możliwość określania:
 - dozwolonych kierunków komunikacji,
 - typów danych dopuszczonych do transmisji,
- możliwość przypisywania polityk do segmentów sieci lub grup użytkowników.

4. Reakcja na zdarzenia:

- możliwość:
 - monitorowania (tryb pasywny),
 - generowania alertów,
 - blokowania transmisji danych,
- możliwość działania w trybie monitorowania (monitoring-only) bez blokowania ruchu,
- możliwość integracji z systemami reagowania (np. blokowanie sesji, reset połączeń).

5. Raportowanie i logowanie:

- rejestrowanie zdarzeń związanych z przepływem danych,
- możliwość generowania raportów,
- archiwizacja zdarzeń.

6. Integracja z systemami bezpieczeństwa:

- możliwość integracji z systemami monitorowania i analizy bezpieczeństwa,
- możliwość przekazywania zdarzeń do centralnego systemu zarządzania bezpieczeństwem,
- możliwość wykorzystania mechanizmów korelacji zdarzeń.

Wymagania techniczne:

- system musi umożliwiać wdrożenie jako:
 - serwer fizyczny,
 - maszyna wirtualna,
 - komponent infrastruktury sieciowej,
 - moduł lub grupa funkcyjna centralnego systemu cyberbezpieczeństwa SIEM/IDS
- dostęp do systemu musi być realizowany przez interfejs administracyjny (webowy),
- komunikacja administracyjna musi być szyfrowana (HTTPS),
- system musi umożliwiać skalowanie.

3.5.5. 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 pulpitów do wprowadzenia	Bez ograniczeń
Ilość instancji	Ilość wymaganych instalacji przez Zamawiającego	1
Miejsce instalacji	Lokalna u Zamawiającego	n/d
Instalacja chmurowa	Nie dopuszczalna	n/d
Wymagana integracja	ITSM, XDR	n/d

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 IT/OT szybki wgląd w sytuację bezpieczeństwa, liczbę zdarzeń, alarmów oraz aktywność urządzeń w sieci.

Zamawiający oczekuje zintegrowanego systemu klasy **SIEM/CMDB/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.

Wymagane minimalne funkcjonalności systemu SIEM/IDS:

1. Monitoring i korelacja zdarzeń (SIEM)

- 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.
- Integracja z silnikiem reguł alarmowych (Zasady alarmowe).
- Wsparcie dla korelacji według MITRE ATT&CK (np. T1040, T1071).
- Pełna historia i oś czasu zdarzeń (timeline).
- Możliwość filtrowania, eksportu i analizy porównawczej.

2. System alarmowy (IDS/IPS/Anomalie sieciowe)

- Wykrywanie anomalii sieciowych w oparciu o sygnatury i heurystykę.
- Detekcja nieautoryzowanego ruchu, nietypowych portów i protokołów.
- Identyfikacja potencjalnych prób eksfiltracji danych lub sniffingu.
- Integracja z modulem **Network Anomalies**.
- Wsparcie dla CVE i korelacja podatności
- Rozwiązanie musi umożliwiać tak zwane badanie podatności, czyli wykrywanie czy podatności istnieją w infrastrukturze lub na hostach
- Klasyfikacja alarmów wg typu i priorytetu ryzyka.
- Mapowanie powiązanych zasobów i adresów IP/MAC.
- Powiązanie alarmów z konkretnymi urządzeniami USS DNC.
- Możliwość ręcznego lub automatycznego zamykania alarmów.
- Historia alarmów i statusów (aktywny, ponownie otwarty, zamknięty).

3. Inwentarz zasobów (Asset & CMDB)

- Automatyczna identyfikacja zasobów w sieci (adres MAC, IP, model, OS).
- Profilowanie urządzeń i przypisywanie ich do grup lub sieci.
- Baza konfiguracji sprzętowych i programowych (CPU, RAM, porty, OS).
- Klasyfikacja urządzeń: ICS Dev, Router, Switch, Serwer, Host, SCADA itp.
- Przypisywanie wartości aktywa (1–10) oraz poziomu ryzyka.
- Rejestr zdarzeń powiązanych z zasobem.
- Historia zmian konfiguracji i aktualizacji.
- Wbudowany edytor zasobu i przypisanie do sieci/peryferii.
- Możliwość dodania notatek technicznych lub operacyjnych.
- Integracja z modulem *Diagram PERA* — wizualizacja topologii.

4. Profile komunikacyjne (Network Behavior Profiling)

- Tworzenie profili zachowań sieciowych dla każdego adresu MAC.

- Rejestr interfejsów, ruchu i komunikacji między urządzeniami.
- Analiza różnic w zachowaniu (detekcja odchyłań od normy).
- Automatyczne tworzenie i aktualizacja profili.
- Eksport listy profili do raportów i porównań audytowych.
- Wizualne odwzorowanie relacji z urządzeniami aktywnymi sieci tego samego producenta co system SIEM/IDS

5. Analiza danych i ryzyka

- Automatyczna analiza zidentyfikowanych anomalii.
- Raporty o potencjalnych wektorach ataku (MITRE ATT&CK).
- Wskazanie nieautoryzowanych portów i usług.
- Analiza zgodności z **IEC 62443** i **ISO 27001**.
- Raport z zaleceniami: „Zagrożenia – Konsekwencje – Działania”.
- Ocena ryzyka braku działań korygujących (np. w 90 dni).
- Szacowanie wpływu incydentu na zasoby i infrastrukturę.

6. Wizualizacja i topologia sieci (Diagram PERA)

- Automatyczna mapa relacji między zasobami i segmentami sieci.
- Kolorystyczne oznaczenia poziomu ryzyka i statusu połączeń.
- Możliwość interakcji z elementami (kliknięcie → szczegóły zasobu).
- Integracja z danymi z modułów *Zdarzenia* i *Alarmy*.
- Widok struktury per strefy PERA (Enterprise / Control / Field / DMZ).

7. Zasady alarmowe i polityki bezpieczeństwa (NSPM)

- Definiowanie reguł alarmowych (np. porty, IP, usługi, typ zdarzenia).
- Priorytetyzacja zasad i poziomy alarmowe.
- Automatyczne uruchamianie alarmów po spełnieniu warunków.
- Możliwość wyciszania określonych alarmów lub źródeł.
- Integracja z tabelą interfejsów i reguł firewall (USS DNC).
- Pełna zgodność z architekturą **Zone-Based Firewall**.

8. Raportowanie i analityka

- Generowanie raportów z analizy ryzyka i podatności.
- Podsumowania incydentów i trendów zagrożeń.
- Raporty dla audytów (IEC 62443, ISO 27001, ISO 22301).
- Możliwość eksportu do PDF, CSV, XLSX.

- Raporty z przypisaniem do zasobów, sieci i alarmów.

9. Integracja z urządzeniami aktywnymi sieci

- Pełna integracja z urządzeniami aktywnymi sieci tego samego producenta co system SIEM/IDS.
- Odczyt metadanych sprzętowych (model, CPU, pamięć, porty, firmware).
- Monitorowanie stanu portów, interfejsów i komunikacji L2/L3.
- Wykorzystanie urządzeń aktywnych sieci tego samego producenta jako źródeł danych IDS i monitoringu sieciowego.
- 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
- Synchronizacja polityk bezpieczeństwa między systemem a urządzeniami aktywnymi tego samego producenta

10. Dodatkowe funkcje operacyjne

- Historia działań administratora (logi operacyjne).
- Panel użytkownika i uprawnienia administracyjne.
- Przegląd wszystkich interfejsów sieciowych i tabeli firewall.
- Możliwość wizualizacji alarmów w czasie rzeczywistym (Alarms live).
- Panel wydajności systemu (monitor CPU, pamięci, dysków).
- Integracja z modułem raportów dziennych / tygodniowych.
- Mechanizmy wykluczeń i filtrów do analizy danych.

11. Normy, zgodność i audyt

- Zgodność z normami **IEC 62443, ISO 27001, ISO 22301**.
- Struktura raportów i klasyfikacja ryzyk zgodna z IEC 62443-3-3.
- Analiza niezgodności i rekomendacje działań korygujących.
- Mapowanie do wymagań bezpieczeństwa OT i IT.

12. Architektura i integracja

- Działanie w środowisku Linux / Vmware / HyperV / KVM / Proxmox.
- Baza danych PostgreSQL
- Możliwość pracy w środowiskach mieszanych (OT, IT, Cloud).
- API do integracji z zewnętrznymi systemami.
- Zdalna administracja i aktualizacje systemu.

13. Wyróżniki unikalne

- Dedykowane dla środowisk **OT / ICS / SCADA**.

- Całkowicie **autorskie rozwiązanie** – brak komponentów wymagających dodatkowych licencji.
- Pełna integracja z fizycznymi urządzeniami aktywnymi sieci tego samego producenta.
- Wysoka czytelność interfejsu – jeden panel łączący SIEM, Asset i NSPM.
- Polski interfejs i struktura raportowania zgodna z wymogami krajowymi (np. PCA, PSE)
- Polskie komunikaty w szczególności dane analityczne.

3.5.6. System SOAR

- System musi stanowić platformę klasy SOAR (Security Orchestration, Automation and Response) 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

4. USŁUGI

WYMAGANIA DOTYCZĄCE ZESPOŁU REALIZUJĄCEGO ZAMÓWIENIE

- Według oceny ZMAWIAJĄCEGO, i zapewnienia bezpieczeństwa realizacji zamówienia, zespół WYKONAWCY musi zostać przedstawiony na spotkaniu w siedzibie ZAMAWIAJĄCEGO
- Według oceny ZMAWIAJĄCEGO, i zapewnienia bezpieczeństwa realizacji zamówienia, zespół WYKONAWCY musi dysponować celem realizacji

zamówienia następującymi kwalifikacjami potwierdzonymi poniższymi lub równoważnymi certyfikatami:

Rodzaj certyfikatu	Minimalna Ilość osób
CCIE Routing & Switching	2
Ethical Hacking & Computer Security	2
MASE	2
VCP NX	2
Audytor wiodący ISO 27001	2
CCNA Industry	1
MCITP Enterprise	1
CCNP Security	1
SCPIN	2
MCSE Security	1
MASE Security	1
CCDP	2

- Dopuszcza się zespół złożony z minimum 2 osób w następujących rolach.
 - Kierownik projektu
 - Projektant systemów
 - Projektant sieci komunikacyjnych
 - Analityk bezpieczeństwa
- Wymienione wyżej osoby muszą posiadać certyfikaty wymienione w tabeli w dowolnej konfiguracji.

4.1. Szkolenia

Przedmiotem zamówienia są szkolenia z zakresu cyberbezpieczeństwa w zakresie:

- Przeprowadzenie szkoleń dla kadry kierowniczej w centrum edukacyjnym, które ma na celu podniesienie świadomości kadry zarządzającej w zakresie cyberbezpieczeństwa, skupiające się na aspekcie strategicznym, ryzyku biznesowym i wymaganiach regulacyjnych.
- Przeprowadzenie szkoleń dla Szkolenie w centrum edukacyjnym, dedykowane kadrze zarządzającej i specjalistom IT/OT.
Uczestnicy zdobędą praktyczną wiedzę na temat wdrożonych lub planowanych do wdrożenia środków bezpieczeństwa. Szkolenie zapewni umiejętności niezbędne do efektywnego wykorzystywania narzędzi, takich jak systemy monitorujące czy systemy zarządzania incydentami
- Szkolenia z testami socjotechnicznymi
Szkolenia które odbędą się w siedzibie Spółki. Celem jest praktyczna weryfikacja świadomości zagrożeń socjotechnicznych, takich jak phishing czy spoofing, oraz ocena reakcji personelu. Szkolenia te pozwolą na identyfikację luk w wiedzy i dopasowanie procedur reagowania, zwłaszcza w przypadku kluczowych pracowników i specjalistów odpowiedzialnych za SZBI. Podmiot odpowiedzialny: Zewnętrzna firma szkoleniowa, specjalizująca się w nowoczesnych metodach weryfikacji kompetencji

Terminy i zakres szkoleń

Szkolenia wykonywane są dla minimum 2 a maksimum 20 osób ZAMAWIAJACEGO na każdym szkoleniu

Zakres szkoleń i czas ich trwania przedstawiono poniżej

- W fazie I - Realizacja szkolenia: Podstawowe szkolenie (lub dostęp do platform szkoleniowych) budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników
 - a. Czas trwania – 1 dzień roboczy dla maksimum 20 osób na terenie ZAMAWIAJĄCEGO
- W fazie II - Realizacja szkolenia: Szkolenie z zakresu cyberbezpieczeństwa kadry, istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji
 - a. Czas trwania – 1 dzień roboczy dla maksimum 20 osób na terenie ZAMAWIAJĄCEGO
- W fazie II -Realizacja szkolenia: Szkolenie specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych środków bezpieczeństwa w ramach zamówienia
 - a. Czas trwania – 3 dni robocze dla maksimum 6 osób na terenie WYKONAWCY

ZAMAWIAJĄCY zapewnia dla realizacji szkoleń:

- Salę szkoleniową z dostępem do sieci Internet, możliwością zasilania 230V minimum 7 urządzeń (np. komputerów słuchaczy i instruktora oraz rzutnika multimedialnego), meblami (minimum stoły i krzesła dla słuchaczy), rzutnikiem multimedialnym, tablicą sucho ścierną, dostępem do sanitariatów dla słuchaczy i instruktora.
- Komputer z dostępem do sieci Internet dla słuchaczy

Wymagania ogólne

- Dzień szkoleniowy oznacza realizację zadania w dniach i godzinach roboczych tj. od 9:00 do 15:00 danego dnia. W ramach dnia szkoleniowego ZAMAWIAJĄCY uwzględnia minimum 3 przerwy 15-sto minutowych oraz jedną przerwę minimum 45-cio minutowej.
- Ilość dni szkoleniowych określono na 4 dni robocze.
- WYKONAWCA zapewnia:
 - a) wystawienie zaświadczenia uczestnictwa w szkoleniu podpisanego przez Instruktora, który posiada potwierdzony przez niezależną, międzynarodową instytucję, certyfikat/poświadczenie o realizacji szkoleń od minimum 15 lat na poziomie Excellence lub równoważny

- b) prowadzenie szkoleń przez instruktora, który posiada potwierdzony przez niezależną międzynarodową instytucję certyfikat/poświadczenie o realizacji szkoleń od minimum 15 lat na poziomie Excellence lub równoważny
- c) przygotowany plan szkoleń korespondujący z przewodnim zakresem szkolenia.
- Szczegółowy zakres szkolenia będzie ustalony z ZAMAWIAJĄCYM w fazie I.
- Czas szkoleń nie wpływa na czas realizacji całości zamówienia

4.2. Prace projektowe i wdrożeniowe zgodnie z rekomendacjami audytu Systemu Zarządzania Bezpieczeństwem Informacji

Wykonawca zobowiązany jest do realizacji prac projektowych i wdrożeniowych w sposób zapewniający zgodność z rekomendacjami wynikającymi z audytu cyberbezpieczeństwa oraz obowiązującymi wymaganiami bezpieczeństwa systemów OT.

Szczegółowe wyniki audytu, w tym zalecenia poaudytowe, zostaną udostępnione Wykonawcy po podpisaniu umowy, z zachowaniem zasad poufności i ochrony informacji.

4.3. Testy bezpieczeństwa infrastruktury sieciowej, serwisów internetowych, IT/OT/ICS/IIoT

Przedmiotem zadania jest przeprowadzenie testów bezpieczeństwa obejmujących infrastrukturę sieciową, serwisy internetowe oraz systemy informatyczne i przemysłowe (IT/OT/ICS/IIoT), w celu identyfikacji podatności, oceny poziomu zabezpieczeń oraz określenia ryzyk związanych z potencjalnymi zagrożeniami cybernetycznymi.

Zakres prac obejmuje w szczególności:

Testy bezpieczeństwa infrastruktury sieciowej:

- identyfikację aktywów sieciowych (urządzeń, segmentów, usług),
- analizę architektury sieci (L2/L3, segmentacja, strefy bezpieczeństwa),
- wykrywanie podatności w urządzeniach sieciowych (routery, przełączniki, firewalle, urządzenia OT),
- weryfikację konfiguracji zabezpieczeń (ACL, firewall, IDS/IPS, segmentacja VLAN, strefy IEC 62443),
- testy odporności na ataki (np. skanowanie, próby obejścia zabezpieczeń, testy dostępności).

Testy bezpieczeństwa serwisów internetowych i aplikacji:

- analiza podatności aplikacji webowych (OWASP Top 10),
- testy uwierzytelniania i autoryzacji,
- testy odporności na ataki (np. SQL Injection, XSS, CSRF, SSRF, RCE),
- analiza konfiguracji serwerów aplikacyjnych i webowych,
- testy bezpieczeństwa API (REST, SOAP).

Testy bezpieczeństwa systemów IT:

- skanowanie podatności systemów operacyjnych i usług,
- analiza konfiguracji systemów (hardening),
- testy uprawnień użytkowników i kontroli dostępu,

- o identyfikacja nieaktualnego oprogramowania i podatności CVE,
- o weryfikacja mechanizmów logowania i monitoringu.

Testy bezpieczeństwa systemów OT/ICS/IIoT:

- o identyfikacja i analiza protokołów przemysłowych (np. Modbus, DNP3, IEC 60870-5-104, OPC, PROFINET),
- o wykrywanie podatności w urządzeniach sterowania i systemach SCADA/DCS,
- o ocena segmentacji sieci przemysłowej zgodnie z IEC 62443,
- o testy komunikacji między strefami (IT–OT),
- o analiza możliwości ingerencji w proces technologiczny,
- o ocena odporności na anomalie i ataki specyficzne dla OT.

Testy integracyjne IT/OT:

- o analiza punktów styku między siecią IT i OT,
- o weryfikacja zabezpieczeń transmisji danych między strefami,
- o identyfikacja potencjalnych wektorów ataku z IT do OT,
- o ocena zastosowanych mechanizmów separacji.

Analiza podatności i ocena ryzyka:

- o klasyfikacja wykrytych podatności (np. CVSS),
- o określenie poziomu ryzyka dla organizacji,
- o wskazanie potencjalnych scenariuszy ataku.

Raportowanie i rekomendacje:

- o przygotowanie raportu technicznego zawierającego:
 - opis wykrytych podatności,
 - ich wpływ na bezpieczeństwo systemu,
 - dowody,
 - rekomendacje działań naprawczych,
- o przygotowanie raportu zarządczego (Executive Summary),
- o wskazanie priorytetów działań naprawczych.

Wymagania dotyczące realizacji:

- testy muszą być prowadzone w sposób kontrolowany, bez zakłócania pracy systemów produkcyjnych,
- w przypadku środowisk OT dopuszcza się wyłącznie metody nieinwazyjne lub uzgodnione z Zamawiającym,
- działania muszą być zgodne z obowiązującymi normami i standardami, w szczególności:
 - o PN-EN IEC 62443,
 - o ISO/IEC 27001,
 - o OWASP Testing Guide,
 - o NIST SP 800-82,
- wszystkie działania muszą być uzgodnione i autoryzowane przez Zamawiającego.

4.4. Audyt cyberbezpieczeństwa sieci

Audyt cyberbezpieczeństwa sieci w oparciu o metodykę OSSTMM 3.0

Przedmiotem zadania jest przeprowadzenie audytu cyberbezpieczeństwa infrastruktury sieciowej z wykorzystaniem metodyki **OSSTMM 3.0 (Open Source Security Testing Methodology Manual)**, w celu obiektywnej oceny poziomu bezpieczeństwa, identyfikacji podatności oraz określenia rzeczywistego poziomu ekspozycji na zagrożenia.

Cel audytu:

- określenie rzeczywistego poziomu bezpieczeństwa infrastruktury,
- identyfikacja podatności technicznych i organizacyjnych,
- pomiar poziomu zabezpieczeń w sposób mierzalny (RAV – Risk Assessment Values),
- wskazanie obszarów wymagających poprawy.

Zakres audytu obejmuje:**1. Analiza powierzchni ataku (Attack Surface Analysis):**

- identyfikację dostępnych punktów wejścia do systemu,
- analizę dostępności usług sieciowych (wewnętrznych i zewnętrznych),
- identyfikację zasobów widocznych z Internetu oraz sieci wewnętrznych.

2. Testy bezpieczeństwa w pięciu obszarach OSSTMM:**a) Human Security**

- analiza podatności wynikających z czynników ludzkich (np. polityki, procedury, świadomość),
- ocena ryzyka socjotechnicznego (bez prowadzenia nieautoryzowanych ataków socjotechnicznych).

b) Physical Security

- ocena zabezpieczeń fizycznych infrastruktury sieciowej,
- weryfikacja kontroli dostępu do urządzeń i pomieszczeń.

c) Wireless Security

- analiza bezpieczeństwa sieci bezprzewodowych (Wi-Fi, inne technologie radiowe),
- identyfikacja nieautoryzowanych punktów dostępowych.

d) Telecommunications Security

- analiza bezpieczeństwa transmisji danych,
- ocena zabezpieczeń komunikacji (protokoły, szyfrowanie, separacja).

e) Data Networks Security

- testy bezpieczeństwa infrastruktury sieciowej (L2/L3),
- analiza konfiguracji urządzeń (routery, przełączniki, firewalle),
- weryfikacja segmentacji sieci oraz stref bezpieczeństwa (np. zgodnie z IEC 62443),
- testy podatności usług i systemów.

3. Weryfikacja mechanizmów bezpieczeństwa:

- kontrola skuteczności mechanizmów ochronnych (firewall, IDS/IPS, NAC),
- analiza polityk bezpieczeństwa i ich implementacji,
- ocena mechanizmów kontroli dostępu i uwierzytelniania.

4. Pomiar bezpieczeństwa (OSSTMM Metrics):

- określenie wartości **RAV (Risk Assessment Value)**,
- ocena:
 - **Controls** (zabezpieczenia),
 - **Limitations** (ograniczenia systemowe),
 - **Visibility** (widoczność zasobów),
 - **Trust** (zaufanie w relacjach systemowych),
- przedstawienie wyników w formie mierzalnej i porównywalnej.

5. Analiza ryzyka i scenariusze zagrożeń:

- identyfikacja możliwych scenariuszy ataku,

- określenie wpływu podatności na ciągłość działania,
- ocena ryzyka dla systemów IT oraz OT (jeśli występują).

6. Raportowanie:

Wykonawca zobowiązany jest do przygotowania:

a) Raportu technicznego:

- opis wykrytych podatności,
- analiza ich wpływu,
- dowody (jeśli możliwe),
- odniesienie do OSSTMM oraz standardów (IEC 62443, ISO 27001).

b) Raportu zarządczego (Executive Summary):

- syntetyczna ocena poziomu bezpieczeństwa,
- kluczowe ryzyka,
- rekomendacje działań naprawczych.

c) Wyników metrycznych:

- prezentacja wartości RAV,
- interpretacja wyników w kontekście bezpieczeństwa organizacji.

Wymagania realizacyjne:

- audyt musi być prowadzony zgodnie z metodyką OSSTMM 3.0,
- działania muszą być wykonywane w sposób kontrolowany i niezakłócający pracy systemów,
- testy w środowiskach OT muszą być ograniczone do metod bezpiecznych (non-intrusive),
- wszystkie działania wymagają uprzedniej autoryzacji Zamawiającego,
- audyt powinien uwzględniać zgodność z normami:
 - PN-EN IEC 62443,
 - ISO/IEC 27001,
 - NIST SP 800-82.

4.5. Usługi MDR, MIDS, CTI

Nazwa parametru/cechy	Wartość / zapis oczekiwany
Obszar objęty monitorowaniem	IT oraz OT
Zakres SOC	<p>Zespół SOC odpowiada za bieżące monitorowanie, analizę i reagowanie na incydenty bezpieczeństwa w infrastrukturze Zamawiającego.</p> <p>Jego głównym celem jest zapewnienie ciągłej ochrony środowiska IT/OT, minimalizacja czasu reakcji oraz wsparcie w podejmowaniu decyzji obronnych.</p> <p>1. Ciągłe monitorowanie bezpieczeństwa</p> <ul style="list-style-type: none"> • 24/7 analiza logów, zdarzeń i anomalii w systemach IT, OT, IoT oraz chmurze. • Monitorowanie infrastruktury Zamawiającego z wykorzystaniem systemów i/lub grup funkcyjnych XDR, SIEM, ITSM, CMDB, ITDR, SOAR • Wykrywanie podejrzanych działań, naruszeń polityk bezpieczeństwa i prób nieautoryzowanego dostępu.

	<p>2. Korelacja i analiza zdarzeń</p> <ul style="list-style-type: none"> • Automatyczna i manualna korelacja zdarzeń z wielu źródeł (firewalle, serwery, stacje robocze, systemy OT). • Wykorzystanie reguł detekcji opartych o MITRE ATT&CK, IEC 62443, NIST 800-82. • Klasyfikacja i priorytetyzacja incydentów według ich wpływu na ciągłość działania i bezpieczeństwo Zamawiającego. <p>3. Reagowanie na incydenty</p> <ul style="list-style-type: none"> • Identyfikacja, izolacja i ograniczanie skutków incydentów bezpieczeństwa. • Analiza przyczyn źródłowych (Root Cause Analysis) oraz rekomendacje działań naprawczych. • Wsparcie w odbudowie środowiska po incydencie i wdrożeniu środków prewencyjnych. • Raportowanie incydentów zgodnie z wymogami ISO 27001 / NIS2 / IEC 62443 / Ustawy o KSC. <p>4. Współpraca z zespołami CTI i MDR</p> <ul style="list-style-type: none"> • Integracja danych o zagrożeniach z zespołem CTI (Cyber Threat Intelligence). • Współdziałanie z usługami MDR (Managed Detection and Response) w zakresie analizy i automatycznej reakcji. • Aktualizacja reguł detekcji i polityk bezpieczeństwa w oparciu o nowe dane o zagrożeniach. <p>5. Raportowanie i komunikacja z Klientem</p> <ul style="list-style-type: none"> • Codzienne, tygodniowe i miesięczne raporty z incydentów – w przypadku wystąpienia • Powiadamianie o krytycznych zdarzeniach w trybie natychmiastowym. • Dedykowany kanał komunikacji z zespołem SOC (e-mail, telefon, SIEM). • Przeglądy bezpieczeństwa i omówienia incydentów (cykliczne spotkania z Zamawiającym – w ramach comiesięcznych spotkań). <p>6. Utrzymanie i rozwój systemów bezpieczeństwa</p> <ul style="list-style-type: none"> • Weryfikacja poprawności konfiguracji urządzeń zabezpieczających (firewalle, IDS/IPS, serwery logów). • Aktualizacje i rozwój reguł korelacji w SIEM. • Testy skuteczności detekcji (np. symulacje ataków, Purple Teaming). • Stałe doskonalenie procedur reagowania i procesów SOC. <p>7. Wsparcie compliance i audytów</p> <ul style="list-style-type: none"> • Przygotowanie danych i raportów do audytów bezpieczeństwa. • Mapowanie zdarzeń i incydentów do wymagań norm i regulacji (ISO 27001, NIS2, KSC, IEC 62443). • Udział w opracowaniu planów ciągłości działania (BCP/DRP).
Zakres CTI Cyber Threat Intelligence	<p>Przygotowywanie ekstrakcji, normalizacji, parserów, wtyczek celem wprowadzania danych postanalitycznych zespołu do systemów cyberbezpieczeństwa</p> <p>1. Monitorowanie zagrożeń</p> <ul style="list-style-type: none"> • Ciągłe śledzenie globalnych i lokalnych źródeł informacji o cyberatakach (OSINT, feedy komercyjne, dark web, CERT/CSIRT). • Wczesne wykrywanie nowych kampanii, grup APT, exploitów i podatności. • Analiza wpływu aktualnych trendów zagrożeń na sektor działalności Zamawiającego. <p>2. Analiza techniczna i kontekstowa</p> <ul style="list-style-type: none"> • Analiza próbek złośliwego oprogramowania i incydentów zidentyfikowanych przez SOC/MDR. • Korelacja wskaźników kompromitacji (IoC) z infrastrukturą Zamawiającego.

	<ul style="list-style-type: none"> • Ustalanie motywacji, metod i narzędzi atakujących (TTP – tactics, techniques, procedures). <p>3. Opracowanie raportów i rekomendacji</p> <ul style="list-style-type: none"> • Tworzenie raportów CTI: <ul style="list-style-type: none"> ◦ operacyjnych – zawierających konkretne wskaźniki i działania, ◦ strategicznych – opisujących trendy, ryzyka i potencjalne kierunki ataków. • Rekomendacje dotyczące aktualizacji, konfiguracji i wzmocnienia zabezpieczeń. • Powiadomienia o krytycznych podatnościach oraz ich wpływie na środowisko Zamawiającego. <p>4. Wsparcie zespołów bezpieczeństwa</p> <ul style="list-style-type: none"> • Współpraca z SOC i zespołem reagowania na incydenty (CSIRT/MDR). • Pomoc w klasyfikacji i priorytetyzacji incydentów bezpieczeństwa. • Aktualizacja reguł detekcji (np. Suricata, Sigma, ASL) na podstawie najnowszych informacji o zagrożeniach. <p>5. Utrzymanie świadomości sytuacyjnej Zamawiającego</p> <ul style="list-style-type: none"> • Comiesięczne raporty o aktualnych zagrożeniach. • Alerty o krytycznych kampaniach lub zagrożeniach sektorowych. • Briefingi i warsztaty dla kadry technicznej i zarządczej Zamawiającego. <p>6. Wsparcie strategiczne</p> <ul style="list-style-type: none"> • Budowa świadomości cyberzagrożeń w organizacji. • Mapowanie ryzyk i incydentów do frameworków MITRE ATT&CK, NIST oraz IEC 62443 (dla środowisk OT). • Udział w projektowaniu i rozwoju strategii bezpieczeństwa Zamawiającego.
Zakres MDR	<p>Zespół MDR odpowiada za aktywną detekcję, analizę i reakcję na zagrożenia w środowisku Zamawiającego. Jego celem jest szybkie i skuteczne reagowanie na ataki, zanim spowodują szkody, oraz ciągłe podnoszenie odporności środowiska IT/OT na incydenty.</p> <p>1. Aktywna detekcja zagrożeń</p> <ul style="list-style-type: none"> • Stały nadzór nad środowiskiem Zamawiającego z wykorzystaniem zaawansowanych czujników i agentów bezpieczeństwa (EDR/XDR, IDS/IPS,). • Identyfikacja anomalii i zachowań wskazujących na naruszenia bezpieczeństwa. • Automatyczne powiązanie zdarzeń z wiedzą o zagrożeniach (Threat Intelligence, TTP z MITRE ATT&CK). • Wykrywanie ataków typu ransomware, phishing, exploit, lateral movement oraz APT. <p>2. Analiza i triage incydentów</p> <ul style="list-style-type: none"> • Automatyczna klasyfikacja i korelacja incydentów wykrytych przez SOC lub systemy detekcyjne. • Ocena wpływu i krytyczności zagrożenia w kontekście środowiska Zamawiającego. • Manualna analiza przez ekspertów MDR w przypadkach wysokiego ryzyka. • Opracowanie rekomendacji działań natychmiastowych i długofalowych. <p>3. Reakcja na incydenty</p> <ul style="list-style-type: none"> • Szybka izolacja zainfekowanych hostów, segmentów sieci lub usług. • Blokowanie nieautoryzowanych połączeń i procesów w czasie rzeczywistym. – automatyka wprowadzana po uzgodnieniach z Zamawiającym • Przywracanie poprawnego stanu systemów sieci po incydencie (remediation).

	<ul style="list-style-type: none"> • Współpraca z zespołem Zamawiającego przy odbudowie i zabezpieczeniu infrastruktury. <p>4. Automatyzacja i orkiestracja reakcji (SOAR)</p> <ul style="list-style-type: none"> • Automatyczne wykonywanie akcji obronnych na podstawie reguł korelacji i polityk bezpieczeństwa. • Integracja z systemami SIEM, EDR, firewallami,. • Tworzenie playbooków reakcji i scenariuszy obronnych. • Eliminacja powtarzalnych zadań i skrócenie czasu reakcji (MTTR). <p>5. Współpraca z SOC i CTI</p> <ul style="list-style-type: none"> • Odbieranie alarmów i logów z SOC, a następnie eskalacja lub automatyczna reakcja. • Wykorzystanie danych i analiz zespołu CTI do wczesnego wykrywania i blokowania nowych zagrożeń. • Zwrotna informacja o skuteczności detekcji i obrony w celu doskonalenia reguł i procesów. • Wspólne raporty i analizy po incydentach. <p>6. Raportowanie i komunikacja z Klientem</p> <ul style="list-style-type: none"> • Raporty z incydentów w formie technicznej i zarządczej (Executive Summary). • Statystyki skuteczności detekcji, czasu reakcji i trendów bezpieczeństwa. • Powiadomienia o kluczowych działaniach w czasie rzeczywistym. • Dostęp do panelu Zamawiającego w systemie SIEM/IDS (wgląd w status incydentów i reakcje). <p>7. Ciągłe doskonalenie ochrony</p> <ul style="list-style-type: none"> • Regularne testy skuteczności systemów detekcji (Red Teaming / Purple Teaming). • Udoskonalanie reguł korelacji i scenariuszy reakcji w oparciu o rzeczywiste przypadki. • Analiza post-incident (Lessons Learned) i wdrażanie usprawnień w procesach bezpieczeństwa. • Konsultacje i doradztwo w zakresie poprawy architektury bezpieczeństwa Zamawiającego.
<p>Zakres zespołu inżynierskiego</p>	<p>Zespół Inżynierski IT/OT odpowiada za projektowanie, rozwój, modernizację i wsparcie techniczne infrastruktury sieciowej Zamawiającego, zarówno w obszarze informatycznym (IT), jak i przemysłowym (OT).</p> <p>Celem zespołu jest zapewnienie, aby środowisko sieciowe Zamawiającego było niezawodne, aktualne, skalowalne i zgodne z najlepszymi praktykami bezpieczeństwa.</p> <p>1. Wsparcie techniczne i rozwiązywanie problemów</p> <ul style="list-style-type: none"> • Analiza i rozwiązywanie zagadnień technicznych w zakresie sieci IT i OT. • Weryfikacja błędów konfiguracji, problemów wydajnościowych i nieprawidłowości w komunikacji między segmentami. • Współpraca z zespołami Administracji Siecią, SOC i MDR przy diagnozowaniu incydentów sieciowych. • Wsparcie techniczne użytkowników i zespołów Zamawiającego w zakresie infrastruktury sieciowej. <p>2. Aktualizacje i utrzymanie technologiczne</p> <ul style="list-style-type: none"> • Planowanie i realizacja aktualizacji oprogramowania urządzeń sieciowych (firmware, systemy operacyjne routerów, przełączników, NGFW, UTM). • Testowanie kompatybilności i bezpieczeństwa nowych wersji przed wdrożeniem w środowisku produkcyjnym.

	<ul style="list-style-type: none"> • Udział w cyklicznych przeglądach technicznych i rekomendacjach modernizacyjnych. • Zapewnienie zgodności urządzeń z wymaganiami bezpieczeństwa i normami IEC 62443, ISO 27001. <p>3. Projektowanie i rozwój infrastruktury</p> <ul style="list-style-type: none"> • Opracowywanie koncepcji technicznych, architektury sieci i dokumentacji projektowej. • Projektowanie nowych połączeń, segmentów, stref i sieci VLAN w środowiskach IT i OT. • Udział w projektach inwestycyjnych, modernizacyjnych i migracyjnych Zamawiającego. • Wsparcie w przygotowaniu specyfikacji technicznych i wymagań dla nowych instalacji lub modernizacji. <p>4. Współpraca z zespołami Zamawiającego</p> <ul style="list-style-type: none"> • Bieżąca współpraca z działami IT, OT, utrzymania ruchu oraz bezpieczeństwa informacji Zamawiającego. • Doradztwo techniczne i merytoryczne przy planowaniu rozbudowy infrastruktury. • Konsultacje z kadrą kierowniczą Zamawiającego w zakresie optymalnych rozwiązań technologicznych i organizacyjnych. • Przekazywanie wiedzy i wsparcie w podnoszeniu kompetencji zespołów Zamawiającego. <p>5. Koordynacja współpracy z dostawcami i wykonawcami zewnętrznymi</p> <ul style="list-style-type: none"> • Nadzór techniczny nad pracami firm trzecich w zakresie instalacji, konfiguracji lub serwisu urządzeń sieciowych w zakresie cyberbezpieczeństwa i komunikacji sieciowej • Weryfikacja poprawności wykonania prac i zgodności z dokumentacją techniczną. • Współpraca przy odbiorach technicznych, testach akceptacyjnych (SAT/FAT) i uruchomieniach. • Reprezentowanie interesów Zamawiającego w kontaktach technicznych z dostawcami sprzętu i usług. <p>6. Doradztwo technologiczne i rozwój środowiska</p> <ul style="list-style-type: none"> • Analiza aktualnych trendów technologicznych i rekomendacja rozwiązań podnoszących niezawodność i bezpieczeństwo sieci. • Przygotowywanie koncepcji integracji nowych technologii z istniejącym środowiskiem (np. SDN, NAC, ICS Visibility). • Opracowywanie planów migracji i harmonogramów wdrożeń nowych rozwiązań. • Udział w planowaniu długoterminowej strategii rozwoju infrastruktury sieciowej Zamawiającego.
<p>Zakres zespołu administracyjnego</p>	<p>Zespół Administracji Siecią IT/OT odpowiada za utrzymanie, konfigurację, bezpieczeństwo i rozwój infrastruktury sieciowej Zamawiającego, obejmującej zarówno środowiska informatyczne (IT), jak i przemysłowe (OT). Celem zespołu jest zapewnienie ciągłej dostępności, wydajności i bezpieczeństwa komunikacji sieciowej w całym środowisku organizacji.</p> <p>1. Utrzymanie infrastruktury sieciowej</p> <ul style="list-style-type: none"> • Stała administracja i nadzór nad urządzeniami sieciowymi: <ul style="list-style-type: none"> ○ przełącznikami warstwy L2/L3, ○ routerami, ○ zaporami sieciowymi (FW, NGFW, UTM),

	<ul style="list-style-type: none"> o urządzeniami segmentującymi sieć OT. • Monitorowanie poprawności działania infrastruktury oraz stanu połączeń. • Wykrywanie i usuwanie awarii sieciowych w trybie reaktywnym i proaktywnym. <p>2. Zarządzanie konfiguracją urządzeń</p> <ul style="list-style-type: none"> • Tworzenie, aktualizacja i utrzymanie konfiguracji sieciowych zgodnie z politykami bezpieczeństwa. • Kontrola wersji i kopie zapasowe konfiguracji (backup & restore). • Wdrażanie zmian konfiguracyjnych w ramach uzgodnionych procedur (Change Management). • Utrzymanie adekwatności i spójności konfiguracji styków pomiędzy segmentami IT i OT. <p>3. Zarządzanie adresacją IP i segmentacją sieci</p> <ul style="list-style-type: none"> • Projektowanie, dokumentowanie i utrzymanie planu adresacji IP. • Zarządzanie przydziałem i rezerwacjami adresów (IPAM). • Utrzymywanie logicznej segmentacji sieci (VLAN, VRF, subnety) zgodnie z politykami bezpieczeństwa. • Współpraca z zespołami SOC i CTI w zakresie analizy ruchu sieciowego i mapowania stref bezpieczeństwa. <p>4. Bezpieczeństwo i kontrola dostępu (w ramach narzędzi sieciowych)</p> <ul style="list-style-type: none"> • Konfiguracja i utrzymanie mechanizmów ochronnych: ACL, NAT, VPN, IDS/IPS, DPI. • Zarządzanie regułami zapór sieciowych (firewall policies) i listami kontroli dostępu. • Monitorowanie logów bezpieczeństwa urządzeń sieciowych. • Weryfikacja integralności konfiguracji i wdrażanie zaleceń bezpieczeństwa zgodnych z IEC 62443 oraz ISO 27001. <p>5. Monitoring i raportowanie</p> <ul style="list-style-type: none"> • Ciągły nadzór nad wydajnością sieci oraz jej dostępnością (SLA, latency, packet loss). • Analiza trendów obciążenia i raportowanie potencjalnych wąskich gardeł. • Regularne raporty stanu infrastruktury i zmian konfiguracyjnych. • Integracja monitoringu z centralną platformą SOC <p>6. Aktualizacje i utrzymanie systemowe urządzeń</p> <ul style="list-style-type: none"> • Aktualizacje firmware i zabezpieczeń urządzeń sieciowych po uprzedniej weryfikacji. • Kontrola zgodności wersji oprogramowania z wymaganiami producentów. • Testowanie poprawek i wdrażanie ich w zaplanowanych oknach serwisowych. <p>7. Wsparcie projektowe i doradcze</p> <ul style="list-style-type: none"> • Konsultacje przy projektowaniu nowych segmentów sieci IT/OT. • Udział w projektach modernizacji i rozbudowy infrastruktury. • Rekomendacje rozwiązań zwiększających wydajność, redundancję i bezpieczeństwo.
Tryb pracy SOC	Zdalny
Tryb pracy interwencyjny	Lokalny i zdalny
Czas pracy SOC	24 h na dobę / 7 dni w tygodniu
Ilość obsługiwany	Bez limitu

ch scenariuszy	
Miejsce instalacji systemów monitorowania i cyberbezpieczeństwa	Lokalnie w miejscu wskazanym przez Zamawiającego. MDR wykorzystuje zainstalowane systemy cyberbezpieczeństwa
Ilość godzin wsparcia zespołu MDR, inżynierskiego, administracyjnego, CTI	360

4.6. Usługa APN

Usługa Private APN – 14 kart SIM - oparta o usługę dostarczoną przez Wykonawcę. Bezpieczeństwo transmisji musi być zapewniane przez Wykonawcę poprzez monitorowanie ruchu przez SOC i własne systemy cyberbezpieczeństwa zlokalizowane u Wykonawcy. SOC Wykonawcy musi legitymować się certyfikacją akredytowaną przez PCA w zakresie minimum ISO 27001 oraz ISO 9001. Dopuszcza się konsorcja lub podwykonawstwo w którym Wykonawca bierze odpowiedzialność za działanie usługi APN.

Karty SIM muszą być aktywowane.

Karty SIM muszą być zamontowane w urządzeniach dostarczonych przez Wykonawcę w części OT

Komunikacja w ramach GMS/APN musi być zgodna z projektem Wykonawczym

Komunikacja nie może ograniczać pasma ani ilości danych. Jakość transferów jest oczywiście uzależniona od warunków panujących lokalnie w miejscu montażu.

4.7. Usługi SOC

Nazwa parametru/cechy	Wartość / zapis oczekiwany
Obszar objęty monitorowaniem	IT oraz OT
Zakres SOC	<p>Zespół SOC odpowiada za bieżące monitorowanie, analizę incydentów bezpieczeństwa w infrastrukturze Zamawiającego.</p> <p>Jego głównym celem jest wsparcie zapewnienia ciągłej ochrony środowiska IT/OT, minimalizacja czasu reakcji oraz wsparcie w podejmowaniu decyzji obronnych.</p> <p>1. Ciągłe monitorowanie bezpieczeństwa</p> <ul style="list-style-type: none"> • 24/7 analiza logów, zdarzeń i anomalii w systemach IT, OT, IoT oraz chmurze. • Monitorowanie infrastruktury Zamawiającego z wykorzystaniem systemów i/lub grup funkcyjnych XDR, SIEM, ITSM, CMDB, ITDR, SOAR • Wykrywanie podejrzanych działań, naruszeń polityk bezpieczeństwa i prób nieautoryzowanego dostępu.

	<p>2. Korelacja i analiza zdarzeń</p> <ul style="list-style-type: none"> • Automatyczna i manualna korelacja zdarzeń z wielu źródeł (firewalle, serwery, stacje robocze, systemy OT). • Wykorzystanie reguł detekcji opartych o MITRE ATT&CK, IEC 62443, NIST 800-82. • Klasyfikacja i priorytetyzacja incydentów według ich wpływu na ciągłość działania i bezpieczeństwo Zamawiającego. <p>3. Reagowanie na incydenty</p> <ul style="list-style-type: none"> • Identyfikacja, incydentów bezpieczeństwa. • Analiza przyczyn źródłowych (Root Cause Analysis) oraz rekomendacje działań naprawczych. • Wsparcie w odbudowie środowiska po incydencie i wdrożeniu środków prewencyjnych. • Raportowanie incydentów zgodnie z wymogami ISO 27001 / NIS2 / IEC 62443 / Ustawy o KSC. <p>4. Współpraca z zespołami CTI i MDR</p> <ul style="list-style-type: none"> • Integracja danych o zagrożeniach z zespołem CTI (Cyber Threat Intelligence). • Współdziałanie z usługami MDR (Managed Detection and Response) w zakresie analizy i automatycznej reakcji. • Aktualizacja reguł detekcji i polityk bezpieczeństwa w oparciu o nowe dane o zagrożeniach. <p>5. Raportowanie i komunikacja z Klientem</p> <ul style="list-style-type: none"> • Miesięczne raporty z incydentów • Powiadamianie o krytycznych zdarzeniach w trybie niezwłocznym. • Dedykowany kanał komunikacji z zespołem SOC (e-mail, telefon, SIEM). • Przeglądy bezpieczeństwa i omówienia incydentów (cykliczne spotkania z Zamawiającym – w ramach comiesięcznych spotkań). <p>6. Utrzymanie i rozwój systemów bezpieczeństwa</p> <ul style="list-style-type: none"> • Weryfikacja poprawności konfiguracji urządzeń zabezpieczających (firewalle, IDS/IPS, serwery logów). • Aktualizacje i rozwój reguł korelacji w SIEM. • Stałe doskonalenie procedur reagowania i procesów SOC. <p>7. Wsparcie compliance i audytów</p> <ul style="list-style-type: none"> • Przygotowanie danych i raportów do audytów bezpieczeństwa na życzenie Zamawiającego. • Mapowanie zdarzeń i incydentów do wymagań norm i regulacji (ISO 27001, NIS2, KSC, IEC 62443). • Udział w opracowaniu planów ciągłości działania (BCP/DRP) na życzenie Zamawiającego .
Tryb pracy SOC	Zdalny
Tryb pracy interwencyjny	Lokalny i zdalny
Czas pracy automatycznego SOC	24 h na dobę / 7 dni w tygodniu Wsparcie AI
Ilość obsługiwanych scenariuszy	Bez limitu
Miejsce instalacji systemów	Lokalnie w miejscu wskazanym przez Zamawiającego

monitorowa nia i cyberbezpie czeństwa	
Ilość godzin wsparcia zespołu SOC w zakresie 36 miesięcy	3600 godzin zagwarantowanej asysty zespołu do wykorzystania w okresie 36 miesięcy Uruchomienie SOC zostanie uzgodnione z Zamawiającym po zakończeniu usługi MDR

5. WDROŻENIE, SEGMENTACJA SIECI, ODBIORY

5.1. Wdrożenie

Wdrożenie ma odbyć się zgodnie z zapisami Projektu Wykonawczego

5.2. Usługi hardeningu systemów i urządzeń

Utwardzenie systemów i urządzeń wymienionych w zakresie dostaw sprzętu i oprogramowania przez Wykonawcę. Utwardzenie ma być wykonane zgodnie z zapisami Projektu Wykonawczego

5.3. Segmentacja sieci

Segmentacja sieci ma odbyć się zgodnie z zapisami Projektu Wykonawczego

5.4. Odbiory

Odbiór przedmiotu zamówienia będzie realizowany zgodnie z poniższą procedurą, gdzie wszystkie elementy dostarczane i wdrażane przez Wykonawcę są określone w OPZ jako System.

- Odbiorowi częściowemu podlegają poszczególne Zadania zgodnie z przyjętym harmonogramem.
- Z każdego Odbioru danego zadania będzie sporządzany Częstkowy Protokół Odbioru, na zasadach określonych w niniejszym punkcie.
- W trakcie procedury Odbioru Zamawiający dokona weryfikacji, czy przedmiot Odbioru spełnia wymagania określone w OPZ.
- Terminy przedstawienia do Odbioru poszczególnych Zadań określone są w Harmonogramie Szczegółowym ustalonym po podpisaniu Umowy.
- Przez Czas Odbioru Strony rozumieją okres czasu pomiędzy zgłoszeniem do Odbioru Zadania lub zgłoszenia wszystkich Zadań do Odbioru Końcowego, a dokonaniem przez Zamawiającego Odbioru potwierdzonego podpisaniem przez Zamawiającego stosownego Protokołu Odbioru lub Protokołu Końcowego.
- Niezwłocznie po ukończeniu Zadania podlegającego Odbiorowi Wykonawca zobowiązany jest zgłosić Zamawiającemu Zadanie do Odbioru.
- Zamawiający potwierdzi zgłoszenia Zadania do Odbioru.
- Po protokolarnym potwierdzeniu przez Zamawiającego przedstawienia Zadania do Odbioru Zamawiający przystąpi do sprawdzenia czy przedmiot Odbioru jest zgodny z celem i wymaganiami niniejszego OPZ, oraz czy Produkt stanowiący:

- System w tym: System / modyfikacja, zmiana lub uaktualnienie Systemu - jest sprawny, nie zawiera Wad, jest zgodny z Projektem Wykonawczym oraz wymogami OPZ;
- Dokument – nie zawiera braków w zawartości dokumentu w stosunku do Umowy oraz Projektu Wykonawczego lub poczynionych uzgodnień, błędów merytorycznych, usterek językowych;
- Szkolenie – jest zgodne z wymaganiami Zamawiającego określonymi w OPZ;
- Produkt wykonany w ramach Usługi – jest zgodny z wymogami Zamawiającego określonymi w dokumencie Zapotrzebowania, oraz innymi wymogami odnoszącymi się do poszczególnych Produktów podlegających Odbiorowi, jeśli w wyniku realizacji Usługi powstał konkretny Produkt, dla którego określone zostały szczególne kryteria, wskazane w punktach powyżej.
- Niezależnie od postanowień zawartych w ustępie powyżej, Zamawiający ma prawo do weryfikacji należytego wykonania Zadań podlegających Odbiorom dowolną metodą oraz skorzystania z opinii Kontrolera Jakości. Zamawiający ma w szczególności prawo przeprowadzić testy dostarczonych do Odbioru Produktów za pomocą samodzielnie zdefiniowanych scenariuszy testowych.
- Czas Odbioru poszczególnych Zadań nie będzie krótszy niż 3 Dni Robocze, a ewentualne skrócenie tego czasu jest wyłącznym uprawnieniem Zamawiającego.
- Strony zgodnie postanawiają, iż brak podjęcia decyzji przez Zamawiającego odnośnie Odbioru poszczególnych Zadań i Produktów nie będzie w żadnym razie uważany za Odbiór bez zastrzeżeń.
- W przypadku stwierdzenia przez Zamawiającego niezgodności pracy podlegającej Odbiorowi, a w szczególności w przypadku wystąpienia Wady lub niezgodności prac z Projektem Wykonawczym lub OPZ, Wykonawca poprawi przedmiot Odbioru w terminie wskazanym przez Zamawiającego. W takim przypadku Procedurę Odbioru opisaną powyżej powtarza się aż do czasu dokonania przez Zamawiającego Odbioru („ponowna procedura Odbioru”) albo skorzystania przez Zamawiającego z prawa odstąpienia od Umowy zgodnie z przepisami prawa lub z podpisaną Umową.
- Jeśli Wykonawca odmawia wprowadzenia zmian do Produktów w ramach ponownej procedury Odbioru lub odmawia wprowadzenia takich zmian w terminach określonych w ustępie powyżej, Wykonawca niezwłocznie poinformuje o tym fakcie Zamawiającego, przedstawiając przyczyny takiej odmowy. Zamawiający podejmie decyzję co do zasadności odmowy Wykonawcy lub podejmie decyzję co do zmiany terminu na wprowadzenie przez Wykonawcę zmian, przy czym zmiana terminu przez Zamawiającego nie ma wpływu na Harmonogram Szczegółowy realizacji pozostałych prac przez Wykonawcę w ramach Umowy, chyba, że Zamawiający postanowi inaczej.
- W przypadku przedstawienia do Częstkowego Odbioru Zadania, Zamawiający może dokonać również warunkowego przyjęcia Zadania przedstawionego do Odbioru. W takim wypadku Wykonawca usunie stwierdzone w danym Zadaniu niezgodności przed przedstawieniem do Odbioru właściwego Zadania lub Odbioru Końcowego.
- Strony sporządzą w dwóch egzemplarzach Protokół Odbioru w formie pisemnej, zastrzeżonej pod rygorem nieważności. Protokół Odbioru podpisany jest przez przedstawicieli Zamawiającego oraz upoważnionych przedstawicieli Wykonawcy.
- Odbiór określonych prac przez Zamawiającego nie zwalnia Wykonawcy od odpowiedzialności, jeżeli na podstawie dotychczasowych prac Wykonawca wiedział lub jako profesjonalista powinien był wiedzieć, że odebrane Zadania przez Zamawiającego nie spełniają wymagań określonych w OPZ (wraz z Załącznikami) lub Istniejącym Projekcie oraz Projekcie Wykonawczym.

- Odbiór poszczególnych Zadań może nastąpić wyłącznie wówczas, gdy wszystkie Produkty przewidziane do realizacji przez Wykonawcę w danym Zadaniu zostały Odebrane przez Zamawiającego (nastąpił Odbiór końcowy wszystkich Produktów z danego Zadania).
- Odbiór Końcowy nastąpi po dokonaniu odbioru wszystkich Zadań oraz po przeprowadzeniu przez Zamawiającego w Czasie Odbioru procesu sprawdzenia obejmującego wszelkie niezbędne testy, w szczególności testy „ad hoc” pozwalające na sprawdzenie prawidłowego działania Systemu na Infrastrukturze Zamawiającego.
- Odbiór Końcowy nastąpi z chwilą podpisania przez Zamawiającego Protokołu Odbioru Końcowego, zawierającego stwierdzenie, że Zamawiający przyjmuje System bez zastrzeżeń. Protokół Końcowy sporządzany jest w dwóch egzemplarzach, w formie pisemnej, zastrzeżonej pod rygorem nieważności.
- Dokonanie Odbioru Częstkowego lub Odbioru Końcowego nie zwalnia Wykonawcy od odpowiedzialności, jeżeli na podstawie dotychczasowych prac Wykonawca wiedział lub jako profesjonalista powinien był wiedzieć, że Produkty odebrane przez Zamawiającego nie spełniają wymagań określonych w OPZ (wraz z Załącznikami), Istniejącym Projekcie lub Projekcie Wykonawczym oraz nie wpływa na możliwość skorzystania przez Zamawiającego z uprawnień przysługujących mu na mocy powszechnie obowiązujących przepisów prawa oraz postanowień OPZ w wypadku nienależytego wykonania zadań zgodnie z zapisami OPZ.

Zaznacza się, że wszelkie protokoły odbioru będą podpisane po przejściu wymaganych weryfikacji, sprawdzeń i testów zgodnie z procedurą kwalifikacji opisaną poniżej.

Po dostawie i wdrożeniu poszczególnych elementów Systemu, należy przeprowadzić niezbędne testy odbiorowe. Testy odbiorowe będą realizowane etapowo, zgodnie terminami oddania poszczególnych segmentów infrastruktury oraz jej funkcjonalności.

Wzory testów odbiorowych, na których należy oprzeć przygotowanie opis scenariuszy testów docelowych Systemu (w fazie projektowania) znajdują się w Załączniku nr 7 OPZ.

Tryb kwalifikacji został przywołany z obszaru wymagań GMP (Good Manufacturing Practice – Dobre Praktyki Wytwarzania), który jest zestawem zasad i wymagań, których zastosowanie w fazach projektu i wdrożenia powoduje uzyskanie produktów o wysokiej jakości, zgodnej z wymaganiami Zamawiającego i praw / normatyw nadrzędnych. Produktem w tym przypadku jest system sieci przemysłowej oraz jej automatyzacji Harmonogram i ograniczenia zakresu prac procesu kwalifikacji

Szczegółowe harmonogramy opracowywania i realizacji protokołów muszą być przygotowywane stosownie do rzeczywistej realizacji projektu. Harmonogram powinien być aktualizowany i omawiany na spotkaniach Zespołu Kwalifikacyjnego w trakcie realizacji projektu.

6. PRACE DODATKOWE

- 6.1. Zamawiający może udzielić wybranemu Wykonawcy zamówień na dodatkowe usługi, polegających na wprowadzeniu nowej lub rozbudowanej funkcjonalności, która nie była przewidziana na etapie realizacji przedmiotu zamówienia.
- 6.2. Czas trwania umowy w sprawie zamówienia na dostawy dodatkowe nie może przekraczać 3 lat, a liczba roboczogodzin nie może przekroczyć 100.
- 6.3. Szczegółowe procedury związane z pracami dodatkowymi zawarte są w załączniku nr 2 do umowy