Cyberbezpieczne Wodociągi

Załącznik nr 5 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA.

Pakiet 1:

1) Dostawa, instalacja, parametryzacja **systemu klasy GRC** (Governance, Risk and Compliance), wraz z przeprowadzeniem pełnej analizy ryzyka, inwentaryzacji zasobów oraz wdrożeniem procesów zarządzania bezpieczeństwem informacji:
   - Model licencjonowania i architektura (On-Premise): udzielenie licencji na system klasy GRC, na okres nie krótszy niż 24 miesiące wolnego od opłat licencyjnych za liczbę wprowadzonych danych, zasobów (assets), podatności czy użytkowników. System musi umożliwiać pełną instalację lokalną w infrastrukturze wirtualizacji (Vmware) Zamawiającego (On-Premise). Wsparcie techniczne w zakresie aktualizacji oprogramowania musi być zapewnione na okres minimum 24 miesiące od dnia odbioru. W przypadku, gdy oferowane oprogramowanie klasy GRC lub któryś z jego składników wymaga do poprawnej instalacji i stabilnego działania w modelu On-Premise dedykowanego systemu operacyjnego klasy serwerowej, dedykowanej bazy danych itp. - wykonawca zobowiązany jest dołączyć do oferty i dostarczyć w cenie niezbędną liczbę komercyjnych, wieczystych licencji pokrywających potrzeby oferowanego rozwiązania NMS
   - Kluczowe funkcjonalności techniczne systemu (wymagania równoważności): system musi natywnie posiadać powiązane ze sobą moduły do zarządzania zgodnością (Compliance Management), zarządzania ryzykiem (Risk Management z rejestrem ryzyk), zarządzania wewnętrznymi politykami i procedurami kontrolnymi (Internal Controls) oraz moduł ewidencjonowania incydentów i procesowania wyjątków bezpieczeństwa.
   - Wymagania dotyczące środowiska systemowego (Licencja OS): W przypadku, gdy oferowane oprogramowanie klasy GRC do poprawnej instalacji i stabilnego działania w modelu On-Premise wymaga dedykowanego systemu operacyjnego klasy serwerowej, Wykonawca zobowiązany jest dołączyć do oferty i dostarczyć w cenie niezbędną liczbę komercyjnych, wieczystych licencji na stabilny system operacyjny.
   - Wymagany zakres profesjonalnych usług analitycznych i wdrożeniowych (Analiza Ryzyka i Procesy GRC): Wykonawca w ramach realizacji zamówienia zobowiązany jest do przeprowadzenia pełnego procesu przedwdrożeniowego i analitycznego przez osoby skierowane do wykonania zamówienia, w tym do pełnej konfiguracji i sparametryzowania modułów systemu obejmujących co najmniej:
     - Zarządzanie dokumentacją i procesem obiegowym (Workflow): konfiguracja modułu do zarządzania dokumentacją (polityki, procedury, instrukcje) wraz z odwzorowaniem pełnego cyklu życia dokumentu (opracowanie, opiniowanie/przegląd, zatwierdzanie oraz publikacja).

- Zarządzanie ryzykiem i ciągłością działania: konfiguracja modułu zarządzania ryzykiem oraz procesów zarządzania ciągłością działania (BCP – Business Continuity Plan / DRP – Disaster Recovery Plan) w ujęciu analizy wpływu biznesowego (BIA).
- Zarządzanie operacyjne i rejestry: konfiguracja modułu zarządzania incydentami oraz uruchomienie i parametryzacja centralnych rejestrów (rejestr aktywów/zasobów, rejestr ryzyk, rejestr incydentów, rejestr zgodności z przepisami i normami).
- Struktura i uprawnienia: pełne odzwierciedlenie struktury organizacyjnej Zamawiającego, zdefiniowanie ról, powiązań oraz uprawnień dostępowych dla użytkowników.
- Automatyzacja i raportowanie: konfiguracja automatycznych mechanizmów powiadomień oraz wielostopniowej eskalacji zadań (np. powiadomienia o zbliżającym się terminie przeglądu procedury lub przekroczeniu poziomu ryzyka), a także przygotowanie dedykowanych dashboardów (paneli menedżerskich) i raportów monitorujących bieżący poziom zgodności.
- Opracowanie metodyki szacowania ryzyka: stworzenie i uzgodnienie z Zamawiającym sformalizowanej metodyki analizy ryzyka (zgodnej z wytycznymi normy ISO/IEC 27005 lub równoważnej), określającej skale prawdopodobieństwa, skutków biznesowych oraz progi akceptacji ryzyka. Metodyka ta musi zostać odzwierciedlona i sparametryzowana w konfiguracji systemu GRC.
- Inwentaryzacja i klasyfikacja zasobów: identyfikacja, skatalogowanie oraz przypisanie właścicieli biznesowych dla kluczowych zasobów informacyjnych, sprzętowych i aplikacyjnych Zamawiającego, a następnie wprowadzenie tej struktury (bazy zasobów) do dostarczonego systemu GRC.

- Wymagany zakres świadczeń, szkoleń i dokumentacji:
  - Przeprowadzenie warsztatów i rzeczywistej analizy ryzyka: przeprowadzenie sesji warsztatowych z pracownikami i kadrą zarządzającą Zamawiającego, identyfikacja podatności i zagrożeń dla zinwentaryzowanych zasobów, oszacowanie poziomów ryzyka pierwotnego oraz opracowanie planów postępowania z ryzykiem (mitygacja, transfer, akceptacja). Kompletny, zidentyfikowany rejestr ryzyk musi zostać wprowadzony do systemu GRC.
  - Mapowanie zgodności i procedur kontrolnych: wprowadzenie do systemu wybranego szablonu normatywnego: ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20 z późn. zm.) oraz powiązanie (zmapowanie) zidentyfikowanych ryzyk z obowiązującymi u Zamawiającego politykami i wewnętrznymi mechanizmami kontrolnymi.
  - Szkolenie techniczne (Administratorzy IT): Wykonawca przeprowadzi praktyczne szkolenie z zakresu administracji technicznej systemu (w tym procedury backupu, aktualizacji, nadawania uprawnień w systemie) dla minimum 2 osób z Działu IT w wymiarze minimum 4 godzin zegarowych.
  - Szkolenie merytoryczno-warsztatowe (Osoby zajmujące się systemem): Wykonawca przeprowadzi kompleksowe szkolenie merytoryczno-warsztatowe dla minimum 3 osób merytorycznych zajmujących się zarządzaniem bezpieczeństwem, zgodnością i ryzykiem (użytkowników biznesowych/oficerów bezpieczeństwa) w wymiarze minimum 16 godzin zegarowych (rozłożonych na minimum 2 dni szkoleniowe). Szkolenie musi obejmować część warsztatową polegającą na wspólnym,

samodzielnym wprowadzaniu i mapowaniu realnych zasobów oraz ryzyk Zamawiającego w środowisku produkcyjnym pod nadzorem trenera.

- Dokumentacja: Przygotowanie i przekazanie Zamawiającemu szczegółowej dokumentacji w języku polskim, zawierającej: potwierdzenie zgodności rozwiązania z przepisami ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20 z późn. zm.), opis techniczny wdrożonego systemu, dokument opisujący przyjętą metodykę szacowania ryzyka oraz kompletny raport z przeprowadzonej analizy ryzyka wraz z planem działań korygujących.

Pakiet 2

2) Przeprowadzenie **testów bezpieczeństwa infrastruktury sieciowej** Zamawiającego w obszarach IT, OT/ICS oraz IIoT, z wykorzystaniem narzędzi klasy vulnerability scanner, obejmujących w szczególności:
   - identyfikację i inwentaryzację zasobów sieciowych podlegających testom (urządzenia, systemy, usługi),
   - przeprowadzenie skanowania podatności infrastruktury sieciowej oraz systemów informatycznych,
   - analizę konfiguracji systemów, usług oraz urządzeń sieciowych pod kątem bezpieczeństwa,
   - identyfikację podatności, błędów konfiguracyjnych oraz potencjalnych wektorów ataku,
   - klasyfikację podatności według poziomu ryzyka (np. CVSS) oraz ich wpływu na działalność Zamawiającego,
   - uwzględnienie specyfiki środowisk OT/ICS (testy nieinwazyjne, bez wpływu na ciągłość działania systemów sterowania),
   - opracowanie raportów z testów zawierających wyniki, ocenę ryzyka oraz rekomendacje działań naprawczych,
   - przedstawienie wyników testów oraz omówienie rekomendacji z Zamawiającym,
   - wsparcie w planowaniu działań remediacyjnych oraz ponowna weryfikacja po ich wdrożeniu (retest).
3) **Usługa inwentaryzacji aktywów teleinformatycznych** IT/OT/ICS/IIoT
   a) Usługa ma na celu inwentaryzację wszystkich zasobów IT/OT/ICS/IIoT dla potrzeb stworzenia i wdrożenia polityk obowiązujących operatorów usług kluczowych

Pakiet 3

4) Dostawa, konfiguracja oraz uruchomienie **urządzeń klasy UTM** (Unified Threat Management) stanowiących zabezpieczenie łączy sieciowych w lokalizacji głównej i lokalizacjach dodatkowych Zamawiającego, obejmujące w szczególności:
   - dostawę **2 urządzeń** klasy UTM pracujących w trybie HA (rozwiązanie ma być dostarczone jako klaster HA dwóch urządzeń działających co najmniej w trybie Active/Passive) o parametrach wydajnościowych co najmniej: przepustowość Firewalla min. 10 Gbps, przepustowość IPS min. 5 Gbps, przepustowość IPSec VPN min. 2,5 Gbps, przepustowość antywirusa min. 1,3 Gbps - jako zabezpieczenie łącza głównego wraz z niezbędnymi licencjami i subskrypcjami bezpieczeństwa na

okres minimum 24 miesiące z zapewnieniem funkcjonalności co najmniej równoważnych do urządzeń klasy Stormshield SN520,[1] w tym:

a) zapora sieciowa (Firewall) nowej generacji (NGFW),
b) system zapobiegania włamaniom (IPS),
c) ochrona przed złośliwym oprogramowaniem (urządzenie ma być dostarczone wraz z komercyjnym skanerem antywirusowym oraz umożliwiać skanowanie plików w oparciu o sandboxing zlokalizowany w Internecie na serwerach producenta i na terenie Unii Europejskiej).
d) filtrowanie treści WWW (URL filtering, DNS filtering),
e) kontrola aplikacji (Application Control),
f) ochrona antyspamowa,
g) obsługa bezpiecznych połączeń VPN (site-to-site oraz zdalny dostęp),
h) zapewnienie centralnego zarządzania oraz monitorowania zdarzeń bezpieczeństwa,
i) redundantne zasilanie umożliwiające wymianę zasilacza bez przerywania pracy (hot-swap) – urządzenie musi zostać dostarczone z fabrycznie zainstalowanymi dwoma sprawnymi modułami zasilaczy
j) Obsługa wielu łączy internetowych oraz redundancja tuneli VPN:
   - Urządzenie musi sprzętowo i programowo umożliwiać jednoczesne zakończenie i obsługę minimum 2 (dwóch) niezależnych, fizycznych łącz internetowych od różnych dostawców telekomunikacyjnych (funkcja Multi-WAN).
   - System operacyjny urządzenia musi zapewniać funkcję automatycznego wykrywania awarii łącza podstawowego (WAN Failover) i natychmiastowego przełączania całego ruchu użytkowników na łącze zapasowe.
   - W zakresie połączeń VPN (Lan2Lan / Site-to-Site): Urządzenie musi obsługiwać mechanizm automatycznego, bezprzerwowego przełączania tuneli szyfrowanych (Failover VPN) pomiędzy dostawcami internetu. W przypadku awarii łącza u operatora podstawowego, system musi automatycznie zestawić tunel VPN Lan2Lan z wykorzystaniem łącza operatora zapasowego (zapasowej bramy / zapasowego adresu IP) bez konieczności manualnej interwencji administratora.
k) konfigurację urządzeń zgodnie z polityką bezpieczeństwa Zamawiającego,
l) integrację z istniejącą infrastrukturą sieciową oraz systemami bezpieczeństwa,
m) wdrożenie mechanizmów aktualizacji sygnatur oraz baz zagrożeń,
n) uruchomienie i testy poprawności działania w środowisku produkcyjnym,
o) przygotowanie dokumentacji powdrożeniowej (schematy, konfiguracja, polityki),

[1] Zamawiający zgodnie z postanowieniami SWZ dopuszcza rozwiązania równoważne, a użycie nazw własnych służy wyłącznie opisowi oczekiwań Zamawiającego co do klasy i możliwości technicznych oferowanych rozwiązań.

p) zapewnienie wsparcia technicznego producenta przez okres minimum 24 miesiące.

- dostawę **2 urządzeń** klasy UTM pracujących w trybie HA (rozwiązanie ma być dostarczone jako klaster HA dwóch urządzeń działających co najmniej w trybie Active/Passive) wraz z niezbędnymi licencjami i subskrypcjami bezpieczeństwa na okres minimum 24 miesiące z zapewnieniem funkcjonalności co najmniej równoważnych do urządzeń klasy Stormshield SN220 o parametrach wydajnościowych co najmniej: przepustowość Firewalla min. 4 Gbps, przepustowość IPS min. 2 Gbps, przepustowość IPSec VPN min. 1 Gbps - jako zabezpieczenie łącza zdalnego pracującego w trybie site-to-site z łączem głównym, w tym:
  a) zapora sieciowa (Firewall) nowej generacji (NGFW),
  b) system zapobiegania włamaniom (IPS),
  c) obsługa bezpiecznych połączeń VPN (site-to-site oraz zdalny dostęp),
  d) zapewnienie centralnego zarządzania oraz monitorowania zdarzeń bezpieczeństwa,
  e) Obsługa wielu łączy internetowych oraz redundancja tuneli VPN:
     - Urządzenie musi sprzętowo i programowo umożliwiać jednoczesne zakończenie i obsługę minimum 2 (dwóch) niezależnych, fizycznych łącz internetowych od różnych dostawców telekomunikacyjnych (funkcja Multi-WAN).
     - System operacyjny urządzenia musi zapewniać funkcję automatycznego wykrywania awarii łącza podstawowego (WAN Failover) i natychmiastowego przełączania całego ruchu użytkowników na łącze zapasowe.
     - W zakresie połączeń VPN (Lan2Lan / Site-to-Site): Urządzenie musi obsługiwać mechanizm automatycznego, bezprzerwowego przełączania tuneli szyfrowanych (Failover VPN) pomiędzy dostawcami internetu. W przypadku awarii łącza u operatora podstawowego, system musi automatycznie zestawić tunel VPN Lan2Lan z wykorzystaniem łącza operatora zapasowego (zapasowej bramy / zapasowego adresu IP) bez konieczności manualnej interwencji administratora.
  f) konfigurację urządzeń zgodnie z polityką bezpieczeństwa Zamawiającego,
  g) integrację z istniejącą infrastrukturą sieciową oraz systemami bezpieczeństwa,
  h) wdrożenie mechanizmów aktualizacji sygnatur oraz baz zagrożeń,
  i) uruchomienie i testy poprawności działania w środowisku produkcyjnym,
  j) przygotowanie dokumentacji powdrożeniowej (schematy, konfiguracja, polityki),
  k) zapewnienie wsparcia technicznego producenta przez okres minimum 24 miesiące

- dostawę **1 urządzenia** klasy UTM wraz z niezbędnymi licencjami i subskrypcjami bezpieczeństwa na okres minimum 24 miesiące z zapewnieniem funkcjonalności co najmniej równoważnych do urządzeń klasy Stormshield SN170 o parametrach wydajnościowych co najmniej: przepustowość Firewalla min. 2 Gbps, przepustowość IPS min. 1 Gbps, przepustowość IPSec VPN min. 500 Mbps - jako zabezpieczenie łącza zdalnego pracującego w trybie site-to-site z łączem głównym.

a) zapora sieciowa (Firewall) nowej generacji (NGFW),
b) system zapobiegania włamaniom (IPS),
c) obsługa bezpiecznych połączeń VPN (site-to-site oraz zdalny dostęp),
d) zapewnienie centralnego zarządzania oraz monitorowania zdarzeń bezpieczeństwa,
e) Obsługa wielu łączy internetowych oraz redundancja tuneli VPN:
   - Urządzenie musi sprzętowo i programowo umożliwiać jednoczesne zakończenie i obsługę minimum 2 (dwóch) niezależnych, fizycznych łącz internetowych od różnych dostawców telekomunikacyjnych (funkcja Multi-WAN).
   - System operacyjny urządzenia musi zapewniać funkcję automatycznego wykrywania awarii łącza podstawowego (WAN Failover) i natychmiastowego przełączania całego ruchu użytkowników na łącze zapasowe.
   - W zakresie połączeń VPN (Lan2Lan / Site-to-Site): Urządzenie musi obsługiwać mechanizm automatycznego, bezprzerwowego przełączania tuneli szyfrowanych (Failover VPN) pomiędzy dostawcami internetu. W przypadku awarii łącza u operatora podstawowego, system musi automatycznie zestawić tunel VPN Lan2Lan z wykorzystaniem łącza operatora zapasowego (zapasowej bramy / zapasowego adresu IP) bez konieczności manualnej interwencji administratora.
f) konfigurację urządzeń zgodnie z polityką bezpieczeństwa Zamawiającego,
g) integrację z istniejącą infrastrukturą sieciową oraz systemami bezpieczeństwa,
h) wdrożenie mechanizmów aktualizacji sygnatur oraz baz zagrożeń,
i) uruchomienie i testy poprawności działania w środowisku produkcyjnym,
j) przygotowanie dokumentacji powdrożeniowej (schematy, konfiguracja, polityki),
k) zapewnienie wsparcia technicznego producenta przez okres minimum 24 miesiące

- przeszkolenie administratorów z zakresu obsługi i zarządzania urządzeniami klasy UTM

5) Dostawę **1 przełącznika sieciowego,** zarządzalnego (L2/L3) o funkcjonalności zapewniających minimalne parametry techniczne:
   - **min. 48 portów** 10/100/1000BASE-T,
   - min. 4 porty uplink SFP/SFP+ (10G lub równoważne),
   - obsługa VLAN (IEEE 802.1Q),
   - obsługa uwierzytelniania portowego 802.1X (integracja z NAC/RADIUS),
   - obsługa szyfrowania ruchu na poziomie warstwy 2 (MACsec – IEEE 802.1AE),
   - zapewnienie funkcjonalności bezpieczeństwa i zarządzania:
   - segmentacja sieci (VLAN),
   - kontrola dostępu do portów (ACL),

- ochrona przed atakami warstwy 2 (np. DHCP snooping, ARP inspection, BPDU guard lub równoważne),
- QoS (priorytetyzacja ruchu),
- integrację z infrastrukturą sieciową Zamawiającego,
- możliwość centralnego zarządzania i monitorowania (WWW/CLI/SNMP lub równoważne),
- konfigurację urządzeń zgodnie z polityką bezpieczeństwa Zamawiającego,
- przygotowanie dokumentacji powdrożeniowej (schematy sieci, konfiguracja VLAN, polityki dostępu),
- przeprowadzenie testów poprawności działania (w tym 802.1X, VLAN, segmentacja),
- przeszkolenie administratorów w zakresie zarządzania przełącznikami,
- zapewnienie wsparcia technicznego producenta przez okres minimum 24 miesiące.

6) Dostawę **3 przełączników sieciowych,** zarządzalnego (L2/L3) o funkcjonalności zapewniających minimalne parametry techniczne:
   - **min. 24 portów** 10/100/1000BASE-T,
   - min. 4 porty uplink SFP/SFP+ (10G lub równoważne),
   - obsługa VLAN (IEEE 802.1Q),
   - obsługa uwierzytelniania portowego 802.1X (integracja z NAC/RADIUS),
   - obsługa szyfrowania ruchu na poziomie warstwy 2 (MACsec – IEEE 802.1AE),
   - zapewnienie funkcjonalności bezpieczeństwa i zarządzania:
   - segmentacja sieci (VLAN),
   - kontrola dostępu do portów (ACL),
   - ochrona przed atakami warstwy 2 (np. DHCP snooping, ARP inspection, BPDU guard lub równoważne),
   - QoS (priorytetyzacja ruchu),
   - integrację z istniejącą infrastrukturą sieciową Zamawiającego,
   - możliwość centralnego zarządzania i monitorowania (WWW/CLI/SNMP lub równoważne),
   - konfigurację urządzeń zgodnie z polityką bezpieczeństwa Zamawiającego,
   - przygotowanie dokumentacji powdrożeniowej (schematy sieci, konfiguracja VLAN, polityki dostępu),
   - przeprowadzenie testów poprawności działania (w tym 802.1X, VLAN, segmentacja),
   - przeszkolenie administratorów w zakresie zarządzania przełącznikami,
   - zapewnienie wsparcia technicznego producenta przez okres minimum 24 miesiące.

7) dostawa, instalacja oraz konfiguracja **3 zarządzalnych przełączników sieciowych** (switchy) o parametrach co najmniej:
   - **min. 24 portów POE** 10/100/1000BASE-T,
   - zapewnienie funkcjonalności bezpieczeństwa:
   - obsługa VLAN (IEEE 802.1Q),

- obsługa uwierzytelniania portowego 802.1X (integracja z NAC/RADIUS),
- obsługa szyfrowania ruchu MACsec (IEEE 802.1AE) lub równoważnego mechanizmu zabezpieczenia komunikacji,
- zapewnienie podstawowych mechanizmów zarządzania i ochrony:
- kontrola dostępu do portów (ACL),
- ochrona warstwy 2 (np. DHCP snooping, ARP inspection lub równoważne),
- możliwość centralnego zarządzania i monitorowania (WWW/CLI/SNMP lub równoważne),
- integrację z istniejącą infrastrukturą sieciową Zamawiającego,
- konfigurację urządzeń zgodnie z polityką bezpieczeństwa Zamawiającego,
- przygotowanie dokumentacji powdrożeniowej (schematy połączeń, konfiguracja VLAN i polityk dostępu),
- przeprowadzenie testów poprawności działania (w tym 802.1X i segmentacja VLAN),
- przeszkolenie administratorów w zakresie zarządzania urządzeniami,
- zapewnienie wsparcia technicznego producenta przez okres minimum 24 miesiące.

8) dostawa, instalacja oraz konfiguracja **4 Przemysłowych zarządzalnych przełączników PoE** (switchy) o parametrach co najmniej:
   - **min. 8 portów POE** 10/100/1000BASE-T,
   - zapewnienie funkcjonalności bezpieczeństwa:
   - obsługa VLAN (IEEE 802.1Q),
   - obsługa uwierzytelniania portowego 802.1X (integracja z NAC/RADIUS),
   - obsługa szyfrowania ruchu MACsec (IEEE 802.1AE) lub równoważnego mechanizmu zabezpieczenia komunikacji,
   - zapewnienie podstawowych mechanizmów zarządzania i ochrony:
   - kontrola dostępu do portów (ACL),
   - ochrona warstwy 2 (np. DHCP snooping, ARP inspection lub równoważne),
   - możliwość centralnego zarządzania i monitorowania (WWW/CLI/SNMP lub równoważne),
   - integrację z istniejącą infrastrukturą sieciową Zamawiającego,
   - Możliwość montażu na szynie DIN lub montaż ścienny
   - Wilgotność: 5%~90%
   - Temperatura pracy: -40+85 C
   - konfigurację urządzeń zgodnie z polityką bezpieczeństwa Zamawiającego,
   - przygotowanie dokumentacji powdrożeniowej (schematy połączeń, konfiguracja VLAN i polityk dostępu),
   - przeprowadzenie testów poprawności działania (w tym 802.1X i segmentacja VLAN),
   - przeszkolenie administratorów w zakresie zarządzania urządzeniami,
   - zapewnienie wsparcia technicznego producenta przez okres minimum 24 miesiące.

9) dostawa, instalacja oraz konfiguracja **3 punktów dostępowych sieci bezprzewodowej (Access Point)** spełniających co najmniej poniższe parametry:
   - Standard Wi-Fi: Wsparcie dla standardu IEEE 802.11be (Wi-Fi 7) oraz wsteczna kompatybilność z 802.11a/b/g/n/ac/ax.
   - Praca wielopasmowa (Tri-Band): Jednoczesna obsługa trzech pasm częstotliwości: 2.4 GHz, 5 GHz oraz 6 GHz.
   - Wydajność radiowa (MIMO / Streamy): Minimum 2x2 MIMO w paśmie 2.4 GHz.Minimum 2x2 MIMO w paśmie 5 GHz.Minimum 4x4 MIMO w paśmie 6 GHz.
   - Interfejs przewodowy: Minimum 1 port Ethernet RJ45 o prędkości min. 2.5 Gbps (2.5 GbE) z obsługą zasilania PoE+ (Power over Ethernet, standard 802.3at).
   - Zysk i konstrukcja anten: Zintegrowane anteny wielokierunkowe o podwyższonym zysku energetycznym zapewniające optymalne pokrycie sygnałem w trudnych warunkach propagacyjnych.
   - Bezpieczeństwo: Obsługa szyfrowania WPA-PSK, WPA-Enterprise (WPA2/WPA3), izolacja klientów, obsługa VLAN (802.1Q).
   - Zarządzanie: Centralny system zarządzania (kontroler programowy lub sprzętowy) umożliwiający konfigurację masową, monitorowanie ruchu, aktualizacje firmware oraz uwierzytelnianie użytkowników (np. przez serwer RADIUS / system NAC).
   - konfigurację urządzeń zgodnie z polityką bezpieczeństwa Zamawiającego,
   - przygotowanie dokumentacji powdrożeniowej (schematy połączeń, konfiguracja VLAN i polityk dostępu),
   - przeprowadzenie testów poprawności działania (w tym 802.1X i segmentacja VLAN),
   - przeszkolenie administratorów w zakresie zarządzania urządzeniami,
   - zapewnienie wsparcia technicznego producenta przez okres minimum 24 miesiące.

10) **Zaprojektowanie, wdrożenie oraz uruchomienie segmentacji sieci** Zamawiającego w obszarach IT, OT/ICS oraz IIoT, w celu zwiększenia poziomu bezpieczeństwa, ograniczenia rozprzestrzeniania się incydentów oraz zapewnienia zgodności z wymaganiami regulacyjnymi (m.in. NIS2), obejmujące w szczególności:
   - przeprowadzenie analizy stanu obecnego infrastruktury sieciowej (IT/OT/ICS/IIoT),
   - identyfikację zasobów, systemów oraz przepływów komunikacyjnych (mapowanie ruchu),
   - klasyfikację systemów i stref bezpieczeństwa (np. model Purdue lub równoważny),
   - opracowanie architektury segmentacji sieci (strefy, podsieci, VLAN, strefy bezpieczeństwa),
   - zaprojektowanie zasad komunikacji między segmentami (reguły firewall, ACL, mikrosegmentacja),
   - wdrożenie segmentacji logicznej (VLAN, routing, ACL) oraz – w uzasadnionych przypadkach – fizycznej separacji sieci,

- integrację segmentacji z systemami bezpieczeństwa (UTM, NAC, systemy monitorowania),
- konfigurację mechanizmów kontroli dostępu do sieci (802.1X, NAC, przypisywanie do VLAN),
- wdrożenie zasad ograniczania ruchu między strefami IT i OT (kontrola komunikacji, dostęp uprzywilejowany),
- przeprowadzenie testów poprawności działania segmentacji oraz odporności na nieautoryzowany dostęp,
- opracowanie dokumentacji powdrożeniowej (architektura, schematy, polityki komunikacji),
- przeszkolenie administratorów w zakresie zarządzania segmentacją,
- opracowanie wytycznych utrzymania i dalszego rozwoju segmentacji.
- technicznego producenta przez okres minimum 24 miesiące.

Pakiet 4

11) Dostawa 1 macierzy dyskowej typu NAS (Network Attached Storage), przeznaczonej do realizacji kopii zapasowych danych Zamawiającego, o parametrach minimalnych:
    - Konstrukcja i pojemność: urządzenie klasy NAS w obudowie dedykowanej do montażu w szafie rack (wraz z kompletem szyn montażowych), wyposażone w min. dwa zasilacze redundantne pracujące w trybie hot-plug.
    - Urządzenie musi zapewniać łączną pojemność użytkową (dostępną dla systemu po skonfigurowaniu macierzy RAID 6) o wartości minimum 20 TB, zrealizowaną przy użyciu minimum 6 (sześciu) fizycznych dysków twardych klasy Enterprise (dedykowanych do pracy ciągłej 24/7 w macierzach NAS/RAID).
    - Obsługa pamięci blokowej: system operacyjny urządzenia musi natywnie i stabilnie obsługiwać funkcję celu iSCSI (iSCSI Target) w celu umożliwienia wydzielenia i zaprezentowania przestrzeni dyskowej jako logicznego wolumenu (LUN) do serwera kopii zapasowych.
    - Interfejsy sieciowe: minimum 2 × karta sieciowa o prędkości min. 10 GbE każda, wyposażona w miedziane złącza typu RJ-45, z obsługą agregacji łączy (Link Aggregation) oraz optymalizacji pod kątem ruchu iSCSI (w tym wsparcie dla mechanizmu Jumbo Frames).
    - Monitoring i alerty: system operacyjny urządzenia musi zapewniać funkcjonalność automatycznego monitoringu stanu zdrowia dysków i podzespołów, raportowania oraz wysyłania powiadomień o alertach i awariach (np. poprzez e-mail lub protokół SNMP).
    - Dokumentacja: dostarczenie wraz ze sprzętem standardowej dokumentacji technicznej i instrukcji obsługi dostarczanej przez producenta urządzenia.
    - Wsparcie i gwarancja: zapewnienie oficjalnego wsparcia technicznego i gwarancji producenta sprzętu przez okres minimum 12 miesięcy, realizowanej w miejscu instalacji sprzętu (on-site).

12) Dostawa, instalacja oraz konfiguracja 1 serwera fizycznego klasy enterprise (w obudowie typu rack 1U lub 2U, dopasowanej do posiadanej szafy serwerowej Zamawiającego) o parametrach minimalnych:

- Procesor: minimum 1 × procesor klasy serwerowej Intel Xeon Gold (co najmniej model 5318Y lub procesor równoważny, posiadający min. 24 rdzenie fizyczne / 48 wątków logicznych).
- Pamięć RAM: minimum 256 GB pamięci operacyjnej typu DDR4 (lub nowszej) z funkcją korekcji błędów ECC (np. w konfiguracji 8 × 32 GB lub równoważnej, zapewniającej optymalne wykorzystanie wielokanałowości kontrolera pamięci).
- Pojemność dyskowa: dyski SSD klasy enterprise w technologii min. SAS lub NVMe, zapewniające łączną pojemność użytkową (dostępną dla systemu operacyjnego po skonfigurowaniu macierzy RAID 6) o wartości minimum 10 TB, zrealizowaną przy użyciu macierzy składającej się z minimum 6 (sześciu) fizycznych dysków zainstalowanych w serwerze, oraz dodatkowo minimum 1 (jednego) dedykowanego dysku fizycznego o tej samej pojemności i parametrach, skonfigurowanego jako dysk zapasowy typu Hot Spare (gotowy do automatycznej odbudowy macierzy w przypadku awarii jednego z dysków głównych). Łączna liczba fizycznych dysków SSD zainstalowanych w serwerze musi wynosić minimum 7 (siedem) sztuk.
- Kontroler dyskowy: sprzętowy kontroler RAID wyposażony w podtrzymywaną bateryjnie lub za pomocą pamięci flash pamięć podręczną (Cache o wielkości min. 2 GB), obsługujący sprzętowo poziomy min. RAID 0, 1, 5, 6, 10.
- Karta sieciowa: zintegrowana lub w formie kart rozszerzeń PCIe, oferująca łącznie minimum 6 portów o prędkości min. 10 GbE każdy, wyposażona w miedziane złącza typu RJ-45.
- Zasilanie: minimum dwa zasilacze redundantne pracujące w trybie hot-plug (z możliwością wymiany uszkodzonego modułu podczas pracy serwera), o mocy dobranej do maksymalnego obciążenia konfiguracji sprzętowej.
- Zdalne zarządzanie: serwer musi być wyposażony w dedykowany, niezależny sprzętowo od głównego procesora i systemu operacyjnego podsystem zdalnego zarządzania i diagnostyki (klasy iDRAC Enterprise lub rozwiązanie równoważne), posiadający wydzielony fizyczny port sieciowy RJ-45 o prędkości min. 100/1000 Mbps, zapewniający pełny podgląd graficzny ekranu (KVM over IP) bez ograniczeń czasowych, możliwość zdalnego włączania/wyłączania/resetu, zdalne alertowanie o awariach podzespołów oraz pełną obsługę wirtualnych mediów.
- Kontroler SAS (do biblioteki taśmowej): serwer musi zostać wyposażony w zewnętrzny kontroler dedykowany do obsługi pamięci masowych typu SAS (klasy Host Bus Adapter – HBA, działający w trybie non-RAID / Pass-through) montowany w porcie PCI-Express, wyposażony w zewnętrzny port/porty SAS o przepustowości min. 12Gb/s. Wraz z kontrolerem należy dostarczyć dedykowany kabel SAS o długości min. 2m umożliwiający fizyczne połączenie serwera z napędem biblioteki taśmowej.
- Kompatybilność: pełna, oficjalna certyfikacja i wsparcie producenta dla pracy w środowisku wirtualizacji i klastrach wysokiej dostępności (VMware vSphere / ESXi).

- Wsparcie i gwarancja: zapewnienie oficjalnego wsparcia technicznego i gwarancji producenta sprzętu przez okres minimum 24 miesiące, realizowanej w miejscu instalacji sprzętu (on-site) z czasem reakcji i naprawy w następny dzień roboczy od momentu zgłoszenia (Next Business Day - NBD).

13) Dostawa systemu archiwizacji danych opartego o bibliotekę taśmową (autoloader), przeznaczonego do długoterminowego przechowywania kopii zapasowych, o parametrach minimalnych:
    - Konstrukcja i napęd: urządzenie klasy autoloader taśmowy w obudowie dedykowanej do montażu w szafie rack (wraz z kompletem szyn montażowych), wyposażone w minimum 1 (jeden) wewnętrzny napęd taśmowy w technologii LTO-8 z fizycznym interfejsem SAS o przepustowości min. 6 Gb/s lub 12 Gb/s.
    - Pojemność i sloty: urządzenie musi posiadać minimum 8 (osiem) fizycznych slotów na nośniki taśmowe oraz minimum 1 (jeden) slot typu mail-slot (do bezpiecznego wprowadzania/wyjmowania pojedynczych kaset bez przerywania pracy urządzenia).
    - Autoloader musi obsługiwać łączną pojemność natywną (bez kompresji) na poziomie minimum 96 TB.
    - Nośniki danych (Kasety) w zestawie: wraz z urządzeniem wykonawca musi dostarczyć: minimum 10 (dziesięć) fabrycznie nowych, dedykowanych kaset taśmowych w standardzie LTO-8 o pojemności natywnej min. 12 TB każda, minimum 1 (jedną) kompatybilną kasetę czyszczącą (Cleaning Cartridge), komplet samoprzylepnych etykiet z kodami kreskowymi (barcodes) dedykowanych do obsługi dostarczonych kaset w bibliotece taśmowej.
    - Zarządzanie i bezpieczeństwo: urządzenie musi posiadać wbudowany, dedykowany port sieciowy RJ-45 do zdalnego zarządzania biblioteką przez przeglądarkę WWW (interfejs graficzny) oraz wspierać sprzętowe szyfrowanie danych zapisywanych na taśmach (AES 256-bit).
    - Dokumentacja: dostarczenie wraz ze sprzętem standardowej dokumentacji technicznej i instrukcji obsługi dostarczanej przez producenta urządzenia.
    - Wsparcie i gwarancja: zapewnienie oficjalnego wsparcia technicznego i gwarancji producenta sprzętu przez okres minimum 24 miesiące, realizowanej w miejscu instalacji sprzętu (on-site).

Pakiet 5

14) Dostawa oprogramowania cyberbezpieczeństwa klasy EDR/XDR (Extended Detection and Response) wraz z modułem centralnego zarządzania i wielowarstwową ochroną punktów końcowych, o parametrach minimalnych:
    - Okres i model licencjonowania: dostawa fabrycznie nowych, komercyjnych subskrypcji licencyjnych dla łącznie 55 (pięćdziesięciu pięciu) urządzeń końcowych na okres minimum 24 miesiące. Licencjonowanie musi być realizowane w modelu na urządzenie (per device/endpoint) i obejmować pełny pakiet funkcjonalny, w strukturze: minimum 50 licencji przeznaczonych dla stacji roboczych (Windows / macOS / Linux), minimum 5 licencji przeznaczonych dla serwerów plikowych/systemowych (Windows Server).

- Konsola centralnego zarządzania (w modelu On-Premise): główna konsola zarządzająca oprogramowaniem oraz serwer bazy danych systemowych muszą być dostarczone w wersji umożliwiającej instalację i uruchomienie lokalnie na własnych serwerach w infrastrukturze wirtualizacji (Vmware) Zamawiającego (On-Premise). Konsola musi zapewniać jednorodne zarządzanie całą flotą urządzeń, politykami bezpieczeństwa, aktualizacjami oraz wgląd w wykryte podatności i incydenty z poziomu lokalnego panelu administratora.
- Zaawansowana analityka i detekcja incydentów (Moduł EDR/XDR): system musi zapewniać ciągły monitoring zachowań, procesów i zdarzeń na stacjach roboczych i serwerach w czasie rzeczywistym. Serwer analityczny gromadzący i korelujący dane z końcówek musi umożliwiać instalację w modelu On-Premise na własnych serwerach w infrastrukturze wirtualizacji (Vmware) Zamawiającego. System musi oferować funkcje przeszukiwania historii zdarzeń (Threat Hunting), analizy behawioralnej, mapowania anomalii do bazy MITRE ATT&CK oraz zdalnej remediacji (np. izolacja zainfekowanego urządzenia od sieci, blokowanie procesów z poziomu konsoli).Zarządzanie podatnościami i poprawkami (Vulnerability & Patch Management): wbudowany mechanizm automatycznego, regularnego skanowania stacji roboczych oraz serwerów pod kątem znanych podatności (luk bezpieczeństwa) w systemach operacyjnych oraz popularnych aplikacjach firm trzecich, wraz z możliwością centralnego, zdalnego instalowania łatek (patchowanie) bezpośrednio z poziomu lokalnej konsoli zarządzającej.
- - Zgodność z przepisami: konfiguracja raportów i mechanizmów umożliwiających Zamawiającemu spełnienie wymagań sprawozdawczych i audytowych wynikających z aktualnych przepisów prawa (w tym dyrektywy NIS2, ustawy o Krajowym Systemie Cyberbezpieczeństwa – KSC, Krajowych Ram Interoperacyjności – KRI).
- Wielowarstwowa ochrona punktów końcowych: ochrona maszyn końcowych oraz serwerów przed złośliwym oprogramowaniem w oparciu o sztuczną inteligencję (uczenie maszynowe), analizę reputacji plików oraz dwukierunkowy firewall brzegowy. Dedykowane moduły ochrony przed atakami typu Ransomware, Anti-Phishing oraz blokada nieautoryzowanych urządzeń peryferyjnych (np. pamięci USB).
- Zaawansowany Sandboxing w chmurze: ochrona przed złośliwym oprogramowaniem realizowana poprzez automatyczne przesyłanie nieznanych i podejrzanych plików (np. załączników mailowych, pobranych skryptów) do odizolowanego, bezpiecznego środowiska testowego (sandbox) zlokalizowanego w Internecie na serwerach producenta i na terenie Unii Europejskiej, w celu detekcji zagrożeń typu Zero-Day.
- Ochrona serwerów pocztowych oraz aplikacji chmurowych: dedykowany moduł filtrujący i zabezpieczający firmowe skrzynki pocztowe oraz usługi chmurowe (klasy Microsoft 365 / Google Workspace), realizujący funkcje antyspamowe, antywirusowe i antyphishingowe.

- Pełne szyfrowanie dysków: zintegrowany z konsolą zarządzającą moduł umożliwiający centralne wymuszanie i zarządzanie pełnym szyfrowaniem dysków systemowych i partycji (FDE) na chronionych urządzeniach końcowych w celu ochrony danych przed kradzieżą.
- Uwierzytelnianie wieloskładnikowe (MFA/2FA): system musi dostarczać 55 licencji na oprogramowanie do dwuskładnikowego uwierzytelniania użytkowników (np. generowanie kodów jednorazowych lub zatwierdzanie powiadomień Push na smartfonach) zabezpieczające logowanie do systemów Windows, połączeń VPN lub firmowych usług webowych (serwer uwierzytelniający musi umożliwiać instalację w modelu On-Premise).
- Wsparcie techniczne i aktualizacje: zapewnienie oficjalnego wsparcia technicznego producenta oraz dostępu do bezpłatnych aktualizacji baz sygnatur i wersji oprogramowania przez cały okres obowiązywania subskrypcji (24 miesiące), wraz z kompletem dokumentacji technicznej w języku polskim.
- W przypadku, gdy oferowane oprogramowanie klasy EDR/XDR lub któryś z jego składników wymaga do poprawnej instalacji i stabilnego działania w modelu On-Premise dedykowanego systemu operacyjnego klasy serwerowej, dedykowanej bazy danych itp. - wykonawca zobowiązany jest dołączyć do oferty i dostarczyć w cenie niezbędną liczbę komercyjnych, wieczystych licencji pokrywających potrzeby oferowanego rozwiązania EDR/XDR.
- Wymagany zakres usług wdrożeniowych, konfiguracyjnych i szkoleniowych:
  - Wykonawca zobowiązany jest do przeprowadzenia pełnej instalacji oraz konfiguracji dostarczonego systemu klasy EDR/XDR w środowisku produkcyjnym Zamawiającego (w tym instalacji i parametryzacji lokalnej konsoli zarządzającej oraz lokalnych serwerów analitycznych EDR/XDR). Zakres prac obejmuje wdrożenie agentów ochronnych na wszystkich 55 urządzeniach końcowych (50 stacjach roboczych i 5 serwerach), konfigurację wstępnych polityk bezpieczeństwa (antywirus, firewall, reguły HIPS, wykluczenia), konfigurację reguł powiadomień, integrację z lokalną strukturą sieciową Zamawiającego oraz przygotowanie i przekazanie zwięzłej dokumentacji powdrożeniowej (zawierającej opis struktury, kluczowych ustawień oraz kont administracyjnych).
  - Przeprowadzenie praktycznego szkolenia (min. 8 godzin zegarowych) dla administratorów Zamawiającego z zakresu obsługi systemu.

  Dokumentacja: Przygotowanie i przekazanie Zamawiającemu szczegółowej dokumentacji w języku polskim, zawierającej: potwierdzenie zgodności rozwiązania z przepisami ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20 z późn. zm.), opis techniczny wdrożonego oprogramowania.

Pakiet 6

15) Dostawa, instalacja, konfiguracja, uruchomienie oraz przeprowadzenie szkolenia dla systemu klasy SIEM (Security Information and Event Management) służącego do centralnego zbierania, korelacji i analizy zdarzeń bezpieczeństwa, o parametrach minimalnych:
    - Model licencjonowania i wydajność: dostawa systemu klasy SIEM licencja na okres nie krótszy niż 24 miesięcy, wolne od opłat licencyjnych za wolumen danych, liczbę zdarzeń (EPS) oraz liczbę

monitorowanych hostów. Dostarczone rozwiązanie i architektura serwerowa wdrożona przez Wykonawcę muszą w cenie zamówienia zapewniać pełną obsługę, zbieranie i korelację danych z minimum 100 zasobów sieciowych i systemowych (assets) Zamawiającego.

- Architektura wdrożenia: instalacja i pełna konfiguracja systemu lokalnie w strukturze Zamawiającego (w modelu On-Premise w środowisku wirtualizacji (Vmware) Zamawiającego).
- Wymagany zakres integracji i zbierania logów: Wykonawca zobowiązany jest do zintegrowania i uruchomienia przesyłania logów do systemu SIEM z następujących zasobów Zamawiającego:
- urządzeń sieciowych i brzegowych (firewalle UTM, przełączniki sieciowe zarządzalne), systemów serwerowych (w tym Active Directory / Windows Server / Linux) oraz kluczowych stacji roboczych (poprzez instalację dedykowanych agentów SIEM), systemów i urządzeń sieci automatyki przemysłowej OT/ICS (w zakresie dostępności logów systemowych/protokołu syslog).
- Wymagania funkcjonalne wdrożenia:

  - Centralizacja i bezpieczeństwo: zapewnienie mechanizmów bezpiecznego, centralnego i niezaprzeczalnego przechowywania logów historycznych.

  - Korelacja i detekcja: konfiguracja reguł korelacyjnych, scenariuszy detekcji i wykrywania incydentów bezpieczeństwa oraz mapowanie zagrożeń do globalnej bazy wiedzy o cyberatakach MITRE ATT&CK.

  - Monitorowanie i alerty: uruchomienie monitorowania zdarzeń w czasie rzeczywistym oraz konfiguracja powiadomień i alertów o incydentach (np. drogą mailową).

  - Wizualizacja: dostarczenie i spersonalizowanie graficznych paneli menedżerskich (dashboards), raportów oraz wizualizacji zdarzeń bezpieczeństwa dopasowanych do potrzeb Zamawiającego.

  - Zgodność z przepisami: konfiguracja raportów i mechanizmów umożliwiających Zamawiającemu spełnienie wymagań sprawozdawczych i audytowych wynikających z aktualnych przepisów prawa (w tym dyrektywy NIS2, ustawy o Krajowym Systemie Cyberbezpieczeństwa – KSC, Krajowych Ram Interoperacyjności – KRI).

  - Retencja danych: konfiguracja czasu przechowywania (retencji) logów surowych oraz poindeksowanych zgodnie z wytycznymi i polityką bezpieczeństwa wskazaną przez Zamawiającego.

  - Interakcja systemowa: konfiguracja wzajemnej korelacji danych pomiędzy SIEM a innymi komponentami bezpieczeństwa (UTM, EDR/XDR, NMS).
- Wymagania dotyczące środowiska systemowego: W przypadku, gdy oferowane oprogramowanie klasy SIEM lub któryś z jego składników wymaga do poprawnej instalacji i stabilnego działania w modelu On-Premise dedykowanego systemu operacyjnego klasy serwerowej, dedykowanej bazy danych itp. - wykonawca zobowiązany jest dołączyć do oferty i dostarczyć w cenie niezbędną liczbę komercyjnych, wieczystych licencji pokrywających potrzeby oferowanego rozwiązania SIEM.
- Zakres usług wdrożeniowych, konfiguracyjnych i szkoleniowych:

  - Instalacja i uruchomienie kompletnej architektury serwerowej SIEM w środowisku wirtualnym Zamawiającego przez Wykonawcę.

- Instalacja, konfiguracja i uruchomienie agentów SIEM na stacjach roboczych oraz serwerach Zamawiającego.
- Skonfigurowanie zbierania logów metodą bezagentową (syslog/SNMP) z posiadanych przez Zamawiającego urządzeń sieciowych oraz firewalli UTM.
- Dostrojenie (tuning) reguł korelacji w celu eliminacji fałszywych alarmów (False Positives) oraz konfiguracja powiadomień mailowych o alertach o wysokim priorytecie.
- Przygotowanie dedykowanych paneli (dashboards) dla administratora oraz wygenerowanie raportów zgodności z wybranym standardem bezpieczeństwa.
- Przygotowanie i przekazanie szczegółowej dokumentacji powdrożeniowej, schematów oraz opisów wdrożonych scenariuszy użycia (use-case) w języku polskim.
- Przeprowadzenie praktycznego szkolenia (min. 8 godzin zegarowych) dla administratorów Zamawiającego z zakresu obsługi konsoli, interpretacji alertów i dodawania nowych źródeł danych.
- Zapewnienie oficjalnego wsparcia technicznego producenta oraz prawa do bezpłatnych aktualizacji systemu i sygnatur przez okres minimum 24 miesiące od dnia odbioru.

Dokumentacja: Przygotowanie i przekazanie Zamawiającemu szczegółowej dokumentacji w języku polskim, zawierającej: potwierdzenie zgodności rozwiązania z przepisami ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20 z późn. zm.), opis techniczny wdrożonego oprogramowania.

Pakiet 7

16) Dostawa, instalacja, konfiguracja oraz przeprowadzenie szkolenia dla systemu klasy NMS (Network Management System):

- Okres i model licencjonowania: dostawa systemu klasy NMS do monitorowania infrastruktury IT , licencja na okres nie krótszy niż 24 miesięcy, wolna od opłat licencyjnych za liczbę monitorowanych hostów, sensorów, użytkowników oraz wielkość bazy danych. Wsparcie techniczne producenta (w zakresie aktualizacji oprogramowania) musi być zapewnione na okres minimum 24 miesiące od dnia odbioru.
- Architektura i komponenty systemu (On-Premise): system musi umożliwiać pełną instalację lokalną w środowisku wirtualizacji (Vmware) Zamawiającego (On-Premise) i składać się z dedykowanego serwera monitoringu wydajnej relacyjnej bazy danych oraz interfejsu WWW do zarządzania i wizualizacji.
- Kluczowe funkcjonalności techniczne:
  - Monitoring w czasie rzeczywistym serwerów (Windows, Linux), urządzeń sieciowych (switche, routery, UTM), macierzy NAS oraz środowisk wirtualnych (VMware).
  - Obsługa różnorodnych metod zbierania danych: dedykowane agenty (protokoły bezagentowe (SNMP v1/v2c/v3, ICMP, IPMI, JMX, HTTP) oraz bezpośrednie zapytania do baz danych.
  - Silnik wykrywania anomalii oparty o progi elastyczne, wyrażenia regularne oraz mechanizmy analizy trendów (predykcja zapełnienia dysków).

- Automatyczne wykrywanie urządzeń w sieci (Network Autodiscovery) i automatyczne przypisywanie szablonów monitoringu na podstawie typu urządzenia.

- System powiadomień (alerty) zintegrowany z wieloma kanałami (e-mail, SMS, komunikatory internetowe) z obsługą eskalacji (jeśli problem nie zostanie rozwiązany w określonym czasie, powiadomienie trafia do kolejnej osoby).

- Wymagania dotyczące środowiska systemowego (Licencja): W przypadku, gdy oferowane oprogramowanie klasy NMS lub któryś z jego składników wymaga do poprawnej instalacji i stabilnego działania w modelu On-Premise dedykowanego systemu operacyjnego klasy serwerowej, dedykowanej bazy danych itp. - wykonawca zobowiązany jest dołączyć do oferty i dostarczyć w cenie niezbędną liczbę komercyjnych, wieczystych licencji pokrywających potrzeby oferowanego rozwiązania NMS
- Zakres usług wdrożeniowych, konfiguracyjnych i szkoleniowych:

- Instalacja, uruchomienie oraz optymalizacja (tuning bazy danych pod kątem liczby operacji zapisu na sekundę – NVPS) serwera monitoringu NMS w środowisku Zamawiającego.

- Konfiguracja monitoringu dla kluczowej infrastruktury Zamawiającego obejmująca minimum: 3 serwerów fizycznych, 10 wirtualnych, 11 przełączników sieciowych, firewalli UTM oraz macierzy NAS.

- Skonfigurowanie dedykowanych ekranów statusowych (Maps / Dashboards) przedstawiających topologię sieci Zamawiającego oraz stan zdrowia kluczowych usług.

- Skonfigurowanie reguł alarmowania (progi ostrzeżeń i awarii) oraz integracja z systemem pocztowym Zamawiającego w celu wysyłki alertów.

- Przygotowanie dokumentacji powdrożeniowej (instrukcja dodawania hostów, opisy zastosowanych szablonów, schemat bazy) w języku polskim.

- Przeprowadzenie praktycznego szkolenia (min. 8 godzin zegarowych) dla administratorów Zamawiającego z zakresu konfiguracji szablonów, tworzenia map sieci, zarządzania użytkownikami i odczytu wykresów wydajnościowych.

Dokumentacja: Przygotowanie i przekazanie Zamawiającemu szczegółowej dokumentacji w języku polskim, zawierającej: potwierdzenie zgodności rozwiązania z przepisami ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20 z późn. zm.), opis techniczny wdrożonego oprogramowania.