EKOPRZEDSIĘBIORSTWO Sp. z o.o.
ul. gen. Stanisława Maczka 44, 76-032 Mielno
NIP 4990555465 · REGON 320419702

OPIS PRZEDMIOTU ZAMÓWIENIA

„Dostawa, wdrożenie i usługi z zakresu cyberbezpieczeństwa dla EKOPRZEDSIĘBIORSTWA Sp. z o.o. w Mielnie”

postępowanie nr ZR-EKO/1009/44-10/2026

Zamówienie obejmuje dwa ściśle zintegrowane zadania. Zamawiający nie dopuszcza składania ofert częściowych z przyczyn wskazanych w SWZ i pkt 1.2 OPZ.

Zadanie 1 – Obszar techniczny IT

Zadanie 2 – Obszar techniczny OT

Finansowane ze środków KPO – inwestycja C3.1.1 CyberPL, Konkurs Grantowy „Cyberbezpieczne Wodociągi”

Mielno, listopad 2026 r.

Signed by / Podpisano przez:
WIOLETTA DYMECKA
Date / Data: 2026-11-19 08:52

Spis treści

1. Postanowienia ogólne 4
1.1. Przedmiot zamówienia i definicje 4
1.2. Zakres zamówienia – zadania i pozycje 4
1.3. Charakterystyka środowiska Zamawiającego 7
1.4. Terminy 7
2. Wymagania wspólne dla wszystkich zadań 9
2.1. Wymagania ogólne 9
2.2. Wymagania dla dostaw sprzętu, oprogramowania i świadczeń okresowych 10
2.3. Rozwiązania równoważne 11
2.4. Wymagania wspólne dla wdrożeń 11
2.4.1. Zakres wdrożenia 11
2.4.2. Wsparcie powdrożeniowe, instruktaże i pule godzin 12
2.5. Wymagania wobec personelu Wykonawcy 12
2.6. Pozycje wydłużenia świadczeń okresowych do 36 miesięcy 13
3. Zadanie 1 – Obszar techniczny IT 14
3.1. Architektura docelowa 14
3.2. Bezpieczeństwo sieci 14
Poz. 1.1 – Firewall sieciowy klasy NGFW/UTM – dostawa urządzenia wraz z pakietem subskrypcji ochronnych (klasy UTM) i wsparciem producenta 14
Poz. 1.9 – Wdrożenie i konfiguracja firewalla NGFW/UTM (poz. 1.1) jako urządzenia brzegowego sieci Zamawiającego 18
Poz. 1.10 – Wdrożenie i konfiguracja VPN na firewallu – tunele do obiektów oraz dostęp zdalny z uwierzytelnianiem wieloskładnikowym 20
Poz. 1.20 – Przygotowanie firewalla do pracy w konfiguracji wysokiej dostępności (HA) i redundancji łączy WAN 21
Poz. 1.12 – Segmentacja sieci – konfiguracja podsieci VLAN/LAN na firewallu i przełącznikach 22
Poz. 1.11 – Hardening urządzeń sieciowych (firewall, przełączniki, sieć bezprzewodowa) 22
Poz. 1.14 – Wdrożenie WPA3-Enterprise (802.1X) na kontrolerze i punktach dostępowych sieci bezprzewodowej 23
Poz. 1.21 – Funkcja sandbox dla ruchu przeglądarek WWW – analiza inline plików na firewallu (licencja usługi sandbox i konfiguracja) 24
3.3. Infrastruktura serwerowa, pamięć masowa i kopie zapasowe 25
Poz. 1.16 – Serwer fizyczny do systemu wirtualizacji z lokalną pamięcią masową (w tym przygotowanie do usług HA) – dostawa 25
Poz. 1.15 – System wirtualizacji – licencja systemu operacyjnego serwera z rolą hypervisora (Windows Server 2025 Standard, 16 rdzeni, lub równoważna) 27
Poz. 1.2 – Macierz dyskowa NAS nr 1 (rack, 12 kieszeni) wraz z 8 dyskami HDD klasy enterprise 16 TB – dostawa 28
Poz. 1.17 – Macierz dyskowa NAS nr 2 – dedykowana stacja kopii zapasowych maszyn wirtualnych i serwerów z deduplikacją – dostawa 30
Poz. 1.4 – Oprogramowanie do kopii zapasowych maszyn wirtualnych i serwerów z deduplikacją – licencja na 10 instancji 30
Poz. 1.18 – Chroniony kryptograficznie backup w chmurze – repozytorium kopii zapasowych o pojemności 8 TB 31
Poz. 1.19 – Konfiguracja redundancji macierzy NAS – replikacja danych pomiędzy macierzą NAS nr 1 i NAS nr 2 32
Poz. 1.13 – Usługa instalacji, konfiguracji i wsparcia serwera, platformy wirtualizacji, macierzy NAS oraz systemu kopii zapasowych 32
Poz. 1.3 – UPS centralny 10 kVA (on-line, 3/3) z kartą zarządzającą – dostawa, instalacja i uruchomienie 35

3.4. Systemy bezpieczeństwa i monitorowania 36
Poz. 1.5 – Platforma XDR/EDR (open source) – wdrożenie ochrony punktów końcowych IT 36
Poz. 1.22 – Scentralizowany serwer logów – menedżer logów / SIEM (open source) – wdrożenie 38
Poz. 1.6 – System monitoringu infrastruktury IT/OT (Zabbix lub równoważny) – wdrożenie 39
Poz. 1.7 – Zapora aplikacyjna WAF (open source) dla systemu eBOK – wdrożenie 40
Poz. 1.8 – Hardening konfiguracji systemów operacyjnych serwerów i stacji roboczych oraz usługi katalogowej Active Directory 41
3.5. Tożsamość i dostęp 43
Poz. 1.23 – Kryptograficzny menedżer haseł (open source, on-premise) – wdrożenie 43
Poz. 1.24 – Wdrożenie uwierzytelniania dwuskładnikowego (2FA/MFA) we wszystkich systemach wspierających tę funkcję, w tym centralnego dostawcy tożsamości 44
Poz. 1.25 – Klucze sprzętowe U2F/FIDO2 – dostawa 23 szt. wraz z wdrożeniem 45
4. Zadanie 2 – Obszar techniczny OT 47
4.1. Ochrona punktów końcowych OT 47
Poz. 2.1 – System EDR dla sieci przemysłowych – ochrona punktów końcowych środowiska OT (serwer SCADA, stanowiska dyspozytorskie) 47
4.2. System monitorowania sieci przemysłowej (IDS OT) – poz. 2.2, 2.3, 2.4 i 2.5 48
4.3. Urządzenia UTM dla obiektów technologicznych 51
Poz. 2.6 – Urządzenia klasy NGFW/UTM dla obiektów technologicznych OT – dostawa, instalacja i konfiguracja (ze wsparciem producenta) 51

1. Postanowienia ogólne

1.1. Przedmiot zamówienia i definicje

Przedmiotem zamówienia jest dostawa, wdrożenie i usługi z zakresu cyberbezpieczeństwa dla EKOPRZEDSIĘBIORSTWA Sp. z o.o. w Mielnie, przedsiębiorstwa wodociągowo-kanalizacyjnego objętego przepisami ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Zamówienie obejmuje dwa zadania: obszar techniczny IT oraz obszar techniczny OT.

Użyte w OPZ określenia oznaczają:

1. Zamawiający – EKOPRZEDSIĘBIORSTWO Sp. z o.o. z siedzibą w Mielnie.
2. Wykonawca – podmiot składający ofertę, a po zawarciu umowy – podmiot realizujący zamówienie.
3. Pozycja – wyodrębniony element przedmiotu zamówienia wskazany w wykazie w pkt 1.2, oznaczony numerem zadania i liczbą porządkową.
4. Firewall – urządzenie klasy NGFW/UTM dostarczane w poz. 1.1, o ile z kontekstu nie wynika inaczej.
5. Dostawca automatyki – podmiot utrzymujący system SCADA i telemetrii Zamawiającego.
6. Strefa pośrednia IT/OT – wydzielony segment sieci (DMZ przemysłowa) pośredniczący w komunikacji między środowiskiem IT i OT.
7. Okno serwisowe – uzgodniony z Zamawiającym przedział czasu, w którym dopuszcza się prace mogące zakłócić pracę systemów.
8. Dzień roboczy – dzień od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy.
9. Godzina – godzina zegarowa (60 minut).
10. Świadczenia okresowe – gwarancja i serwis producenta, wsparcie techniczne producenta, licencje subskrypcyjne, aktualizacje, usługi chmurowe oraz wsparcie powdrożeniowe Wykonawcy, świadczone przez określony czas od dnia odbioru pozycji.

1.2. Zakres zamówienia – zadania i pozycje

1. Zamówienie stanowi jedną funkcjonalnie zintegrowaną całość i obejmuje dwa zadania.
2. Zamawiający nie dopuszcza składania ofert częściowych. Integracje pomiędzy Zadaniem 1 i Zadaniem 2 obejmują w szczególności wspólną infrastrukturę wirtualizacyjną, serwer logów, monitoring, MFA, strefę pośrednią IT/OT oraz współpracę urządzeń brzegowych i systemu IDS OT. Wykonawca odpowiada za kompatybilność i spójność całej architektury.
3. Oferta obejmująca tylko niektóre zadania lub pozycje zostanie odrzucona.
4. Zamówienie jest realizowane na podstawie jednej umowy.
5. Odbiór następuje dla pozycji lub grupy pozycji w ramach jednego zadania. Protokół odbioru wskazuje odrębnie każdą odebraną pozycję. Dla poz. 2.6 dopuszcza się odbiory częściowe dla poszczególnych obiektów.
6. Każda pozycja jest wyceniana odrębnie w Formularzu ofertowym. Dla pozycji wskazanych w wykazie poniżej wydłużenie świadczeń okresowych do 36 miesięcy stanowi odrębną pozycję oznaczoną literą W (np. poz. 1.1W dla poz. 1.1), wycenianą w części IV Formularza ofertowego i wliczaną do ceny oferty (pkt 2.6).
7. Fakturowanie i płatność odbywają się zgodnie z § 8 wzoru umowy. Każda faktura i protokół identyfikują pozycje OPZ i ich wartości w sposób umożliwiający przypisanie wydatku do zakresu projektu.

Wykaz pozycji przedmiotu zamówienia:

Poz.	Nazwa pozycji	J.m.	Ilość
Zadanie 1 – Obszar techniczny IT			
1.1	Firewall sieciowy klasy NGFW/UTM – dostawa urządzenia wraz z pakietem subskrypcji ochronnych (klasy UTM) i wsparciem producenta	kpl.	1
1.2	Macierz dyskowa NAS nr 1 (rack, 12 kieszeni) wraz z 8 dyskami HDD klasy enterprise 16 TB – dostawa	kpl.	1
1.3	UPS centralny 10 kVA (on-line, 3/3) z kartą zarządzającą – dostawa, instalacja i uruchomienie	kpl.	1
1.4	Oprogramowanie do kopii zapasowych maszyn wirtualnych i serwerów z deduplikacją – licencja na 10 instancji	kpl.	1
1.5	Platforma XDR/EDR (open source) – wdrożenie ochrony punktów końcowych IT	kpl.	1
1.6	System monitoringu infrastruktury IT/OT (Zabbix lub równoważny) – wdrożenie	kpl.	1
1.7	Zapora aplikacyjna WAF (open source) dla systemu eBOK – wdrożenie	kpl.	1
1.8	Hardening konfiguracji systemów operacyjnych serwerów i stacji roboczych oraz usługi katalogowej Active Directory	usługa	1
1.9	Wdrożenie i konfiguracja firewalla NGFW/UTM (poz. 1.1) jako urządzenia brzegowego sieci Zamawiającego	usługa	1
1.10	Wdrożenie i konfiguracja VPN na firewallu – tunele do obiektów oraz dostęp zdalny z uwierzytelnianiem wieloskładnikowym	usługa	1
1.11	Hardening urządzeń sieciowych (firewall, przełączniki, sieć bezprzewodowa)	usługa	1
1.12	Segmentacja sieci – konfiguracja podsieci VLAN/LAN na firewallu i przełącznikach	usługa	1
1.13	Usługa instalacji, konfiguracji i wsparcia serwera, platformy wirtualizacji, macierzy NAS oraz systemu kopii zapasowych	usługa	1
1.14	Wdrożenie WPA3-Enterprise (802.1X) na kontrolerze i punktach dostępowych sieci bezprzewodowej	usługa	1
1.15	System wirtualizacji – licencja systemu operacyjnego serwera z rolą hypervisora (Windows Server 2025 Standard, 16 rdzeni, lub równoważna)	kpl.	1
1.16	Serwer fizyczny do systemu wirtualizacji z lokalną pamięcią masową (w tym przygotowanie do usług HA) – dostawa	szt.	1
1.17	Macierz dyskowa NAS nr 2 – dedykowana stacja kopii zapasowych maszyn wirtualnych i serwerów z deduplikacją – dostawa	kpl.	1
1.18	Chroniony kryptograficznie backup w chmurze – repozytorium kopii zapasowych o pojemności 8 TB	kpl.	1
1.19	Konfiguracja redundancji macierzy NAS – replikacja danych pomiędzy macierzą NAS nr 1 i NAS nr 2	usługa	1
1.20	Przygotowanie firewalla do pracy w konfiguracji wysokiej dostępności (HA) i redundancji łączy WAN	usługa	1
1.21	Funkcja sandbox dla ruchu przeglądarek WWW – analiza inline plików na firewallu (licencja usługi sandbox i konfiguracja)	kpl.	1
1.22	Scentralizowany serwer logów – menedżer logów / SIEM (open source) – wdrożenie	kpl.	1
1.23	Kryptograficzny menedżer haseł (open source, on-premise) – wdrożenie	kpl.	1
1.24	Wdrożenie uwierzytelniania dwuskładnikowego (2FA/MFA) we wszystkich systemach wspierających tę funkcję, w tym centralnego dostawcy tożsamości	usługa	1
1.25	Klucze sprzętowe U2F/FIDO2 – dostawa 23 szt. wraz z wdrożeniem	kpl.	1
Zadanie 1 – pozycje wydłużenia świadczeń okresowych do 36 miesięcy (pkt 2.6)			
1.1W	Wydłużenie subskrypcji ochronnych (klasy UTM), wsparcia technicznego i gwarancji producenta firewalla NGFW/UTM (poz. 1.1) do 36 miesięcy od dnia odbioru	kpl.	1
1.2W	Wydłużenie gwarancji i serwisu producenta macierzy NAS nr 1 wraz z dyskami (poz. 1.2) do 36 miesięcy od dnia odbioru	kpl.	1

Poz.	Nazwa pozycji	J.m.	Ilość
1.3W	Wydłużenie gwarancji i serwisu producenta UPS centralnego wraz z bateriami i kartą zarządzającą (poz. 1.3) do 36 miesięcy od dnia odbioru	kpl.	1
1.4W	Wydłużenie subskrypcji i wsparcia producenta oprogramowania do kopii zapasowych dla 10 instancji (poz. 1.4) do 36 miesięcy od dnia odbioru	kpl.	1
1.5W	Wydłużenie wsparcia powdrożeniowego i utrzymania platformy XDR/EDR (poz. 1.5) do 36 miesięcy od dnia odbioru	kpl.	1
1.6W	Wydłużenie wsparcia powdrożeniowego i utrzymania systemu monitoringu infrastruktury IT/OT (poz. 1.6) do 36 miesięcy od dnia odbioru	kpl.	1
1.7W	Wydłużenie wsparcia powdrożeniowego i utrzymania zapory aplikacyjnej WAF dla systemu eBOK (poz. 1.7) do 36 miesięcy od dnia odbioru	kpl.	1
1.16W	Wydłużenie gwarancji i serwisu producenta serwera fizycznego w miejscu instalacji (poz. 1.16) do 36 miesięcy od dnia odbioru	szt.	1
1.17W	Wydłużenie gwarancji i serwisu producenta macierzy NAS nr 2 wraz z dyskami (poz. 1.17) do 36 miesięcy od dnia odbioru	kpl.	1
1.18W	Wydłużenie usługi chmurowego repozytorium kopii zapasowych o pojemności 8 TB (poz. 1.18) do 36 miesięcy od dnia odbioru	kpl.	1
1.21W	Wydłużenie licencji usługi sandbox inline na firewallu (poz. 1.21) do 36 miesięcy od dnia odbioru	kpl.	1
1.23W	Wydłużenie wsparcia powdrożeniowego i utrzymania menedżera haseł (poz. 1.23) do 36 miesięcy od dnia odbioru	kpl.	1
Zadanie 2 – Obszar techniczny OT			
2.1	System EDR dla sieci przemysłowych – ochrona punktów końcowych środowiska OT (serwer SCADA, stanowiska dyspozytorskie)	kpl.	1
2.2	System IDS dla sieci OT – licencja wieczysta oprogramowania do monitorowania i analizy ruchu w sieci przemysłowej (z aktualizacjami do 31 grudnia 2026 r.)	kpl.	1
2.3	Sprzętowa sonda do monitorowania sieci OT (analiza protokołów przemysłowych) – dostawa	szt.	1
2.4	Utrzymanie i eksploatacja systemu IDS OT – serwis gwarancyjny, wsparcie eksploatacyjne i przegląd do 31 grudnia 2026 r.	usługa	1
2.5	Wdrożenie systemu IDS OT – instalacja, konfiguracja, integracja, testy, dokumentacja i szkolenie	usługa	1
2.6	Urządzenia klasy NGFW/UTM dla obiektów technologicznych OT – dostawa, instalacja i konfiguracja (ze wsparciem producenta)	szt.	4
Zadanie 2 – pozycje wydłużenia świadczeń okresowych do 36 miesięcy (pkt 2.6)			
2.1W	Wydłużenie wsparcia powdrożeniowego i utrzymania ochrony EDR punktów końcowych OT (poz. 2.1) do 36 miesięcy od dnia odbioru	kpl.	1
2.2W	Wydłużenie aktualizacji i wsparcia producenta do licencji wieczystej systemu IDS OT (poz. 2.2) do 36 miesięcy od dnia odbioru	kpl.	1
2.3W	Wydłużenie gwarancji i serwisu producenta sprzętowej sondy IDS OT (poz. 2.3) do 36 miesięcy od dnia odbioru	szt.	1
2.4W	Wydłużenie utrzymania i eksploatacji systemu IDS OT – serwis gwarancyjny, wsparcie eksploatacyjne i coroczny przegląd (poz. 2.4) do 36 miesięcy od dnia odbioru	usługa	1
2.6W	Wydłużenie wsparcia producenta urządzeń NGFW/UTM dla obiektów OT – serwis gwarancyjny z wymianą wyprzedzającą, aktualizacje i wsparcie 24x7 (poz. 2.6) do 36 miesięcy od dnia odbioru	szt.	4

Numer pozycji składa się z numeru zadania i liczby porządkowej pozycji w zadaniu. Litera W po numerze oznacza pozycję wydłużenia świadczeń okresowych pozycji podstawowej o tym numerze (pkt 2.6).

1.3. Charakterystyka środowiska Zamawiającego

Publiczny opis środowiska zawiera wyłącznie informacje niezbędne do przygotowania oferty. Szczegółowy opis aktualnej architektury, konfiguracji, topologii, zabezpieczeń i podatności stanowi Załącznik nr 1A – Poufny opis środowiska Zamawiającego, udostępniany zainteresowanym Wykonawcom na równych zasadach po podpisaniu zobowiązania do zachowania poufności zgodnie z SWZ.

1. Siedziba Zamawiającego: 76-032 Mielno, ul. gen. Stanisława Maczka 44. W siedzibie znajdują się pomieszczenia biurowe, serwerownia i dyspozytornia.
2. Zamawiający eksploatuje rozproszoną infrastrukturę wodociągowo-kanalizacyjną i obiekty technologiczne połączone z siedzibą za pomocą rozwiązań transmisji danych. Informacje o lokalizacjach, połączeniach i topologii udostępniane są w Załączniku nr 1A.
3. Środowisko użytkowników obejmuje stacje robocze i stanowiska operatorskie w skali określonej w wymaganiach szczegółowych OPZ.
4. Liczba użytkowników i administratorów istotna dla licencjonowania została wskazana w odpowiednich pozycjach OPZ; dodatkowe informacje organizacyjne zawiera Załącznik nr 1A.
5. Środowisko serwerowe obejmuje serwery fizyczne i wirtualne realizujące usługi katalogowe, plikowe, systemy dziedzinowe oraz systemy OT. Szczegółowa konfiguracja i role serwerów są informacją poufną i znajdują się w Załączniku nr 1A.
6. Zamawiający wykorzystuje usługę katalogową Active Directory. Szczegóły domeny i kontrolerów udostępniane są w Załączniku nr 1A.
7. Zamawiający wykorzystuje lokalne zasoby pamięci masowej i rozwiązania kopii zapasowych. Szczegółowy stan istniejący, w tym architektura backupu, jest opisany w Załączniku nr 1A.
8. Zamawiający posiada urządzenia brzegowe i połączenia WAN/VPN. Szczegółowe modele, konfiguracja i liczba aktywnych kont zdalnych są opisane w Załączniku nr 1A.
9. Sieć przewodowa obejmuje przełączniki zarządzalne i elementy infrastruktury obiektowej; szczegóły topologii znajdują się w Załączniku nr 1A.
10. Sieć bezprzewodowa obejmuje kontroler i punkty dostępowe; informacje szczegółowe znajdują się w Załączniku nr 1A.
11. Obecna segmentacja sieci oraz planowane strefy bezpieczeństwa są opisane w wymaganiach wdrożeniowych i Załączniku nr 1A.
12. Zamawiający wykorzystuje centralnie zarządzane rozwiązanie ochrony punktów końcowych; szczegóły środowiska znajdują się w Załączniku nr 1A.
13. Środowisko OT obejmuje system SCADA/telemetrii, stanowiska operatorskie, sterowniki PLC i moduły telemetryczne. Zmiany w systemie SCADA wymagają współpracy z dostawcą automatyki. Szczegółowy wykaz i topologia są udostępniane w Załączniku nr 1A.
14. Zamawiający publikuje wybrane usługi internetowe wymagające ochrony aplikacyjnej; szczegóły konfiguracji są udostępniane w Załączniku nr 1A.
15. Utrzymanie środowiska odbywa się z udziałem personelu Zamawiającego i podmiotów zewnętrznych; Wykonawca jest zobowiązany do koordynacji prac zgodnie z pkt 2.1.

1.4. Terminy

1. Wszystkie dostawy, wdrożenia, instruktaże, przekazanie dokumentacji i odbiór wszystkich pozycji podstawowych zostaną zrealizowane do dnia 18 grudnia 2026 r.
2. Realizacja, fakturowanie i zapłata muszą nastąpić w okresie kwalifikowalności wydatków projektu, który upływa w dniu 31 grudnia 2026 r.

3. Faktury dotyczące zakresu rozliczanego w 2026 r. są wystawiane niezwłocznie po odbiorze końcowym, nie później niż do dnia 21 grudnia 2026 r., tak aby płatność mogła nastąpić do dnia 31 grudnia 2026 r.
4. Świadczenia o charakterze okresowym (gwarancja, wsparcie producenta, subskrypcje, usługi chmurowe, wsparcie powdrożeniowe) są realizowane w zakresie podstawowym od dnia odbioru danej pozycji do dnia 31 grudnia 2026 r., zgodnie z pkt 2.2. Dla pozycji wskazanych w pkt 1.2 wydłużenie tych świadczeń do 36 miesięcy od dnia odbioru stanowi odrębne pozycje W (pkt 2.6).
5. Dostawa urządzeń i licencji następuje zgodnie z harmonogramem, w terminie umożliwiającym odbiór zakresu podstawowego do dnia 18 grudnia 2026 r.
6. Szczegółowy harmonogram realizacji Wykonawca przedstawi w terminie 3 dni od zawarcia umowy. Prace w poszczególnych zadaniach powinny być prowadzone równolegle w zakresie, w jakim pozwalają na to zależności techniczne.

2. Wymagania wspólne dla wszystkich zadań

2.1. Wymagania ogólne

1. Usługi, dokumentacja (w tym powykonawcza) oraz materiały instruktażowe są realizowane i przekazywane w języku polskim. Dokumentację producenta sprzętu i oprogramowania dopuszcza się w języku angielskim wyłącznie wtedy, gdy producent nie udostępnia jej w języku polskim.
2. Dokumentację Wykonawca przekazuje w formie edytowalnej (co najmniej .docx lub .xlsx), umożliwiającej samodzielną aktualizację przez Zamawiającego.
3. Dokumenty opracowane przez Wykonawcę i przekazywane w postaci elektronicznej (dokumentacja, raporty, materiały instruktażowe, prezentacje, w tym pliki PDF) muszą być dostępne cyfrowo zgodnie z WCAG 2.1 na poziomie AA. Wymóg nie dotyczy dokumentacji producentów.
4. Prace są realizowane w siedzibie i obiektach Zamawiającego. Praca zdalna jest dopuszczalna w uzasadnionych przypadkach, po uzgodnieniu z Zamawiającym.
5. Zdalny dostęp Wykonawcy do infrastruktury odbywa się wyłącznie przez VPN Zamawiającego, na imienne konta, z uwierzytelnianiem wieloskładnikowym. Dostęp jest rejestrowany.
6. Stosowanie przez Wykonawcę własnych narzędzi zdalnego dostępu bez pisemnej zgody Zamawiającego jest niedopuszczalne.
7. Prace mogące wpłynąć na ciągłość świadczenia usług wodociągowo-kanalizacyjnych lub pracę systemów Zamawiającego (w szczególności w środowisku OT, na styku sieci IT/OT, na urządzeniach brzegowych, przy migracji serwerów i danych) Wykonawca realizuje wyłącznie w oknach serwisowych uzgodnionych z Zamawiającym.
8. Przed pracami w oknie serwisowym Wykonawca przedstawia plan prac oraz plan wycofania zmian.
9. Przed każdą zmianą konfiguracji Wykonawca wykonuje i zabezpiecza kopię konfiguracji bieżącej.
10. Wykonawca współpracuje z dotychczasowymi dostawcami usług IT, systemów dziedzinowych i automatyki Zamawiającego w zakresie niezbędnym do realizacji zamówienia.
11. Wykonawca odpowiada za integrację rozwiązań dostarczanych w ramach wszystkich zadań w spójną całość, w tym za integrację z serwerem logów, systemem monitoringu i systemem MFA.
12. Wykonawca planuje kolejność wdrożeń tak, aby rozwiązania, od których zależą kolejne pozycje, były dostępne w chwili ich wdrażania. Integracje z rozwiązaniami uruchomionymi później Wykonawca wykonuje niezwłocznie po ich uruchomieniu, przed odbiorem końcowym.
13. Jeżeli element infrastruktury nie jest dostępny w terminie z przyczyn niezależnych od Wykonawcy, Wykonawca niezwłocznie zgłasza to Zamawiającemu wraz z dowodami i propozycją rozwiązania zastępczego. Zastosowanie zasobów zastępczych wymaga uprzedniej zgody Zamawiającego i nie zwalnia z obowiązku dotrzymania końcowego terminu realizacji, chyba że termin zostanie zmieniony zgodnie z umową.
14. Opóźnienie wynikające z przyczyn leżących po stronie Zamawiającego lub dostawcy automatyki stanowi podstawę do zmiany terminu realizacji pozycji, nie później jednak niż do dnia 18 grudnia 2026 r.
15. Dane uwierzytelniające (hasła, klucze, certyfikaty) Wykonawca przekazuje Zamawiającemu odrębnym, bezpiecznym kanałem, a po zakończeniu prac usuwa je ze swoich zasobów.
16. Konta wykorzystywane przez Wykonawcę w trakcie wdrożenia są dezaktywowane przy odbiorze końcowym, chyba że Zamawiający postanowi inaczej.
17. Wykonawca zachowuje w poufności wszystkie informacje pozyskane w postępowaniu i podczas realizacji zamówienia. Szczegółowe informacje o środowisku przed złożeniem oferty są udostępniane na zasadach

określonych w SWZ po podpisaniu zobowiązania do zachowania poufności, a po zawarciu umowy obowiązek poufności wynika również z § 15 umowy.

18. Jeżeli realizacja zamówienia wiąże się z przetwarzaniem danych osobowych w imieniu Zamawiającego, Wykonawca przed rozpoczęciem takiego przetwarzania zawiera z Zamawiającym umowę powierzenia przetwarzania danych zgodną z art. 28 RODO.
19. Wykonawca nie może wykorzystywać informacji o Zamawiającym w materiałach referencyjnych bez jego pisemnej zgody.
20. Wykonawca przenosi na Zamawiającego autorskie prawa majątkowe do utworów wytworzonych na potrzeby realizacji zamówienia w zakresie określonym w umowie, a jeżeli przeniesienie praw nie jest możliwe – udziela odpowiedniej licencji na warunkach określonych w umowie. Oprogramowanie producentów i open source pozostaje na warunkach właściwych licencji.
21. Wykonawca wyznacza kierownika realizacji zamówienia odpowiedzialnego za kontakt z Zamawiającym, harmonogram i raportowanie postępu oraz koordynatorów technicznych dla Zadania 1 i Zadania 2.
22. Wykonawca przekazuje Zamawiającemu cotygodniową informację o stanie realizacji.
23. Zamawiający akceptuje projekty techniczne i inne dokumenty podlegające akceptacji w terminie 2 dni roboczych od ich przekazania. Brak uwag w tym terminie oznacza akceptację.
24. Uwagi Zamawiającego Wykonawca uwzględnia w terminie 2 dni roboczych.
25. Odbiór pozycji lub grupy pozycji następuje na podstawie protokołu zdawczo-odbiorczego podpisanego przez obie strony, zgodnie z pkt 1.2.
26. Warunkiem odbioru pozycji technicznej jest pozytywny wynik testów opisanych w danej pozycji oraz przekazanie dokumentacji powykonawczej.

2.2. Wymagania dla dostaw sprzętu, oprogramowania i świadczeń okresowych

1. Dostarczane urządzenia są fabrycznie nowe, nieużywane, nieregenerowane i niepowystawowe, wyprodukowane nie wcześniej niż 12 miesięcy przed dostawą.
2. Urządzenia pochodzą z autoryzowanego kanału dystrybucji producenta na terenie Unii Europejskiej i reprezentują bieżącą linię produkcyjną. Na żądanie Zamawiającego Wykonawca przedstawia oświadczenie producenta lub autoryzowanego dystrybutora o pochodzeniu sprzętu.
3. Urządzenia są oznakowane w sposób umożliwiający identyfikację produktu i producenta.
4. Wraz z urządzeniami Wykonawca dostarcza wszystkie elementy niezbędne do instalacji i uruchomienia: szyny montażowe, okablowanie zasilające i sygnałowe, wkładki lub kable DAC, karty zarządzające – o ile w danej pozycji nie wskazano inaczej.
5. Oprogramowanie i licencje są nowe, legalne, przeznaczone na rynek Unii Europejskiej i zarejestrowane na Zamawiającego (w portalu producenta na konto Zamawiającego).
6. Dla oprogramowania open source Wykonawca dostarcza wersję stabilną, wspieraną przez społeczność lub producenta, i wskazuje w dokumentacji źródło oraz warunki licencji.
7. Wszystkie odpłatne świadczenia okresowe objęte zamówieniem (gwarancja i serwis producenta, wsparcie techniczne producenta, licencje subskrypcyjne, aktualizacje sygnatur i baz, usługi chmurowe, wsparcie powdrożeniowe Wykonawcy) są wymagane w zakresie podstawowym na okres od dnia odbioru (aktywacji) do dnia 31 grudnia 2026 r. i w tym zakresie są objęte ceną pozycji.
8. Dla pozycji wskazanych w pkt 1.2 wydłużenie świadczeń okresowych do 36 miesięcy od dnia odbioru pozycji stanowi odrębną pozycję W, wycenianą w części IV Formularza ofertowego i wliczaną do ceny oferty, zgodnie z pkt 2.6.

9. Jeżeli warunki producenta nie przewidują świadczenia kończącego się w dniu 31 grudnia 2026 r., Wykonawca oferuje w pierwszej kolejności model rozliczenia umożliwiający zakończenie świadczenia z tym dniem (licencje miesięczne, subskrypcje z wyrównaną datą zakończenia, rozliczenie według zużycia).
10. Jeżeli warunki producenta nie przewidują świadczenia kończącego się w dniu 31 grudnia 2026 r. (np. minimalny okres subskrypcji lub standardowa gwarancja producenta jest dłuższa), Wykonawca może zaoferować najkrótszy dostępny okres. Protokół odbioru i faktura wskazują rzeczywisty okres nabytego świadczenia. Standardowy, dłuższy okres gwarancji lub wsparcia producenta nie powoduje zwiększenia wynagrodzenia ponad cenę danej pozycji.
11. Licencje wieczyste są dopuszczalne, o ile w danej pozycji nie wskazano inaczej. Aktualizacje i wsparcie producenta do licencji wieczystej są wymagane w zakresie podstawowym do dnia 31 grudnia 2026 r., a dla pozycji objętych pozycją W – przez 36 miesięcy od dnia odbioru (pkt 2.6).
12. Wynagrodzenie za nabyte w 2026 r. prawa do Świadczeń okresowych, w tym za aktywowane Pozycje W, jest płatne zgodnie z § 8 umowy po spełnieniu warunków odbioru. Zapłata za Pozycję W potwierdza nabycie prawa do świadczenia w okresie przyszłym i nie stanowi potwierdzenia wykonania usług, które zgodnie z umową mają być świadczone po dniu zapłaty.
13. Świadczenia okresowe są aktywowane najpóźniej w dniu odbioru danej pozycji.
14. Wykonawca zapewnia ciągłość subskrypcji, wsparcia producenta i usług chmurowych w okresach objętych zamówieniem, bez wymiany sprzętu, utraty konfiguracji i opłat reaktywacyjnych. Warunki ewentualnych dalszych odnowień po zakończeniu okresów objętych zamówieniem nie są objęte ceną oferty.
15. Najpóźniej w dniu dostawy Wykonawca przekazuje Zamawiającemu wykaz numerów seryjnych urządzeń. Status gwarancji musi być możliwy do sprawdzenia na stronie producenta po numerze seryjnym.
16. Uszkodzone nośniki danych wymieniane w okresie gwarancji pozostają u Zamawiającego.
17. Wykonawca wskazuje w ofercie producenta, model (typ) i wersję oferowanych urządzeń i oprogramowania, a dla świadczeń okresowych – nazwę pakietu wsparcia lub subskrypcji producenta.
18. Parametry techniczne wskazane w OPZ są wymaganiami minimalnymi. Elementy oznaczone jako „zalecane” nie są wymagane i nie podlegają ocenie.
19. Parametry są weryfikowane na podstawie oficjalnej, publicznie dostępnej dokumentacji producenta. Jeżeli dokumentacja nie zawiera danego parametru, Wykonawca dostarcza oświadczenie producenta potwierdzające jego spełnienie.

2.3. Rozwiązania równoważne

1. Nazwy producentów, znaki towarowe, modele, typy rozwiązań i nazwy własne oprogramowania wskazane w OPZ określają wymagany standard jakościowy, funkcjonalny, techniczny lub wymóg kompatybilności z istniejącą infrastrukturą. Każde takie wskazanie należy rozumieć wraz z wyrazami „lub równoważny”, zgodnie z kryteriami określonymi w niniejszym punkcie i wymaganiach danej pozycji.
2. Każdemu takiemu wskazaniu towarzyszą wyrazy „lub równoważny”.
3. Za rozwiązanie równoważne uznaje się rozwiązanie spełniające wszystkie wymagania minimalne określone dla danej pozycji.
4. Rozwiązanie równoważne musi być w pełni kompatybilne z infrastrukturą Zamawiającego i z rozwiązaniami dostarczanymi w pozostałych pozycjach.
5. Rozwiązanie równoważne nie może powodować po stronie Zamawiającego dodatkowych kosztów koniecznych wyłącznie do uzyskania funkcjonalności już objętej OPZ. Jeżeli rozwiązanie równoważne wymaga migracji lub zmiany konfiguracji istniejących systemów, koszty i ryzyko tych prac obciążają Wykonawcę, o ile ich zakres był możliwy do ustalenia na podstawie dokumentacji postępowania i informacji poufnych udostępnionych przed terminem składania ofert.

6. Wykonawca oferujący rozwiązanie równoważne wykazuje w ofercie spełnienie wymagań zestawieniem parametrów z odwołaniem do oficjalnej dokumentacji producenta.
7. Wykonawca ponosi odpowiedzialność za skutki niezgodności rozwiązania równoważnego z pozostałymi elementami zamówienia.
8. W zakresie rozszerzenia lub rekonfiguracji rozwiązań posiadanych przez Zamawiającego równoważność oznacza możliwość współpracy z istniejącym środowiskiem albo przeprowadzenie przez Wykonawcę kompletnej migracji niezbędnego zakresu, bez utraty funkcjonalności i danych oraz bez dodatkowego wynagrodzenia, o ile zakres migracji wynikał z dokumentacji udostępnionej przed terminem składania ofert.
9. Dla rozwiązań określonych w OPZ jako open source Zamawiający dopuszcza rozwiązania komercyjne spełniające wymagania funkcjonalne danej pozycji, pod warunkiem dostarczenia licencji zgodnie z pkt 2.2, bez ograniczeń liczby urządzeń, użytkowników lub wolumenu danych poniżej wartości wymaganych w OPZ. Utrzymanie funkcjonalności po dniu 31 grudnia 2026 r. nie może wymagać ponoszenia przez Zamawiającego opłat licencyjnych (dopuszcza się odpłatne wsparcie producenta).
10. Wszelkie odwołania w OPZ do norm, standardów lub benchmarków należy rozumieć jako obejmujące również rozwiązania równoważne, zapewniające co najmniej taki sam poziom jakości, bezpieczeństwa, wydajności lub interoperacyjności, stosownie do celu danego wymagania.

2.4. Wymagania wspólne dla wdrożeń

2.4.1. Zakres wdrożenia

Dla każdej pozycji obejmującej instalację, konfigurację lub wdrożenie Wykonawca, o ile w pozycji nie wskazano inaczej:

1. przeprowadza analizę przedwdrożeniową i przedstawia jej wyniki Zamawiającemu w formie pisemnej przed przystąpieniem do prac,
2. opracowuje projekt techniczny wdrożenia (architektura logiczna i fizyczna, adresacja, polityki, integracje, plan migracji, plan wycofania zmian) podlegający akceptacji Zamawiającego,
3. dla Zadania 1 i Zadania 2 opracowuje jeden nadrzędny projekt techniczny obejmujący wszystkie pozycje danego zadania (architektura docelowa, strefy bezpieczeństwa, adresacja, macierz przepływów ruchu, integracje z serwerem logów, monitoringiem i MFA); projekty pozycji stanowią jego rozdziały,
4. aktualizuje oprogramowanie układowe i systemowe dostarczanych urządzeń do najnowszej stabilnej wersji rekomendowanej przez producenta na dzień wdrożenia,
5. konfiguruje rozwiązanie zgodnie z zasadami hardeningu, w zakresie wspieranym przez dane urządzenie lub oprogramowanie, co obejmuje co najmniej:
    a) wyłączenie zbędnych usług i interfejsów,
    b) szyfrowane protokoły zarządzania (HTTPS, SSH, SNMPv3),
    c) imienne konta administracyjne,
    d) uwierzytelnianie wieloskładnikowe dla dostępu administracyjnego,
    e) ograniczenie dostępu administracyjnego do strefy zarządzania,
    f) synchronizację czasu NTP,
6. dla urządzeń niewspierających SNMPv3 konfiguruje SNMP tylko do odczytu, ograniczony do serwera monitoringu,
7. konfiguruje przekazywanie logów do serwera logów (poz. 1.22) oraz obejmuje rozwiązanie monitoringiem w systemie z poz. 1.6,

8. przeprowadza testy poprawności działania określone w danej pozycji i dokumentuje ich wyniki w raporcie stanowiącym załącznik do protokołu odbioru,
9. opracowuje dokumentację powykonawczą (konfiguracja, schematy logiczne i fizyczne, wykaz kont i uprawnień, procedury administracyjne i odtworzeniowe, kopie konfiguracji) w formie edytowalnej,
10. przeprowadza instruktaż stanowiskowy administratorów Zamawiającego w wymiarze wskazanym w danej pozycji, nie mniejszym niż 2 godziny zegarowe, potwierdzony listą obecności,
11. zapewnia wsparcie powdrożeniowe (usuwanie błędów konfiguracyjnych, konsultacje, dostrajanie) od dnia odbioru do dnia 31 grudnia 2026 r., w ramach ceny pozycji; dla pozycji wskazanych w pkt 1.2 wydłużenie wsparcia do 36 miesięcy stanowi odrębną pozycję W (pkt 2.6).

2.4.2. Wsparcie powdrożeniowe, instruktaże i pule godzin

1. Zgłoszenia w ramach wsparcia powdrożeniowego są przyjmowane w dni robocze w godzinach 8:00–16:00.
2. Czas reakcji na zgłoszenie wynosi 1 dzień roboczy, a dla awarii uniemożliwiającej pracę systemu – 4 godziny w godzinach przyjmowania zgłoszeń.
3. Godziny instruktaży i konsultacji wskazane w pozycjach są godzinami zegarowymi.
4. Instruktaże i konsultacje są realizowane stacjonarnie lub zdalnie (synchronicznie), w terminach uzgodnionych z Zamawiającym.
5. Pule godzin konsultacji mogą być wykorzystywane od dnia zawarcia umowy do dnia 18 grudnia 2026 r. Wykonawca zapewnia ich dostępność w całym tym okresie w terminach uzgadnianych z Zamawiającym.
6. Wartość puli godzin jest objęta ceną pozycji. Wykonawca przekazuje raport wykorzystania puli wraz z protokołem odbioru pozycji oraz raport końcowy po upływie okresu jej dostępności. Niewykorzystanie części puli z przyczyn leżących po stronie Wykonawcy traktuje się jako niewykonanie odpowiedniej części świadczenia.

2.5. Wymagania wobec personelu Wykonawcy

1. Zadanie 1: co najmniej jeden inżynier z certyfikatem producenta oferowanego firewalla potwierdzającym kompetencje w zakresie konfiguracji polityk bezpieczeństwa, VPN i IPS na poziomie co najmniej „Professional” lub równoważnym w programie certyfikacji danego producenta.
2. Zadanie 1: co najmniej jedna osoba z doświadczeniem w co najmniej dwóch wdrożeniach oferowanej platformy wirtualizacji i oferowanego oprogramowania kopii zapasowych.
3. Zadanie 1: co najmniej jedna osoba z doświadczeniem w co najmniej dwóch wdrożeniach oferowanej platformy XDR.
4. Zadanie 2: co najmniej jedna osoba z certyfikatem producenta oferowanego systemu IDS OT lub potwierdzonymi przez producenta uprawnieniami do wdrażania systemu oraz doświadczeniem w co najmniej jednym wdrożeniu systemu monitorowania sieci przemysłowej.
5. Zadanie 2: co najmniej jeden inżynier z certyfikatem producenta oferowanych urządzeń UTM.
6. Zmiana osoby po złożeniu oferty lub w trakcie realizacji wymaga zgody Zamawiającego i zachowania co najmniej równoważnych kwalifikacji.

2.6. Pozycje wydłużenia świadczeń okresowych do 36 miesięcy

1. Dla pozycji podstawowych wskazanych w wykazie w pkt 1.2 przedmiot zamówienia obejmuje odrębną pozycję wydłużenia, oznaczoną literą W (np. poz. 1.1W dla poz. 1.1), polegającą na wydłużeniu okresu świadczeń okresowych pozycji podstawowej z okresu podstawowego (do dnia 31 grudnia 2026 r.) do 36 miesięcy od dnia odbioru pozycji podstawowej. Dla pozostałych pozycji świadczenia okresowe kończą się z dniem 31 grudnia 2026 r.

2. Pozycje W są wyceniane odrębnie w części IV Formularza ofertowego i wliczane do ceny oferty. Oferta nieobejmująca wszystkich pozycji W zostanie odrzucona.
3. Zakres wydłużenia określa nazwa pozycji W w wykazie w pkt 1.2 i obejmuje, odpowiednio do rodzaju pozycji podstawowej:
   a) dla dostaw urządzeń (poz. 1.2W, 1.3W, 1.16W, 1.17W, 2.3W, 2.6W) – gwarancję i serwis producenta na warunkach określonych w pozycji podstawowej, a dla poz. 1.1W i 2.6W także subskrypcje i wsparcie techniczne producenta wymagane w pozycji podstawowej,
   b) dla licencji (poz. 1.4W, 1.21W, 2.2W) – subskrypcję albo wsparcie i aktualizacje producenta do licencji wieczystej, na warunkach określonych w pozycji podstawowej,
   c) dla usługi chmurowej (poz. 1.18W) – kontynuację usługi o parametrach określonych w pozycji podstawowej,
   d) dla wdrożonych systemów (poz. 1.5W, 1.6W, 1.7W, 1.23W, 2.1W) – wsparcie powdrożeniowe i utrzymanie systemu przez Wykonawcę na warunkach określonych w pkt 2.4.2, w tym aktualizacje oprogramowania do wersji stabilnych,
   e) dla poz. 2.4W – serwis gwarancyjny, wsparcie eksploatacyjne i coroczny przegląd systemu IDS OT na warunkach określonych w poz. 2.4.
4. Pozycja W obejmuje okres od dnia następującego po zakończeniu świadczenia podstawowego do upływu 36 miesięcy od dnia odbioru pozycji podstawowej, tak aby zachować ciągłość świadczeń. Warunki świadczeń w okresie wydłużenia (zakres, poziom wsparcia, czasy reakcji, tryb zgłoszeń) są co najmniej takie same jak w okresie podstawowym.
5. Jeżeli warunki producenta nie przewidują wydłużenia kończącego się dokładnie z upływem 36 miesięcy od dnia odbioru, Wykonawca dostarcza najbliższy dłuższy okres dostępny u producenta, w ramach ceny pozycji W.
6. Wykonawca aktywuje lub rejestruje na Zamawiającego wydłużone świadczenia najpóźniej w dniu odbioru pozycji podstawowej, jeżeli producent umożliwia taką aktywację z wyprzedzeniem. Jeżeli model producenta przewiduje aktywację dopiero z początkiem okresu wydłużenia, Wykonawca przed odbiorem przedstawia wiążące potwierdzenie nabycia świadczenia na rzecz Zamawiającego. Świadczenia muszą następować bez przerwy po okresie podstawowym.
7. Odbiór Pozycji W w 2026 r. oznacza potwierdzenie nabycia i skutecznego zabezpieczenia prawa Zamawiającego do Świadczenia okresowego na wymagany okres (np. przez rejestrację u producenta, certyfikat wsparcia, dokument subskrypcji albo bezwarunkowe zobowiązanie Wykonawcy do świadczeń własnych). Odbiór Pozycji W nie oznacza potwierdzenia wykonania usług przypadających na okres po dniu odbioru. Wykonanie tych usług podlega bieżącej kontroli na zasadach umowy.
8. Pozycje W są fakturowane i płatne zgodnie z § 8 umowy po spełnieniu warunków odbioru określonych powyżej. Dokumenty rozliczeniowe wskazują rzeczywisty okres, którego dotyczy nabyte świadczenie.

3. Zadanie 1 – Obszar techniczny IT

Przedmiotem Zadania 1 jest dostawa, instalacja i konfiguracja infrastruktury serwerowej, sieciowej i narzędzi bezpieczeństwa dla środowiska IT Zamawiającego wraz z usługami wdrożeniowymi, hardeningiem, segmentacją sieci i wsparciem. Pozycje opisano w grupach funkcjonalnych. Numeracja pozycji jest zgodna z pkt 1.2.

1. Wszystkie pozycje Zadania 1 muszą tworzyć jedną, zintegrowaną architekturę.
2. Wykonawca opracuje jeden nadrzędny projekt techniczny dla Zadania 1 zgodnie z pkt 2.4. Projekt podlega akceptacji Zamawiającego przed rozpoczęciem prac instalacyjnych.
3. Do pozycji obejmujących instalację, konfigurację lub wdrożenie stosuje się wymagania wspólne określone w pkt 2.4.

3.1. Architektura docelowa

1. Urządzeniem brzegowym sieci Zamawiającego jest firewall (poz. 1.1). Na firewallu są terminowane oba łącza WAN, tunele VPN do obiektów i dostęp zdalny.
2. Dotychczasowy router brzegowy jest wycofywany z ruchu produkcyjnego po okresie równoległej pracy i pozostaje urządzeniem zapasowym (poz. 1.9, 1.10 i 1.20).
3. Sieć jest podzielona na strefy bezpieczeństwa (VLAN). Routing między strefami odbywa się wyłącznie przez firewall, z polityką domyślnego blokowania (poz. 1.12).
4. Środowisko OT (serwer SCADA, dyspozytornia, łącze telemetrii APN, tunele do obiektów) tworzy odrębną strefę lub odrębną instancję logiczną firewalla.
5. Serwer (poz. 1.16) z systemem wirtualizacji (poz. 1.15) jest platformą dla maszyn wirtualnych systemów bezpieczeństwa dostarczanych w Zadaniach 1 i 2: platformy XDR, monitoringu, WAF, dostawcy tożsamości, menedżera haseł i serwera systemu IDS OT.
6. Na serwer z poz. 1.16 są przenoszone maszyny wirtualne z kontrolera domeny. Kontroler domeny nie pełni docelowo roli hosta wirtualizacji.
7. Kopie zapasowe są realizowane zgodnie z regułą 3-2-1-1. Oprogramowanie kopii zapasowych (poz. 1.4) zapisuje kopie na macierzy NAS nr 2 (poz. 1.17) z kopiami niemodyfikowalnymi.
8. Macierz NAS nr 1 (poz. 1.2) przechowuje dane operacyjne oraz replikę repozytorium kopii (poz. 1.19). Wybrane zasoby są kopiowane do szyfrowanego repozytorium w chmurze (poz. 1.18).
9. Instalację i konfigurację serwera, systemu wirtualizacji, macierzy i systemu kopii zapasowych obejmuje poz. 1.13.
10. Warstwę wykrywania i reagowania tworzą: platforma XDR/EDR z agentami na stacjach i serwerach (poz. 1.5), centralny serwer logów (poz. 1.22), system monitoringu (poz. 1.6), WAF dla systemu eBOK (poz. 1.7) oraz funkcja sandbox na firewallu (poz. 1.21).
11. Warstwę tożsamości tworzą: hardening Active Directory (poz. 1.8), centralny dostawca tożsamości z MFA (poz. 1.24), klucze sprzętowe FIDO2 (poz. 1.25) i menedżer haseł (poz. 1.23).

3.2. Bezpieczeństwo sieci

Poz. 1.1 – Firewall sieciowy klasy NGFW/UTM – dostawa urządzenia wraz z pakietem subskrypcji ochronnych (klasy UTM) i wsparciem producenta

Przedmiotem pozycji jest dostawa jednego urządzenia klasy NGFW/UTM wraz z pakietem subskrypcji usług ochronnych i wsparciem producenta aktywnymi do dnia 31 grudnia 2026 r. Urządzenie pełni funkcję urządzenia

brzegowego, koncentratora VPN oraz punktu kontroli ruchu między strefami sieci wewnętrznej, w tym między środowiskiem IT i OT. Instalacja i konfiguracja urządzenia jest przedmiotem poz. 1.9, 1.10, 1.12 i 1.20.

Wymagania ogólne

1. Urządzenie sprzętowe (appliance) producenta systemu, przeznaczone do montażu w szafie rack 19" (zestaw montażowy w komplecie) lub na półce.
2. Wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa są realizowane przez jedno urządzenie.
3. Praca w trybie routera z funkcją NAT, w trybie transparentnym oraz w trybie monitorowania na porcie SPAN.
4. Możliwość utworzenia co najmniej 2 odrębnych instancji logicznych (virtual domains) w zakresie routingu, firewalla, IPsec VPN, antywirusa, IPS i kontroli aplikacji, z pełną izolacją polityk, tablic routingu i przestrzeni adresowej.
5. Możliwość utworzenia co najmniej 5 kont administratorów przypisanych do poszczególnych instancji.
6. Obsługa IPv4 i IPv6 w zakresie firewalla, ochrony w warstwie aplikacji i protokołów routingu dynamicznego.

Redundancja i wykrywanie awarii

1. Możliwość łączenia w klaster Active-Active lub Active-Passive w zakresie funkcji firewalla, IPsec, kontroli aplikacji i IPS, z synchronizacją sesji w obu trybach.
2. Monitoring i wykrywanie uszkodzeń elementów sprzętowych i programowych urządzenia oraz łączy sieciowych.
3. Monitoring stanu połączeń VPN.
4. Agregacja łączy statyczna oraz z wykorzystaniem protokołu LACP.
5. Możliwość tworzenia interfejsów redundantnych.

Interfejsy i zasilanie

1. Co najmniej 8 portów Gigabit Ethernet RJ-45 z możliwością swobodnego przypisania do stref bezpieczeństwa określonych w projekcie technicznym, w tym do obu łączy WAN i do połączeń klastra HA.
2. Wbudowany port konsoli szeregowej oraz gniazdo USB.
3. Jeżeli urządzenie nie posiada portu SFP, Wykonawca dostarcza w cenie pozycji konwerter mediów umożliwiający podłączenie łącza światłowodowego.
4. Możliwość skonfigurowania co najmniej 200 interfejsów wirtualnych VLAN zgodnych ze standardem 802.1Q.
5. Zasilanie 230 V AC. Dopuszcza się zasilacz zewnętrzny.

Parametry wydajnościowe

1. Obsługa nie mniej niż 1 mln jednoczesnych połączeń oraz 50 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 8 Gbps dla pakietów 512 B.
3. Przepustowość firewalla z włączoną kontrolą aplikacji: nie mniej niż 3 Gbps.
4. Wydajność szyfrowania IPsec VPN (AES-128): nie mniej niż 5 Gbps.
5. Wydajność modułu IPS (client side i server side) dla ruchu o charakterystyce Enterprise Traffic Mix: nie mniej niż 2 Gbps.
6. Wydajność skanowania ruchu Enterprise Traffic Mix z włączonymi funkcjami IPS, kontrola aplikacji i antywirus: nie mniej niż 1 Gbps.
7. Wydajność inspekcji komunikacji szyfrowanej SSL/TLS dla ruchu HTTP: nie mniej niż 1 Gbps.

Funkcje bezpieczeństwa

Urządzenie realizuje co najmniej następujące funkcje. Wymagania szczegółowe dla poszczególnych funkcji określają dalsze punkty.

1. Zapora sieciowa klasy Stateful Inspection.
2. Kontrola aplikacji.
3. Połączenia szyfrowane IPsec VPN oraz VPN dostępu zdalnego.
4. Ochrona przed złośliwym oprogramowaniem.
5. Ochrona przed atakami (IPS).
6. Filtrowanie stron WWW.
7. Filtrowanie zapytań DNS.
8. Antyspam dla protokołu SMTP.
9. Zarządzanie pasmem (QoS).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych.
11. Integracja z zewnętrznym systemem MFA przez RADIUS i SAML.
12. Inspekcja ruchu szyfrowanego SSL/TLS (co najmniej w zakresie IPS) dla protokołów HTTP (w tym HTTP/2), SMTP, FTP i POP3, z możliwością wyłączenia inspekcji dla wskazanych kategorii URL.
13. Mechanizmy automatyzacji: wykonanie sekwencji akcji (zmiana konfiguracji, powiadomienie administratora, blokada adresu) po wystąpieniu wybranego zdarzenia.

Polityki i translacja adresów

1. Polityka firewalla uwzględnia adresy IP, użytkowników i grupy (w tym grupy Active Directory), protokoły, usługi, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń oraz rejestrowanie zdarzeń.
2. Przedziały czasowe aktywności reguły.
3. Filtrowanie w zależności od kraju przypisanego do adresu IP.
4. Obsługa zewnętrznych repozytoriów adresów URL i IP (listy zewnętrzne).
5. Translacja adresów NAT źródłowego i docelowego, PAT, translacja jeden do jeden i jeden do wielu.
6. Dedykowany ALG dla protokołu SIP.
7. Obsługa stref bezpieczeństwa grupujących interfejsy.

Połączenia VPN

1. IPsec VPN z obsługą IKEv1 i IKEv2.
2. Szyfrowanie co najmniej AES-128 i AES-256 w trybie GCM oraz grupy Diffie-Hellman 19 i 20.
3. Topologie hub-and-spoke i mesh.
4. Połączenia site-to-site i client-to-site.
5. Monitorowanie stanu tuneli i automatyczna aktywacja tunelu zapasowego.
6. Uwierzytelnianie kluczem współdzielonym i certyfikatem.
7. Obsługa IPsec NAT Traversal, DPD i XAuth.
8. Split tunneling dla połączeń client-to-site.
9. Wybór tunelu przez routing statyczny i dynamiczny (OSPF).
10. Dostęp zdalny użytkowników (client-to-site) w technologii IPsec IKEv2 lub SSL VPN.
11. Dla dostępu zdalnego IPsec IKEv2 wymagana jest możliwość pracy przez TCP/443 w sieciach blokujących UDP.

12. Oprogramowanie klienckie producenta dla systemów Windows, macOS, iOS i Android. Dopuszcza się klienta bezpłatnego w zakresie funkcji VPN.

Routing, łącza WAN i zarządzanie pasmem

1. Routing statyczny i Policy Based Routing.
2. Protokoły RIPv2 (w tym RIPng), OSPF (w tym OSPFv3) i BGP.
3. Filtrowanie tras, ECMP oraz BFD.
4. Monitoring dostępności wskazanego adresu IP z danego interfejsu z automatycznym usuwaniem tras.
5. Funkcje SD-WAN: równoważenie i przełączanie ruchu między co najmniej dwoma łączami WAN na podstawie opóźnienia, utraty pakietów i jitter.
6. Funkcje SD-WAN dla interfejsów fizycznych i wirtualnych, w tym VLAN i IPsec.
7. Zarządzanie pasmem: pasmo maksymalne i gwarantowane, oznaczanie DSCP, priorytety.
8. Przydział pasma dla aplikacji, użytkowników i kategorii URL.

Ochrona przed złośliwym oprogramowaniem i analiza sandbox

1. Skanowanie ruchu w obu kierunkach dla protokołów HTTP, HTTPS, FTP, POP3, IMAP, SMTP i CIFS, także na niestandardowych portach.
2. Konfigurowalna głębokość dekompresji archiwów.
3. Blokowanie i logowanie archiwów, których nie można przeskanować.
4. Sygnatury dla urządzeń mobilnych, co najmniej dla systemu Android.
5. Automatyczna aktualizacja bazy sygnatur.
6. Silnik wykrywania oparty na modelach uczenia maszynowego producenta.
7. Współpraca z usługą sandbox w chmurze producenta, z przetwarzaniem w centrach danych na terenie Unii Europejskiej lub Europejskiego Obszaru Gospodarczego.
8. Jeżeli w związku z oferowaną usługą lub funkcją dochodzi do przetwarzania danych osobowych poza EOG, Wykonawca przed zawarciem umowy wskazuje lokalizację przetwarzania i wykazuje zgodność transferu z rozdziałem V RODO. Zamawiający preferuje przetwarzanie danych w EOG; zastosowanie transferu poza EOG wymaga uprzedniej akceptacji Zamawiającego.
9. Licencje usługi sandbox w zakresie objętym dostarczanym pakietem. Rozszerzenie o tryb inline jest przedmiotem poz. 1.21.
10. Możliwość uruchomienia ochrony przed złośliwym oprogramowaniem dla wybranego zakresu ruchu.
11. Zalecane (nie podlega ocenie): usuwanie aktywnej zawartości plików Microsoft Office i PDF bez blokowania transferu całych plików (CDR).

Ochrona przed atakami (IPS)

1. Ochrona oparta co najmniej na analizie sygnaturowej oraz analizie anomalii protokołów.
2. Ochrona aplikacji pracujących na niestandardowych portach.
3. Baza co najmniej 5000 sygnatur aktualizowana automatycznie.
4. Możliwość definiowania własnych sygnatur i wyjątków.
5. Wykrywanie anomalii ruchu i ochrona przed atakami DoS/DDoS.
6. Sygnaturowa ochrona aplikacji WWW, co najmniej przed XSS, SQL Injection, trojanami, exploitami i botami.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
8. Możliwość uruchomienia IPS dla wybranych zakresów komunikacji, a nie wyłącznie globalnie.

Kontrola aplikacji i filtrowanie WWW

1. Kontrola aplikacji na podstawie głębokiej analizy pakietów, niezależnie od portów.
2. Baza co najmniej 2000 sygnatur aplikacji aktualizowana automatycznie.
3. Kontrola czynności w aplikacjach chmurowych, co najmniej pobierania i wysyłania plików.
4. Kategorie aplikacji proxy i P2P.
5. Blokowanie aplikacji na niestandardowych portach oraz ograniczanie dopuszczalnych protokołów na danym porcie.
6. Filtr WWW z bazą co najmniej 40 mln adresów URL w kategoriach, w tym: malware, phishing, spam, Dynamic DNS, proxy oraz strony zabronione prawem.
7. Nadpisywanie kategorii, białe i czarne listy oraz wyrażenia regularne.
8. Akcja ostrzegawcza z możliwością kontynuacji (warning), wymuszanie bezpiecznego wyszukiwania (Safe Search) oraz własne strony komunikatów dla użytkownika.
9. Określanie kategorii wyłączonych z inspekcji SSL.

Uwierzytelnianie użytkowników

1. Weryfikacja tożsamości użytkowników w bazie lokalnej, LDAP/Active Directory, RADIUS i SAML.
2. Uwierzytelnianie wieloskładnikowe.
3. Single Sign-On z Active Directory przez agenta lub mechanizmy RADIUS, API lub SYSLOG.

Zarządzanie i logowanie

1. Zarządzanie lokalne przez HTTPS i SSH.
2. Współpraca z platformami centralnego zarządzania producenta.
3. MFA dla dostępu administracyjnego.
4. Ograniczenie dostępu administracyjnego do wskazanych adresów źródłowych.
5. Role administracyjne (RBAC).
6. Zatwierdzanie zmian konfiguracji przed ich wdrożeniem.
7. Interfejs API z dokumentacją producenta.
8. SNMP v2c i v3 oraz NetFlow lub sFlow.
9. Wbudowane narzędzia diagnostyczne: ping, traceroute, podgląd pakietów, monitorowanie sesji.
10. Logowanie zdarzeń wszystkich modułów sieciowych i bezpieczeństwa: ruch zaakceptowany i blokowany, aktywność administratorów, zużycie zasobów, stan systemu.
11. Logowanie zdarzeń dla każdej reguły z osobna.
12. Jednoczesne wysyłanie logów do wielu serwerów SYSLOG z wykorzystaniem TCP i szyfrowania TLS.
13. Logowanie lokalne lub do usługi producenta w zakresie dostępnym bez dodatkowych opłat.

Licencje, gwarancja i wsparcie

1. Licencje uprawniające do korzystania z aktualnych baz funkcji ochronnych producenta w zakresie co najmniej: kontrola aplikacji, IPS, antywirus (w tym sygnatury dla urządzeń mobilnych), analiza sandbox w chmurze, antyspam, filtrowanie WWW i DNS, bazy reputacyjne adresów IP i domen oraz wykrywanie komunikacji botnet/C&C (pakiet klasy „Unified Threat Protection” lub równoważny).
2. Licencje są aktywne od dnia aktywacji do dnia 31 grudnia 2026 r., na zasadach określonych w pkt 2.2.
3. Serwis gwarancyjny producenta obejmujący naprawę lub wymianę urządzenia w trybie wymiany wyprzedzającej (advance replacement) po potwierdzeniu awarii, do dnia 31 grudnia 2026 r.

4. Dostęp do aktualizacji oprogramowania oraz wsparcie techniczne producenta w trybie 24x7 przez portal i infolinię, do dnia 31 grudnia 2026 r.
5. Urządzenie jest rejestrowane w portalu producenta na konto Zamawiającego.
6. Wykonawca przekazuje dokumenty potwierdzające aktywację licencji i serwisu z datami ich obowiązywania.

Dostawa i odbiór

1. Dostawa do siedziby Zamawiającego wraz z zasilaczem, zestawem montażowym do szafy rack, kablami oraz dokumentacją producenta.
2. W zestawie co najmniej 2 tokeny sprzętowe lub programowe do uwierzytelniania dwuskładnikowego administratorów lub użytkowników VPN.
3. Wykaz numerów seryjnych zgodnie z pkt 2.2.
4. Odbiór pozycji następuje po dostawie, weryfikacji numerów seryjnych i aktywacji licencji. Uruchomienie funkcjonalne urządzenia jest przedmiotem poz. 1.9.

Poz. 1.9 – Wdrożenie i konfiguracja firewalla NGFW/UTM (poz. 1.1) jako urządzenia brzegowego sieci Zamawiającego

Przedmiotem pozycji jest instalacja i konfiguracja urządzenia z poz. 1.1 w roli urządzenia brzegowego sieci Zamawiającego, w tym przejęcie funkcji dotychczasowego routera brzegowego DrayTek Vigor 3910 oraz uruchomienie mechanizmów ochronnych dla ruchu do i z Internetu. Funkcje routingu, NAT, obsługi łączy WAN i VPN przejmuje w całości firewall. Dostawa odrębnego routera nie jest przedmiotem zamówienia.

Analiza i projekt

1. Wykonawca przeprowadzi analizę obecnej konfiguracji routera brzegowego: łącza WAN, adresacja, podsieci, przekierowania portów i publikacje usług, filtry, konta i profile VPN, usługi DHCP i DNS.
2. Wykonawca sporządzi wykaz usług publikowanych w Internecie z ustaleniem ich właścicieli i zasadności publikacji, w uzgodnieniu z Zamawiającym i dostawcami aplikacji.
3. Wykonawca opracuje projekt architektury bezpieczeństwa jako rozdział projektu technicznego Zadania 1: umiejscowienie firewalla, podział na strefy, zasady przepływu ruchu, plan migracji i plan wycofania zmian.
4. Podział na strefy jest zgodny z planem segmentacji opracowanym w poz. 1.12.

Zakres prac

1. Montaż urządzenia w szafie rack Zamawiającego z zasilaniem z UPS (poz. 1.3).
2. Aktualizacja oprogramowania urządzenia do najnowszej stabilnej wersji rekomendowanej przez producenta.
3. Konfiguracja obu łączy WAN, w tym łącza radiowego i łącza zapasowego, oraz przygotowanie do wykorzystania łącza światłowodowego.
4. Konfiguracja NAT, DNS i NTP.
5. Konfiguracja serwera DHCP dla stref, w których nie realizuje go kontroler domeny.
6. Konfiguracja polityk bezpieczeństwa zgodnie z zasadą minimalnych uprawnień i domyślnego blokowania.
7. Ruch wychodzący użytkowników do Internetu jest objęty filtrowaniem WWW i DNS, kontrolą aplikacji, ochroną przed złośliwym oprogramowaniem i IPS.
8. Inspekcja SSL/TLS dla wybranych kategorii ruchu, z wyłączeniem bankowości, ochrony zdrowia i innych kategorii uzgodnionych z Zamawiającym.
9. Dystrybucja certyfikatu inspekcji SSL/TLS na stacje robocze przez GPO.

10. Konfiguracja filtrowania geolokalizacyjnego oraz ochrony przed atakami DoS.
11. Przeniesienie publikacji usług z routera brzegowego do strefy DMZ za firewallem, z ochroną IPS.
12. Aplikacje WWW są publikowane za zaporą WAF z poz. 1.7.
13. Usługi administracyjne (RDP, SSH, bazy danych, panele urządzeń) nie mogą być publikowane bezpośrednio w Internecie. Dostęp do nich odbywa się wyłącznie przez VPN z MFA (poz. 1.10).
14. Publikacje usług niepotwierdzone przez właściciela usługi są likwidowane.
15. Integracja z Active Directory w zakresie identyfikacji użytkowników w politykach.
16. Integracja z serwerem logów (poz. 1.22) i systemem monitoringu (poz. 1.6).
17. Konfiguracja logowania do usługi producenta w chmurze w zakresie dostępnym w licencji.
18. Konfiguracja automatycznych kopii konfiguracji urządzenia.

Uruchomienie produkcyjne i testy

1. Uruchomienie produkcyjne następuje w oknie serwisowym, po testach konfiguracji z wykorzystaniem stacji testowych i łącza testowego, jeżeli są dostępne.
2. Dotychczasowy router pozostaje przez co najmniej 3 dni w gotowości do przywrócenia zgodnie z planem wycofania zmian, a następnie jest wycofywany z ruchu produkcyjnego.
3. Wykonawca przekazuje Zamawiającemu kopię konfiguracji dotychczasowego routera.
4. Testy obejmują dostępność Internetu z każdej strefy.
5. Testy obejmują działanie publikacji usług.
6. Testy obejmują działanie mechanizmów ochronnych (IPS, filtr WWW, ochrona przed złośliwym oprogramowaniem) z użyciem plików i adresów testowych.
7. Testy obejmują identyfikację użytkowników oraz przekazywanie logów.
8. Raport z testów stanowi załącznik do protokołu odbioru.

Dokumentacja, instruktaż i wsparcie

1. Dokumentacja powykonawcza obejmuje architekturę, strefy, wykaz polityk z uzasadnieniem, wykaz publikowanych usług oraz procedurę odtworzenia konfiguracji.
2. Instruktaż administratorów w wymiarze co najmniej 6 godzin: zarządzanie politykami, analiza logów, reagowanie na incydenty.
3. Pula co najmniej 16 godzin zdalnych konsultacji, wykorzystywana i rozliczana zgodnie z pkt 2.4.

Poz. 1.10 – Wdrożenie i konfiguracja VPN na firewallu – tunele do obiektów oraz dostęp zdalny z uwierzytelnianiem wieloskładnikowym

Przedmiotem pozycji jest przeniesienie i przebudowa połączeń VPN Zamawiającego na firewall z poz. 1.1: tuneli LAN-to-LAN do obiektów technologicznych oraz dostępu zdalnego pracowników, kierownictwa i dostawców, z uwierzytelnianiem wieloskładnikowym i integracją z dostawcą tożsamości z poz. 1.24.

Analiza i porządkowanie dostępu

1. Wykonawca zinwentaryzuje istniejące połączenia VPN LAN-to-LAN z obiektami (w tym SUW Łazy, zbiornik Mielno, obiekt Kiszkowo oraz tunel dostawcy usług IT) oraz konta dostępu zdalnego.
2. Wykonawca uzgodni z Zamawiającym połączenia i konta do zachowania.
3. Połączenia i konta nieużywane są likwidowane.
4. Konta współdzielone są zastępowane kontami imiennymi.

Tunele do obiektów i telemetria

1. Konfiguracja tuneli IPsec site-to-site do obiektów z wykorzystaniem IKEv2, AES-256 GCM oraz grup DH 19 lub 20 albo wyższych.
2. Uwierzytelnianie tuneli certyfikatami lub silnymi kluczami współdzielonymi.
3. Monitorowanie tuneli i alarmowanie o ich utracie.
4. Tunele są terminowane w strefie telemetrii z politykami ograniczającymi ruch do niezbędnych przepływów SCADA.
5. Do czasu wdrożenia urządzeń z poz. 2.6 tunele są zestawiane z istniejącymi urządzeniami w obiektach. Po ich wdrożeniu Wykonawca przełącza tunele na urządzenia z poz. 2.6.
6. Włączenie łącza prywatnego APN telemetrii GSM do strefy telemetrii z kontrolą ruchu na firewallu, w uzgodnieniu z dostawcą automatyki i operatorem APN.
7. Koszty ewentualnych zmian po stronie operatora GSM nie są objęte zamówieniem.

Dostęp zdalny użytkowników

1. Konfiguracja dostępu zdalnego w technologii IPsec IKEv2 lub SSL VPN, zgodnie z możliwościami dostarczonego urządzenia i wspieranej wersji oprogramowania.
2. Dostęp zdalny pracowników i kierownictwa wymaga uwierzytelniania dwuskładnikowego: integracja z systemem MFA z poz. 1.24 (klucze FIDO2 lub TOTP), a do czasu jego uruchomienia – tokeny producenta.
3. Uprawnienia dostępu zdalnego są przypisywane na podstawie grup Active Directory.
4. Użytkownicy VPN są izolowani od siebie i mają dostęp wyłącznie do niezbędnych zasobów.
5. Zdalny dostęp kierownictwa do stanowisk SCADA odbywa się wyłącznie przez VPN z MFA, z urządzeń służbowych.
6. Połączenia VPN i zdarzenia uwierzytelnienia są rejestrowane.
7. Wykonawca zainstaluje i skonfiguruje klienta VPN na stacjach wskazanych przez Zamawiającego (do 15 stanowisk) oraz przygotuje pakiet instalacyjny do dystrybucji przez GPO.
8. Wykonawca przekaże instrukcję użytkownika VPN.

Dostęp serwisowy dostawców

1. Dostawcy usług IT, systemów dziedzinowych i automatyki otrzymują konta imienne z MFA.
2. Profile dostępu ograniczają dostęp dostawcy do wskazanych systemów i portów.
3. Dostęp dostawców jest ograniczony oknami czasowymi lub aktywowany na żądanie.
4. Wszystkie połączenia dostawców (adres źródłowy, konto, czas, zasoby docelowe) są logowane do serwera logów.
5. Wykonawca opracuje instrukcję dostępu serwisowego dla dostawców.

Testy, dokumentacja i instruktaż

1. Testy obejmują zestawienie każdego tunelu oraz działanie przepływów SCADA.
2. Testy obejmują logowanie użytkownika z MFA oraz odmowę dostępu bez drugiego składnika.
3. Testy obejmują ograniczenia profili dostawców oraz rejestrowanie połączeń.
4. Dokumentacja obejmuje wykaz tuneli, kont i profili oraz procedurę nadawania i odbierania dostępu zdalnego.
5. Instruktaż administratorów w wymiarze co najmniej 2 godzin.

Poz. 1.20 – Przygotowanie firewalla do pracy w konfiguracji wysokiej dostępności (HA) i redundancji łączy WAN

Redundancję urządzeń brzegowych zapewniają firewall z poz. 1.1 oraz dotychczasowy router utrzymywany jako urządzenie zapasowe. Redundancję łączy WAN zapewniają mechanizmy SD-WAN firewalla. Przedmiotem pozycji jest konfiguracja tej redundancji oraz przygotowanie firewalla do pracy w klastrze HA.

Redundancja łączy WAN

1. Konfiguracja SD-WAN: monitorowanie jakości obu łączy, automatyczne przełączenie awaryjne i powrót.
2. Reguły wyboru łącza dla ruchu krytycznego: SCADA i telemetria, VPN, eBOK.
3. Powiadomienia o przełączeniu łącza do systemu monitoringu i serwera logów.
4. Dynamiczny DNS lub równoważny mechanizm zachowania osiągalności usług publikowanych i tuneli VPN po przełączeniu łącza.

Przygotowanie do pracy w klastrze HA

1. Konfiguracja parametrów HA: tryb Active-Passive, interfejsy heartbeat, priorytety, monitorowane interfejsy.
2. Rezerwacja portów i okablowania dla drugiego urządzenia.
3. Opracowanie procedury dołączenia drugiego urządzenia tego samego typu (zakup poza niniejszym zamówieniem) bez przebudowy konfiguracji.

Urządzenie zapasowe

1. Opracowanie procedury awaryjnego przywrócenia łączności w przypadku awarii firewalla z wykorzystaniem dotychczasowego routera jako urządzenia zapasowego (cold standby).
2. Przygotowanie konfiguracji minimalnej routera zapasowego: łącza WAN, tunele do obiektów, dostęp zdalny. Konfiguracja jest przechowywana w sposób bezpieczny.
3. Określenie czasu przywrócenia łączności w procedurze awaryjnej.

Testy i dokumentacja

1. Symulacja awarii każdego łącza WAN z pomiarem czasu przełączenia.
2. Test procedury awaryjnej z użyciem urządzenia zapasowego.
3. Dokumentacja konfiguracji SD-WAN, parametrów HA i procedury awaryjnej.

Poz. 1.12 – Segmentacja sieci – konfiguracja podsieci VLAN/LAN na firewallu i przełącznikach

Przedmiotem pozycji jest podział sieci Zamawiającego na strefy bezpieczeństwa (VLAN) z routingiem międzystrefowym wyłącznie przez firewall oraz przeniesienie urządzeń do właściwych stref.

Plan segmentacji

1. Wykonawca opracuje plan segmentacji jako rozdział projektu technicznego Zadania 1: tabela VLAN, adresacja, przypisanie urządzeń do stref oraz macierz dozwolonych przepływów między strefami.
2. Plan przewiduje co najmniej strefy: użytkownicy IT, serwery, OT/SCADA (serwer SCADA i stanowiska dyspozytorskie), telemetria (tunele do obiektów, APN), strefa pośrednia IT/OT, monitoring wizyjny (odrębnie dla poszczególnych systemów), VoIP, drukarki i IoT, goście, DMZ, zarządzanie urządzeniami oraz kopie zapasowe.
3. Strefa zarządzania obejmuje karty zarządzające serwerów, przełączniki, macierze, UPS i kontroler WLAN.
4. Strefa pośrednia IT/OT (DMZ przemysłowa) jest przeznaczona dla kolektora platformy XDR, proxy systemu monitoringu i serwera systemu IDS OT.

5. Plan wskazuje porty, do których są podłączone urządzenia niezarządzalne (w tym przełącznik w dyspozytorni), przypisuje je do właściwej strefy i zawiera rekomendację ich wymiany.

Zakres prac

1. Konfiguracja VLAN na przełączniku rdzeniowym HPE Aruba Instant On 1830 i pozostałych zarządzalnych urządzeniach sieciowych Zamawiającego.
2. Konfiguracja VLAN na kontrolerze i punktach dostępowych UniFi oraz na firewallu.
3. Konfiguracja portów trunk i access zgodnie z projektem.
4. Routing między strefami wyłącznie przez firewall, z politykami zgodnymi z macierzą przepływów. Bezpośredni routing między podsieciami na routerze brzegowym jest likwidowany.
5. Strefa OT/SCADA jest wydzielona jako odrębna instancja logiczna firewalla (virtual domain) lub odrębna strefa z polityką domyślnego blokowania.
6. W strefie OT/SCADA dopuszcza się wyłącznie przepływy uzgodnione z dostawcą automatyki.
7. Ruch kierowany do strefy OT jest objęty inspekcją IPS, a wszystkie sesje międzystrefowe są rejestrowane.
8. Przeniesienie urządzeń do właściwych stref odbywa się w oknach serwisowych, w kolejności uzgodnionej z Zamawiającym, z aktualizacją zakresów DHCP, rekordów DNS i konfiguracji aplikacji.
9. Przeniesienie urządzeń strefy OT/SCADA odbywa się w uzgodnieniu z dostawcą automatyki.

Testy, dokumentacja i instruktaż

1. Weryfikacja braku nieautoryzowanego ruchu między strefami przez skanowanie z każdej strefy.
2. Weryfikacja działania przepływów dozwolonych, w tym SCADA – obiekty, dyspozytornia – serwer SCADA, drukowanie i VoIP.
3. Weryfikacja logowania ruchu dla każdej strefy.
4. Dokumentacja obejmuje schemat logiczny i fizyczny, tabelę VLAN, macierz przepływów oraz procedurę dodawania urządzenia do strefy.
5. Instruktaż administratorów w wymiarze co najmniej 2 godzin.

Poz. 1.11 – Hardening urządzeń sieciowych (firewall, przełączniki, sieć bezprzewodowa)

Przedmiotem pozycji jest hardening konfiguracji urządzeń sieciowych Zamawiającego: firewalla z poz. 1.1, przełączników (HPE Aruba Instant On 1830 i inne zarządzalne), kontrolera i punktów dostępowych UniFi oraz innych urządzeń wskazanych w inwentaryzacji, zgodnie z zaleceniami producentów i CIS Benchmarks lub równoważnymi.

1. Wymagania stosuje się w zakresie wspieranym przez dane urządzenie.
2. Posiadany przełącznik Instant On 1830 nie wspiera SSH, SNMPv3 ani 802.1X. Dla tego urządzenia stosuje się zarządzanie HTTPS ze strefy zarządzania oraz SNMPv2c tylko do odczytu, ograniczony do serwera monitoringu.
3. Funkcje niedostępne na danym urządzeniu Wykonawca wskazuje w raporcie wraz z rekomendacją, w tym rekomendacją wymiany przełącznika.

Zakres prac

1. Raport z analizy konfiguracji każdego urządzenia względem dobrych praktyk, sporządzony przed przystąpieniem do prac.
2. Plan hardeningu uzgodniony z Zamawiającym.
3. Wyłączenie dostępu administracyjnego z sieci WAN i z sieci użytkowników. Zarządzanie odbywa się wyłącznie ze strefy zarządzania przez HTTPS lub SSH.

4. Zmiana lub wyłączenie domyślnych kont oraz utworzenie kont imiennych.
5. MFA dla dostępu administracyjnego tam, gdzie urządzenie to wspiera.
6. Polityka haseł i blokada po nieudanych logowaniach.
7. Ograniczenie uprawnień kont dostawców.
8. Wyłączenie niezabezpieczonych i zbędnych protokołów i usług: HTTP, Telnet, SNMPv1, SNMPv2c (tam, gdzie dostępny jest SNMPv3), UPnP oraz nieużywane usługi chmurowe producenta.
9. Wyłączenie nieużywanych portów fizycznych.
10. Aktualizacja oprogramowania układowego do wersji rekomendowanych przez producentów.
11. Zabezpieczenia warstwy 2 na przełącznikach w zakresie wspieranym przez urządzenia: ochrona portów (limit adresów MAC), DHCP snooping, ochrona przed ARP spoofing, BPDU guard, ograniczenie VLAN dozwolonych na portach trunk oraz izolacja portów w strefach gości i IoT.
12. Konfiguracja NTP oraz SNMP (v3 tam, gdzie wspierane) z integracją z poz. 1.6.
13. Konfiguracja SYSLOG do serwera logów (poz. 1.22).
14. Banery ostrzegawcze na urządzeniach.
15. Automatyczne kopie konfiguracji do repozytorium Zamawiającego.

Dokumentacja i instruktaż

1. Raport przed/po z wykazem zmian dla każdego urządzenia.
2. Dokumentacja standardu konfiguracji (baseline) do stosowania przy nowych urządzeniach.
3. Instruktaż administratorów w wymiarze co najmniej 2 godzin.

Poz. 1.14 – Wdrożenie WPA3-Enterprise (802.1X) na kontrolerze i punktach dostępowych sieci bezprzewodowej

Przedmiotem pozycji jest uruchomienie uwierzytelniania 802.1X w sieci bezprzewodowej Zamawiającego w trybie WPA3-Enterprise oraz uporządkowanie sieci gości i urządzeń IoT.

Zakres prac

1. Przegląd konfiguracji kontrolera i punktów dostępowych UniFi, aktualizacja oprogramowania oraz uporządkowanie sieci SSID.
2. Konfiguracja sieci służbowej w trybie WPA3-Enterprise z uwierzytelnianiem 802.1X przez serwer RADIUS zintegrowany z Active Directory (Microsoft NPS na posiadanej licencji Windows Server lub równoważny, np. FreeRADIUS).
3. Dynamiczne przypisywanie VLAN na podstawie grup użytkowników lub urządzeń.
4. Tryb przejściowy WPA2/WPA3-Enterprise jest dopuszczalny wyłącznie dla urządzeń niewspierających WPA3, po pisemnej akceptacji Zamawiającego, na czas określony.
5. Metoda uwierzytelniania urządzeń domenowych: EAP-TLS z certyfikatami urządzeń wydawanymi przez urząd certyfikacji Zamawiającego (poz. 1.8) i dystrybuowanymi przez GPO.
6. Metoda uwierzytelniania urządzeń nieobjętych domeną: PEAP-MSCHAPv2 z weryfikacją certyfikatu serwera RADIUS.
7. Wyłączenie WPS i przestarzałych standardów oraz włączenie ochrony ramek zarządzających (PMF).
8. Sieć gości:
    a) izolacja klientów,
    b) dostęp wyłącznie do Internetu,
    c) ograniczenie pasma,

d) portal z akceptacją regulaminu.

9. Sieć urządzeń IoT:
   a) odrębny VLAN,
   b) zabezpieczenie WPA3-Personal, a dla urządzeń niewspierających WPA3 – WPA2,
   c) izolacja klientów.
10. Logowanie zdarzeń uwierzytelniania do serwera logów oraz objęcie kontrolera i punktów dostępowych monitoringiem.

Testy, dokumentacja i instruktaż

1. Test uwierzytelnienia urządzeń domenowych i niedomenowych.
2. Test przypisania VLAN.
3. Test odrzucenia urządzeń nieuprawnionych oraz izolacji gości.
4. Dokumentacja konfiguracji oraz instrukcja podłączania urządzeń.
5. Instruktaż administratorów w wymiarze co najmniej 2 godzin.

Poz. 1.21 – Funkcja sandbox dla ruchu przeglądarek WWW – analiza inline plików na firewallu (licencja usługi sandbox i konfiguracja)

Przedmiotem pozycji jest uruchomienie na firewallu z poz. 1.1 analizy plików pobieranych z Internetu w izolowanym środowisku (sandbox) w trybie inline, z wstrzymaniem dostarczenia pliku do czasu uzyskania werdyktu, wraz z dostawą licencji usługi producenta oraz utwardzeniem konfiguracji przeglądarek WWW na stacjach roboczych. Funkcja obejmuje ruch WWW wszystkich użytkowników i nie wymaga agentów na stacjach roboczych.

Wymagania

1. Usługa sandbox zintegrowana z firewallem z poz. 1.1, realizowana w chmurze producenta lub przez urządzenie lokalne.
2. Lokalizacja przetwarzania w chmurze spełnia wymagania określone dla usługi sandbox w poz. 1.1.
3. Licencja usługi jest aktywna do dnia 31 grudnia 2026 r., na zasadach określonych w pkt 2.2.
4. Tryb inline: wstrzymanie dostarczenia pliku do czasu otrzymania werdyktu dla plików pobieranych przez HTTP i HTTPS (z inspekcją SSL/TLS).
5. Analiza inline obejmuje co najmniej pliki wykonywalne, biblioteki, skrypty, dokumenty Microsoft Office i PDF oraz archiwa.
6. Pliki z werdyktem złośliwym są blokowane, a werdykty logowane.
7. Dla protokołów innych niż HTTP i HTTPS dopuszcza się tryb asynchroniczny z blokowaniem kolejnych pobrań tego samego pliku.
8. Analiza dynamiczna (uruchomienie w izolowanym środowisku) oraz statyczna z wykorzystaniem modeli uczenia maszynowego producenta.
9. Raport z analizy pliku jest dostępny administratorowi.

Zakres wdrożenia

1. Konfiguracja profili ochrony z przekazywaniem plików do sandbox w trybie inline dla polityk ruchu użytkowników do Internetu.
2. Polityka postępowania z plikami nieprzeskanowanymi (archiwa zaszyfrowane, przekroczenie rozmiaru).
3. Wyłączenia dla zaufanych źródeł uzgodnionych z Zamawiającym.

4. Utwardzenie przeglądarek Microsoft Edge i Google Chrome na stacjach roboczych przez GPO: wymuszenie automatycznych aktualizacji, ochrona SmartScreen lub Safe Browsing w trybie rozszerzonym, izolacja witryn, blokada instalacji niezaufanych rozszerzeń, blokada automatycznego otwierania pobranych plików.
5. Wyłączenie zapisywania haseł w przeglądarkach na rzecz menedżera haseł (poz. 1.23).

Testy, dokumentacja i instruktaż

1. Testy z użyciem próbek testowych (EICAR oraz próbki producenta usługi) potwierdzające wstrzymanie i blokadę pliku.
2. Weryfikacja raportowania werdyktów do serwera logów.
3. Dokumentacja konfiguracji profili i polityk GPO.
4. Instruktaż administratorów w wymiarze co najmniej 2 godzin.

3.3. Infrastruktura serwerowa, pamięć masowa i kopie zapasowe

1. Pozycje 1.2, 1.3, 1.15, 1.16 i 1.17 obejmują dostawy sprzętu i licencji (poz. 1.3 wraz z instalacją).
2. Pozycje 1.4 i 1.18 obejmują licencję oprogramowania kopii zapasowych oraz usługę chmurową.
3. Pozycje 1.13 i 1.19 obejmują usługi instalacji, konfiguracji, migracji i wsparcia dla tych elementów.
4. Wykonawca odpowiada za dobór elementów zapewniający ich wzajemną zgodność, w szczególności zgodność serwera z systemem wirtualizacji, oprogramowania kopii zapasowych z platformą wirtualizacji i macierzami oraz usługi chmurowej z oprogramowaniem kopii zapasowych.

Poz. 1.16 – Serwer fizyczny do systemu wirtualizacji z lokalną pamięcią masową (w tym przygotowanie do usług HA) – dostawa

Przedmiotem pozycji jest dostawa jednego serwera fizycznego stanowiącego host platformy wirtualizacji dedykowanej systemom bezpieczeństwa dostarczanym w Zadaniach 1 i 2 (platforma XDR, monitoring, WAF, dostawca tożsamości, menedżer haseł, serwer systemu IDS OT, serwer kopii zapasowych). Serwer jest przygotowany do pracy w układzie wysokiej dostępności (replikacja maszyn wirtualnych na posiadany przez Zamawiającego host) oraz do rozbudowy o kolejny host. Na serwer są przenoszone również maszyny wirtualne z kontrolera domeny (rozdzielenie ról). Instalacja i konfiguracja serwera jest przedmiotem poz. 1.13.

Wymagania dotyczące dostawy

1. Komponenty serwera muszą być produktami producenta serwera lub produktami przez niego certyfikowanymi i objętymi gwarancją producenta.
2. Dostawa w oryginalnym opakowaniu producenta z kompletem dokumentacji.
3. Konfiguracja sprzętowa serwera musi być możliwa do sprawdzenia na stronie producenta po numerze seryjnym.
4. Producent serwera zapewnia ogólnopolską infolinię techniczną w języku polskim.

Obudowa i płyta główna

1. Obudowa rack 19" o wysokości maksymalnie 2U, z kompletem wysuwanych szyn oraz ramieniem do prowadzenia kabli.
2. Zamykany panel przedni chroniący dyski.
3. Wysuwana karta identyfikacyjna serwera.
4. Płyta główna zaprojektowana i wyprodukowana przez producenta serwera.
5. Co najmniej 16 gniazd pamięci z możliwością rozbudowy do co najmniej 2 TB RAM.

6. Moduł TPM 2.0.

Procesor i pamięć

1. Zainstalowany co najmniej jeden procesor klasy x86-64 o co najmniej 16 rdzeniach i częstotliwości bazowej co najmniej 2,3 GHz. Dopuszcza się serwer jednoprocesorowy.
2. Procesor osiąga wynik co najmniej 190 punktów w teście SPECrate2017_int_base dla konfiguracji jednoprocesorowej oferowanego modelu serwera. Wynik musi być opublikowany na stronie spec.org.
3. Zainstalowane co najmniej 128 GB pamięci DDR5 RDIMM z korekcją ECC.
4. Moduły pamięci o jednakowej pojemności, obsadzone w sposób umożliwiający pracę wielokanałową.

Kontroler i dyski

1. Sprzętowy kontroler RAID obsługujący dyski SAS, SATA i NVMe, z pamięcią cache co najmniej 4 GB z podtrzymaniem.
2. Obsługa poziomów RAID 0, 1, 5, 6, 10, 50 i 60.
3. Dyski systemowe: 2 dyski SSD o pojemności co najmniej 480 GB każdy, w sprzętowym RAID 1 (dedykowany moduł rozruchowy lub kieszenie hot-plug).
4. Dyski na dane: co najmniej 3 dyski SSD klasy enterprise typu mixed-use (co najmniej 3 DWPD), o pojemności co najmniej 1,92 TB każdy, z interfejsem SAS lub NVMe, hot-plug.
5. Co najmniej 4 wolne kieszenie dyskowe umożliwiające rozbudowę.

Interfejsy

1. Co najmniej 2 porty 10 Gb Ethernet SFP+ z wkładkami lub kablami DAC zgodnymi z infrastrukturą Zamawiającego.
2. Co najmniej 2 porty 10 Gb Ethernet RJ-45 (10GBASE-T).
3. Co najmniej 2 porty 1 Gb Ethernet RJ-45.
4. Dedykowany port RJ-45 karty zarządzającej.
5. Wymagana liczba portów sieciowych nie może być osiągnięta przez zewnętrzne przejściówki.
6. Port VGA na tylnym panelu.
7. Co najmniej 4 porty USB, w tym co najmniej 1 wewnątrz obudowy i 2 z tyłu.
8. Dedykowany port USB modułu zarządzającego z przodu obudowy.

Zasilanie i chłodzenie

1. Redundantne zasilacze hot-plug o mocy co najmniej 800 W każdy, o sprawności klasy co najmniej Platinum.
2. Kable zasilające C13–C14 o długości co najmniej 1,8 m.
3. Redundantne wentylatory hot-plug.

Karta zarządzająca

1. Karta zarządzająca niezależna od systemu operacyjnego, z dedykowanym portem Ethernet.
2. Monitorowanie podzespołów (temperatura, zasilacze, wentylatory, procesory, pamięć, kontroler i dyski) bez agenta w systemie operacyjnym.
3. Alerty SNMPv3 i e-mail.
4. Dostęp przez przeglądarkę (HTTPS), linię komend, IPMI 2.0 oraz RESTful API (Redfish).
5. Wirtualna konsola HTML5 z podłączaniem wirtualnych nośników.
6. Nagrywanie sekwencji wideo ostatniej awarii i startu systemu.

7. Monitorowanie zużycia energii oraz limit pobieranej mocy.
8. Zdalna aktualizacja oprogramowania układowego.
9. Obsługa co najmniej 2 administratorów jednocześnie.
10. Uwierzytelnianie dwuskładnikowe oraz integracja z Active Directory.
11. Obsługa IPv6 oraz zdalnego SYSLOG.
12. Wsparcie dla automatycznego zgłaszania awarii do centrum serwisowego producenta.

Bezpieczeństwo i zgodność

1. Sprzętowy mechanizm weryfikacji integralności oprogramowania układowego (Root of Trust) zgodny z NIST SP 800-147B lub SP 800-193 albo równoważny.
2. Secure Boot.
3. Czujnik otwarcia obudowy.
4. Możliwość dynamicznego wyłączania portów USB.
5. Możliwość bezpiecznego wymazania danych z dysków z poziomu karty zarządzającej.
6. Serwer znajduje się na liście Windows Server Catalog ze statusem „Certified for Windows” dla Windows Server 2022 i 2025 lub na liście zgodności oferowanej platformy wirtualizacji.
7. Deklaracja zgodności CE.
8. Produkcja zgodna z ISO 9001 i ISO 14001.
9. Certyfikat EPEAT co najmniej na poziomie Bronze lub równoważny.
10. Dokumentacja w języku polskim lub angielskim oraz nośniki lub obrazy oprogramowania systemowego i narzędzi diagnostycznych producenta.

Gwarancja i wsparcie

1. Gwarancja producenta do dnia 31 grudnia 2026 r., na zasadach określonych w pkt 2.2.
2. Gwarancja jest świadczona w miejscu instalacji przez autoryzowanego inżyniera serwisowego, z reakcją w następnym dniu roboczym od zgłoszenia.
3. Zgłoszenia są przyjmowane w trybie 24x7 telefonicznie i przez portal producenta, w języku polskim.
4. Pojedynczy punkt kontaktu dla sprzętu i dostarczonego z nim oprogramowania.
5. W okresie gwarancji Zamawiający ma dostęp do aktualizacji oprogramowania układowego, narzędzi diagnostycznych i wsparcia technicznego producenta.

Poz. 1.15 – System wirtualizacji – licencja systemu operacyjnego serwera z rolą hypervisora (Windows Server 2025 Standard, 16 rdzeni, lub równoważna)

Przedmiotem pozycji jest dostawa licencji systemu wirtualizacji dla serwera z poz. 1.16: Microsoft Windows Server 2025 Standard w licencjonowaniu na rdzenie (16 rdzeni) lub równoważnej. System jest przeznaczony do uruchamiania maszyn wirtualnych, na których zostaną zainstalowane produkty z zakresu cyberbezpieczeństwa dostarczane w Zadaniach 1 i 2. Instalacja i konfiguracja systemu wirtualizacji jest przedmiotem poz. 1.13.

Wymagania licencyjne

1. Licencja wieczysta, nowa, zarejestrowana na Zamawiającego.
2. Licencja w programie licencyjnym umożliwiającym legalne użytkowanie przez Zamawiającego. Dopuszcza się licencję OEM przypisaną do dostarczanego serwera lub licencję wolumenową.
3. Liczba licencjonowanych rdzeni pokrywa wszystkie rdzenie fizyczne procesorów dostarczanego serwera, nie mniej niż 16.

4. Jeżeli dostarczany serwer ma więcej niż 16 rdzeni, Wykonawca dostarczy dodatkowe pakiety rdzeni w ramach ceny pozycji.
5. Prawo do uruchomienia na dostarczanym hoście co najmniej 2 maszyn wirtualnych z systemem Windows Server w edycji Standard bez dodatkowych opłat oraz nieograniczonej liczby maszyn wirtualnych z systemem Linux.
6. Aktualizacje zabezpieczeń producenta dostępne dla dostarczanej wersji co najmniej do dnia 31 grudnia 2026 r., w ramach standardowego wsparcia producenta.
7. Pozycja nie obejmuje licencji dostępowych (CAL).

Wymagania funkcjonalne

1. Hypervisor typu 1 (rola wirtualizacji).
2. Obsługa maszyn wirtualnych generacji 2 z UEFI, Secure Boot i wirtualnym TPM.
3. Obsługa systemów gości Windows Server 2016–2025, Windows 10/11 oraz Linux, w tym dystrybucji wykorzystywanych przez dostarczane systemy bezpieczeństwa.
4. Migawki (checkpointy) maszyn wirtualnych.
5. Replikacja asynchroniczna maszyn wirtualnych do drugiego hosta z możliwością planowanego i awaryjnego przełączenia.
6. Migracja maszyn wirtualnych między hostami.
7. Wirtualne przełączniki z obsługą VLAN 802.1Q i agregacji łączy.
8. Wirtualny TPM i szyfrowanie dysków maszyn wirtualnych, np. BitLocker w systemie gościa.
9. Interfejs zarządzania graficzny i skryptowy.
10. Interfejs API umożliwiający kopie zapasowe na poziomie hosta ze śledzeniem zmienionych bloków, współpracujący z oprogramowaniem z poz. 1.4.
11. Integracja z Active Directory.
12. Logowanie zdarzeń do SYSLOG/SIEM przez agenta.

Bilans licencji

1. Projekt techniczny (poz. 1.13) zawiera bilans instancji systemów Windows Server: prawa z dostarczanej licencji oraz licencje posiadane przez Zamawiającego.
2. Projekt techniczny zawiera bilans licencji dostępowych (CAL).
3. Projekt rozmieszcza usługi tak, aby nie wymagały dodatkowych licencji. Jeżeli nie jest to możliwe, projekt wskazuje liczbę i rodzaj licencji do nabycia przez Zamawiającego.

Poz. 1.2 – Macierz dyskowa NAS nr 1 (rack, 12 kieszeni) wraz z 8 dyskami HDD klasy enterprise 16 TB – dostawa

Przedmiotem pozycji jest dostawa macierzy NAS klasy Synology RackStation RS2423RP+ (lub RS2423RP+II) z 8 dyskami HAT5300-16T lub równoważnej, przeznaczonej do przechowywania danych operacyjnych Zamawiającego (zasoby plikowe, dane systemów dziedzinowych, archiwum). Macierz stanowi jedno z dwóch urządzeń redundantnego układu przechowywania danych, wraz z macierzą z poz. 1.17 (replikacja – poz. 1.19). Konfiguracja macierzy jest przedmiotem poz. 1.13.

Wymagania dotyczące dostawy

1. Komplet okablowania i dokumentacji.
2. Wszystkie licencje oprogramowania niezbędne do uruchomienia wymaganych funkcji są wieczyste lub aktywne do dnia 31 grudnia 2026 r.

Obudowa, procesor i pamięć

1. Obudowa rack 19" o wysokości maksymalnie 2U, z szynami przesuwnymi.
2. Co najmniej 12 kieszeni na dyski 3,5"/2,5" SATA hot-swap.
3. Możliwość rozbudowy o jednostkę rozszerzającą do co najmniej 24 dysków.
4. Procesor x86-64 o co najmniej 4 rdzeniach i 8 wątkach, ze wsparciem pamięci ECC.
5. Co najmniej 8 GB pamięci DDR4 ECC z możliwością rozbudowy do co najmniej 32 GB.

Interfejsy

1. Co najmniej 2 porty 1 GbE RJ-45 oraz co najmniej 1 wbudowany port 10 GbE RJ-45.
2. Obsługa agregacji łączy (LACP), VLAN 802.1Q i ramek Jumbo.
3. Co najmniej 1 gniazdo PCIe (co najmniej Gen3 x4) umożliwiające instalację karty sieciowej 10/25 GbE (w tym SFP+) lub karty cache NVMe.
4. Co najmniej 2 porty USB 3.2 Gen 1.
5. Port do podłączenia jednostki rozszerzającej.

Dyski

1. 8 dysków HDD klasy enterprise 3,5" SATA 6 Gb/s o pojemności co najmniej 16 TB każdy.
2. Prędkość obrotowa 7200 obr./min oraz pamięć cache co najmniej 512 MB.
3. MTBF co najmniej 2 500 000 godzin oraz obciążenie roczne co najmniej 550 TB.
4. Dyski znajdują się na liście kompatybilności producenta oferowanej macierzy.

RAID, system plików i ochrona danych

1. Obsługa co najmniej RAID 0, 1, 5, 6 i 10 oraz dysków hot spare.
2. Rozbudowa puli o kolejne dyski bez utraty danych.
3. Wymiana dysków na dyski o większej pojemności bez utraty danych.
4. System plików z sumami kontrolnymi danych i metadanych (samonaprawa) oraz kompresją danych.
5. Migawki na poziomie folderów współdzielonych i jednostek iSCSI LUN, co najmniej 128 migawek na folder.
6. Migawki niemodyfikowalne (immutable) z określonym okresem ochrony.
7. Replikacja migawek do drugiego urządzenia według harmonogramu.
8. Przywracanie plików do wybranej migawki.
9. Szyfrowanie AES-256 folderów współdzielonych lub wolumenów, z bezpiecznym przechowywaniem kluczy.
10. Szyfrowanie transmisji: SMB3 encryption, HTTPS, SFTP.

Protokoły i usługi

1. Obsługa SMB/CIFS (w tym SMB3), NFS, iSCSI, FTP/SFTP, WebDAV, SSH oraz SNMP v3.
2. Integracja z Active Directory z obsługą uprawnień Windows ACL.
3. Wbudowany serwer kopii zapasowych stacji roboczych, serwerów i maszyn wirtualnych (bezagentowo dla platformy z poz. 1.15) z globalną deduplikacją, dostępny bez dodatkowych opłat licencyjnych.
4. Kopie zapasowe systemu i danych macierzy do chmury oraz na nośniki zewnętrzne.
5. Obsługa sieciowych zasilaczy UPS.

Bezpieczeństwo i zarządzanie

1. Uwierzytelnianie dwuskładnikowe dla kont administracyjnych.
2. Blokada konta po nieudanych logowaniach.
3. Wbudowana zapora sieciowa.
4. Możliwość wyłączenia domyślnego konta administratora.
5. Logowanie zdarzeń do zewnętrznego serwera SYSLOG oraz powiadomienia e-mail i SNMP.
6. Automatyczne aktualizacje zabezpieczeń.
7. Graficzny interfejs zarządzania w języku polskim dostępny przez przeglądarkę (HTTPS), interfejs wiersza poleceń (SSH) oraz API.
8. Monitorowanie SMART i temperatury dysków.

Zasilanie

1. Redundantne zasilacze (2 moduły hot-swap) o mocy zapewniającej pracę w pełnej konfiguracji dyskowej.
2. Zasilanie 230 V AC.

Gwarancja i wsparcie

1. Gwarancja producenta na macierz i dyski do dnia 31 grudnia 2026 r., na zasadach określonych w pkt 2.2.
2. Gwarancja obejmuje naprawę lub wymianę urządzenia i dysków oraz dostęp do aktualizacji oprogramowania.

Poz. 1.17 – Macierz dyskowa NAS nr 2 – dedykowana stacja kopii zapasowych maszyn wirtualnych i serwerów z deduplikacją – dostawa

Przedmiotem pozycji jest dostawa macierzy NAS o parametrach nie gorszych niż określone dla poz. 1.2 (ten sam typ urządzenia i dysków: 8 dysków HDD klasy enterprise o pojemności co najmniej 16 TB każdy), pełniącej rolę dedykowanego repozytorium kopii zapasowych maszyn wirtualnych, serwerów fizycznych i stacji krytycznych z deduplikacją danych. Konfiguracja macierzy i systemu kopii zapasowych jest przedmiotem poz. 1.13.

Lokalizacja i okablowanie

1. Macierz jest instalowana w pomieszczeniu wskazanym przez Zamawiającego w jego siedzibie, odrębnym od serwerowni: w innej strefie pożarowej tego samego budynku lub w budynku sąsiednim połączonym istniejącą infrastrukturą kablową Zamawiającego.
2. Wykonawca zapewnia okablowanie miedziane między macierzą a punktem dystrybucyjnym wskazanym przez Zamawiającego, o długości trasy do 50 m.
3. Jeżeli lokalizacja wymaga łącza światłowodowego, Zamawiający udostępnia istniejące włókna, a Wykonawca dostarcza kartę sieciową SFP+ do macierzy oraz wkładki.

Wymagania dodatkowe

1. Obsługa repozytorium kopii zapasowych dla oprogramowania z poz. 1.4 jako udziału SMB3, jednostki iSCSI lub repozytorium obiektowego S3, zgodnie z projektem.
2. Wydajność repozytorium umożliwia zapis kopii przez interfejs 10 GbE.
3. Ochrona repozytorium migawkami niemodyfikowalnymi (immutable) z okresem ochrony nie krótszym niż 14 dni.
4. Wbudowane lub dostarczone z licencją oprogramowanie kopii zapasowych z deduplikacją globalną na poziomie bloków dla stacji roboczych i serwerów fizycznych (Windows, Linux) oraz maszyn wirtualnych, jako uzupełnienie systemu z poz. 1.4, bez dodatkowych opłat licencyjnych.

5. Odrębne konta uwierzytelniania dla systemu kopii, poza domeną produkcyjną, oraz MFA dla administratorów.
6. Macierz nie należy do domeny produkcyjnej. Dopuszcza się integrację z Active Directory wyłącznie w trybie odczytu, do celów uprawnień do odtwarzania.
7. Macierz jest izolowana w odrębnej strefie sieciowej (poz. 1.12).
8. Możliwość replikacji migawek z macierzą z poz. 1.2 (poz. 1.19) oraz wysyłania kopii do repozytorium chmurowego (poz. 1.18) lub do usługi chmurowej producenta.

Poz. 1.4 – Oprogramowanie do kopii zapasowych maszyn wirtualnych i serwerów z deduplikacją – licencja na 10 instancji

Przedmiotem pozycji jest dostawa licencji oprogramowania do kopii zapasowych klasy Veeam Data Platform (w edycji umożliwiającej ochronę maszyn wirtualnych i serwerów fizycznych w modelu uniwersalnym) lub równoważnego, dla co najmniej 10 instancji (maszyn wirtualnych, serwerów fizycznych lub stacji roboczych w dowolnej kombinacji), z subskrypcją i wsparciem producenta do dnia 31 grudnia 2026 r. Instalacja i konfiguracja jest przedmiotem poz. 1.13.

Kopie zapasowe

1. Bezagentowe kopie zapasowe maszyn wirtualnych platformy z poz. 1.15 na poziomie hosta, ze śledzeniem zmienionych bloków (CBT).
2. Kopie przyrostowe w trybie „forever incremental” z syntetycznymi kopiami pełnymi.
3. Kopie świadome aplikacji (Microsoft SQL Server, Active Directory) z obcinaniem logów transakcyjnych.
4. Agenty dla serwerów fizycznych i stacji roboczych Windows oraz Linux, w ramach tej samej puli instancji.
5. Kopie obrazów i plików oraz odtwarzanie bare-metal, w tym na inny sprzęt.
6. Centralne zarządzanie agentami z konsoli.
7. Wbudowana deduplikacja i kompresja danych kopii (inline).
8. Szyfrowanie kopii AES-256 z hasłem lub kluczem pozostającym w dyspozycji Zamawiającego.
9. Weryfikacja integralności kopii co najmniej przez weryfikację sum kontrolnych (health check).
10. Zalecane (nie podlega ocenie): automatyczne testy odtwarzalności przez uruchomienie kopii w izolowanym środowisku.

Repozytoria i odtwarzanie

1. Repozytoria na udziałach SMB i NFS, jednostkach iSCSI oraz w repozytoriach obiektowych S3, w tym chmurowych z blokadą niemodyfikowalności.
2. Repozytoria z blokadą niemodyfikowalności kopii (immutability).
3. Repozytorium typu scale-out z warstwą pojemnościową w chmurze (poz. 1.18).
4. Realizacja reguły 3-2-1-1 przez kopie kopii (backup copy), replikację i kopie niemodyfikowalne.
5. Odtwarzanie całych maszyn wirtualnych oraz natychmiastowe uruchomienie maszyny z kopii (instant recovery).
6. Odtwarzanie pojedynczych plików i folderów oraz elementów aplikacji (obiekty Active Directory, bazy SQL).
7. Odtwarzanie do platformy wirtualizacji z poz. 1.15 oraz na sprzęt fizyczny.

Zarządzanie i licencja

1. Retencja według zasad GFS (kopie dzienne, tygodniowe, miesięczne), harmonogramy, okna kopii i ograniczanie obciążenia.

2. Powiadomienia e-mail o wynikach zadań i błędach oraz raporty.
3. Role administracyjne oraz MFA dla konsoli.
4. Przekazywanie zdarzeń do SYSLOG/SIEM.
5. Licencja subskrypcyjna dla co najmniej 10 instancji, zarejestrowana na Zamawiającego, ze wsparciem i aktualizacjami producenta do dnia 31 grudnia 2026 r., na zasadach określonych w pkt 2.2.

Poz. 1.18 – Chroniony kryptograficznie backup w chmurze – repozytorium kopii zapasowych o pojemności 8 TB

Przedmiotem pozycji jest dostawa usługi chmurowego repozytorium kopii zapasowych klasy Veeam Data Cloud Vault (edycja Foundation) lub równoważnej, o pojemności 8 TB, zintegrowanej z oprogramowaniem z poz. 1.4. Repozytorium służy do przechowywania poza siedzibą Zamawiającego szyfrowanych, niemodyfikowalnych kopii wybranych zasobów: systemów dziedzinowych, baz danych, kontrolerów domeny, kluczowych zasobów plikowych oraz konfiguracji urządzeń i systemów bezpieczeństwa. Usługa jest opłacona od dnia aktywacji do dnia 31 grudnia 2026 r. Konfiguracja jest przedmiotem poz. 1.13.

Wymagania

1. Repozytorium obiektowe w chmurze, w pełni zarządzane przez dostawcę usługi, o pojemności co najmniej 8 TB.
2. Dostęp przez protokół S3 lub natywną integrację z oprogramowaniem z poz. 1.4 jako repozytorium kopii, w tym jako warstwa pojemnościowa repozytorium scale-out.
3. Niezmienność danych (immutability, object lock) z konfigurowalnym okresem ochrony zarządzanym przez oprogramowanie kopii.
4. Ochrona przed usunięciem kopii przez skompromitowane konto: poświadczenia dostępu do repozytorium odrębne od poświadczeń serwera kopii zapasowych.
5. Szyfrowanie kopii przed wysłaniem, po stronie Zamawiającego, z kluczem lub hasłem wyłącznie w dyspozycji Zamawiającego.
6. Szyfrowanie transmisji TLS oraz szyfrowanie w spoczynku po stronie dostawcy.
7. Dane są przechowywane w centrach danych na terenie Unii Europejskiej.
8. Umowa powierzenia przetwarzania danych osobowych i warunki zgodne z RODO.
9. Trwałość przechowywania co najmniej 99,999999999% w skali roku.
10. Cena obejmuje opłaty za przechowywanie, operacje API oraz pobieranie danych w celu odtworzenia w wymiarze co najmniej 20% pojemności repozytorium w skali roku.

Wdrożenie (w ramach poz. 1.13)

1. Wybór zasobów kopiowanych do chmury następuje według wskazań Zamawiającego, na podstawie posiadanej przez niego analizy ryzyka.
2. Konfiguracja zadań kopii do chmury.
3. Bezpieczne zdeponowanie klucza szyfrującego wraz z procedurą awaryjnego dostępu.
4. Test odtworzenia danych z chmury.
5. Dokumentacja konfiguracji.

Poz. 1.19 – Konfiguracja redundancji macierzy NAS – replikacja danych pomiędzy macierzą NAS nr 1 i NAS nr 2

Redundancję macierzy zapewniają urządzenia z poz. 1.2 i 1.17. Przedmiotem pozycji jest konfiguracja ich wzajemnej replikacji, tak aby kluczowe dane były przechowywane w dwóch niezależnych urządzeniach w odrębnych lokalizacjach w siedzibie Zamawiającego.

1. Dane operacyjne z macierzy NAS nr 1 są replikowane na macierz NAS nr 2.
2. Repozytorium kopii zapasowych z macierzy NAS nr 2, lub jego wskazana część, jest replikowane na macierz NAS nr 1.
3. Harmonogram replikacji jest zgodny z RPO określonym przez Zamawiającego, nie rzadziej niż co 1 godzinę dla danych operacyjnych.
4. Transmisja replikacji jest szyfrowana.
5. Replika jest chroniona migawkami niemodyfikowalnymi.
6. Stan replikacji jest monitorowany z alarmowaniem w systemie z poz. 1.6.
7. Wykonawca opracuje i przetestuje procedurę przełączenia udziałów na replikę (failover) i powrotu (failback).
8. Wykonawca opracuje i przetestuje procedurę odtworzenia danych z repliki.
9. Dokumentacja konfiguracji replikacji i procedur.

Poz. 1.13 – Usługa instalacji, konfiguracji i wsparcia serwera, platformy wirtualizacji, macierzy NAS oraz systemu kopii zapasowych

Przedmiotem pozycji jest usługa uruchomienia infrastruktury dostarczanej w poz. 1.2, 1.4, 1.15, 1.16, 1.17 i 1.18: analiza, projekt, instalacja, konfiguracja, migracja, testy i dokumentacja oraz wsparcie powdrożeniowe do dnia 31 grudnia 2026 r.

Analiza i projekt

1. Analiza przedwdrożeniowa w formie warsztatów z Zamawiającym i dostawcami systemów dziedzinowych: inwentaryzacja serwerów, maszyn wirtualnych, usług i danych.
2. Określenie wymagań wydajnościowych i pojemnościowych w perspektywie 3–5 lat.
3. Określenie systemów objętych kopiami zapasowymi, parametrów RPO i RTO (uzgodnionych z Zamawiającym), retencji i przyrostu danych.
4. Wykaz licencji systemów operacyjnych posiadanych przez Zamawiającego.
5. Projekt architektury platformy wirtualizacji: rozmieszczenie maszyn wirtualnych na nowym hoście i hoście zapasowym, replikacja, sieci wirtualne i VLAN, w tym sieć zarządzania, sieć kopii zapasowych i sieć replikacji.
6. Projekt układu pamięci masowej serwera (RAID, wolumeny).
7. Projekt konfiguracji macierzy NAS: RAID 6 lub równoważny o odporności na awarię dwóch dysków, wolumeny, udziały, uprawnienia, migawki.
8. Projekt systemu kopii zapasowych zgodny z regułą 3-2-1-1: repozytoria, zadania, harmonogramy, retencja GFS, kopie niemodyfikowalne, kopia w chmurze.
9. Plan migracji i plan wycofania zmian.

Instalacja i konfiguracja serwera i macierzy

1. Montaż serwera i macierzy NAS nr 1 w szafie rack serwerowni oraz macierzy NAS nr 2 w lokalizacji wskazanej przez Zamawiającego.

2. Zasilanie z UPS (poz. 1.3) lub z zabezpieczonego obwodu.
3. Połączenia sieciowe serwera i macierzy do strefy serwerowej i strefy kopii zapasowych. Połączenia 10 GbE między serwerem a macierzami są realizowane bezpośrednio lub przez przełącznik 10 GbE, jeżeli Zamawiający go posiada.
4. Okablowanie zapewnia Wykonawca.
5. Aktualizacja oprogramowania układowego serwera i macierzy.
6. Konfiguracja kontrolera RAID oraz BIOS (Secure Boot, TPM, wyłączenie nieużywanych urządzeń).
7. Konfiguracja karty zarządzającej serwera: adresacja w strefie zarządzania, konta imienne, MFA, SYSLOG, SNMP.
8. Konfiguracja macierzy NAS nr 1: RAID, wolumeny, udziały i uprawnienia zgodnie z zasadą minimalnych uprawnień.
9. Integracja macierzy NAS nr 1 z Active Directory.
10. Migawki macierzy NAS nr 1, w tym niemodyfikowalne, z harmonogramem i retencją.
11. Szyfrowanie wskazanych w projekcie folderów współdzielonych lub wolumenów na macierzach.
12. MFA dla kont administracyjnych i wyłączenie domyślnych kont na macierzach.
13. Konfiguracja SYSLOG i SNMP na macierzach.
14. Migracja danych z dotychczasowej macierzy w zakresie wskazanym przez Zamawiającego, z zachowaniem uprawnień.
15. Ewentualne włączenie dotychczasowej macierzy jako dodatkowego celu kopii, zgodnie z projektem.
16. Konfiguracja macierzy NAS nr 2 jako repozytorium kopii: odrębne konta, izolacja sieciowa, migawki niemodyfikowalne oraz wbudowane oprogramowanie kopii dla stacji roboczych, jeżeli ujęto je w projekcie.

Platforma wirtualizacji i migracja

1. Instalacja systemu wirtualizacji (poz. 1.15) z hardeningiem zgodnym z zaleceniami producenta i CIS Benchmark.
2. Host pracuje wyłącznie z rolą wirtualizacji i niezbędnymi narzędziami.
3. Zarządzanie hostem odbywa się ze stacji administracyjnej, na konta imienne.
4. Dostęp administracyjny do hosta jest zabezpieczony MFA, jeżeli platforma to wspiera, a zdarzenia administracyjne są logowane.
5. Konfiguracja wirtualnych przełączników i VLAN.
6. Przyłączenie hosta do domeny lub praca w grupie roboczej, zgodnie z projektem i modelem administracji warstwowej (poz. 1.8).
7. Utworzenie maszyn wirtualnych dla systemów bezpieczeństwa Zadań 3 i 4, z zasobami zgodnymi z wymaganiami producentów i systemami Linux w wersjach LTS z aktualizacjami.
8. Przygotowanie szablonu maszyny wirtualnej z utwardzonym systemem.
9. Przeniesienie maszyn wirtualnych z kontrolera domeny na nową platformę, w uzgodnieniu z dostawcami systemów, w oknach serwisowych, z testami akceptacyjnymi aplikacji.
10. Wyłączenie roli wirtualizacji na kontrolerze domeny.
11. Konfiguracja replikacji maszyn krytycznych na host zapasowy wskazany w projekcie technicznym spośród posiadanych serwerów Zamawiającego, innych niż kontroler domeny.
12. Z uwagi na wymóg zgodności wersji systemu hosta repliki z hostem podstawowym Wykonawca stosuje replikację natywną platformy, jeżeli wersje na to pozwalają, albo replikację realizowaną przez oprogramowanie z poz. 1.4.

13. Procedura przełączenia replikowanych maszyn wraz z testem.

System kopii zapasowych

1. Instalacja serwera oprogramowania kopii zapasowych (poz. 1.4) na maszynie wirtualnej.
2. Serwer kopii jest instalowany jako utwardzone urządzenie programowe producenta oparte na systemie Linux albo na maszynie Windows Server w ramach licencji z poz. 1.15 lub licencji posiadanej przez Zamawiającego, zgodnie z bilansem instancji w projekcie.
3. Serwer kopii posiada odrębne poświadczenia, MFA i hardening.
4. Konfiguracja repozytoriów: macierz NAS nr 2 oraz repozytorium chmurowe z poz. 1.18.
5. Konfiguracja zadań kopii dla wszystkich maszyn wirtualnych, serwerów fizycznych (w tym serwera SCADA, w uzgodnieniu z dostawcą automatyki) oraz wskazanych stacji roboczych.
6. Konfiguracja harmonogramów, retencji GFS, kopii niemodyfikowalnych, szyfrowania, weryfikacji kopii i powiadomień.
7. Zastąpienie dotychczasowych mechanizmów kopii po okresie równoległej pracy trwającym co najmniej 5 dni.
8. Integracja hosta, maszyn wirtualnych, macierzy i zadań kopii z systemem monitoringu (poz. 1.6) i serwerem logów (poz. 1.22).

Testy

1. Test obciążeniowy serwera.
2. Testy awarii dysku, zasilacza i łącza sieciowego.
3. Test przełączenia replikowanej maszyny wirtualnej na host zapasowy.
4. Test odtworzenia pełnej maszyny wirtualnej.
5. Test odtworzenia serwera fizycznego (bare-metal do środowiska testowego lub maszyny wirtualnej).
6. Test odtworzenia pojedynczego pliku oraz bazy danych.
7. Test odtworzenia z repozytorium chmurowego.
8. Weryfikacja integralności danych po odtworzeniu oraz pomiar czasu odtworzenia względem RTO.
9. Raport z testów stanowi załącznik do protokołu odbioru.

Dokumentacja, instruktaż i wsparcie

1. Dokumentacja powykonawcza obejmuje konfigurację serwera, platformy wirtualizacji, macierzy i systemu kopii, wykaz maszyn wirtualnych i zasobów, schematy oraz procedury administracyjne.
2. Dokumentacja zawiera procedurę odtworzenia systemów po awarii (techniczna część DRP).
3. Instruktaż administratorów: platforma wirtualizacji i serwer – co najmniej 6 godzin, macierze – co najmniej 3 godziny, system kopii zapasowych – co najmniej 4 godziny.
4. Wsparcie powdrożeniowe do dnia 31 grudnia 2026 r. zgodnie z pkt 2.4.
5. Pula co najmniej 40 godzin prac inżynierskich do wykorzystania na zmiany konfiguracji, dodawanie maszyn wirtualnych i zadań kopii, aktualizacje, obsługę zdarzeń z systemów monitoringu i kopii zapasowych oraz konsultacje, wykorzystywana i rozliczana zgodnie z pkt 2.4.
6. Miesięczny raport wykorzystania puli godzin.

Poz. 1.3 – UPS centralny 10 kVA (on-line, 3/3) z kartą zarządzającą – dostawa, instalacja i uruchomienie

Przedmiotem pozycji jest dostawa, instalacja i uruchomienie centralnego zasilacza awaryjnego klasy EVER Powerline Green 10-33 PRO lub równoważnego, zabezpieczającego serwerownię Zamawiającego (serwery,

macierze, urządzenia sieciowe i bezpieczeństwa, serwer SCADA) przed skutkami zaniku i nieprawidłowości napięcia zasilającego.

Parametry elektryczne

1. Topologia on-line z podwójnym przetwarzaniem (VFI-SS-111 według PN-EN 62040-3).
2. Moc znamionowa nie mniejsza niż 10 kVA / 10 kW.
3. Wejście i wyjście trójfazowe 3×400 V (3/3).
4. Zakres napięcia wejściowego bez przejścia na baterie co najmniej 190–480 V.
5. Współczynnik mocy wejściowej nie mniejszy niż 0,99 oraz THDi poniżej 3%.
6. Sprawność w trybie on-line (VFI) nie mniejsza niż 93% przy obciążeniu znamionowym.
7. Tryb ECO o sprawności nie mniejszej niż 98%.

Baterie i bypass

1. Baterie szczelne VRLA AGM wewnętrzne, z możliwością dołączenia zewnętrznych modułów bateryjnych.
2. Czas podtrzymania przy obciążeniu 5 kW nie krótszy niż 10 minut.
3. Ładowanie prądem umożliwiającym odbudowę pojemności w czasie nie dłuższym niż 8 godzin.
4. Funkcja startu z baterii.
5. Bypass automatyczny oraz ręczny bypass serwisowy (wewnętrzny lub w postaci zewnętrznego panelu obejściowego), dostarczony w komplecie również wtedy, gdy u producenta stanowi wyposażenie opcjonalne.
6. Wejście EPO oraz wyjścia bezpotencjałowe.

Zarządzanie

1. Karta zarządzająca sieciowa (Ethernet RJ-45) dostarczona w komplecie również wtedy, gdy u producenta stanowi wyposażenie opcjonalne.
2. Obsługa SNMP co najmniej w wersji v2c, HTTPS oraz powiadomień e-mail.
3. Integracja z systemem monitoringu (poz. 1.6).
4. Oprogramowanie umożliwiające kontrolowane wyłączanie serwerów fizycznych, maszyn wirtualnych platformy z poz. 1.15 oraz macierzy NAS przez protokół obsługiwany przez macierz.
5. Panel LCD, rejestr zdarzeń oraz automatyczne i ręczne testy baterii.
6. Interfejsy RS-232 i USB.
7. Obudowa wolnostojąca.
8. Certyfikat CE oraz zgodność z PN-EN 62040-1 i PN-EN 62040-2.

Gwarancja i wsparcie

1. Gwarancja producenta na UPS i baterie do dnia 31 grudnia 2026 r., na zasadach określonych w pkt 2.2.
2. Serwis na terenie Polski z reakcją w miejscu instalacji nie dłuższą niż 2 dni robocze.
3. Dostęp do aktualizacji oprogramowania karty zarządzającej.

Instalacja i uruchomienie

1. Wykonawca zweryfikuje instalację elektryczną serwerowni (rozdzielnica, zabezpieczenia, przekroje, uziemienie).
2. Projekt podłączenia podlega uzgodnieniu z Zamawiającym.
3. Dostawa, rozładunek i ustawienie urządzenia w miejscu wskazanym przez Zamawiającego.
4. Podłączenie do instalacji elektrycznej wykonują osoby posiadające świadectwa kwalifikacyjne SEP (E i D).

5. Wykonanie obwodu zasilającego UPS z rozdzielnicy oraz obwodów odbiorczych dla urządzeń w szafie rack, w zakresie do 20 m tras kablowych, z niezbędnymi zabezpieczeniami.
6. Dostawa co najmniej 2 listew zasilających PDU 19" z co najmniej 8 gniazdami C13 i 2 gniazdami C19 każda.
7. Pomiary elektryczne z protokołem.
8. Uruchomienie przez serwis autoryzowany przez producenta oraz konfiguracja parametrów pracy.
9. Konfiguracja karty zarządzającej: adresacja w strefie zarządzania, konta imienne, SNMP (v3, jeżeli karta wspiera, w przeciwnym razie v2c tylko do odczytu), SYSLOG.
10. Integracja z systemem monitoringu i serwerem logów.
11. Konfiguracja sekwencji kontrolowanego wyłączania wskazanych systemów (kolejność: maszyny wirtualne, hosty, macierze) oraz ponownego uruchomienia.
12. Przełączenie odbiorników na zasilanie z UPS w oknie serwisowym.
13. Testy: przejście na zasilanie bateryjne i powrót, pomiar czasu podtrzymania przy rzeczywistym obciążeniu, test sekwencji wyłączania, test bypassu.
14. Dokumentacja powykonawcza: schemat zasilania, wykaz odbiorników, konfiguracja alarmów.
15. Instruktaż administratorów w wymiarze co najmniej 2 godzin.
16. Odbiór i zagospodarowanie opakowań oraz urządzeń i baterii wycofywanych z eksploatacji, zgodnie z przepisami o odpadach, zużytym sprzęcie elektrycznym i elektronicznym oraz bateriach i akumulatorach.

3.4. Systemy bezpieczeństwa i monitorowania

Poz. 1.5 – Platforma XDR/EDR (open source) – wdrożenie ochrony punktów końcowych IT

Przedmiotem pozycji jest wdrożenie platformy klasy XDR opartej na oprogramowaniu open source Wazuh lub równoważnym w infrastrukturze Zamawiającego oraz objęcie ochroną agentami EDR punktów końcowych środowiska IT: stacji roboczych, serwerów fizycznych i wirtualnych oraz hostów wirtualizacji (na dzień przygotowania OPZ około 45 systemów, przy czym Wykonawca przyjmuje do wyceny maksymalnie 50 systemów; z wyłączeniem hostów OT objętych poz. 2.1). Dotychczasowe oprogramowanie antywirusowe Zamawiającego pozostaje w eksploatacji jako warstwa ochrony przed złośliwym oprogramowaniem.

1. Zakres poz. 1.5 obejmuje platformę, agentów, funkcje EDR i reagowanie.
2. Zakres poz. 1.22 obejmuje podłączenie źródeł infrastrukturalnych, retencję, archiwum i raportowanie.
3. Ochrona punktów końcowych OT jest przedmiotem poz. 2.1.

Architektura

1. Rozwiązanie instalowane lokalnie (on-premise) na platformie wirtualizacji z poz. 1.15.
2. Komponenty: serwer analityczny (manager), warstwa indeksująca i przechowująca dane, interfejs webowy oraz agenty instalowane na monitorowanych systemach.
3. Możliwość instalacji rozproszonej i skalowania warstwy indeksującej.
4. Brak wymogu stałego połączenia z chmurą producenta.
5. Pełna administracja przez Zamawiającego bez konieczności wykupienia subskrypcji.
6. Kod źródłowy dostępny na licencji open source.
7. Dla rozwiązania komercyjnego, dopuszczonego na zasadach pkt 2.3, wymagana jest licencja wieczysta albo aktywna do dnia 31 grudnia 2026 r., bez limitu agentów poniżej 100 i źródeł SYSLOG poniżej 50.
8. Szyfrowana komunikacja TLS między agentami a serwerem oraz między komponentami.
9. Kontrola dostępu oparta na rolach (RBAC).

10. Uwierzytelnianie administratorów z MFA, natywnie lub przez dostawcę tożsamości z poz. 1.24 (SAML/OIDC).
11. Rejestrowanie działań administratorów.

Funkcje agentów i detekcji

1. Agenty dla systemów Windows 10/11, Windows Server 2016–2025 oraz Linux.
2. Zbieranie logów systemowych i aplikacyjnych.
3. Monitorowanie integralności plików (FIM) i rejestru Windows.
4. Inwentaryzacja systemu: sprzęt, oprogramowanie, porty, procesy.
5. Wykrywanie podatności na podstawie bazy CVE.
6. Ocena zgodności konfiguracji z CIS Benchmarks (SCA).
7. Monitorowanie poleceń i procesów oraz wykrywanie rootkitów.
8. Monitorowanie zdarzeń podłączenia urządzeń USB.
9. Reguły detekcji mapowane na MITRE ATT&CK, z możliwością definiowania własnych reguł i dekoderów oraz modyfikowania istniejących.
10. Korelacja zdarzeń z wielu źródeł: punkty końcowe, serwery, urządzenia sieciowe, firewall, platforma wirtualizacji.
11. Grupowanie zdarzeń w incydenty oraz oś czasu incydentu.
12. Wykrywanie ruchu bocznego (lateral movement) i podejrzanych procesów.
13. Integracja z bazami reputacyjnymi (threat intelligence).

Reagowanie i integracje

1. Reagowanie automatyczne (active response): blokada adresu IP na hoście, zakończenie procesu, dezaktywacja konta, izolacja hosta od sieci z zachowaniem komunikacji z serwerem zarządzającym oraz uruchomienie skryptu.
2. Własne scenariusze reakcji oraz reakcja ręczna z konsoli.
3. Funkcje reakcji nieobjęte skryptami producenta platformy Wykonawca realizuje skryptami własnymi, przekazanymi Zamawiającemu wraz z dokumentacją i wynikami testów.
4. Integracja z urządzeniami sieciowymi przez SYSLOG oraz z Active Directory.
5. Integracja z systemem ESET PROTECT Zamawiającego (import alertów), platformą wirtualizacji i systemem kopii zapasowych.
6. Alerty e-mail i webhook (komunikator, system zgłoszeń).
7. Eksport surowych logów i danych incydentu oraz interfejs API.
8. Obsługa co najmniej 100 agentów i 50 źródeł SYSLOG, z możliwością rozbudowy.
9. Zasoby maszyn wirtualnych dobiera Wykonawca z uwzględnieniem retencji wymaganej w poz. 1.22.
10. Odbiór logów z systemów OT przez kolektor w strefie pośredniej, bez bezpośredniego dostępu z sieci IT do urządzeń przemysłowych (wykorzystywany w poz. 2.1 i 2.5).

Zakres wdrożenia

1. Analiza przedwdrożeniowa: wykaz systemów, źródeł i wymagań retencji.
2. Projekt architektury jako rozdział projektu technicznego Zadania 1.
3. Instalacja komponentów na utwardzonych maszynach wirtualnych.
4. Konfiguracja TLS i certyfikatów, RBAC oraz MFA.
5. Kopie zapasowe konfiguracji i danych platformy w systemie z poz. 1.4.

6. Instalacja agentów na wszystkich stacjach roboczych i serwerach IT, z dystrybucją przez GPO lub narzędzie zarządzania.
7. Konfiguracja FIM dla katalogów systemowych i konfiguracji aplikacji.
8. Konfiguracja SCA według CIS dla Windows 10/11 i Windows Server oraz wykrywania podatności.
9. Zbieranie zdarzeń bezpieczeństwa Windows, w tym instalacja i konfiguracja narzędzia Sysmon lub równoważnego z zestawem reguł oraz monitorowanie PowerShell.
10. Reguły detekcji obejmujące co najmniej: próby nieautoryzowanego dostępu i ataki brute force, eskalację uprawnień, zmiany w grupach uprzywilejowanych i politykach domenowych, modyfikację kluczowych plików, wykonanie podejrzanych procesów i skryptów, wskaźniki ransomware oraz podatności krytyczne.
11. Okres uczenia i strojenie reguł ograniczające fałszywe alarmy.
12. Scenariusze reakcji automatycznej uzgodnione z Zamawiającym, w tym wyłączenia dla serwerów krytycznych.
13. Pulpity operacyjne: stan agentów, alerty według ważności, podatności, zgodność SCA.
14. Raporty okresowe dla administratora i kierownictwa.
15. Procedura obsługi alertu spójna z procedurą zarządzania incydentami Zamawiającego.

Testy, dokumentacja, instruktaż i wsparcie

1. Symulacja zdarzeń testowych (np. Atomic Red Team lub narzędzie równoważne) z weryfikacją detekcji i reakcji.
2. Test izolacji hosta.
3. Raport z testów stanowi załącznik do protokołu odbioru.
4. Dokumentacja powykonawcza obejmuje architekturę, wykaz agentów i źródeł, reguły oraz procedurę reagowania.
5. Instruktaż administratorów w wymiarze co najmniej 8 godzin.
6. Pula co najmniej 16 godzin konsultacji, wykorzystywana i rozliczana zgodnie z pkt 2.4.

Poz. 1.22 – Scentralizowany serwer logów – menedżer logów / SIEM (open source) – wdrożenie

Przedmiotem pozycji jest uruchomienie na platformie z poz. 1.5 funkcji scentralizowanego serwera logów gromadzącego, normalizującego i przechowującego logi z infrastruktury Zamawiającego (źródła inne niż agenty z poz. 1.5), wraz z retencją, archiwum, regułami alertowania i raportowaniem. Zamawiający dopuszcza realizację tej funkcji przez odrębny komponent open source (np. Graylog lub równoważny) zintegrowany z platformą z poz. 1.5, jeżeli wynika to z projektu technicznego.

Źródła logów

1. Odbiór logów przez SYSLOG (UDP, TCP, TLS) z urządzeń sieciowych i systemów.
2. Odbiór dzienników zdarzeń Windows przez agentów z poz. 1.5 lub Windows Event Forwarding.
3. Odbiór plików logów aplikacji oraz logów przez API.
4. Parsowanie i normalizacja co najmniej dla: firewalla (poz. 1.1), przełączników i kontrolera WLAN, serwerów Windows i kontrolerów domeny (w tym zdarzeń uwierzytelniania, zmian w AD i zdarzeń audytu), platformy wirtualizacji, kart zarządzających serwerów, macierzy NAS, systemu kopii zapasowych, UPS, systemu ESET PROTECT, WAF (poz. 1.7), dostawcy tożsamości i MFA (poz. 1.24), menedżera haseł (poz. 1.23) oraz systemu monitoringu (poz. 1.6).
5. Odbiór logów z urządzeń UTM OT i systemu IDS OT (Zadanie 2) przez strefę pośrednią.

Retencja i integralność

1. Dane indeksowane (przeszukiwalne) są przechowywane co najmniej 180 dni.
2. Archiwum surowych logów jest przechowywane co najmniej 12 miesięcy w postaci skompresowanej, z sumami kontrolnymi umożliwiającymi kontrolę integralności.
3. Automatyczne zarządzanie cyklem życia danych.
4. Weryfikacja synchronizacji czasu NTP wszystkich źródeł.
5. Konta źródeł nie posiadają uprawnień do modyfikacji logów.
6. Kopie archiwum są wykonywane w systemie kopii zapasowych.

Analiza, alerty i dostęp

1. Wyszukiwanie pełnotekstowe i filtrowanie oraz pulpity operacyjne.
2. Reguły alertów obejmujące co najmniej: nieudane logowania i ataki brute force, logowania kont uprzywilejowanych poza godzinami pracy, zmiany w grupach uprzywilejowanych AD, zmiany konfiguracji urządzeń sieciowych i firewalla, utratę tuneli VPN, błędy kopii zapasowych, alerty EDR, IDS i WAF oraz zatrzymanie strumienia logów ze źródła.
3. Powiadomienia e-mail i webhook.
4. Raporty okresowe, w tym tygodniowy raport bezpieczeństwa.
5. RBAC oraz integracja z Active Directory lub dostawcą tożsamości, z MFA.
6. Rejestrowanie działań administratorów serwera logów.

Testy, dokumentacja i instruktaż

1. Zdarzenia testowe z każdego źródła oraz wyzwolenie każdej reguły alertu.
2. Dokumentacja obejmuje listę źródeł i formatów, reguły, retencję oraz procedurę przeglądu logów spójną z procedurami Zamawiającego.
3. Instruktaż administratorów w wymiarze co najmniej 4 godzin.

Poz. 1.6 – System monitoringu infrastruktury IT/OT (Zabbix lub równoważny) – wdrożenie

Przedmiotem pozycji jest wdrożenie systemu monitorowania dostępności i wydajności infrastruktury IT oraz wybranych elementów środowiska OT Zamawiającego z wykorzystaniem oprogramowania Zabbix w wersji LTS lub równoważnego. Dotychczasowy system monitoringu eksploatowany przez dostawcę usług IT Zamawiającego nie jest przedmiotem migracji.

Architektura i funkcje

1. Rozwiązanie instalowane lokalnie (on-premise) na platformie z poz. 1.15, bez wymogu stałego połączenia z chmurą producenta i bez konieczności wykupienia subskrypcji.
2. Komponenty: serwer monitoringu, baza danych, interfejs webowy, agenty oraz komponent pośredniczący (proxy).
3. Komponent proxy umożliwia monitorowanie odseparowanych segmentów sieci, w tym strefy OT i obiektów za tunelami VPN.
4. Monitoring przez ICMP, SNMP v2c/v3 (w tym trapy), agentów Windows i Linux, IPMI/Redfish, HTTP/API oraz JMX.
5. Monitorowanie certyfikatów TLS i usług sieciowych.
6. Wykrywanie niskopoziomowe (LLD) interfejsów, dysków i systemów plików.
7. Własne szablony i elementy monitorowania.

8. Zależności między wyzwalaczami, wielopoziomowe progi alarmowe, eskalacje oraz harmonogramy przerw serwisowych.
9. Powiadomienia e-mail i webhook (komunikator, SMS przez bramkę, jeżeli Zamawiający ją posiada).
10. Pulpity operacyjne z odrębną prezentacją IT i OT, mapy sieci oraz raporty dostępności (SLA).
11. Retencja danych historycznych co najmniej 180 dni, a trendów co najmniej 2 lata.
12. Skalowalność do co najmniej 300 urządzeń.
13. Szyfrowanie komunikacji agent/proxy–serwer (TLS lub PSK).
14. RBAC oraz integracja z Active Directory (LDAP) lub dostawcą tożsamości (SAML), z MFA dla interfejsu webowego.
15. Rejestrowanie zmian konfiguracji oraz otwarte API do integracji z serwerem logów.

Zakres wdrożenia

1. Analiza przedwdrożeniowa: wykaz monitorowanych zasobów IT i OT z uwzględnieniem zasad separacji.
2. Projekt jako rozdział projektu technicznego Zadania 1.
3. Instalacja serwera, bazy danych, interfejsu i proxy na utwardzonych maszynach wirtualnych.
4. Instalowana wersja LTS jest objęta pełnym wsparciem producenta. Dla nowej gałęzi LTS instalacja następuje po wydaniu pierwszej wersji poprawkowej.
5. Kopie zapasowe konfiguracji i bazy danych systemu.
6. Objęcie monitoringiem firewalla, w tym stanu tuneli VPN, łączy WAN, sesji i licencji.
7. Objęcie monitoringiem przełączników, kontrolera i punktów dostępowych WLAN.
8. Objęcie monitoringiem serwerów fizycznych (w tym kart zarządzających), hostów i maszyn wirtualnych (w tym replikacji).
9. Objęcie monitoringiem kontrolerów domeny i usług: AD, DNS, DHCP, SQL, RDS oraz serwera eBOK.
10. Objęcie monitoringiem macierzy NAS (w tym replikacji i migawek) oraz UPS.
11. Objęcie monitoringiem systemów bezpieczeństwa: platformy XDR, WAF, dostawcy tożsamości, menedżera haseł oraz systemu kopii zapasowych (status zadań).
12. Monitorowanie certyfikatów TLS i dostępności usług publikowanych.
13. Monitoring elementów OT przez proxy w strefie pośredniej lub OT, z ruchem ograniczonym do niezbędnych portów i protokołów, bez bezpośredniego dostępu z sieci IT do urządzeń przemysłowych.
14. Monitoring OT obejmuje serwer i stanowiska SCADA (agent lub SNMP), urządzenia UTM w obiektach (poz. 2.6) i ich tunele, sondę i serwer IDS OT (poz. 2.2–2.5) oraz dostępność urządzeń w obiektach osiągalnych przez tunele VPN i APN (ICMP/SNMP, w zakresie uzgodnionym z dostawcą automatyki).
15. Progi alarmowe są konfigurowane odrębnie dla IT i OT.
16. Konfiguracja pulpitów, map, raportów dostępności oraz powiadomień dla osób wskazanych przez Zamawiającego, w tym administratora IT i dostawcy usług IT.
17. Przekazywanie zdarzeń krytycznych do serwera logów (poz. 1.22).

Testy, dokumentacja, instruktaż i wsparcie

1. Symulacja niedostępności urządzenia IT i elementu OT, przekroczenia progu oraz utraty tunelu, z weryfikacją alarmów i powiadomień.
2. Dokumentacja obejmuje architekturę, listę monitorowanych zasobów, szablony oraz procedurę dodawania hosta.
3. Instruktaż administratorów w wymiarze co najmniej 6 godzin.
4. Pula co najmniej 16 godzin konsultacji, wykorzystywana i rozliczana zgodnie z pkt 2.4.

Poz. 1.7 – Zapora aplikacyjna WAF (open source) dla systemu eBOK – wdrożenie

Przedmiotem pozycji jest wdrożenie zapory aplikacyjnej (Web Application Firewall) opartej na oprogramowaniu open source (BunkerWeb, ModSecurity lub Coraza z OWASP Core Rule Set, lub równoważne), chroniącej system Elektronicznego Biura Obsługi Klienta (eBOK) publikowany z infrastruktury Zamawiającego.

Wymagania

1. Rozwiązanie programowe instalowane lokalnie na platformie z poz. 1.15 (maszyna wirtualna lub kontenery), w strefie DMZ.
2. Praca w trybie reverse proxy z możliwością ochrony wielu aplikacji.
3. Brak ograniczeń licencyjnych liczby chronionych aplikacji i ruchu.
4. Aktualizacje reguł dostępne bez opłat lub z subskrypcją do dnia 31 grudnia 2026 r.
5. Ochrona przed zagrożeniami z listy OWASP Top 10 (w tym SQL Injection, XSS, RCE, LFI/RFI, path traversal) na podstawie zestawu reguł OWASP CRS z konfigurowalnym poziomem restrykcyjności (paranoia level).
6. Wirtualne łatanie przez własne reguły.
7. Ochrona przed botami i skanowaniem, w tym wykrywanie niepożądanych botów oraz mechanizmy weryfikacji klienta (challenge).
8. Limity liczby żądań i połączeń (rate limiting) ograniczające skutki ataków DoS w warstwie 7.
9. Blokowanie geolokalizacyjne i reputacyjne (listy adresów IP).
10. Ochrona przed atakami brute force na formularze logowania.
11. Terminacja TLS 1.2/1.3 z bezpiecznymi zestawami szyfrów oraz obsługa certyfikatów automatycznych (ACME) i własnych.
12. HSTS, nagłówki bezpieczeństwa (w tym CSP i X-Frame-Options) oraz przekierowanie HTTP na HTTPS.
13. Tryby wykrywania i blokowania, reguły wyjątków dla poszczególnych aplikacji i ścieżek, białe listy adresów administracyjnych oraz strony błędów.
14. Logowanie żądań i zdarzeń bezpieczeństwa do serwera logów (poz. 1.22) w formacie umożliwiającym analizę.
15. Interfejs administracyjny z uwierzytelnianiem i MFA, natywnie lub przez dostawcę tożsamości.
16. Automatyczne aktualizacje reguł i list.

Zakres wdrożenia

1. Projekt przepływu ruchu (Internet – firewall z IPS – WAF w DMZ – aplikacja) uzgodniony z dostawcą systemu eBOK.
2. Instalacja i hardening maszyny wirtualnej WAF.
3. Konfiguracja ochrony systemu eBOK: tryb uczenia i wykrywania przez co najmniej 7 dni, strojenie wyjątków z udziałem dostawcy aplikacji, a następnie przełączenie do trybu blokowania.
4. Przełączenie publikacji systemu eBOK na WAF w oknie serwisowym (zmiana NAT i DNS), z planem wycofania zmian.

Testy, dokumentacja i instruktaż

1. Skan podatności aplikacji przez WAF (np. OWASP ZAP lub narzędzie równoważne) z porównaniem wyników przed i po wdrożeniu.
2. Weryfikacja blokowania ataków testowych.
3. Test funkcjonalny aplikacji z udziałem dostawcy systemu eBOK oraz test wydajności.

4. Dokumentacja obejmuje konfigurację, reguły oraz procedurę dodawania aplikacji i obsługi fałszywych alarmów.
5. Instruktaż administratorów w wymiarze co najmniej 2 godzin.

Poz. 1.8 – Hardening konfiguracji systemów operacyjnych serwerów i stacji roboczych oraz usługi katalogowej Active Directory

Przedmiotem pozycji jest hardening konfiguracji systemów operacyjnych serwerów (Windows Server, Linux) i stacji roboczych (Windows 10/11) Zamawiającego oraz usługi katalogowej Active Directory (jedna domena, dwa kontrolery), zgodnie z CIS Benchmarks lub równoważnymi (np. Microsoft Security Baselines), z uwzględnieniem wymagań systemów dziedzinowych i systemu SCADA.

Analiza i plan

1. Analiza konfiguracji serwerów, stacji roboczych i Active Directory względem CIS Benchmarks, narzędziowa (np. CIS-CAT, moduł SCA platformy z poz. 1.5) oraz manualna.
2. Analiza Active Directory obejmuje Default Domain Policy, uprawnienia, delegacje, konta usługowe, zaufania, replikację i DNS.
3. Raport z lukami i oceną ryzyka sporządzony przed przystąpieniem do prac.
4. Plan hardeningu uzgodniony z Zamawiającym i dostawcami aplikacji (systemy dziedzinowe, SCADA), z podziałem na etapy, grupą pilotażową i planem wycofania zmian.

Active Directory

1. Model warstwowy administracji (tiering): oddzielne konta i stacje administracyjne dla warstwy kontrolerów domeny, serwerów i stacji.
2. Rozdzielenie kont administracyjnych od kont użytkowych.
3. Eliminacja kont współdzielonych o uprawnieniach administratora domeny, w tym kont dostawców, które są zastępowane kontami imiennymi z ograniczonymi uprawnieniami i czasem ważności.
4. Zastosowanie grupy Protected Users.
5. Polityki haseł i blokady kont, w tym polityki szczegółowe dla kont uprzywilejowanych i usługowych.
6. Przegląd i uporządkowanie kont usługowych (gMSA tam, gdzie możliwe), struktury OU, obiektów nieaktywnych i delegacji.
7. Ochrona przed atakami na środowisko domenowe: wyłączenie NTLMv1, LLMNR, NBT-NS i SMBv1, wymuszenie podpisywania SMB i LDAP, LDAP channel binding oraz ograniczenie replikacji i uprawnień DCSync.
8. Kopie zapasowe stanu systemu kontrolerów domeny w systemie z poz. 1.4.
9. Wdrożenie Windows LAPS lub równoważnego dla lokalnych kont administratorów na wszystkich serwerach i stacjach.

Urząd certyfikacji

1. Uruchomienie urzędu certyfikacji Zamawiającego (Active Directory Certificate Services lub równoważny).
2. Urząd certyfikacji obsługuje co najmniej: LDAPS, uwierzytelnianie 802.1X (poz. 1.14), certyfikaty serwerów wewnętrznych (interfejsy administracyjne, platformy z poz. 1.5 i 1.6) oraz logowanie kartą inteligentną (PIV) dla kont administracyjnych (poz. 1.24 i 1.25).
3. Szablony certyfikatów oraz automatyczna rejestracja przez GPO.
4. Zabezpieczenie kluczy urzędu oraz procedura odnowienia certyfikatów.

Polityki GPO

1. Zestaw obiektów GPO bezpieczeństwa dla kontrolerów domeny, serwerów i stacji roboczych.
2. Polityka audytu zgodna z zaleceniami, z przekazywaniem zdarzeń do serwera logów.
3. Ograniczenie RDP do uprawnionych grup i stref zarządzania, z NLA.
4. Blokada makr z Internetu i ochrona pakietu Office.
5. Polityki PowerShell z logowaniem.
6. Kontrola nośników USB: blokada lub ograniczenie zapisu, z udokumentowanymi wyjątkami.
7. Zapora Windows z regułami dla stref oraz ochrona przed exploitami.
8. Wyłączenie zbędnych usług i protokołów oraz blokada ekranu.
9. Szyfrowanie dysków komputerów przenośnych (BitLocker) z depozytem kluczy w Active Directory.
10. Konfiguracja aktualizacji przez Windows Update for Business lub WSUS.
11. Każdy obiekt GPO jest udokumentowany.

Serwery i stacje robocze

1. Wyłączenie zbędnych ról i usług na serwerach oraz rozdzielenie ról, w tym wyniesienie roli wirtualizacji z kontrolera domeny we współpracy z poz. 1.13.
2. Hardening serwera terminalowego (RDS).
3. Hardening serwera SQL: konta, szyfrowanie połączeń, kopie.
4. Hardening serwera eBOK (Linux) w zakresie uzgodnionym z dostawcą aplikacji: aktualizacje, SSH, zapora, konta.
5. Na serwerze SCADA i stanowiskach dyspozytorskich wprowadza się wyłącznie zmiany zatwierdzone przez dostawcę automatyki, w oknach serwisowych.
6. Wdrożenie zestawu GPO na wszystkich stacjach roboczych.
7. Usunięcie uprawnień administratora lokalnego użytkowników, z wyjątkami uzasadnionymi i udokumentowanymi.
8. Inwentaryzacja i usunięcie nieautoryzowanego oprogramowania zdalnego dostępu.
9. Konfiguracja przeglądarek zgodnie z poz. 1.21.

Testy, dokumentacja, instruktaż i wsparcie

1. Ponowny pomiar zgodności z CIS, z raportem przed/po dla każdej kategorii systemów.
2. Test działania aplikacji dziedzinowych po zmianach.
3. Dokumentacja obejmuje strukturę domeny i model administracji, wykaz GPO, odstępstwa z uzasadnieniem, procedury administracyjne oraz konfigurację PKI i LAPS.
4. Instruktaż administratorów w wymiarze co najmniej 4 godzin.
5. Pula co najmniej 8 godzin konsultacji, wykorzystywana i rozliczana zgodnie z pkt 2.4.

3.5. Tożsamość i dostęp

Poz. 1.23 – Kryptograficzny menedżer haseł (open source, on-premise) – wdrożenie

Przedmiotem pozycji jest wdrożenie centralnego menedżera haseł opartego na oprogramowaniu open source (np. Vaultwarden w wersji co najmniej 1.35, zgodny z klientami Bitwarden, albo Passbolt, lub rozwiązanie równoważne), instalowanego lokalnie w infrastrukturze Zamawiającego, dla administratorów IT, kadry kierowniczej i pracowników biurowych (do 40 kont użytkowników), z sejfami współdzielonymi dla haseł zespołowych i administracyjnych.

Wymagania

1. Szyfrowanie end-to-end danych w sejfie (AES-256 lub równoważne) z kluczami wyprowadzanymi z hasła głównego użytkownika (architektura zero-knowledge).
2. Szyfrowanie transmisji TLS.
3. Instalacja on-premise na platformie z poz. 1.15 (maszyna wirtualna lub kontener), bez przesyłania danych do chmury producenta.
4. Sejfy osobiste i współdzielone (organizacja, zespoły lub kolekcje) z granularnymi uprawnieniami: odczyt, edycja, ukrywanie haseł.
5. Bezpieczne udostępnianie haseł i plików oraz historia zmian.
6. Procedura dostępu awaryjnego (emergency access) oraz konto awaryjne (break-glass) dla haseł krytycznych.
7. Uwierzytelnianie użytkowników z MFA: co najmniej TOTP oraz klucze FIDO2/WebAuthn (poz. 1.25).
8. Logowanie jednokrotne przez OIDC lub SAML z dostawcą tożsamości z poz. 1.24 albo synchronizacja użytkowników i grup z Active Directory/LDAP.
9. Polityki organizacji, w tym wymuszenie MFA i długości hasła głównego.
10. Klienci: rozszerzenia przeglądarek Edge, Chrome i Firefox z autouzupełnianiem, aplikacje desktopowe (Windows) i mobilne (Android, iOS) oraz interfejs webowy.
11. Generator haseł i fraz oraz raporty haseł słabych, powtórzonych i ujawnionych w wyciekach.
12. Przechowywanie kodów TOTP dla kont współdzielonych.
13. Dziennik zdarzeń (dostęp, zmiany, udostępnienia, logowania) z eksportem do serwera logów (poz. 1.22).
14. Kopie zapasowe bazy sejfów w systemie z poz. 1.4, z testem odtworzenia.
15. Rozwiązanie w wersji stabilnej, wspieranej przez producenta lub społeczność, z dostępnymi aktualizacjami bezpieczeństwa.
16. Brak opłat licencyjnych albo licencja wieczysta lub aktywna do dnia 31 grudnia 2026 r., na zasadach pkt 2.3.

Zakres wdrożenia

1. Instalacja i hardening: reverse proxy z TLS, ograniczenie dostępu do sieci wewnętrznej i VPN, MFA administratora.
2. Konfiguracja organizacji, struktury sejfów i uprawnień zgodnie z podziałem odpowiedzialności: administratorzy IT, dostawcy (hasła przekazywane przez sejf), kierownictwo, pracownicy.
3. Konfiguracja polityk organizacji.
4. Migracja haseł administracyjnych infrastruktury z dotychczasowych nośników do sejfu, w obecności Zamawiającego.
5. Rotacja haseł kont uprzywilejowanych po migracji (urządzenia sieciowe, karty zarządzające, macierze, konta usługowe) w zakresie uzgodnionym z Zamawiającym.
6. Wpisy dla wszystkich rozwiązań wdrażanych w Zadaniach 1 i 2.

Testy, dokumentacja i instruktaż

1. Test odtworzenia sejfu z kopii, test dostępu awaryjnego oraz test MFA.
2. Instrukcja użytkownika i administratora oraz dokumentacja konfiguracji.
3. Instruktaż administratorów w wymiarze co najmniej 2 godzin oraz demonstracja dla użytkowników w wymiarze co najmniej 1 godziny.

Poz. 1.24 – Wdrożenie uwierzytelniania dwuskładnikowego (2FA/MFA) we wszystkich systemach wspierających tę funkcję, w tym centralnego dostawcy tożsamości

Przedmiotem pozycji jest wdrożenie uwierzytelniania wieloskładnikowego dla dostępu użytkowników i administratorów do systemów Zamawiającego wspierających tę funkcję, z wykorzystaniem centralnego dostawcy tożsamości (IdP) opartego na oprogramowaniu open source (Keycloak lub równoważne), zintegrowanego z Active Directory. Preferowane są metody odporne na phishing (klucze FIDO2/WebAuthn z poz. 1.25), z metodą zapasową TOTP.

Wymagania dla dostawcy tożsamości

1. Instalacja on-premise na platformie z poz. 1.15.
2. Federacja użytkowników z Active Directory: LDAP/LDAPS, synchronizacja grup, uwierzytelnianie hasłem domenowym.
3. Protokoły OpenID Connect i SAML 2.0 dla aplikacji.
4. Metody MFA: FIDO2/WebAuthn (klucze sprzętowe), TOTP oraz kody zapasowe.
5. Polityki wymuszania MFA dla poszczególnych aplikacji i grup użytkowników.
6. Rejestracja drugiego składnika przez użytkownika po uwierzytelnieniu, wymuszana przez administratora, z możliwością unieważnienia składnika przez administratora.
7. Blokada konta po nieudanych próbach uwierzytelnienia.
8. Logowanie zdarzeń uwierzytelniania do serwera logów.
9. Kopie zapasowe konfiguracji w systemie z poz. 1.4.
10. Interfejs administracyjny zabezpieczony MFA.

Zakres wdrożenia

1. Inwentaryzacja systemów i usług Zamawiającego pod kątem wsparcia MFA i dostępnych metod integracji: SAML/OIDC, RADIUS, natywne TOTP, karta inteligentna.
2. Wykaz systemów z przypisaną metodą MFA, uzgodniony z Zamawiającym.
3. MFA dla dostępu zdalnego VPN (poz. 1.10): integracja firewalla z dostawcą tożsamości (SAML). Tokeny producenta firewalla są stosowane wyłącznie przejściowo, zgodnie z poz. 1.10.
4. MFA dla kont administracyjnych domeny i serwerów: logowanie interaktywne i RDP kartą inteligentną (PIV) z certyfikatami z urzędu certyfikacji Zamawiającego (poz. 1.8) na kluczach z poz. 1.25.
5. MFA dla paneli administracyjnych: firewall, przełączniki i kontroler WLAN (jeżeli wspierane), karty zarządzające serwerów, macierze NAS, platforma wirtualizacji (stacja administracyjna) oraz UPS (jeżeli wspierane).
6. MFA dla konsol systemów bezpieczeństwa: platforma XDR (SAML/OIDC), system monitoringu, WAF, menedżer haseł (OIDC), konsola systemu kopii zapasowych, konsola ESET PROTECT oraz system IDS OT (jeżeli wspierany).
7. MFA dla poczty elektronicznej, usług chmurowych Zamawiającego i systemów dziedzinowych udostępnianych przez Internet, jeżeli wspierają MFA, w uzgodnieniu z dostawcami.
8. SMS nie może być jedyną metodą MFA.
9. Procedury rejestracji, utraty i wymiany drugiego składnika.
10. Kody zapasowe kont awaryjnych są przechowywane w sejfie (poz. 1.23). Konta awaryjne (break-glass) są objęte MFA i monitorowaniem użycia.

Testy, dokumentacja i instruktaż

1. Dla każdego systemu: test logowania z MFA, test odmowy dostępu bez drugiego składnika oraz test odzyskania dostępu.
2. Dokumentacja obejmuje wykaz systemów i metod oraz konfigurację dostawcy tożsamości.
3. Instrukcje dla użytkowników i administratorów.
4. Instruktaż administratorów w wymiarze co najmniej 3 godzin.

Poz. 1.25 – Klucze sprzętowe U2F/FIDO2 – dostawa 23 szt. wraz z wdrożeniem

Przedmiotem pozycji jest dostawa 23 kluczy sprzętowych klasy YubiKey 5 NFC / 5C NFC lub równoważnych wraz z ich wdrożeniem, realizowanym wspólnie z poz. 1.24.

Wymagania

1. Podział na złącza USB-A i USB-C wskazuje Zamawiający przed dostawą.
2. Przydział kluczy (administratorzy, w tym klucze zapasowe, kierownictwo, użytkownicy z dostępem zdalnym) określa Zamawiający w projekcie wdrożenia.
3. Obsługa FIDO2/WebAuthn (CTAP 2.1) z kluczami rezydentnymi (co najmniej 25 poświadczeń) oraz FIDO U2F.
4. Obsługa OATH-TOTP.
5. Funkcja karty inteligentnej PIV (logowanie do Windows certyfikatem) wymagana dla co najmniej 6 kluczy przeznaczonych dla administratorów (klucz podstawowy i zapasowy), zalecana dla pozostałych.
6. Interfejs USB oraz NFC.
7. Ochrona kodem PIN.
8. Obudowa bez baterii i części ruchomych, odporna na wodę.
9. Certyfikacja FIDO Alliance.
10. Wsparcie w systemach Windows 10/11, macOS, Android i iOS oraz w przeglądarkach Edge, Chrome i Firefox.
11. Klucze fabrycznie nowe, z autoryzowanego kanału dystrybucji, w plombowanych opakowaniach producenta.
12. Gwarancja producenta do dnia 31 grudnia 2026 r., na zasadach określonych w pkt 2.2.

Zakres wdrożenia

1. Rejestracja kluczy w dostawcy tożsamości, na firewallu (VPN) oraz w Active Directory (certyfikaty PIV dla administratorów).
2. Konfiguracja kodów PIN i procedur odblokowania.
3. Ewidencja wydania kluczy: protokół z numerem seryjnym i datą.
4. Instrukcja użytkownika.
5. Procedura postępowania w przypadku utraty klucza: unieważnienie poświadczeń i użycie klucza zapasowego.

4. Zadanie 2 – Obszar techniczny OT

Przedmiotem Zadania 2 jest dostawa i wdrożenie rozwiązań bezpieczeństwa dla środowiska OT Zamawiającego: ochrony punktów końcowych OT (poz. 2.1), systemu pasywnego monitorowania sieci przemysłowej klasy IDS (poz. 2.2–2.5) oraz urządzeń UTM dla obiektów technologicznych (poz. 2.6).

1. Wszystkie prace w środowisku OT są prowadzone w sposób niezakłócający procesów technologicznych, w oknach serwisowych, w uzgodnieniu z Zamawiającym i jego dostawcą automatyki (systemu SCADA/telemetrii).
2. Zamawiający zapewnia udział dostawcy automatyki w uzgodnieniach.
3. Wykonawca opracuje projekt techniczny obejmujący wszystkie pozycje Zadania 2, zgodny z modelem stref i kanałów normy IEC 62443 oraz z architekturą Zadania 1 (strefa OT na firewallu, serwer logów, monitoring).
4. Do pozycji obejmujących instalację, konfigurację lub wdrożenie stosuje się wymagania wspólne określone w pkt 2.4.
5. Pozycje 2.2, 2.3, 2.4 i 2.5 tworzą jeden system IDS. Oprogramowanie i sonda sprzętowa mogą pochodzić od jednego producenta albo od różnych producentów, jeżeli Wykonawca wykaże pełną interoperacyjność, wspólne wsparcie eksploatacyjne oraz brak ograniczenia funkcjonalności wymaganych w OPZ.

4.1. Ochrona punktów końcowych OT

Poz. 2.1 – System EDR dla sieci przemysłowych – ochrona punktów końcowych środowiska OT (serwer SCADA, stanowiska dyspozytorskie)

Przedmiotem pozycji jest objęcie ochroną klasy EDR punktów końcowych środowiska OT Zamawiającego: serwera SCADA, 7 stanowisk dyspozytorskich oraz stacji inżynierskich (łącznie do 10 systemów Windows), z wykorzystaniem platformy z poz. 1.5 (agenty tej samej platformy, odrębna grupa polityk OT). Zdarzenia z IT i OT są analizowane w jednej konsoli, z zachowaniem separacji sieciowej. Postępowanie w razie niedostępności platformy w wymaganym terminie określa pkt 2.1.

Wymagania

1. Agent kompatybilny z systemami operacyjnymi hostów OT (Windows 10/11, Windows Server), o niskim narzucie zasobów.
2. Praca agenta bez dostępu do Internetu. Aktualizacje reguł i komunikacja z platformą odbywają się przez kolektor platformy w strefie pośredniej IT/OT.
3. Komunikacja agent–kolektor wyłącznie w kierunku ze strefy OT do strefy pośredniej, przez wskazane porty, z szyfrowaniem TLS.
4. Monitorowanie integralności plików i rejestru: katalogi aplikacji SCADA, konfiguracje, projekty sterowników.
5. Inwentaryzacja i wykrywanie podatności.
6. Monitorowanie procesów, usług i zadań harmonogramu.
7. Wykrywanie zdarzeń podłączenia nośników USB.
8. Wykrywanie narzędzi zdalnego dostępu i nieautoryzowanego oprogramowania.
9. Monitorowanie logowań, w tym kont dostawców.
10. Reguły detekcji dla środowisk przemysłowych (MITRE ATT&CK for ICS) oraz alertowanie.

11. Domyślny tryb pracy: wyłącznie monitorowanie i alertowanie, bez automatycznej reakcji blokującej procesy sterowania.
12. Reakcje automatyczne wyłącznie dla scenariuszy zatwierdzonych przez Zamawiającego i dostawcę automatyki, np. blokada adresu IP atakującego spoza strefy OT.
13. Współpraca z dotychczasowym oprogramowaniem antywirusowym na hostach OT (wzajemne wykluczenia).
14. Zgodność z oprogramowaniem SCADA (lista wykluczeń katalogów i procesów) potwierdzona przez Wykonawcę w uzgodnieniu z dostawcą automatyki.

Zakres wdrożenia

1. Analiza hostów OT: systemy, oprogramowanie SCADA, obciążenie, okna serwisowe.
2. Uzgodnienie z dostawcą automatyki listy wykluczeń, trybu pracy i harmonogramu.
3. Instalacja pilotażowa na jednym stanowisku i obserwacja przez co najmniej 5 dni przed instalacją na pozostałych hostach.
4. Instalacja agentów w oknach serwisowych.
5. Konfiguracja grupy polityk OT: FIM, inwentaryzacja, USB, podatności, reguły ICS.
6. Pulpit OT oraz alerty kierowane do administratora IT i dyspozytorni zgodnie z procedurą obsługi incydentów Zamawiającego.
7. Przekazywanie zdarzeń do platformy przez strefę pośrednią (poz. 1.12).

Testy, dokumentacja i instruktaż

1. Zdarzenia testowe: zmiana pliku konfiguracyjnego w środowisku testowym lub we wskazanym katalogu, podłączenie nośnika USB, nieautoryzowane logowanie.
2. Weryfikacja braku wpływu na pracę systemu SCADA, potwierdzona przez dostawcę automatyki.
3. Dokumentacja obejmuje wykaz hostów, polityki, wykluczenia oraz procedurę obsługi alertu OT.
4. Instruktaż administratorów w wymiarze co najmniej 2 godzin.

4.2. System monitorowania sieci przemysłowej (IDS OT) – poz. 2.2, 2.3, 2.4 i 2.5

Przedmiotem pozycji 2.2–2.5 jest dostawa i wdrożenie systemu monitorowania sieci przemysłowej klasy ScadVance lub równoważnego, służącego do pasywnego monitorowania i analizy ruchu sieciowego w środowisku OT Zamawiającego. Odwołanie do ScadVance określa wymagany poziom funkcjonalny i nie ogranicza możliwości zaoferowania rozwiązania innego producenta spełniającego wymagania niniejszego OPZ.

Zakres pozycji

1. Poz. 2.2: licencja wieczysta na oprogramowanie IDS dla nielimitowanej liczby monitorowanych urządzeń i nielimitowanej liczby użytkowników systemu, obejmująca serwer systemu oraz możliwość instalacji sond programowych (Linux) bez dodatkowych opłat.
2. Poz. 2.2 obejmuje dostęp do nowych wersji, aktualizacji i poprawek oprogramowania, baz podatności oraz oprogramowania sondy do dnia 31 grudnia 2026 r., na zasadach określonych w pkt 2.2.
3. Poz. 2.3: dostawa jednej sondy sprzętowej do monitorowania sieci przemysłowej, instalowanej w punkcie sieci OT wskazanym w projekcie (dyspozytornia lub serwer SCADA – styk sieci OT z siecią telemetrii i strefą pośrednią), wraz z zasilaczem, okablowaniem i elementami montażowymi. Gwarancja producenta obowiązuje do dnia 31 grudnia 2026 r.
4. Poz. 2.4: utrzymanie i eksploatacja systemu, obejmujące serwis gwarancyjny, wsparcie eksploatacyjne administratorów i przegląd konfiguracji od dnia odbioru do dnia 31 grudnia 2026 r. Wynagrodzenie jest płatne jednorazowo po odbiorze, na podstawie faktury wystawionej w okresie kwalifikowalności.

5. Poz. 2.5: analiza, projekt, instalacja, konfiguracja, integracja, testy, dokumentacja i szkolenie.

Wymagania ogólne

1. Oprogramowanie jest niezależne od dostawców automatyki.
2. Oprogramowanie obsługuje urządzenia przemysłowe wykorzystywane przez Zamawiającego (sterowniki PLC i moduły telemetryczne). Wykaz urządzeń jest przekazywany po zawarciu umowy.
3. Przetwarzane dane nie są przesyłane poza infrastrukturę Zamawiającego.
4. System nie wymaga połączenia z Internetem do pracy. Aktualizacje są realizowane w trybie offline.
5. Serwer systemu IDS jest instalowany na maszynie wirtualnej zapewnionej przez Zamawiającego na platformie z poz. 1.15 i 1.16, w strefie OT lub strefie pośredniej.
6. Wykonawca określa w projekcie technicznym minimalne wymagania sprzętowe maszyny wirtualnej: vCPU, RAM oraz przestrzeń dyskową dla archiwum ruchu z co najmniej 90 dni.

Wymagania funkcjonalne oprogramowania

1. Interfejs graficzny co najmniej w języku polskim lub angielskim, dostępny przez przeglądarkę, zabezpieczony TLS z możliwością importu własnego certyfikatu.
2. Konfigurowalne poziomy dostępu użytkowników.
3. Synchronizacja czasu NTP.
4. Aktualizacja bazy danych, oprogramowania i baz podatności w trybie offline.
5. Brak ograniczeń przestrzeni na logi i archiwum ruchu sieciowego.
6. Konfigurowalny czas przechowywania informacji o anomaliach i archiwum ruchu.
7. Pasywne monitorowanie sieci przemysłowej.
8. Automatyczne tworzenie graficznej mapy urządzeń (co najmniej PLC, HMI, RTU, IED, stacje operatorskie SCADA, moduły telemetryczne) z filtrowaniem po urządzeniach, protokołach i portach oraz informacją o sposobie komunikacji.
9. Szczegółowa inwentaryzacja urządzeń oraz automatyczne odzwierciedlenie połączeń komunikacyjnych.
10. Informowanie o zmianach: utrata urządzenia, nowe urządzenie, zmiana komunikacji.
11. Wykrywanie producenta urządzenia na podstawie adresu MAC.
12. Ukrywanie urządzeń MULTICAST i BROADCAST oraz zapamiętywanie widoków.
13. Wykrywanie podatności urządzeń i oprogramowania w sieci przemysłowej z wykorzystaniem baz CVE (MITRE lub NIST).
14. Obsługa protokołów LLDP, CDP, CIP i SSDP.
15. Mechanizmy alarmujące działające w trakcie procesu nauki.
16. Zbudowanie modelu sieci z wykorzystaniem uczenia maszynowego w czasie nie dłuższym niż 5 dni.
17. Dekodowanie i interpretacja komend głównych protokołów OT i IT oraz możliwość dodawania nowych typów protokołów.
18. Praca wyłącznie na kopii ruchu sieciowego, w pełni pasywna (brak generowania ruchu w monitorowanej sieci i wpływu na komunikację), w trybie SPAN/mirror lub pass-through.
19. Analiza plików PCAP.
20. Szyfrowana komunikacja z sondą sprzętową oraz zdalna zmiana konfiguracji i oprogramowania sond.
21. Głęboka analiza pakietów (DPI) co najmniej dla protokołów Modbus RTU, Modbus TCP i DNP3.
22. Analiza behawioralna (ML/AI) co najmniej dla protokołów Modbus RTU, Modbus TCP/IP, DNP3, OPC UA i OPC DA oraz co najmniej 6 spośród: Profinet, Profibus, Powerlink, TASE.2, EtherCAT, GE EGD, EtherNet/IP, CIP, IEC 61850, IEC 60870-5-104, S7, SRTP, BACnet.

23. Możliwość dodawania kolejnych protokołów w ramach aktualizacji.
24. Monitorowanie i klasyfikacja cyberincydentów oraz zdarzeń operacyjnych.
25. Ciągły monitoring online z alarmowaniem w czasie rzeczywistym metodami behawioralnymi.
26. Obsługa incydentów: wykrywanie, rejestrowanie, analiza, priorytet, status, działania naprawcze, rekomendacje.
27. Generowanie potencjalnych wektorów ataku i rekomendacji zwiększenia bezpieczeństwa.
28. Wykrywanie zagrożeń co najmniej w zakresie: złośliwe oprogramowanie i ataki zero-day, DoS/DDoS, APT, spyware i skanowanie sieci, Man-in-the-Middle.
29. Wykrywanie anomalii: częstotliwość komunikacji urządzeń, niezgodność komend, skanowanie PLC i urządzeń sterujących.
30. Wykrywanie połączeń do innych sieci LAN i Internetu oraz połączeń do kluczowych urządzeń, z prezentacją sposobu komunikacji.
31. Sortowanie alarmów według ważności, typu i czasu oraz powiadomienia e-mail.
32. Dla każdego alarmu gromadzony jest opis techniczny, ważność, rekomendacja oraz plik z ruchem sieciowym.
33. Integracja z serwerem logów (poz. 1.22) co najmniej przez SYSLOG.
34. Kreator raportów i szablonów: zagrożenia, anomalie, urządzenia, protokoły.
35. Eksport listy urządzeń i protokołów do CSV i PDF z podziałem na podsieci oraz eksport pakietów do PCAP.
36. Możliwość instalacji sond programowych w środowisku Linux.

Wymagania dla sondy sprzętowej

1. Wykonanie przemysłowe: montaż na szynie DIN lub w szafie 19".
2. Zasilanie 24 V DC. Dopuszcza się zasilanie 230 V AC przez dostarczony zasilacz.
3. Podtrzymanie zasilania przez co najmniej 30 minut po zaniku, wbudowane lub z dostarczonego zasilacza UPS.
4. Obsługa DHCP i stałego adresu IP.
5. Szyfrowanie danych przechowywanych na nośniku sondy, co najmniej AES-128.
6. Uniemożliwienie odczytu danych z nośnika po jego wymontowaniu.
7. Alarm w systemie przy próbie otwarcia obudowy.
8. Co najmniej jeden pasywny interfejs monitorujący RJ-45 10/100 Mbps w trybie SPAN, nieidentyfikujący się w sieci adresem MAC i pozbawiony funkcji nadawania (Tx).
9. Zalecane (nie podlega ocenie): pasywne interfejsy monitorujące magistrale szeregowe RS-485, RS-232, RS-422 i CAN.
10. Przekazywanie do systemu wskazanej części ruchu (wybrane urządzenia i protokoły) oraz strumienia sieciowego w formacie IPFIX.

Wdrożenie (poz. 2.5)

1. Analiza przedwdrożeniowa architektury sieci OT: dyspozytornia, serwer SCADA, tunele do obiektów, łącze APN telemetrii oraz urządzenia z poz. 2.6.
2. Wskazanie punktów monitorowania: kopia ruchu z portu mirror przełącznika rdzeniowego (port serwera SCADA i łącza telemetrii) lub z firewalla, pasywny TAP Ethernet dla segmentu dyspozytorni (przełącznik niezarządzalny) oraz sonda sprzętowa.
3. Wykonawca dostarcza w cenie poz. 2.5 jeden pasywny TAP Ethernet 10/100/1000.
4. Projekt rozmieszczenia i konfiguracji uzgodniony z Zamawiającym i dostawcą automatyki.

5. Instalacja i konfiguracja serwera systemu IDS na maszynie wirtualnej Zamawiającego: utwardzenie, TLS, konta imienne, NTP, SYSLOG.
6. Instalacja sondy sprzętowej w miejscu wskazanym przez Zamawiającego, z wykonaniem niezbędnych połączeń i okablowania. Miejsce w szafach zapewnia Zamawiający.
7. Instalacja odbywa się bez przerw w działaniu sieci i bez zakłóceń w sieci przemysłowej.
8. Konfiguracja portów mirror/SPAN na przełącznikach lub firewallu w niezbędnym zakresie.
9. Konfiguracja sond programowych w obiektach na maszynach lub urządzeniach Linux wskazanych w projekcie, jeżeli projekt je przewiduje.
10. Okres uczenia i obserwacji systemu przed strojeniem reguł, trwający co najmniej 5 dni.
11. Klasyfikacja i opisanie urządzeń oraz strojenie reguł i progów alarmowych.
12. Raport z inwentaryzacji sieci OT oraz wykrytych podatności i anomalii, z rekomendacjami.
13. Integracja z serwerem logów (poz. 1.22) i systemem monitoringu (poz. 1.6) przez strefę pośrednią, z zachowaniem separacji IT/OT.
14. Konfiguracja powiadomień e-mail dla osób wskazanych przez Zamawiającego.
15. Przekazanie wszystkich haseł i kont z opisem funkcji i uprawnień przez menedżer haseł z poz. 1.23.
16. Testy poprawności działania: wykrycie nowego urządzenia, anomalii komunikacji i skanowania, w środowisku testowym lub w uzgodniony sposób niewpływający na produkcję.
17. Prace są realizowane w siedzibie i pod nadzorem Zamawiającego.
18. Szkolenie administratorów Zamawiającego z konfiguracji i administracji systemem IDS w wymiarze co najmniej 8 godzin zegarowych, potwierdzone listą obecności.
19. Dokumentacja powykonawcza opisuje wykonane prace, konfigurację serwera, sondy i przełączników oraz procedurę obsługi alarmów.
20. Dokumentacja jest przekazywana w terminie 14 dni od zrealizowania zakresu, nie później niż w terminie określonym w pkt 1.4. Odbiór następuje po odebraniu dokumentacji.

Utrzymanie i eksploatacja (poz. 2.4)

1. Serwis i wsparcie są świadczone od dnia odbioru do dnia 31 grudnia 2026 r.
2. Dostęp do dokumentacji technicznej i instrukcji systemu w języku polskim.
3. Serwis gwarancyjny sondy sprzętowej z wymianą uszkodzonej sondy w terminie do 10 dni roboczych.
4. Przekazanie danych kontaktowych działu technicznego producenta oraz przyjmowanie zgłoszeń w dni robocze.
5. Zdalne wsparcie administratorów Zamawiającego w obsłudze systemu oraz w identyfikacji i rozwiązywaniu problemów lub zastosowaniu obejścia.
6. Co najmniej jeden przegląd konfiguracji i strojenie reguł po zakończeniu okresu uczenia i pierwszym okresie eksploatacji, nie później niż do dnia 31 grudnia 2026 r., zakończony raportem.
7. Dostęp do aktualizacji oprogramowania i baz jest objęty poz. 2.2.

Odbiór

1. Odbiór następuje na podstawie protokołu zdawczo-odbiorczego.
2. Protokół potwierdza dostawę sondy sprzętowej, aktywację licencji, poprawność konfiguracji systemu, przeprowadzenie okresu uczenia i testów, kompletność dokumentacji powykonawczej oraz przeprowadzenie szkolenia administratorów.
3. Protokół wskazuje odrębnie wykonanie zakresu poz. 2.2, 2.3, 2.4 i 2.5.

4.3. Urządzenia UTM dla obiektów technologicznych

Poz. 2.6 – Urządzenia klasy NGFW/UTM dla obiektów technologicznych OT – dostawa, instalacja i konfiguracja (ze wsparciem producenta)

Przedmiotem pozycji jest dostawa, instalacja i konfiguracja 4 urządzeń klasy NGFW/UTM dla obiektów technologicznych Zamawiającego połączonych z siedzibą tunelami VPN: SUW Łazy, zbiornik Mielno, obiekt Kiszkowo oraz obiekt wskazany przez Zamawiającego w projekcie technicznym. Urządzenia zapewniają kontrolę ruchu na styku sieci obiektowej OT z siecią telemetrii i Internetem, szyfrowane połączenia z siedzibą (firewall z poz. 1.1) oraz segmentację sieci obiektowej.

1. Detekcję zagrożeń w sieci OT realizuje system IDS (poz. 2.2–2.5). Urządzenia z poz. 2.6 są punktami kontroli i segmentacji wyposażonymi w silnik IPS gotowy do aktywacji sygnatur, w tym przemysłowych.
2. Urządzenia są dostarczane ze wsparciem producenta (gwarancja, aktualizacje oprogramowania, wsparcie techniczne) do dnia 31 grudnia 2026 r.
3. Subskrypcje usług ochronnych (IPS, antywirus, filtrowanie WWW) nie są wymagane dla tych urządzeń. Urządzenia muszą umożliwiać ich późniejsze uruchomienie po wykupieniu subskrypcji, bez wymiany sprzętu.
4. Zamawiający zapewnia w każdym obiekcie miejsce instalacji (szafa teletechniczna lub sterownicza), zasilanie 230 V AC oraz istniejące łącze dostępowe do Internetu (przewodowe lub radiowe/LTE za istniejącym urządzeniem operatora). Dostawa łączy nie jest przedmiotem zamówienia.
5. Wykaz obiektów z opisem warunków instalacji (rodzaj szafy, warunki środowiskowe, łącze) Zamawiający udostępnia na wniosek w trakcie postępowania. Zalecana jest wizja lokalna.
6. W obiektach o warunkach środowiskowych wykraczających poza zakres pracy urządzenia biurowego (temperatura, wilgotność) Wykonawca instaluje urządzenie w obudowie zapewniającej warunki pracy określone przez producenta (obudowa w zakresie dostawy Wykonawcy) albo oferuje dla takich obiektów wersję przemysłową urządzenia spełniającą pozostałe wymagania.

Wymagania ogólne (dla każdego z 4 urządzeń)

1. Urządzenie sprzętowe (appliance) realizujące wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa.
2. Praca w trybie routera z NAT, w trybie transparentnym oraz w trybie monitorowania na porcie SPAN.
3. Możliwość utworzenia co najmniej 2 instancji logicznych (virtual domains).
4. Obsługa IPv4 i IPv6 w zakresie firewalla, ochrony w warstwie aplikacji i routingu dynamicznego.
5. Możliwość łączenia w klaster Active-Active lub Active-Passive z synchronizacją sesji.
6. Monitoring i wykrywanie uszkodzeń elementów sprzętowych, programowych i łączy oraz monitoring stanu tuneli VPN.
7. Agregacja łączy statyczna i LACP oraz interfejsy redundantne.
8. Współpraca z firewallem z poz. 1.1 w zakresie: IPsec IKEv2 (AES-256-GCM, DH 19/20, uwierzytelnianie certyfikatami X.509 i kluczem współdzielonym), routingu dynamicznego (BGP lub OSPF) w tunelach IPsec, SYSLOG (TCP/TLS) i SNMPv3.
9. Zamawiający nie wymaga, aby urządzenia pochodziły od producenta firewalla z poz. 1.1. Zalecane (nie podlega ocenie): jednolitość platformy (ten sam system operacyjny) ze względu na kompetencje administratorów.

Interfejsy i zasilanie

1. Co najmniej 5 portów Gigabit Ethernet RJ-45.

2. Wbudowany port konsoli szeregowej oraz gniazdo USB.
3. Co najmniej 200 interfejsów wirtualnych VLAN 802.1Q.
4. Zasilanie 230 V AC, zasilacz w komplecie.
5. Praca bez wentylatora (chłodzenie pasywne) lub o poziomie hałasu odpowiednim dla pomieszczeń technicznych.
6. Możliwość montażu w szafie rack 19" (uchwyt w komplecie) lub na ścianie.

Parametry wydajnościowe

1. Obsługa nie mniej niż 500 tys. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 4 Gbps dla pakietów 512 B.
3. Przepustowość firewalla z włączoną kontrolą aplikacji: nie mniej niż 1,5 Gbps.
4. Wydajność szyfrowania IPsec VPN (AES-128): nie mniej niż 2 Gbps.
5. Liczba tuneli site-to-site: co najmniej 50.
6. Wydajność IPS (Enterprise Traffic Mix): nie mniej niż 1,2 Gbps.
7. Wydajność z włączonymi IPS, kontrolą aplikacji i antywirusem: nie mniej niż 600 Mbps.
8. Wydajność inspekcji SSL dla ruchu HTTP: nie mniej niż 700 Mbps.
9. Parametry dotyczące funkcji ochronnych odnoszą się do funkcji dostępnych po uruchomieniu subskrypcji.

Funkcje

1. Zapora Stateful Inspection z politykami uwzględniającymi adresy, użytkowników, protokoły, usługi, aplikacje, harmonogramy i geolokalizację.
2. NAT/PAT, strefy bezpieczeństwa oraz polityka domyślnego blokowania.
3. IPsec VPN: IKEv1 i IKEv2, AES-128/256 GCM, DH 19/20, site-to-site, hub-and-spoke, monitorowanie tuneli, DPD, NAT-T, uwierzytelnianie kluczem i certyfikatem.
4. VPN dostępu zdalnego: IPsec IKEv2 lub SSL VPN.
5. Routing statyczny, PBR, OSPF, BGP, ECMP i BFD.
6. Funkcje SD-WAN oraz zarządzanie pasmem.
7. Kontrola aplikacji, IPS (z sygnaturami dla protokołów przemysłowych), ochrona przed złośliwym oprogramowaniem, filtrowanie WWW i DNS oraz antyspam – funkcje dostępne w urządzeniu i aktywowane po wykupieniu subskrypcji.
8. Uwierzytelnianie użytkowników: lokalne, LDAP, RADIUS, SAML.
9. MFA dla administratorów i użytkowników VPN.
10. Zarządzanie przez HTTPS i SSH, RBAC, ograniczenie zarządzania do wskazanych adresów, zatwierdzanie zmian oraz API.
11. SNMP v2c/v3, NetFlow lub sFlow oraz narzędzia diagnostyczne.
12. Logowanie ruchu, działań administratorów i stanu systemu do wielu serwerów SYSLOG (TCP, TLS) oraz do usługi producenta w chmurze w zakresie dostępnym bez dodatkowych opłat.
13. Automatyzacja reakcji na zdarzenia.

Gwarancja i wsparcie

1. Serwis gwarancyjny producenta obejmujący naprawę lub wymianę urządzenia w trybie wymiany wyprzedzającej (advance replacement) po potwierdzeniu awarii, dostęp do aktualizacji oprogramowania oraz wsparcie techniczne producenta w trybie 24x7 przez portal i infolinię, od dnia aktywacji do dnia 31 grudnia 2026 r.

2. Rejestracja urządzeń na konto Zamawiającego w portalu producenta.
3. Wszystkie funkcje i parametry wydajnościowe są weryfikowane na podstawie oficjalnej, publicznie dostępnej dokumentacji producenta, zgodnie z pkt 2.2.

Instalacja i konfiguracja

1. Analiza przedwdrożeniowa każdego obiektu: sposób dostępu do Internetu i istniejące urządzenia sieciowe, urządzenia OT (sterowniki, moduły telemetryczne, kamery), wymagane przepływy do systemu SCADA i do dostawcy automatyki, zasilanie oraz warunki środowiskowe. Wyniki analizy są przekazywane w formie pisemnej.
2. Projekt architektury jako rozdział projektu technicznego Zadania 2: schemat tuneli IPsec hub-and-spoke do firewalla w siedzibie (poz. 1.1), tunel zapasowy lub trasa awaryjna (w tym utrzymanie komunikacji telemetrii GSM jako kanału niezależnego), segmentacja sieci obiektowej (strefa OT sterowników, strefa kamer i pozostałych urządzeń, strefa serwisowa), macierz przepływów oraz adresacja.
3. Projekt jest uzgadniany z dostawcą automatyki i podlega akceptacji Zamawiającego.
4. Instalacja fizyczna urządzeń w obiektach wraz z podłączeniem zasilania (z zabezpieczeniem przepięciowym, jeżeli obiekt go nie posiada), interfejsów WAN i LAN, montażem obudowy (jeżeli jest wymagana) i okablowaniem.
5. Instalacja odbywa się w terminach uzgodnionych z Zamawiającym, bez przerwy w komunikacji obiektu z dyspozytornią dłuższej niż uzgodnione okno serwisowe.
6. Wymiana lub rekonfiguracja dotychczasowego urządzenia VPN obiektu.
7. Aktualizacja oprogramowania do najnowszej stabilnej wersji rekomendowanej przez producenta.
8. Konfiguracja parametrów systemowych: adresacja, NTP, konta imienne, MFA, wyłączenie nieużywanych usług i portów.
9. Dostęp administracyjny do urządzeń wyłącznie przez tunel ze strefy zarządzania w siedzibie.
10. Konfiguracja tuneli IPsec (IKEv2, AES-256 GCM, DH 19/20, certyfikaty lub silne klucze) do siedziby, z monitorowaniem.
11. Polityki bezpieczeństwa zgodne z zasadą minimalnych uprawnień: ruch obiekt–SCADA wyłącznie w niezbędnym zakresie protokołów przemysłowych, blokada ruchu wychodzącego z urządzeń OT do Internetu, dostęp serwisowy dostawcy wyłącznie przez siedzibę i VPN z MFA.
12. Segmentacja lokalna (VLAN) oraz logowanie sesji.
13. Integracja z serwerem logów (poz. 1.22) i systemem monitoringu (poz. 1.6), w tym alarm o utracie tunelu.
14. Integracja z systemem IDS OT: przekazanie kopii ruchu przez port SPAN lub sondę programową, jeżeli przewidziano w projekcie.

Testy, dokumentacja, instruktaż i wsparcie

1. Test zestawienia tuneli oraz przełączenia na trasę awaryjną.
2. Test poprawności komunikacji SCADA z każdym obiektem, potwierdzony przez dyspozytornię i dostawcę automatyki.
3. Test blokowania ruchu niedozwolonego, dostępu administracyjnego oraz przekazywania logów.
4. Raport z testów stanowi załącznik do protokołu odbioru.
5. Dokumentacja powykonawcza obejmuje konfigurację każdego urządzenia, schemat połączeń, polityki, procedurę odtworzenia i wymiany urządzenia oraz kopie konfiguracji.
6. Szablon konfiguracji dla kolejnych obiektów.
7. Instruktaż administratorów w wymiarze co najmniej 4 godzin.
8. Pula co najmniej 8 godzin zdalnych konsultacji, wykorzystywana i rozliczana zgodnie z pkt 2.4.

Odbiór

1. Odbiór następuje na podstawie protokołu zdawczo-odbiorczego potwierdzającego dostawę 4 urządzeń (wykaz numerów seryjnych), aktywację wsparcia producenta, poprawność instalacji i konfiguracji w każdym obiekcie, pozytywny wynik testów, kompletność dokumentacji oraz przeprowadzenie instruktażu.
2. Zamawiający dopuszcza odbiory częściowe dla poszczególnych obiektów.