Załącznik nr 1a do Zapytania ofertowego
Znak sprawy: MWiK/NI/988/2026

Szczegółowy opis przedmiotu zamówienia

Dotyczy zamówienia publicznego pn. „Dostawa i wdrożenie rozwiązań cyberbezpieczeństwa IT/OT wraz z usługami doradczymi i szkoleniowymi - Cyberbezpieczne Wodociągi - MWiK Kętrzyn" w ramach projektu „Cyberbezpieczne Wodociągi – MWiK Kętrzyn" (wniosek nr KPOD.05.10-CW.01-001250858), finansowanego ze środków Krajowego Planu Odbudowy i Zwiększania Odporności, inwestycja C3.1.1 Cyberbezpieczeństwo – CyberPL.

Zamawiający: Miejskie Wodociągi i Kanalizacja Sp. z o.o., ul. Poznańska 6, 11-400 Kętrzyn.

Wymagania ogólne

1. Przedmiot zamówienia obejmuje usługi doradcze, audytowe i szkoleniowe, dostawę aplikacji do zarządzania SZBI, dostawy sprzętu z oprogramowaniem oraz usługi wdrożeniowe do poszczególnych lokalizacji Zamawiającego w zakresie i ilościach wskazanych w zestawieniu rzeczowo – ilościowym.
2. Dostarczany sprzęt i oprogramowanie muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich.
3. Oferowane urządzenia w dniu składania ofert nie mogą być przeznaczone przez producenta do wycofania z produkcji (tzw. End of Life).
4. Dostarczany sprzęt i oprogramowanie muszą pochodzić z oficjalnego kanału dystrybucyjnego w UE.
5. Gwarancja na wszystkie dostarczane urządzenia musi być świadczona przez producenta lub autoryzowanego przez producenta partnera serwisowego, na terenie Rzeczypospolitej Polskiej, z przyjmowaniem zgłoszeń i komunikacją w języku polskim. Wymóg nie dotyczy oprogramowania.
6. Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
7. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
8. Wykonawca wyda Zamawiającemu instrukcje obsługi sprzętu lub – jeśli są one udostępniane przez producenta w formie elektronicznej – przekaże adresy WWW, pod którymi można je pobrać.
9. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia Zamawiającemu niewyłącznej licencji lub przeniesienia na Zamawiającego niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.

Zestawienie rzeczowo – ilościowe

Obszar techniczny IT

Lp.	Przedmiot dostawy/usługi	Ilość	Lokalizacja
3.1	Serwer do klastra HA	3 szt.	Siedziba Zamawiającego, ul. Poznańska 6, 11-400 Kętrzyn
3.2	Macierz dyskowa dla klastra HA	1 szt.	Siedziba Zamawiającego, ul. Poznańska 6, 11-400 Kętrzyn
3.3	Serwer kopii zapasowych z licencją oprogramowania do tworzenia kopii zapasowych z funkcją deduplikacji	1 kpl.	Siedziba Zamawiającego, ul. Poznańska 6, 11-400 Kętrzyn
3.4	Przełączniki zarządzalne – sieć biurowa, w tym: przełącznik do klastra HA – 2 szt., przełącznik dystrybucyjny 24-portowy – 2 szt., przełącznik dystrybucyjny 8-portowy PoE – 1 szt.	1 zestaw	Siedziba Zamawiającego, ul. Poznańska 6, 11-400 Kętrzyn
3.5	Biblioteka taśmowa LTO-9 wraz z kasetami	1 kpl.	Siedziba Zamawiającego, ul. Poznańska 6, 11-400 Kętrzyn
3.6	Zasilacz UPS z monitoringiem dla klastra HA	1 kpl.	Siedziba Zamawiającego, ul. Poznańska 6, 11-400 Kętrzyn
3.7	Serwer NAS na odmiejscowione kopie zapasowe	1 szt.	Siedziba Zamawiającego, ul. Poznańska 6, 11-400 Kętrzyn – inny budynek niż serwerownia
3.8	Urządzenie UTM dla sieci IT	1 szt.	Siedziba Zamawiającego, ul. Poznańska 6, 11-400 Kętrzyn
3.9	Szafa rack	1 szt.	Siedziba Zamawiającego, ul. Poznańska 6, 11-400 Kętrzyn
3.10	Punkty dostępowe sieci bezprzewodowej (3 szt.) wraz z kontrolerem (1 szt.)	1 kpl.	Siedziba Zamawiającego, ul. Poznańska 6, 11-400 Kętrzyn
3.11	Licencje serwerowego systemu operacyjnego oraz licencje dostępowe (CAL)	1 kpl.	Siedziba Zamawiającego, ul. Poznańska 6, 11-400 Kętrzyn
3.12	Wdrożenie systemu klasy SIEM/XDR	1 usł.	Siedziba Zamawiającego, ul. Poznańska 6, 11-400 Kętrzyn
3.13	Wdrożenie domeny Active Directory	1 usł.	Siedziba Zamawiającego, ul. Poznańska 6, 11-400 Kętrzyn
3.14	Wdrożenie oprogramowania do monitorowania infrastruktury informatycznej	1 usł.	Siedziba Zamawiającego, ul. Poznańska 6, 11-400 Kętrzyn

Obszar techniczny OT

Lp.	Przedmiot dostawy/usługi	Ilość	Lokalizacja
4.1	Urządzenie UTM dla sieci OT	3 szt.	po 1 szt. w każdej lokalizacji OT
4.2	Przełącznik dystrybucyjny 24-portowy PoE – sieć OT	3 szt.	po 1 szt. w każdej lokalizacji OT
4.3	Szafa rack wisząca 12U	3 szt.	po 1 szt. w każdej lokalizacji OT
4.4	Zasilacz UPS z monitoringiem	3 szt.	po 1 szt. w każdej lokalizacji OT

Obszar organizacyjny

Lp.	Przedmiot dostawy/usługi	Ilość	Lokalizacja
1.1	Opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	1 usł.	Siedziba Zamawiającego oraz obiekty: SUW, przepompownie, oczyszczalnia ścieków
1.2	Wdrożenie narzędzia do zarządzania SZBI, BCP i DRP (open source, w oparciu o GLPI Zamawiającego)	1 kpl.	Siedziba Zamawiającego, ul. Poznańska 6, 11-400 Kętrzyn
1.3	Audyt sieci OT – inwentaryzacja, opis stanu aktualnego, analiza potrzeb modernizacji zabezpieczeń	1 usł.	Siedziba Zamawiającego oraz obiekty: SUW, przepompownie, oczyszczalnia ścieków
1.4	Opracowanie i wdrożenie Systemu Zarządzania Ciągłością Działania (SZCD)	1 usł.	Siedziba Zamawiającego oraz obiekty: SUW, przepompownie, oczyszczalnia ścieków
1.5	Opracowanie i wdrożenie planów ciągłości działania (BCP) i odtwarzania po awarii (DRP)	1 usł.	Siedziba Zamawiającego oraz obiekty: SUW, przepompownie, oczyszczalnia ścieków

Obszar kompetencyjny

Lp.	Przedmiot dostawy/usługi	Ilość	Lokalizacja
2.1	Podstawowe szkolenia z cyberbezpieczeństwa dla pracowników IT/OT - stacjonarne (31 osób)	1 usł.	Siedziba Zamawiającego, ul. Poznańska 6, 11-400 Kętrzyn
2.2	Szkolenie wraz z testami socjotechnicznymi (phishing)	1 usł.	Siedziba Zamawiającego, ul. Poznańska 6, 11-400 Kętrzyn
2.3	Szkolenie kadry zarządzającej z SZBI i świadomości cyberbezpieczeństwa	1 usł.	Siedziba Zamawiającego, ul. Poznańska 6, 11-400 Kętrzyn

Adresy lokalizacji

Lokalizacja	Adres

Lokalizacja	Adres
Siedziba Zamawiającego (biuro)	ul. Poznańska 6, 11-400 Kętrzyn
Stacja Uzdatniania Wody Karolewo	Karolewo, 11-400 Kętrzyn
Stacja Uzdatniania Wody Jeżewo	Jeżewo, 11-400 Kętrzyn
Oczyszczalnia ścieków Trzy Lipy	Trzy Lipy, 11-400 Kętrzyn

Kody CPV

- 48820000-2 Serwery
- 30233000-1 Urządzenia do przechowywania i odczytu danych
- 32420000-3 Urządzenia sieciowe
- 31682530-4 Awaryjne urządzenia energetyczne
- 35120000-1 Systemy i urządzenia nadzoru i bezpieczeństwa
- 31213300-5 Szafy kablowe
- 48000000-8 Pakiety oprogramowania i systemy informatyczne
- 72260000-5 Usługi w zakresie oprogramowania
- 72263000-6 Usługi wdrażania oprogramowania
- 79212000-3 Usługi audytu
- 79417000-0 Usługi doradcze w zakresie bezpieczeństwa
- 72150000-1 Usługi doradztwa w zakresie audytu komputerowego
- 80500000-9 Usługi szkoleniowe
- 80533100-0 Usługi szkoleniowe w zakresie komputerów

Obszar techniczny IT

3.1. Serwer do klastra HA – 3 szt.

Obszar wymagań	Wymagania minimalne
Obudowa	Obudowa do montażu w szafie rack 19", zajmująca nie więcej niż 1U. W zestawie szyny montażowe do instalacji serwera w szafie rack. Możliwość instalacji co najmniej 4 dysków hot-swap 3,5" SAS/SATA.
Procesor	Co najmniej ośmiordzeniowy procesor 64-bitowy, uzyskujący wynik co najmniej 18 100 punktów w teście PassMark – CPU Mark według wyników dostępnych na stronie http://www.cpubenchmark.net 30 dni przed terminem składania ofert lub później. Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim.
Pamięć RAM	Zainstalowane co najmniej 64 GB pamięci RAM DDR5 RDIMM ECC, w modułach o pojemności co najmniej 16 GB każdy. Możliwość rozbudowy pamięci RAM do co najmniej 1 TB.

Obszar wymagań	Wymagania minimalne
Dyski	Zainstalowane co najmniej 2 dyski SSD o pojemności co najmniej 480 GB każdy. Zainstalowane co najmniej 2 dyski HDD SAS lub SATA 7 200 obr./min typu hot-swap o pojemności co najmniej 1 TB każdy. Sprzętowy kontroler RAID obsługujący poziomy RAID co najmniej 0, 1, 5, 10. Możliwość monitorowania stanu dysków i macierzy RAID.
Interfejsy sieciowe	Zainstalowane i w pełni funkcjonalne co najmniej 4 porty 10 Gb/s SFP+ (lub szybsze, wstecznie zgodne z SFP+), wraz z wkładkami SFP+ lub kablami DAC umożliwiającymi podłączenie do przełączników z poz. 3.4.1 i 3.4.2. Zainstalowane i w pełni funkcjonalne co najmniej 4 porty Ethernet 1 Gb/s RJ-45. Dedykowany port zarządzający Ethernet RJ-45.
Porty, złącza	Co najmniej 2 porty USB, w tym co najmniej 1 port USB 3.x. Co najmniej 1 port VGA lub równoważny port umożliwiający podłączenie monitora serwisowego. Wymagane porty nie mogą być realizowane przy użyciu dodatkowych adapterów, przejściówek lub kart rozszerzeń.
Chłodzenie	Redundantne wentylatory z możliwością wymiany w trybie hot-swap. Zainstalowany system chłodzenia musi zapewniać prawidłową pracę serwera dla oferowanej konfiguracji sprzętowej.
Zasilanie	Co najmniej dwa identyczne zasilacze pracujące redundantnie. Możliwość wymiany zasilacza w trybie hot-swap bez przerywania pracy serwera. Zainstalowane zasilacze muszą zapewniać pełną wydajność oferowanej konfiguracji również przy pracy redundantnej.
Zabezpieczenia sprzętowe i firmware	Moduł TPM 2.0. Obsługa weryfikacji integralności firmware z wykorzystaniem podpisów kryptograficznych. Obsługa mechanizmu Secure Boot. Możliwość bezpiecznej aktualizacji firmware. Możliwość automatycznego przywracania firmware po nieudanej aktualizacji lub uszkodzeniu. Możliwość blokady zmian konfiguracji serwera oraz firmware.
Zarządzanie serwera	Kontroler zarządzania typu BMC umożliwiający zdalne zarządzanie serwerem niezależnie od zainstalowanego systemu operacyjnego. Obsługa standardu IPMI 2.0 lub Redfish. Możliwość zdalnego dostępu do konsoli tekstowej i graficznej. Możliwość zdalnego montowania obrazów ISO. Możliwość monitorowania parametrów sprzętowych serwera, w tym temperatury, zasilania, wentylatorów i stanu dysków.
Certyfikaty	Serwer musi posiadać deklarację CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022 oraz Windows Server 2025. Do oferty należy załączyć

Obszar wymagań	Wymagania minimalne
	wydruk z ww. strony, dopuszcza się wydruk w języku angielskim.
Diagnostyka	Diody LED lub wyświetlacz LCD sygnalizujące co najmniej: aktywność dysków, aktywność interfejsów sieciowych, awarię zasilania, stan zasilania oraz stan systemu.
Gwarancja	Co najmniej 36-miesięczna gwarancja producenta, obejmująca wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji. Usługi serwisu gwarancyjnego muszą być realizowane w miejscu instalacji urządzenia. Czas reakcji serwisu – do końca następnego dnia roboczego. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego. Możliwość zgłaszania awarii 24 godziny na dobę, 7 dni w tygodniu w języku polskim poprzez ogólnopolską linię telefoniczną producenta lub dedykowany polskojęzyczny portal techniczny producenta. Gwarancja musi być świadczona przez producenta lub autoryzowanego przez producenta partnera serwisowego, na terenie Rzeczypospolitej Polskiej, z przyjmowaniem zgłoszeń i komunikacją w języku polskim.

3.2. Macierz dyskowa dla klastra HA – 1 szt.

Obszar wymagań	Wymagania minimalne
Ogólne	System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19" i zajmować w szafie maks. 2U. Każdy skonfigurowany moduł/obudowa musi posiadać nadmiarowy układ zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia). Każdy moduł/obudowa musi posiadać widoczne elementy sygnalizacyjne informujące o stanie poprawnej pracy lub awarii. Oferowana macierz musi obsługiwać min. 96 dysków wykonanych w technologii hot-plug. Macierz musi posiadać 4 porty SAS 12 Gb/s do podłączenia dodatkowych półek dyskowych.
Pojemność macierzy	Min. 8 dysków SSD z interfejsem SAS lub NVMe, o pojemności min. 1,92 TB każdy.
Kontrolery	Macierz musi być dostarczona z zainstalowanymi min. 2 kontrolerami. Każdy z kontrolerów macierzy musi posiadać min. 32 GB pamięci podręcznej cache. W przypadku awarii zasilania dane niezapisane na dyski, przechowywane w pamięci kontrolera, muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub poprzez zrzut do pamięci flash. Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji odczytu o min. 5 TB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie pojemności zainstalowanych dysków SSD. Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach. Macierz musi posiadać funkcjonalność automatycznego równoważenia obciążenia kontrolerów poprzez przełączanie w trybie online woluminów logicznych pomiędzy kontrolerami w zależności od generowanego na nich ruchu. Musi istnieć możliwość

Obszar wymagań	Wymagania minimalne
	wyłączenia tej funkcjonalności z poziomu interfejsu użytkownika. Każdy z kontrolerów RAID musi posiadać dedykowany interfejs Ethernet RJ-45 o prędkości min. 1 Gb/s do zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy. Każdy z kontrolerów RAID musi posiadać 2 porty iSCSI 25 Gb/s obsadzone modułami optycznymi 10 Gb/s (złącze LC, światłowód wielomodowy) do podłączenia serwerów bezpośrednio lub poprzez sieć SAN, w tym przełączniki z poz. 3.4.1. Macierz musi umożliwiać dołożenie portów do transmisji danych: SAS 12 Gb/s, iSCSI 10 Gb/s lub 25 Gb/s, FC 32 Gb/s.
Poziomy RAID	Macierz musi zapewniać zabezpieczenie danych na dyskach na poziomach RAID: 1, 10, 3, 5, 6. Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID 5 i RAID 6 musi być realizowane sprzętowo przez dedykowany układ w macierzy. Macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków o dużej pojemności. Macierz musi umożliwiać dynamiczną migrację pomiędzy poziomami RAID, tj. zmianę sposobu zabezpieczenia grupy dyskowej z jednego poziomu RAID na inny.
Dyski	Oferowana macierz musi obsługiwać dyski hot-plug: SSD, HDD z interfejsem SAS 12 Gb/s, HDD o prędkości obrotowej 7,2 krpm i 10 krpm. Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD zainstalowanych w dowolnym module rozwiązania. Wszystkie dyski obsługiwane przez oferowany model macierzy muszą być wykonane w technologii hot-plug. Macierz musi posiadać oprogramowanie do monitorowania stanu dysków, pozwalające na identyfikację dysków potencjalnie zagrożonych awarią, oraz umożliwiać sprawdzenie stanu zużycia dysków SSD z poziomu graficznego interfejsu zarządzania. Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysku zapasowego (hot-spare). W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku zapasowego na wymieniony dysk (tzw. copyback-less) albo macierz musi umożliwiać tworzenie pul dyskowych z rozproszoną przestrzenią rezerwową, w których nie stosuje się dedykowanych dysków zapasowych. Macierz musi umożliwiać szyfrowanie danych na dedykowanych do tego dyskach kluczem AES 256-bit, zgodnie z wytycznymi Information Technology Laboratory przy National Institute of Standards and Technology (NIST). Macierz musi umożliwiać skasowanie wszystkich danych z dysku szyfrującego (FDE) w celu bezpiecznego ponownego użycia w innym środowisku (Secure Erase).
Opcje programowe	Macierz musi być wyposażona w system kopii migawkowych umożliwiający wykonanie 128 kopii migawkowych, z opcją rozbudowy do 512. Macierz musi umożliwiać zdefiniowanie min. 500 woluminów (LUN). Macierz musi umożliwiać podłączenie logiczne min. 250 serwerów.

Obszar wymagań	Wymagania minimalne
	Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy oraz bez konieczności wyłączania ścieżek logicznych FC/iSCSI do podłączonych stacji/serwerów. Macierz musi umożliwiać dynamiczną zmianę rozmiaru woluminów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym woluminie. Macierz musi obsługiwać systemy operacyjne: Microsoft Windows Server 2019, 2022, 2025; SUSE Linux Enterprise Server 12, 15; Red Hat Enterprise Linux 8, 9; VMware vSphere 7, 8. Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię wielościeżkową (multipath – obsługa nadmiarowości ścieżek transmisji danych pomiędzy macierzą a serwerem) dla połączeń FC i iSCSI. Macierz musi umożliwiać uruchomienie mechanizmów zdalnej replikacji danych w trybie asynchronicznym, bez konieczności stosowania zewnętrznych urządzeń konwersji. Replikacja danych musi być realizowana przez oprogramowanie wewnętrzne macierzy (tzw. storage-based data replication) we współpracy z macierzą z tej samej rodziny urządzeń, obsługującą zdalną replikację danych. Funkcjonalność opcjonalna – możliwość wykupienia w przyszłości. Macierz musi obsługiwać mechanizm Thin Provisioning, tj. przydział woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy, oraz umożliwiać odzyskiwanie przestrzeni dyskowej po usuniętych danych w ramach woluminów typu thin.
Zarządzanie	Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym macierzy. Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym (np. przez przeglądarkę WWW) oraz w trybie tekstowym (CLI). Zdalne zarządzanie macierzą musi być możliwe z wykorzystaniem standardowej przeglądarki internetowej (min. Microsoft Edge, Google Chrome, Mozilla Firefox), bez konieczności instalacji dodatkowych aplikacji na stacji administratora. Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy z szyfrowaniem komunikacji: protokołem TLS (HTTPS) dla komunikacji przez przeglądarkę WWW oraz protokołem SSH dla komunikacji przez CLI. Wraz z systemem musi zostać dostarczone narzędzie do monitorowania macierzy w zakresie: wydajności i opóźnień na woluminach, wydajności w IOPS i MB/s, trafności odczytów z pamięci cache. Macierz musi umożliwiać integrację z Active Directory w zakresie definicji i mapowania grup i użytkowników na potrzeby uwierzytelniania. Macierz musi posiadać oprogramowanie umożliwiające integrację z VMware vCenter – udostępnianie zasobów (provisioning) i monitorowanie macierzy z poziomu vCenter. Macierz musi obsługiwać VMware vSphere Storage APIs – Array Integration (VAAI).
Gwarancja i serwis	Całe rozwiązanie musi być objęte min. 36-miesięcznym okresem gwarancji z naprawą w miejscu instalacji urządzenia i gwarantowanym czasem reakcji do końca następnego dnia roboczego od dnia zgłoszenia awarii do organizacji serwisowej producenta

Obszar wymagań	Wymagania minimalne
	macierzy. Uszkodzone dyski (HDD i SSD) nie podlegają zwrotowi do organizacji serwisowej – pozostają u Zamawiającego. Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia. Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta na terenie UE. Nie dopuszcza się macierzy odnawianych, demonstracyjnych ani powystawowych. Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE dotyczącymi unikania i ograniczania stosowania substancji szkodliwych dla zdrowia. Producent oferowanej macierzy musi posiadać dedykowaną, ogólnodostępną stronę internetową, na której po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy, jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego oraz datę zakończenia wsparcia producenta dla oferowanego urządzenia. W formularzu ofertowym należy podać adres strony internetowej producenta macierzy, na której można zweryfikować wymagane informacje. Gwarancja musi być świadczona przez producenta lub autoryzowanego przez producenta partnera serwisowego, na terenie Rzeczypospolitej Polskiej, z przyjmowaniem zgłoszeń i komunikacją w języku polskim.

3.3. Serwer kopii zapasowych z licencją oprogramowania do tworzenia kopii zapasowych z funkcją deduplikacji – 1 kpl.

A. Macierz dyskowa na kopie zapasowe – 1 szt.

Obszar wymagań	Wymagania minimalne
Ogólne	System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19" i zajmować w szafie maks. 2U. Każdy skonfigurowany moduł/obudowa musi posiadać nadmiarowy układ zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia). Każdy moduł/obudowa musi posiadać widoczne elementy sygnalizacyjne informujące o stanie poprawnej pracy lub awarii. Oferowana macierz musi obsługiwać min. 48 dysków wykonanych w technologii hot-plug. Macierz musi posiadać 4 porty SAS 12 Gb/s do podłączenia dodatkowych półek dyskowych.
Pojemność macierzy	Min. 6 dysków NL-SAS 7,2 krpm o pojemności min. 10 TB każdy.
Kontrolery	Macierz musi być dostarczona z zainstalowanymi min. 2 kontrolerami. Każdy z kontrolerów macierzy musi posiadać min. 32 GB pamięci podręcznej cache. W przypadku awarii zasilania dane niezapisane na dyski, przechowywane w pamięci kontrolera, muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub poprzez zrzut do pamięci flash. Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji odczytu o

Obszar wymagań	Wymagania minimalne
	min. 5 TB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie pojemności zainstalowanych dysków SSD. Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach. Macierz musi posiadać funkcjonalność automatycznego równoważenia obciążenia kontrolerów poprzez przełączanie w trybie online woluminów logicznych pomiędzy kontrolerami w zależności od generowanego na nich ruchu. Musi istnieć możliwość wyłączenia tej funkcjonalności z poziomu interfejsu użytkownika. Każdy z kontrolerów RAID musi posiadać dedykowany interfejs Ethernet RJ-45 o prędkości min. 1 Gb/s do zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy. Każdy z kontrolerów RAID musi posiadać 2 porty iSCSI 25 Gb/s obsadzone modułami optycznymi 10 Gb/s (złącze LC, światłowód wielomodowy) do podłączenia serwerów bezpośrednio lub poprzez sieć SAN, w tym przełączniki z poz. 3.4.1. Macierz musi umożliwiać dołożenie portów do transmisji danych: SAS 12 Gb/s, iSCSI 10 Gb/s lub 25 Gb/s, FC 32 Gb/s.
Poziomy RAID	Macierz musi zapewniać zabezpieczenie danych na dyskach na poziomach RAID: 1, 10, 3, 5, 6. Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID 5 i RAID 6 musi być realizowane sprzętowo przez dedykowany układ w macierzy. Macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków o dużej pojemności. Macierz musi umożliwiać dynamiczną migrację pomiędzy poziomami RAID, tj. zmianę sposobu zabezpieczenia grupy dyskowej z jednego poziomu RAID na inny.
Dyski	Oferowana macierz musi obsługiwać dyski hot-plug: SSD, HDD z interfejsem SAS 12 Gb/s, HDD o prędkości obrotowej 7,2 krpm i 10 krpm. Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD zainstalowanych w dowolnym module rozwiązania. Wszystkie dyski obsługiwane przez oferowany model macierzy muszą być wykonane w technologii hot-plug. Macierz musi posiadać oprogramowanie do monitorowania stanu dysków, pozwalające na identyfikację dysków potencjalnie zagrożonych awarią, oraz umożliwiać sprawdzenie stanu zużycia dysków SSD z poziomu graficznego interfejsu zarządzania. Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysku zapasowego (hot-spare). W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku zapasowego na wymieniony dysk (tzw. copyback-less) albo macierz musi umożliwiać tworzenie pul dyskowych z rozproszoną przestrzenią rezerwową, w których nie stosuje się dedykowanych dysków zapasowych. Macierz musi umożliwiać szyfrowanie danych na dedykowanych do tego dyskach kluczem AES 256-bit, zgodnie z wytycznymi Information Technology Laboratory przy National Institute of Standards and Technology (NIST).

Obszar wymagań	Wymagania minimalne
	Macierz musi umożliwiać skasowanie wszystkich danych z dysku szyfrującego (FDE) w celu bezpiecznego ponownego użycia w innym środowisku (Secure Erase).
Opcje programowe	Macierz musi być wyposażona w system kopii migawkowych umożliwiający wykonanie 128 kopii migawkowych, z opcją rozbudowy do 512. Macierz musi umożliwiać zdefiniowanie min. 500 woluminów (LUN). Macierz musi umożliwiać podłączenie logiczne min. 250 serwerów. Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy oraz bez konieczności wyłączania ścieżek logicznych FC/iSCSI do podłączonych stacji/serwerów. Macierz musi umożliwiać dynamiczną zmianę rozmiaru woluminów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym woluminie. Macierz musi obsługiwać systemy operacyjne: Microsoft Windows Server 2019, 2022, 2025; SUSE Linux Enterprise Server 12, 15; Red Hat Enterprise Linux 8, 9; VMware vSphere 7, 8. Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię wielościeżkową (multipath – obsługa nadmiarowości ścieżek transmisji danych pomiędzy macierzą a serwerem) dla połączeń FC i iSCSI. Macierz musi umożliwiać uruchomienie mechanizmów zdalnej replikacji danych w trybie asynchronicznym, bez konieczności stosowania zewnętrznych urządzeń konwersji. Replikacja danych musi być realizowana przez oprogramowanie wewnętrzne macierzy (tzw. storage-based data replication) we współpracy z macierzą z tej samej rodziny urządzeń, obsługującą zdalną replikację danych. Funkcjonalność opcjonalna – możliwość wykupienia w przyszłości. Macierz musi obsługiwać mechanizm Thin Provisioning, tj. przydział woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy, oraz umożliwiać odzyskiwanie przestrzeni dyskowej po usuniętych danych w ramach woluminów typu thin.
Zarządzanie	Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym macierzy. Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym (np. przez przeglądarkę WWW) oraz w trybie tekstowym (CLI). Zdalne zarządzanie macierzą musi być możliwe z wykorzystaniem standardowej przeglądarki internetowej (min. Microsoft Edge, Google Chrome, Mozilla Firefox), bez konieczności instalacji dodatkowych aplikacji na stacji administratora. Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy z szyfrowaniem komunikacji: protokołem TLS (HTTPS) dla komunikacji przez przeglądarkę WWW oraz protokołem SSH dla komunikacji przez CLI. Wraz z systemem musi zostać dostarczone narzędzie do monitorowania macierzy w zakresie: wydajności i opóźnień na woluminach, wydajności w IOPS i MB/s, trafności odczytów z pamięci cache. Macierz musi umożliwiać integrację z Active Directory w zakresie definicji i mapowania grup i użytkowników na potrzeby uwierzytelniania.

Obszar wymagań	Wymagania minimalne
	Macierz musi posiadać oprogramowanie umożliwiające integrację z VMware vCenter – udostępnianie zasobów (provisioning) i monitorowanie macierzy z poziomu vCenter. Macierz musi obsługiwać VMware vSphere Storage APIs – Array Integration (VAAI).
Gwarancja i serwis	Całe rozwiązanie musi być objęte min. 36-miesięcznym okresem gwarancji z naprawą w miejscu instalacji urządzenia i gwarantowanym czasem reakcji do końca następnego dnia roboczego od dnia zgłoszenia awarii do organizacji serwisowej producenta macierzy. Uszkodzone dyski (HDD i SSD) nie podlegają zwrotowi do organizacji serwisowej – pozostają u Zamawiającego. Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia. Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta na terenie UE. Nie dopuszcza się macierzy odnawianych, demonstracyjnych ani powystawowych. Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE dotyczącymi unikania i ograniczania stosowania substancji szkodliwych dla zdrowia. Producent oferowanej macierzy musi posiadać dedykowaną, ogólnodostępną stronę internetową, na której po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy, jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego oraz datę zakończenia wsparcia producenta dla oferowanego urządzenia. W formularzu ofertowym należy podać adres strony internetowej producenta macierzy, na której można zweryfikować wymagane informacje. Gwarancja musi być świadczona przez producenta lub autoryzowanego przez producenta partnera serwisowego, na terenie Rzeczypospolitej Polskiej, z przyjmowaniem zgłoszeń i komunikacją w języku polskim.

B. Licencja oprogramowania do tworzenia kopii zapasowych z funkcją deduplikacji

Obszar wymagań	Wymagania minimalne
Licencja i wsparcie	Dostarczone oprogramowanie musi zawierać licencję wieczystą, umożliwiać obsługę min. 30 wirtualnych maszyn oraz posiadać co najmniej 24-miesięczne wsparcie techniczne. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk centrów danych.
Kompatybilność	Oprogramowanie musi współpracować z infrastrukturą Proxmox VE 8.2 lub nowszy. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej. Oprogramowanie musi współpracować z dostarczoną infrastrukturą. Oprogramowanie musi współpracować z hostami zarządzanymi przez wirtualizator oraz pojedynczymi hostami. Oprogramowanie musi współpracować z hostami zarządzanymi przez system centralny, klastrami hostów oraz pojedynczymi hostami.

Obszar wymagań	Wymagania minimalne
Tworzenie kopii zapasowych	Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych. Oprogramowanie musi tworzyć „samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków. Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: pełny, przyrostowy. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji. Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków. Oprogramowanie musi mieć możliwość tworzenia retencji. Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc.
Bezpieczeństwo	Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej.
Kopie na taśmy	Oprogramowanie musi wspierać kopiowanie plików na taśmy.
Odtwarzanie	Oprogramowanie musi umożliwiać uruchomienie maszyny wirtualnej z kopii zapasowej z dowolnego punktu przywracania przed zakończeniem jej odtwarzania (odtwarzanie danych w tle). Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM.
Zarządzanie i monitorowanie	System musi dawać możliwość podłączenia się do kilku instancji i serwerów jednocześnie. System musi mieć centralną konsolę (dashboard) z sumarycznym podglądem stanu serwera kopii zapasowych, magazynów danych i zadań, a także – z wykorzystaniem bezpłatnego narzędzia producenta – zasobów infrastruktury wirtualnej. System musi mieć możliwość monitorowania stanu sprzętu serwera kopii zapasowych, w tym stanu dysków (S.M.A.R.T.). System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.

3.4. Przełączniki zarządzalne – sieć biurowa – 1 zestaw

3.4.1. Przełącznik do klastra HA – 2 szt.

Obszar wymagań	Wymagania minimalne
Obudowa	Obudowa urządzenia musi być przystosowana do montażu w standardowej szafie 19" i zajmować maksymalnie 1U.
Zasilanie	2 redundantne zasilacze AC 100-240 V. Maksymalna moc pobierana przez urządzenie nie może przekraczać 80 W.
Chłodzenie	Co najmniej 2 wentylatory.

Obszar wymagań	Wymagania minimalne
Pamięć	Minimum RAM: 1 GB Minimum FLASH: 16 MB
Interfejsy sieciowe	Porty minimum: 16 portów 10Gb SFP+ oraz 1 port 10/100/1000 Mb/s RJ-45. Port konsoli szeregowej RJ-45. Do każdego portu SFP+ wkładka SFP+ 10GB umożliwiająca połączenia pomiędzy dostarczanymi i posiadanymi urządzeniami.
Wydajność i funkcjonalności	– Potencjał przełączania nie mniejszy niż 320 Gbps – Przepustowość w warstwie 2 dla ramek 1518 B nie mniejsza niż 150 Gbps – VLAN, – (RSTP), – ACL – co najmniej 1000 reguł, – LACP, – QoS, – port mirroring, – SNMP, 802.1Q – Baza danych przekazywania oparta na SVL (Shared VLAN Learning) lub IVL (Independent VLAN Learning) – Izolacja portów – Obsługa ramek Jumbo – 10218 bajtów – Obsługa IGMP Snooping – Obsługa DHCP Snooping – Filtrowanie nieznanych transmisji multicast
Zarządzanie	Interfejs webowy (GUI), dostęp przez SSH i konsolę szeregową (port RJ45).
Routing	– Static route – Policy-based route
Agregacja łączy	Obsługa grup LACP zgodnych z 802.3ad Obsługa statycznych grup agregacji łączy Co najmniej 8 portów członkowskich na grupę Sprzętowa obsługa automatycznego przełączania awaryjnego i równoważenia obciążenia
VLAN	Pełna zgodność z IEEE 802.1Q VLAN oparty na porcie Obsługa co najmniej 4000 aktywnych sieci VLAN Filtrowanie VLAN
Zgodność ze standardami	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.3ab, IEEE 802.3ae, IEEE 802.1Q, IEEE 802.1p, IEEE 802.1D, IEEE 802.1w, IEEE 802.3ad, IEEE 802.1X
Gwarancja	Gwarancja na okres co najmniej 24 miesięcy. Gwarancja musi być świadczona przez producenta lub autoryzowanego przez producenta partnera serwisowego, na terenie Rzeczypospolitej Polskiej, z przyjmowaniem zgłoszeń i komunikacją w języku polskim.

Obszar wymagań	Wymagania minimalne
Serwis	W przypadku awarii wymiana urządzenia na nowe, wolne od wad, w terminie do 5 dni roboczych od dnia zgłoszenia awarii.
Wymagane Certyfikaty	Bezpieczeństwo: CE, RoHS
Pozostałe	Sprzęt musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE.

3.4.2. Przełącznik dystrybucyjny 24-portowy – 2 szt.

Obszar wymagań	Wymagania minimalne
Obudowa	Obudowa urządzenia musi być przystosowana do montażu w standardowej szafie 19” i zajmować maksymalnie 1U.
Interfejsy	Minimum 24 gigabitowe interfejsy RJ-45 100/1000 Mbps, 4 interfejsy 10 Gigabit SFP+. Wszystkie porty SFP+ muszą być dostarczone z wkładkami SFP+.
Wydajność i funkcjonalności	– Potencjał przełączania nie mniejszy niż 128 Gbps – Wydajność przekazywania pakietów nie mniejsza niż 95,2 Mpps – Bufor pakietu nie mniejszy niż 1500 KB – Tabela adresów MAC nie mniejsza niż 16K – Jumbo frame (byte) – 9K – Flash/RAM (MB): 32/512 – L3 forwarding table: Max. 512 IPv4 entries; Max. 512 IPv6 entries – Routing table: 32 – VLAN routing – IP interface (IPv4/IPv6): 32/32
Tryby pracy	– Urządzenie musi umożliwiać zdalną konfigurację i monitorowanie poprzez panel sterowania dostępny w technologii chmurowej, dostarczony bezpłatnie przez producenta urządzenia
Zgodność ze standardami	– IEEE 802.3 10BASE-T Ethernet – IEEE 802.3u 100BASE-TX Ethernet – IEEE 802.3ab 1000BASE-T Ethernet – IEEE 802.3z 1000BASE-X – IEEE 802.3az EEE – IEEE 802.3x flow control – IEEE 802.3ad LACP aggregation – IEEE 802.1D Spanning Tree Protocol (STP) – IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) – IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) – IEEE 802.1p Class of Service (CoS) prioritization – IEEE 802.1X port authentication
Odporność i dostępność	– IEEE 802.1D Spanning Tree Protocol (STP) – IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)

Obszar wymagań	Wymagania minimalne
	– IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) – IEEE 802.3ad LACP. Max # Trunks/ Links per Trunk: 24/8
Kontrola ruchu	– 802.1Q static VLANs/dynamic VLANs: 1 K/4 K – Support up to 4K VLAN ID – Independent VLAN Learning (IVL) – L2TP – Port-based VLAN – Voice VLAN – VLAN trunking – GVRP
Bezpieczeństwo	– 802.1X – Port security – MAC authentication – Static MAC forwarding – SSL – Static ARP – Policy-based security filtering – Port isolation – MAC search – Guest VLAN – PPPoE relay agent – PPPoE option 82 – PPPoE IA – Interface related trap enable/ disable (by port) – CPU protection – SHA2 HTTPS certification – Login authentication by RADIUS – RADIUS accounting – Authorization on RADIUS – Multiple RADIUS servers – 802.1x VLAN and bandwidth assignment by RADIUS – ACL packet filtering (IPv4)
QoS	– No. of hardware queues per port: 8 – 802.1p queuing methods: SPQ, WRR, WFQ – Storm control: broadcast, unknown L2MC, unknown unicast (DLF) – Rate limiting per port – Policy-based rate limiting – Policy-based prioritization
Layer 2 Multicast	– L2 multicast group: 1K – IGMP snooping (v1, v2, v3)

Obszar wymagań	Wymagania minimalne
	– Configurable IGMP snooping timer and priority – IGMP snooping statistics – IGMP throttling – IGMP filtering – Static multicast
Zarządzanie	– SNMP v1, v2c, v3 – SNMP trap group – RMON (1, 2, 3, 9) – Syslog ((IPv4/v6) – IEEE 802.1AB LLDP – IEEE 802.1AB LLDP-MED
Zarządzanie IPv6	– IPv6 over Ethernet (RFC 2464) – IPv6 addressing architecture (RFC 4291) – Dual stack (RFC 4213) – ICMPv6 (RFC4884) – Path MTU (RFC 1981) – Minimum path MTU size of 1280 (RFC 5095) – Encapsulation for maximum PMTU of 1500 – Neighbor discovery (RFC 4861) – DHCPv6 relay – Default DHCP client mode – Duplicated Address Detection (DAD)
Zarządzanie urządzeniem	– Standalone management by Web interface – Setup Wizard – Management through Telnet – Management through Web, SNMP – Firmware upgrade by FTP/Web – Configuration saving and retrieving – Multiple logins supported – Configure clone – DHCP relay per VLAN – DHCP client IPv4 – DHCP client IPv6 – DHCP option 82 – Daylight saving – NTP Server (IPv4/IPv6) Support DNS format – Display port utilization – Port mirroring – Web login warning page – Restore to last custom default

Obszar wymagań	Wymagania minimalne
MIB	– RFC 1213, 1157 SNMPv2c/v3 MIB – RFC 1493 bridge MIB – RFC 1643 Ethernet MIB – RFC 1757 RMON group 1, 2, 3, 9 – RFC 2011, 2012, 2013 SNMPv2 MIB – RFC 2233 SMIv2 MIB – RFC 2819, 2925 remote management MIB – RFC 4292 IP forwarding table MIB – RFC 4293 Management Information Base (MIB) for IP
Gwarancja	Gwarancja producenta na okres co najmniej 24 miesięcy od dnia odbioru. Gwarancja musi być świadczona przez producenta lub autoryzowanego przez producenta partnera serwisowego, na terenie Rzeczypospolitej Polskiej, z przyjmowaniem zgłoszeń i komunikacją w języku polskim.
Serwis	W przypadku awarii urządzenia, wysyłka zastępczego produktu następuje w następnym dniu roboczym, po którym zgłoszona zostanie awaria. Urządzenie musi być objęte ww. opcją serwisową przez cały okres gwarancji.
Wymagane Certyfikaty	Bezpieczeństwo – LVD – CE – RoHS
Pozostałe	Sprzęt musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE.

3.4.3. Przełącznik dystrybucyjny 8-portowy PoE – 1 szt.

Obszar wymagań	Wymagania minimalne
Obudowa	Obudowa urządzenia musi być pozbawiona wentylatorów
Pamięć	Minimum RAM: 256 MB Minimum FLASH: 32 MB
Interfejsy	8 gigabitowych interfejsów RJ-45 100/1000 Mbps z obsługą PoE/PoE+, 2 interfejsy Gigabit Combo (RJ-45/SFP).
Wydajność	– Potencjał przełączania nie mniejszy niż 20 Gbps – Wydajność przekazywania pakietów nie mniejsza niż 14 Mpps – Bufor pakietu nie mniejszy niż 1500 KB – Tabela adresów MAC nie mniejsza niż 8K – Minimalny budżet PoE – 120W
Tryby pracy	– Urządzenie musi umożliwiać zdalną konfigurację i monitorowanie poprzez panel sterowania dostępny w technologii chmurowej, dostarczony bezpłatnie przez producenta urządzenia

Obszar wymagań	Wymagania minimalne
Zgodność ze standardami	– IEEE 802.3u 100BASE-TX Ethernet – IEEE 802.3ab 1000BASE-T Ethernet – IEEE 802.3z 1000BASE-X – IEEE 802.3af PoE – IEEE 802.3at PoE Plus – IEEE 802.3az EEE – IEEE 802.3x flow control – IEEE 802.1AB LLDP/LLDP-MED – IEEE 802.3ad LACP aggregation – IEEE 802.1D Spanning Tree Protocol (STP) – IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) – IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) – IEEE 802.1Q VLAN tagging – IEEE 802.1p Class of Service (CoS) prioritization – IEEE 802.1X port authentication
Odporność i dostępność	– IEEE 802.1D Spanning Tree Protocol (STP) – IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) – IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) – IEEE 802.3ad LACP (Max # Trunks/ Links per Trunk): 8/8
Kontrola ruchu	– 802.1Q Static VLANs/Dynamic VLANs: 1 K/4 K – Port-based VLAN – Protocol-based VLAN – IP Subnet-based VLAN – MAC-based VLAN – Private VLAN – Voice VLAN – VLAN ingress filtering – LACP algorithm of source/ destination MAC/IP – GVRP – L2PT
Bezpieczeństwo	– 802.1X – Port security – Layer 2 MAC filtering – Layer 3 IP filtering – Layer 4 TCP/UDP socket filtering – Static MAC forwarding – Multiple RADIUS servers – Multiple TACACS+ servers – 802.1x VLAN and 802.1p assignment by RADIUS – Login authentication by RADIUS – Login authentication by TACACS+

Obszar wymagań	Wymagania minimalne
	– TACACS+ accounting – Authorization on RADIUS – Authorization on TACACS+ – SSL – MAC freeze – DHCP snooping IPv4 – DHCP snooping IPv6 – ARP inspection – Static IP-MAC-Port binding – Policy-based security filtering – Port isolation – IP source guard – MAC search – Guest VLAN – ACL packet filtering (IPv4/IPv6) – CPU protection – Interface related trap enable/disable (by port) – IPv6 Duplicated Address Detection (DAD)
QoS	– No. of hardware queues per port: 8 – 802.1p queuing methods: SPQ, WRR, WFQ – Storm control: broadcast, multicast, unknown unicast (DLF) – Port-based rate limiting (ingress/egress) – Rate limiting per IP/TCP/UDP per port – Policy-based rate limiting – 802.3x flow control – 802.1p Class of Service (SPQ, WFQ, SPQ/WFQ combination capable) – DiffServ (DSCP)
Layer 2 Multicast	– L2 multicast – IGMP snooping (v1, v2, v3) – IGMP snooping fast Leave – Configurable IGMP snooping timer and priority – IGMP snooping statistics – IGMP throttling – MVR support – IGMP filtering – IGMP snooping immediate leave – IGMP proxy mode & snooping mode selection – MLD snooping
Zarządzanie	– SNMP v1, v2c, v3 – SNMP trap group – RMON (1, 2, 3, 9)

Obszar wymagań	Wymagania minimalne
	– ICMP echo/echo reply – IEEE 802.1AB LLDP – IEEE 802.1AB LLDP-MED – Custom default – Syslog (IPv4/IPv6) – Display port utilization
Zarządzanie IPv6	– IPv6 over Ethernet (RFC 2464) – IPv6 addressing architecture (RFC 4291) – Dual stack (RFC 4213) – ICMPv6 (RFC 4443) – Path MTU (RFC 1981) – Minimum path MTU size of 1280 (RFC 5095) – Encapsulation for maximum MTU of 1500 – Neighbor discovery (RFC 4861) – DHCPv6 relay – Default DHCP client mode – DAD (Duplicated Address Detection)
Zarządzanie urządzeniem	– Standalone management by Web interface – Web interface – Management through SNMP – Remote firmware upgrade by Web – Configuration saving and retrieving – Configure clone – DHCP relay per VLAN – DHCP client IPv4 – DHCP client IPv6 – Daylight saving – NTP Server (IPv4/IPv6) – Support DNS format – Port mirroring – Scheduled PoE – PoE default consumption mode – Restore to last custom default
MIB	– RFC 1213, 1157 SNMPv2c/v3 MIB – RFC 1493 bridge MIB – RFC 1643 Ethernet MIB – RFC 1757 RMON Group 1, 2, 3, 9 – RFC 2011, 2012, 2013 SNMPv2 MIB – RFC 2233 SMIv2 MIB – RFC 2819, 2925 remote management MIB – RFC 3621 power Ethernet MIB – RFC 4292 IP forwarding table MIB

Obszar wymagań	Wymagania minimalne
	– RFC 4293 Management Information Base (MIB) for IP
Gwarancja	Gwarancja producenta na okres co najmniej 24 miesięcy od dnia odbioru. Gwarancja musi być świadczona przez producenta lub autoryzowanego przez producenta partnera serwisowego, na terenie Rzeczypospolitej Polskiej, z przyjmowaniem zgłoszeń i komunikacją w języku polskim.
Serwis	W przypadku awarii urządzenia, wysyłka zastępczego produktu następuje w następnym dniu roboczym, po którym zgłoszona zostanie awaria. Urządzenie musi być objęte ww. opcją serwisową przez cały okres gwarancji.
Wymagane Certyfikaty	Bezpieczeństwo – LVD – CE – RoHS
Pozostałe	Sprzęt musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE.

3.5. Biblioteka taśmowa LTO-9 wraz z kasetami – 1 kpl.

Obszar wymagań	Wymagania minimalne
Obudowa	Przystosowana do montażu w szafie rack 19", wysokość nie większa niż 2U, wraz z kompletem szyn montażowych.
Napędy taśmowe	Biblioteka taśmowa musi być wyposażona w min. 1 napęd taśmowy LTO-9 o natywnym interfejsie SAS o prędkości min. 12 Gb/s.
Liczba slotów – storage	Biblioteka musi mieć min. 8 kieszeni na nośniki taśmowe, wszystkie możliwe do użycia przez Zamawiającego, z możliwością rozbudowy do min. 16 kieszeni. Biblioteka musi umożliwiać import i eksport pojedynczych nośników bez wyjmowania magazynka (kieszeń typu „mail slot" lub port importu). Wbudowany czytnik kodów kreskowych.
Zarządzanie	Biblioteka musi być zarządzana z poziomu frontowego panelu urządzenia wyposażonego w wyświetlacz oraz zdalnie przez przeglądarkę WWW. Biblioteka musi udostępniać funkcje monitorowania stanu napędu i robota, przeglądania dzienników zdarzeń, przeprowadzania testów diagnostycznych oraz aktualizacji oprogramowania układowego. Powiadamianie o zdarzeniach co najmniej pocztą elektroniczną lub przez SNMP. Biblioteka musi posiadać min. 1 interfejs sieciowy RJ-45 do zarządzania.
Bezpieczeństwo danych	Sprzętowe szyfrowanie danych AES 256-bit. Obsługa nośników WORM.
Dodatkowe oprogramowanie	Biblioteka musi współpracować z oprogramowaniem do tworzenia kopii zapasowych dostarczonym w poz. 3.3 B.
Kontroler	Wraz z biblioteką Zamawiający wymaga dostarczenia kontrolera HBA SAS 12 Gb/s do

Obszar wymagań	Wymagania minimalne
	serwera z poz. 3.1 (wskazanego przez Wykonawcę w projekcie klastra HA – pkt W.2), aby obsłużyć połączenie z biblioteką, oraz kabla SAS.
Kompatybilność	Microsoft Windows, Linux (co najmniej Red Hat Enterprise Linux, SUSE Linux Enterprise Server).
Gwarancja	Biblioteka musi posiadać gwarancję producenta min. 36 miesięcy. Gwarancja musi być świadczona przez producenta lub autoryzowanego przez producenta partnera serwisowego, na terenie Rzeczypospolitej Polskiej, z przyjmowaniem zgłoszeń i komunikacją w języku polskim.
Taśmy	Sprzęt musi być dostarczony wraz z 5 taśmami LTO-9, 1 taśmą czyszczącą oraz etykietami z kodami kreskowymi.
Certyfikaty	Zgodność z normami: IEC 62368-1 lub EN 62368-1, EN 55032 klasa A, EN 300 386 lub równoważnymi; oznakowanie CE.
Inne	Jeśli do jakiejkolwiek wyżej opisanej funkcjonalności lub rozbudowy fizycznej wymagane jest dostarczenie licencji, to licencje muszą być dostarczone w ramach tego postępowania.

3.6. Zasilacz UPS z monitoringiem dla klastra HA – 1 kpl.

Obszar wymagań	Wymagania minimalne
Moc	Moc pozorna: min. 8000 VA. Moc czynna: min. 8000 W.
Technologia	On-line (podwójna konwersja, VFI), czysta sinusoida na wyjściu. Czas przełączenia: 0 ms (praca on-line). Możliwość pracy w trybie ekonomicznym (ECO/Green), z możliwością jego wyłączenia.
Wejście	Napięcie znamionowe: 220/230/240 V. Możliwość zasilania jednofazowego lub trójfazowego (konfiguracja 1:1 lub 3:1). Zakres częstotliwości wejściowej: co najmniej 45–65 Hz.
Wyjście	Napięcie wyjściowe: 220/230/240 V, 50/60 Hz. Porty wyjściowe: min. 6x IEC C13 oraz 4x IEC C19, w podziale na co najmniej 3 grupy gniazd sterowanych niezależnie.
Baterie	Baterie bezobsługowe VRLA w wymiennych modułach. Możliwość rozbudowy o dodatkowe zewnętrzne moduły bateryjne w celu wydłużenia czasu podtrzymania.
Komunikacja i zarządzanie	Karta zarządzająca sieciowa (RJ-45) zainstalowana w zestawie wraz z oprogramowaniem do zarządzania poprzez sieć LAN, z możliwością konfiguracji automatycznego, bezpiecznego wyłączania serwerów i maszyn wirtualnych. Porty USB oraz szeregowy. Dodatkowe gniazdo na karty rozszerzeń.

Obszar wymagań	Wymagania minimalne
	Wyświetlacz LCD na panelu przednim. Złącze EPO (awaryjnego wyłączenia zasilania).
Obudowa i montaż	Obudowa typu tower/rack (konwertowalna), wysokość w szafie rack maks. 6U. W zestawie komplet szyn do montażu w szafie rack 19".
Certyfikaty	IEC/EN 62040-1 lub równoważną, CE.
Gwarancja	Standardowa gwarancja producenta na okres min. 24 miesięcy. Gwarancja musi być świadczona przez producenta lub autoryzowanego przez producenta partnera serwisowego, na terenie Rzeczypospolitej Polskiej, z przyjmowaniem zgłoszeń i komunikacją w języku polskim.
Wymagania dodatkowe	Wykonawca wykona podłączenie zasilacza UPS do instalacji elektrycznej Zamawiającego, w tym ewentualne podłączenie typu hardwire, przez osobę posiadającą odpowiednie uprawnienia elektryczne.

3.7. Serwer NAS na odmiejscowione kopie zapasowe – 1 szt.

Obszar wymagań	Wymagania minimalne
Procesor	Procesor o architekturze x86 64-bit, posiadający co najmniej 4 rdzenie, uzyskujący wynik co najmniej 4 300 punktów w teście PassMark – CPU Mark według wyników dostępnych na stronie http://www.cpubenchmark.net 30 dni przed terminem składania ofert lub później. Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim.
Obudowa	Obudowa rack 19", wysokość maks. 2U, dostarczona wraz z szynami do montażu w szafie rack 19".
Pamięć RAM	Co najmniej 4 GB DDR4 ECC. Możliwość rozbudowy do co najmniej 32 GB.
Ilość obsługiwanych dysków	Co najmniej 8 kieszeni na dyski 3,5" lub 2,5" SATA HDD/SSD. Możliwość rozbudowy o jednostkę rozszerzającą.
Zainstalowane dyski	Co najmniej 5 dysków HDD 3,5" klasy NAS lub enterprise o pojemności co najmniej 4 TB każdy, znajdujących się na liście kompatybilności producenta urządzenia.
Interfejsy sieciowe	Co najmniej 4 porty 1GbE RJ-45.
Porty	Co najmniej 2 porty USB 3.2 Gen 1. Port rozszerzeń (eSATA lub równoważny) do podłączenia jednostki rozszerzającej.
Port PCIe	Co najmniej 1 gniazdo PCIe Gen3 umożliwiające instalację karty sieciowej 10GbE.
Wskaźniki LED	Wskaźniki stanu zasilania, stanu systemu, alertów, stanu poszczególnych dysków oraz stanu zasilaczy.
Obsługa RAID	SHR lub równoważne, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10.

Obszar wymagań	Wymagania minimalne
Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online.
Szyfrowanie	Możliwość szyfrowania wybranych udziałów sieciowych kluczem AES-256.
Protokoły	SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN, L2TP).
Funkcje i usługi	Wsparcie dla wirtualizacji. Scentralizowana pamięć masowa na dane. Kopia zapasowa. Udostępnianie i przywracanie systemu po awarii. Mechanizm szyfrowania sprzętowego. Uprawnienia listy kontroli dostępu systemu Windows (ACL). Wymagana kompatybilność z usługą katalogową serwera Windows (możliwość logowania użytkowników domeny za pośrednictwem protokołów SMB/FTP/WebDAV oraz interfejsu WWW).
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów.
Język GUI	Polski.
System plików	Dyski wewnętrzne: system plików z obsługą migawek i sum kontrolnych (Btrfs lub równoważny) oraz EXT4. Dyski zewnętrzne: co najmniej FAT, NTFS, EXT4, EXT3, HFS+, exFAT.
Parametry wydajnościowe	Liczba wolumenów: co najmniej 64. Liczba iSCSI Targetów: co najmniej 64. Liczba iSCSI LUN: co najmniej 128. Liczba kont użytkowników: co najmniej 1024. Liczba grup: co najmniej 256. Liczba folderów udostępnionych: co najmniej 256. Liczba zadań synchronizacji folderów udostępnionych: co najmniej 8. Liczba jednoczesnych połączeń SMB: co najmniej 180.
Bezpieczeństwo	Obsługa WORM (Write Once Read Many) dla folderów współdzielonych i migawek, zapora sieciowa, szyfrowanie folderu współdzielonego, szyfrowanie całego woluminu, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania przy nieuprawnionym dostępie dla protokołów HTTP, HTTPS, SMB, SSH, Telnet, rsync, FTP, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania), dwuetapowa weryfikacja logowania (2FA), możliwość logowania za pomocą klucza sprzętowego w standardzie FIDO2/U2F, grupowanie reguł powiadomień (zdarzenia systemowe) dla różnych adresów e-mail.
Oprogramowanie	– Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych, a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych. – Możliwość tworzenia klastra wysokiej dostępności (HA) z dwóch identycznych

Obszar wymagań	Wymagania minimalne
	serwerów, bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system), z funkcją automatycznego przełączania dostępu do usług i danych na serwer pasywny w przypadku awarii serwera aktywnego. – Możliwość tworzenia kopii zapasowej danych z serwera na zewnętrzne dyski twarde (USB), do chmur publicznych i serwera rsync. – Obsługa minimum 256 migawek na folder współdzielony i minimum 4096 migawek na cały system. – Funkcja serwera VPN (OpenVPN, L2TP/IPSec i PPTP) dla minimum 8 jednoczesnych połączeń.
Oprogramowanie do kopii zapasowej	Zakup urządzenia musi uprawniać do instalacji i eksploatacji oprogramowania do kopii zapasowej bez konieczności ponoszenia dodatkowych kosztów. Minimalne wymagane funkcje oprogramowania do backupu: – oprogramowanie musi być w pełni zgodne z oferowanym urządzeniem, – kopia zapasowa całego systemu Windows (bare-metal), przywracanie w trybie bare-metal, – kopia zapasowa maszyn wirtualnych (VMware, Hyper-V), – kopia zapasowa serwerów fizycznych (Windows, Linux), – obsługa deduplikacji, kopii przyrostowej, kompresji i szyfrowania, – obsługa wielu wersji i retencji, – możliwość wyzwalania kopii zapasowej według harmonogramu, – obsługa klastra przełączania awaryjnego Microsoft Hyper-V, – centralne zarządzanie, – konfiguracja nowych i edycja istniejących zadań kopii zapasowej wielu komputerów i serwerów fizycznych z poziomu jednej centralnej konsoli zarządzającej, w tym minimum w zakresie liczby i czasu przechowywanych wersji, harmonogramu i woluminów objętych backupem dla poszczególnych zadań, – portal użytkownika do przywracania danych kopii zapasowej (bez uprawnień administratora), – delegowanie uprawnień do zarządzania kopią zapasową i przywracaniem dla użytkowników bez uprawnień administratora, – kopia zapasowa usług chmur publicznych Microsoft 365 i Google Workspace.
Zasilanie	Redundantne zasilacze o mocy min. 350 W.
Chłodzenie	Co najmniej 2 wentylatory.
Gwarancja	36 miesięcy gwarancji producenta. Gwarancja musi być świadczona przez producenta lub autoryzowanego przez producenta partnera serwisowego, na terenie Rzeczypospolitej Polskiej, z przyjmowaniem zgłoszeń i komunikacją w języku polskim.

3.8. Urządzenie UTM dla sieci IT – 1 szt.

Pkt	Wymagania minimalne
1	**Funkcje modułu Firewall**

Pkt	Wymagania minimalne
1.1	Musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2).
1.2	Możliwość uruchomienia w formie klastra wysokiej dostępności (HA) – co najmniej Active-Passive.
1.3	Musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP) lub jako bridge (transparent mode).
1.4	Musi obsługiwać protokoły dynamicznego routingu: RIP v1/v2, OSPF i BGP4.
1.5	Musi obsługiwać Multicast routing.
1.6	Musi obsługiwać Policy Based routing.
1.7	Musi umożliwiać znakowanie QoS w oparciu o ToS (Type of Service) lub DSCP (Differentiated Service Code Point) w ramach zapewnienia jakości usług.
1.8	Musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPPoE) na zewnętrznym interfejsie.
1.9	Musi obsługiwać DHCPv6 na zewnętrznym interfejsie.
1.10	Musi obsługiwać funkcję agregacji linków (802.3ad dynamic, static, active/backup).
1.11	Musi obsługiwać Dynamic DNS.
1.12	Musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1.
1.13	Musi obsługiwać translację portów: PAT.
1.14	Musi obsługiwać IPSec NAT traversal.
1.15	Musi obsługiwać mechanizm Policy Based NAT.
1.16	Musi obsługiwać VLAN 802.1Q.
1.17	Musi zapewniać funkcję serwera DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.
1.18	Musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP.
1.19	Musi mieć możliwość obsługi zapasowego łącza typu 4G LTE/5G poprzez podłączenie zewnętrznego modemu USB.
1.20	Musi mieć możliwość automatycznego przełączania ruchu pomiędzy interfejsami zewnętrznymi w przypadku awarii jednego z nich.
1.21	Musi zapewniać funkcję równoważenia obciążenia pomiędzy interfejsami zewnętrznymi.
1.22	Musi zapewniać funkcjonalność SD-WAN w ramach automatycznej dystrybucji ruchu na podstawie jakości łącza, minimum dla wartości: utrata pakietów, opóźnienie, jitter.
1.23	Musi zapewniać funkcję równoważenia obciążenia w ramach połączeń do wewnętrznych serwerów.
1.24	Musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.
1.25	Musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: Active Directory, LDAP, RADIUS, SecurID, VASCO oraz wewnętrznej bazy użytkowników.
1.26	Musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z Active Directory.

Pkt	Wymagania minimalne
1.27	Musi posiadać co najmniej dwie metody transparentnej autoryzacji nie wymagające instalacji dedykowanego agenta na stacjach roboczych użytkowników.
1.28	Musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z usług terminalowych Microsoft oraz Citrix.
1.29	Nie może ograniczać ilości urządzeń, adresów IP czy użytkowników sieci wewnętrznej.
1.30	Musi dostarczać mechanizm identyfikacji urządzeń w sieci w tym co najmniej identyfikację systemu operacyjnego, otwartych portów i usług.
1.31	Musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.
1.32	Musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.
1.33	Musi posiadać mechanizmy rozpoznawania anomalii w protokołach sieciowych – dla najpopularniejszych protokołów.
1.34	Musi umożliwiać sterowanie przepustowością w oparciu o politykę zapory sieciowej oraz wybraną aplikację.
1.35	Musi dostarczać mechanizmów limitowania dostępu do sieci użytkownikom w oparciu o quoty czasowe lub transferu danych, co najmniej dla komunikacji http.
1.36	Musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMTPS, POP3S, IMAPS, H.323, SIP.
1.37	Musi zapewniać funkcjonalność Content Routing w ramach protokołu HTTP/HTTPS na podstawie co najmniej nagłówka hosta HTTP i żądania HTTP.
1.38	Musi zapewniać funkcjonalność TLS/SSL Offloading dla protokołu HTTPS w ramach połączeń do wewnętrznych serwerów.
1.39	Musi ochraniać przed minimum: atakami DoS, pofragmentowanymi i zniekształconymi pakietami, zagrożeniami mieszanymi (Blended threats).
1.40	Musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site.
1.41	VPN site-to-site musi wspierać minimum: IKEv2, IPSec, tunele oparte na politykach i routingu, TLS hub and spoke.
1.42	VPN client-to-site musi wspierać minimum: IKEv2, IPSec, L2TP, TLS
2	**Specyfikacja UTM**
2.1	Firewall musi zapewnić obsługę na poziomie minimalnym: – 3.90 Gbps dla pracy w trybie firewall dla pakietów UDP 1518, – 710 Mbps dla pracy w trybie full scan (włączone mechanizmy bezpieczeństwa takie jak: AV, IPS), – 1.94 Gbps dla pracy w trybie VPN dla pakietów UDP 1518, – 1.03 Gbps dla modułu IPS w trybie full scan, – 1.06 Gbps dla skanowań antywirusa – 380 Mbps dla protokołu HTTPS z włączonym IPS oraz pełnym skanowaniem

Pkt	Wymagania minimalne
2.2	Nielimitowana sprzętowo ilość obsługi VLAN
2.3	Firewall musi obsługiwać 3 850 000 jednoczesnych połączeń TCP oraz przyjmować nowe połączenia z wydajnością minimalną 26 500 połączeń na sekundę.
2.4	Minimalna ilość portów 10/100/1000 BaseT: 4
2.5	Minimalna ilość portów 2.5 GbE: 1
2.6	Minimalna ilość portów SFP/SFP+: 1
2.7	Wsparcie połączeń VPN site-to-site lub client-to-site dla minimum 25 użytkowników.
2.8	Sieć bezprzewodowa: a. Urządzenie musi wspierać Wi-Fi 7 b. Urządzenie musi posiadać minimum 3 anteny zewnętrzne SMA o częstotliwościach: – 2x 2,4 GHz i 5 GHz – 1x 5 GHz c. Bezprzewodowe radia muszą spełniać poniższe parametry: d. Radio 1 (2,4 GHz) e. Wi-Fi 7 2x2 802.11be/ax/b/g/n f. Prędkość transmisji danych do 688 Mb/s g. Radio 2 (5 GHz) h. Wi-Fi 7 3x3 802.11be/ax/ac/a/n i. Prędkość transmisji danych do 4323 Mb/s
3	**Dostarczony system bezpieczeństwa (UTM) musi zapewniać**
3.1	Ochronę z wykorzystaniem mechanizmów IPS.
3.2	Ochronę antywirusową opartą na sygnaturach.
3.3	Ochronę przed niechcianą pocztą.
3.4	Kontrolę wykorzystywanych aplikacji.
3.5	Możliwość filtrowania URL.
3.6	Ochronę przed Advanced Persistent Threat.
3.7	Ochronę antywirusową opartą na sztucznej inteligencji i uczenia maszynowego.
4	**W ramach ochrony przed atakami system musi zapewniać**
4.1	Automatyczną aktualizację bazy sygnatur IPS. Powinna ona zawierać co najmniej 8000 definicji sygnatur.
4.2	Automatyczne blokowanie znanych źródeł ataków.
4.3	Ochronę przed lukami w zabezpieczeniach w aplikacjach, bazach danych, systemach operacyjnych.
4.4	Mechanizmy ochrony przed atakami typu DoS i DDoS co najmniej (IPsec Flood, IKE Flood, ICMP Flood, Syn Flood, UDP Flood, IP Scan, Ilość połączeń, Port Scan, IP Source Route, ARP/IP Spoofing).
4.5	Mechanizmy blokowania przed atakami typu: SQL Injection, Cross-Site-Scripting, Buffer Overflow, Remote File Inclusions.

Pkt	Wymagania minimalne
4.6	Mechanizm, który pozwoli generować alarmy – dla wskazanego poziomu nasilenia ataku.
5	**W ramach kontroli antywirusowej system musi zapewniać**
5.1	Możliwość rozbudowy (np. w oparciu o licencję) o możliwość uruchomienia co najmniej 2 skanerów antywirusowych opartych na analizie sygnaturowej oraz bezsygnaturowej lokalnie
5.2	Automatyczną aktualizację baz sygnatur, nie rzadziej niż co 12 godzin.
5.3	Możliwość skanowania plików o rozmiarze co najmniej 10MB.
5.4	Możliwość zdefiniowania rozmiaru skanowanego pliku.
5.5	Możliwość skanowania plików w wielokrotnie skompresowanych archiwach.
5.6	Możliwość tworzenia wyjątków (biała lista) dla określonych adresów URL, typów plików, sygnatury pliku MD5.
5.7	Wykrywanie i blokowanie złośliwego oprogramowania typu: Virus, Trojan, Worms, Spyware, Rogueware, Malware.
5.8	Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS.
5.9	Minimum jeden silnik ochronny oparty na sztucznej inteligencji i uczeniu maszynowym, w tym: – nie może się on opierać na sygnaturach – musi skanować pliki typu: dokumenty Microsoft Office (doc, docx, xls, xlsx), pliki wykonywalne Windows (exe, dll), dokumenty PDF, formaty Mach-O, pliki binarne ELF
6	**W ramach kontroli antyspamowej system musi zapewniać**
6.1	Analizę wiadomości pocztowych w oparciu o technologię Recurrent Pattern Detection.
6.2	Możliwość oznaczania wiadomości e-mail określonych jako spam poprzez dodanie informacji do tematu wiadomości e-mail.
6.3	Blokowanie spamu w oparciu o język, format i zawartość wiadomości e-mail.
6.4	Możliwość usuwania złośliwego oprogramowania z wiadomości e-mail.
7	**W ramach filtrowania zawartości URL system musi zapewniać**
7.1	Filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji.
7.2	Baza filtra URL musi zawierać co najmniej 130 kategorii stron, w tym kategorie istotne z punktu widzenia bezpieczeństwa: Command&Control, Proxy Avoidance, Bot Networks, Malicious sites, Phishing, Spyware.
7.3	Odpytywanie bazy on-line w czasie rzeczywistym.
7.4	Możliwość wysłania modyfikowalnej notyfikacji do użytkownika o tym, dlaczego dostęp do strony www został zablokowany.
7.5	Możliwość uzyskania dostępu do zablokowanych stron www na podstawie grupy użytkownika lub hasła.
7.6	Możliwość określenia różnego rodzaju akcji dla nieskategoryzowanych stron www.
7.7	Możliwość tworzenia białych/czarnych list wyjątków dla filtrowania zawartości URL.

Pkt	Wymagania minimalne
7.8	Możliwość określenia różnego rodzaju akcji dla połączeń do wybranych adresów URL na podstawie reputacji.
7.9	Możliwość filtrowania treści w oparciu o typy MIME.
7.10	Możliwość blokowania plików cookies dla określonych domen.
7.11	Możliwość filtrowania metod żądań i odpowiedzi protokołu HTTP.
7.12	Analizę treści dla protokołu https.
7.13	Wyłączenie inspekcji https dla wybranych kategorii stron www.
8	**W ramach ochrony przed Advanced Persistent Threat system musi zapewniać**
8.1	Oparty na chmurze silnik ochronny, wykorzystujący pełną analizę emulacji systemu w celu identyfikacji cech i zachowania złośliwego oprogramowania.
8.2	Zabezpieczenie przed plikami i załącznikami wiadomości e-mail, które wchodzą do sieci.
8.3	Ochronę nie opartą na sygnaturach.
8.4	Wsparcie dla plików: windows PE, PDF, dokumenty Microsoft Office, dokumenty RTF, pliki .apk, pliki .app, pliki .js w załącznikach e-mail, pliki .hwp, pliki .iso.
8.5	Wsparcie dla plików archiwalnych: gzip, tar, zip, rar, 7z.
8.6	Kategoryzację aktywności APT w oparciu o stopień zagrożenia: wysokie, średnie, niskie, czyste.
9	**W ramach kontroli aplikacyjnej system musi zapewniać**
9.1	Rozpoznawanie aplikacji oraz kategorii aplikacji w oparciu o analizę ruchu a nie przez porty i protokoły.
9.2	Ilość rozpoznawanych aplikacji: nie mniej niż 1000, podzielonych na kategorie.
9.3	W ramach konkretnych aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe, blokować wysyłanie plików).
9.4	Rozpoznawanie aplikacji co najmniej: Tor, CryptoAdmin, Proxy, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online.
10	**Wymagane funkcje VPN systemu**
10.1	Musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz IPSec over GRE.
10.2	W zakresie IPSec site-to-site VPN musi współpracować z rozwiązaniami innych producentów.
10.3	Musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256.
10.4	Musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, certyfikaty.
10.5	Obsługa Dead Peer Detection (DPD).
10.6	Wsparcie dla IKEv1 i IKEv2.
10.7	Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman.
10.8	Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego).

Pkt	Wymagania minimalne
10.9	Musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu.
10.10	Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP, IKEv2.
10.11	Połączenia client-to-site muszą być możliwe z systemów: Windows 10 i 11, MacOS, iOS i Android.
10.12	Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu Windows.
11	**Zarządzanie**
11.1	Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) oraz za pomocą wbudowanego interfejsu www.
11.2	Interfejs www do zarządzania musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.
11.3	Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.
11.4	W ramach dostarczonego rozwiązania musi istnieć możliwość wyświetlenia mapy sieci wewnętrznej zawierającej szczegółowe dane na temat urządzeń (MAC, IP, System operacyjny).
11.5	Elementy systemu bezpieczeństwa pełniące funkcje: Firewall, VPN, Ochrona przed atakami, Kontrola Aplikacji – muszą integrować się z dedykowaną aplikacją lub platformą centralnego zarządzania instalowaną lokalnie.
11.6	Elementy systemu bezpieczeństwa muszą zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania.
11.7	Komunikacja do systemów logowania i raportowania musi być szyfrowana.
11.8	W ramach postępowania koniecznym jest dostarczenie dedykowanej aplikacji lub platformy centralnego zarządzania, logowania, raportowania.
12	**Wymagania dotyczące systemu centralnego zarządzania, logowania, raportowania**
12.1	Musi zapewniać możliwość zarządzania elementami systemu jednocześnie przez wielu administratorów.
12.2	Musi zapewniać zarządzanie w oparciu o role przypisywane dla poszczególnych administratorów.
12.3	Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online
12.4	Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline
12.5	Musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.
12.6	Możliwość rozbudowy (np. w oparciu o licencję) o graficzną konsolę do zarządzania połączeniami VPN. W ramach postępowania muszą zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.
12.7	System musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi.
12.8	Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
12.9	System musi umożliwiać zbieranie i przechowywanie logów oraz generowanie raportów.

Pkt	Wymagania minimalne
12.10	Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.
12.11	Umożliwia przeglądanie logów ruchu w czasie rzeczywistym.
12.12	Rozwiązanie musi udostępniać narzędzie analizy całości ruchu.
12.13	Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa.
12.14	Rozwiązanie musi posiadać zestaw predefiniowanych typów raportów.
12.15	Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie.
12.16	System ma mieć możliwość generowania raportów w formacie PDF oraz opcję eksportowania szczegółowych informacji do pliku CSV.
12.17	System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania ich pocztą e-mail.
12.18	Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.
12.19	System musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów.
12.20	System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.
12.21	Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.
12.22	Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów.
12.23	W ramach licencji, musi zostać dostarczony system XDR dla produktów producenta.
12.24	XDR musi zapewniać rozszerzone możliwości wykrywania poprzez korelację danych z różnych produktów zabezpieczających od producenta, które wskazują na obecność zagrożeń.
12.25	XDR musi być hostowany w chmurze producenta.
12.26	XDR musi zapewniać informację, ze wszystkich produktów producenta z wymaganą licencją.
12.27	XDR musi posiadać tworzenie automatycznych polityk.
12.28	Automatyczna polityka, musi zawierać minimum: zakres ryzyka, typ incydentu, typ urządzenia, zablokowanie adresu IP zagrożenia, usunięcie pliku, wyizolowanie urządzenia, zatrzymanie złośliwego procesu.
13	**Ochrona stacji końcowych**
13.1	Licencja musi obejmować dodatkową ochronę stacji końcowych w formie agentów (minimum 20).
13.2	Rozwiązanie musi pochodzić od producenta rozwiązania.
13.3	Rozwiązanie musi minimum: ochraniać przed oprogramowaniem ransomware, posiadać zaawansowane techniki ochrony przed złośliwym oprogramowaniem, posiadać ochronę antytamperową, aktualizować sygnatury i heurystykę.
14	**Gwarancja**
14.1	Gwarancja na urządzenie musi obejmować wszystkie wymienione powyżej funkcjonalności, które muszą działać (wraz z aktualizacjami sygnatur, baz i oprogramowania) przez okres co najmniej 36 miesięcy od

Pkt	Wymagania minimalne
	dnia odbioru.
14.2	Gwarancja musi być świadczona przez producenta lub autoryzowanego przez producenta partnera serwisowego, na terenie Rzeczypospolitej Polskiej, z przyjmowaniem zgłoszeń i komunikacją w języku polskim.

3.9. Szafa rack – 1 szt.

Obszar wymagań	Wymagania minimalne
Typ urządzenia	Szafa serwerowa stojąca 19" przeznaczona do instalacji urządzeń aktywnych, serwerów, urządzeń zasilania awaryjnego oraz okablowania strukturalnego
Obudowa	Obudowa do montażu w szafie rack zajmująca wysokość 42U Głębokość szafy co najmniej 1000 mm Konstrukcja umożliwiająca montaż urządzeń o głębokości co najmniej 800 mm Nośność statyczna co najmniej 1000 kg Możliwość wprowadzenia okablowania od góry oraz od dołu szafy Zdejmowane panele boczne z możliwością zamknięcia Drzwi przednie perforowane lub wyposażone w elementy wentylacyjne zapewniające prawidłowy przepływ powietrza Drzwi tylne perforowane lub wyposażone w elementy wentylacyjne zapewniające prawidłowy przepływ powietrza Zamki w drzwiach przednich, tylnych oraz panelach bocznych Regulowane pionowe szyny montażowe 19" z oznaczeniem jednostek U
Wentylacja	Szafa musi zapewniać możliwość montażu aktywnych modułów wentylacyjnych Wymagany co najmniej jeden moduł wentylacyjny wyposażony w minimum 4 wentylatory Moduł wentylacyjny musi być przystosowany do montażu w górnej części szafy
Wyposażenie podstawowe	Wymagana co najmniej 1 półka 19" do montażu w szafie, przeznaczona do instalacji urządzeń nieposiadających uchwytów rack (np. urządzenia UTM). Wymagany komplet elementów montażowych umożliwiających instalację w szafie urządzeń będących przedmiotem zamówienia dla danej lokalizacji
Uziemienie	Szafa musi posiadać elementy umożliwiające wykonanie połączeń wyrównawczych i uziemiających
Gwarancja	Gwarancja producenta co najmniej 24 miesiące. Gwarancja musi być świadczona przez producenta lub autoryzowanego przez producenta partnera serwisowego, na terenie Rzeczypospolitej Polskiej, z przyjmowaniem zgłoszeń i komunikacją w języku polskim.

3.10. Punkty dostępowe sieci bezprzewodowej (3 szt.) wraz z kontrolerem (1 szt.) – 1 kpl.

A. Punkt dostępowy sieci bezprzewodowej – 3 szt.

Obszar wymagań	Wymagania minimalne
Typ urządzenia	Punkt dostępowy Wi-Fi do zastosowań wewnętrznych
Standard Wi-Fi	Obsługa standardów IEEE 802.11n/ac/ax/be (Wi-Fi 7) Jednoczesna praca w pasmach 2,4 GHz, 5 GHz oraz 6 GHz Obsługa kanałów o szerokości do 320 MHz w paśmie 6 GHz
Maksymalne prędkości transmisji	Pasmo 2,4 GHz: przepustowość co najmniej 500 Mb/s Pasmo 5 GHz: przepustowość co najmniej 4,8 Gb/s Pasmo 6 GHz: przepustowość co najmniej 4,8 Gb/s
Anteny	Wewnętrzne anteny Zysk anten dla pasma 2,4 GHz co najmniej 4 dBi Zysk anten dla pasma 5 GHz co najmniej 5 dBi Zysk anten dla pasma 6 GHz co najmniej 5 dBi Deklarowany zasięg pokrycia co najmniej 140 m²
Funkcje radiowe	Obsługa technologii MU-MIMO (downlink i uplink) Obsługa OFDMA Obsługa Beamforming Obsługa szybkiego roamingu (802.11r/k/v) Obsługa sieci Mesh Obsługa co najmniej 8 identyfikatorów SSID na radio Obsługa izolacji klientów sieci bezprzewodowej Analiza widma radiowego w czasie rzeczywistym
Wydajność	Obsługa co najmniej 300 jednoczesnych klientów
Porty	Co najmniej 1 port Ethernet 2,5 Gb/s RJ-45
Zasilanie	Zasilanie PoE+ zgodne z IEEE 802.3at
Bezpieczeństwo	Obsługa WPA2-Enterprise oraz WPA3-Enterprise Obsługa uwierzytelniania 802.1X (RADIUS) Obsługa VLAN, w tym dynamicznego przypisywania VLAN przez serwer RADIUS
Zarządzanie	Centralne zarządzanie wszystkimi dostarczanymi punktami dostępowymi z jednej konsoli (kontroler sprzętowy, programowy lub chmurowy). Jeżeli do centralnego zarządzania wymagany jest kontroler sprzętowy lub licencja, Wykonawca dostarczy go w ramach zamówienia. Zarządzanie przez interfejs WWW Możliwość monitorowania parametrów pracy urządzenia oraz klientów Wi-Fi
Montaż	Możliwość montażu sufitowego lub ściennego Zestaw montażowy wymagany w komplecie

Obszar wymagań	Wymagania minimalne
Certyfikaty	CE
Gwarancja	Gwarancja producenta co najmniej 24 miesiące. Gwarancja musi być świadczona przez producenta lub autoryzowanego przez producenta partnera serwisowego, na terenie Rzeczypospolitej Polskiej, z przyjmowaniem zgłoszeń i komunikacją w języku polskim.

B. Kontroler punktów dostępowych – 1 szt.

Obszar wymagań	Wymagania minimalne
Typ urządzenia	Dedykowany kontroler sprzętowy do centralnego zarządzania punktami dostępowymi dostarczanymi w ramach poz. 3.10 A, w pełni kompatybilny z tymi punktami dostępowymi.
Funkcje	Centralna konfiguracja sieci bezprzewodowych (SSID, VLAN, WPA3-Enterprise, uwierzytelnianie 802.1X/RADIUS, sieć gościnna z izolacją klientów). Centralna aktualizacja oprogramowania punktów dostępowych. Monitorowanie stanu punktów dostępowych i podłączonych klientów, statystyki ruchu, analiza wykorzystania kanałów radiowych. Powiadomienia o zdarzeniach (co najmniej e-mail). Automatyczne tworzenie kopii zapasowej konfiguracji. Możliwość zarządzania co najmniej 20 punktami dostępowymi.
Zarządzanie	Zarządzanie przez interfejs WWW (HTTPS) oraz aplikację mobilną. Możliwość bezpiecznego zdalnego dostępu do konsoli przez szyfrowane połączenie. Brak dodatkowych opłat licencyjnych za zarządzanie dostarczanymi punktami dostępowymi.
Sprzęt	Wbudowana pamięć masowa do przechowywania konfiguracji, logów i statystyk. Co najmniej 1 port Ethernet 1 Gb/s RJ-45. Zasilanie PoE (IEEE 802.3af) lub z zasilacza. Wbudowany mechanizm podtrzymania zasilania umożliwiający bezpieczne wyłączenie urządzenia po zaniku zasilania.
Montaż	Możliwość ustawienia na półce w szafie rack 19" lub montażu biurkowego.
Gwarancja	Gwarancja producenta co najmniej 24 miesiące. Gwarancja musi być świadczona przez producenta lub autoryzowanego przez producenta partnera serwisowego, na terenie Rzeczypospolitej Polskiej, z przyjmowaniem zgłoszeń i komunikacją w języku polskim.

3.11. Licencje serwerowego systemu operacyjnego oraz licencje dostępowe (CAL) – 1 kpl.

Obszar wymagań	Wymagania minimalne
Zakres licencji	Wymagane dostarczenie licencji na serwerowy system operacyjny dla każdego z 3

Obszar wymagań	Wymagania minimalne
	serwerów dostarczanych w ramach poz. 3.1, przy czym licencja ta: 1. musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta i pozwalała na legalne używanie na oferowanym serwerze, 2. musi obejmować najnowszą wersję systemu dostępną na dzień składania oferty, 3. musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym oferowanego serwera oraz umożliwiać uruchomienie na każdym z serwerów co najmniej dwóch maszyn wirtualnych (instancji wirtualnych) tego serwerowego systemu operacyjnego; licencja musi obejmować wszystkie rdzenie fizyczne procesorów zainstalowanych w serwerze, 4. musi obejmować co najmniej 40 licencji dostępowych użytkownika (User CAL) do oferowanego serwerowego systemu operacyjnego, jeśli takie licencje są wymagane przez producenta do dostępu do oprogramowania serwerowego.
Wymagania minimalne systemu	Serwerowy system operacyjny musi spełniać nw. wymagania minimalne: 1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 4) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 6) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 7) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 8) Wbudowane wsparcie instalacji i pracy na wolumenach, które: a) pozwalają na zmianę rozmiaru w czasie pracy systemu, b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d) umożliwiają zdefiniowanie list kontroli dostępu (ACL). 9) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 10) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 11) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET

Obszar wymagań	Wymagania minimalne
	12) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 13) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 14) Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 15) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 16) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 17) Mechanizmy logowania w oparciu o: a) login i hasło, b) karty z certyfikatami (smartcard), c) wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 18) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. 19) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 20) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 21) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 22) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 23) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 24) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: i) Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii) Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii) Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. iv) Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 10 i wyższych.

Obszar wymagań	Wymagania minimalne
	c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej. e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: i) dystrybucję certyfikatów poprzez http, ii) konsolidację CA dla wielu lasów domeny, iii) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, iv) automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f) Szyfrowanie plików i folderów. g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i) Serwis udostępniania stron WWW. j) Wsparcie dla protokołu IP w wersji 6 (IPv6), k) Wsparcie dla algorytmów Suite B (RFC 4869), l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: i) Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii) Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii) Obsługi 4-KB sektorów dysków iv) Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra v) Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi) Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 25) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 26) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 27) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 28) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie)

Obszar wymagań	Wymagania minimalne
	administracji przez skrypty. 29) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 30) Zorganizowany system szkoleń i dostępne materiały edukacyjne w języku polskim.
Nośniki i kompatybilność	Wymagane dostarczenie nośników instalacyjnych umożliwiających instalację zarówno najnowszej, jak i poprzedniej wersji systemu. Do oferty należy załączyć potwierdzenie kompatybilności serwera z oferowanym systemem operacyjnym (wydruk ze strony producenta systemu operacyjnego, dopuszcza się wydruk w języku angielskim).

3.12. Wdrożenie systemu klasy SIEM/XDR – 1 usł.

A. Wymagania dotyczące systemu

Obszar wymagań	Wymagania minimalne
Przeznaczenie	System klasy SIEM/XDR służący do centralnego zbierania, normalizacji, korelacji, analizy i przechowywania zdarzeń z systemów IT i OT Zamawiającego, wykrywania incydentów bezpieczeństwa oraz raportowania na potrzeby obowiązków wynikających z przepisów o krajowym systemie cyberbezpieczeństwa i Krajowych Ram Interoperacyjności. Dopuszcza się rozwiązanie zbudowane z komponentów o otwartym kodzie źródłowym, pod warunkiem że tworzą spójne, udokumentowane i utrzymywane środowisko.
Licencjonowanie	Licencja nieograniczona czasowo albo odnawialna nieodpłatnie, również po zakończeniu okresu wsparcia. Licencja nie może ograniczać liczby źródeł logów, liczby agentów, wolumenu przetwarzanych danych ani liczby kont użytkowników. Dostęp do aktualizacji oprogramowania oraz bazy reguł detekcyjnych przez okres co najmniej 12 miesięcy od odbioru. Wykonawca wskaże w ofercie nazwy, wersje i typy licencji wszystkich komponentów.
Architektura i wydajność	Możliwość uruchomienia systemu na maszynach wirtualnych w klastrze HA Zamawiającego (pkt W.2), w tym w konfiguracji jednowęzłowej, z możliwością późniejszej rozbudowy o kolejne węzły. Obsługa co najmniej 100 agentów oraz źródeł syslog wskazanych w opisie wdrożenia.
Retencja danych	Alerty oraz zdarzenia objęte regułami detekcyjnymi dostępne w warstwie wyszukiwania bezpośredniego przez co najmniej 90 dni. Zdarzenia surowe przechowywane w skompresowanym archiwum przez co najmniej 24 miesiące, z możliwością ich ponownego wczytania do wyszukiwania. Archiwum składowane na zasobie zabezpieczonym przed modyfikacją i usunięciem (np. migawki niezmienialne, WORM lub kopia poza klastrem).
Szyfrowanie	Komunikacja agentów z serwerem szyfrowana (TLS co najmniej 1.2 lub szyfr symetryczny z kluczem co najmniej 256 bitów), z indywidualnym kluczem dla każdego agenta i możliwością odwołania klucza pojedynczego agenta. Dostęp do interfejsu użytkownika oraz komunikacja pomiędzy komponentami

Obszar wymagań	Wymagania minimalne
	szyfrowane protokołem TLS w wersji co najmniej 1.2.
Zbieranie i przetwarzanie danych	Zbieranie zdarzeń przez agentów (co najmniej Windows i Linux) oraz bezagentowo – co najmniej przez syslog. Obsługa formatów: syslog, pliki tekstowe, dziennik zdarzeń Windows (w tym kanały zdarzeń), JSON. Predefiniowany zestaw parserów (dekoderów) dla popularnych systemów operacyjnych i aplikacji. Tworzenie i edycja własnych parserów w oparciu o wyrażenia regularne, z możliwością testu na przykładowym zdarzeniu. Normalizacja formatów daty i czasu, obsługa zdarzeń jedno- i wielowierszowych. Przechowywanie i prezentacja zdarzenia w postaci surowej obok postaci znormalizowanej. Przeszukiwanie danych z filtrowaniem po sparsowanych polach. Geolokalizacja zdarzeń na podstawie adresów IP. Możliwość importu wskaźników kompromitacji (IoC) do list referencyjnych i wykorzystania ich w regułach.
Detekcja i alarmowanie	Korelacja zdarzeń w czasie zbliżonym do rzeczywistego. Aktualizowana przez producenta baza reguł detekcyjnych obejmująca co najmniej: systemy Windows i Linux, usługi katalogowe, dostęp zdalny, integralność plików i ocenę konfiguracji, z mapowaniem na taktyki i techniki MITRE ATT&CK. Tworzenie własnych reguł oraz modyfikacja istniejących z poziomu interfejsu oraz przez interfejs programistyczny (API). Reguły umożliwiające wykrywanie co najmniej: określonej treści lub wartości pola, wartości z listy referencyjnej, zdarzeń o określonej częstotliwości w oknie czasowym oraz sekwencji zdarzeń. Wykrywanie zaniku komunikacji z agentem. Poziom istotności każdego alarmu, z możliwością zmiany na poziomie reguły. Powiadamianie o alarmach co najmniej pocztą elektroniczną. Przeglądanie alarmów w układzie MITRE ATT&CK.
Reagowanie	Możliwość automatycznego i ręcznego wykonania akcji reagowania na systemie monitorowanym, co najmniej: zablokowanie adresu IP oraz zablokowanie konta użytkownika. Każde wykonanie akcji musi być rejestrowane.
Bezpieczeństwo systemów końcowych	Badanie integralności plików (zmiany zawartości, uprawnień i atrybutów, sumy kontrolne co najmniej SHA-256). Ocena zgodności konfiguracji systemów z uznanymi zaleceniami hardeningu (np. CIS), z raportem odchyleń i rekomendacjami. Wykrywanie oprogramowania ukrywającego swoją obecność (rootkit). Identyfikacja podatności systemów operacyjnych i oprogramowania na systemach z agentem, wraz z inwentaryzacją oprogramowania. Gotowe zestawy reguł i pulpitów dla wymagań ochrony danych osobowych i standardów bezpieczeństwa informacji.
Dostęp i rozliczalność	Interfejs WWW w języku polskim lub angielskim.

Obszar wymagań	Wymagania minimalne
	Integracja uwierzytelniania z usługą katalogową Active Directory (LDAP). Zarządzanie użytkownikami i rolami z uprawnieniami co najmniej do odczytu i pełnymi. Zarządzanie czasem wygasania sesji. Rejestrowanie audytu aktywności użytkowników (logowania, zmiany konfiguracji i uprawnień).
Raportowanie i wizualizacja	Wizualizacje w postaci list zdarzeń, tabel i wykresów oraz możliwość tworzenia własnych pulpitów. Generowanie raportów do formatu PDF – ręcznie oraz cyklicznie, z dystrybucją pocztą elektroniczną. Eksport danych o zdarzeniach do formatu CSV.
Dokumentacja producenta	Dokumentacja techniczna dostępna w języku polskim lub angielskim.

B. Zakres wdrożenia

1. Analiza przedwdrożeniowa: inwentaryzacja źródeł danych, projekt techniczny wdrożenia wraz z harmonogramem oraz lista proponowanych reguł detekcyjnych i pulpitów – do akceptacji Zamawiającego.
2. Instalacja systemu na maszynie wirtualnej (lub maszynach wirtualnych) w klastrze HA (pkt W.2), konfiguracja szyfrowania komunikacji, integracji z Active Directory (poz. 3.13), ról i uprawnień, retencji oraz archiwum zdarzeń na zasobie z ochroną przed modyfikacją (macierz kopii zapasowych z poz. 3.3 A lub serwer NAS z poz. 3.7).
3. Instalacja i konfiguracja agentów na:
   1) serwerach Windows (w tym kontrolerach domeny) i maszynach wirtualnych Linux,
   2) hostach platformy wirtualizacji (poz. 3.1) oraz serwerze systemu kopii zapasowych,
   3) stacjach roboczych wszystkich użytkowników (31 użytkowników) w siedzibie Zamawiającego,
   4) stacjach roboczych OT oraz komputerach biurowych obsługi obiektów w lokalizacjach OT (stacje uzdatniania wody, oczyszczalnia ścieków) – z konfiguracją nieingerującą w pracę systemów sterowania i w uzgodnionych oknach serwisowych,
   5) wraz z konfiguracją rozszerzonego rejestrowania zdarzeń Windows (polityka audytu, rejestrowanie poleceń PowerShell) ograniczającą nadmiarowy wolumen danych.
4. Podłączenie źródeł syslog:
   1) urządzeń UTM (poz. 3.8 i 4.1) – ruch blokowany, zdarzenia IPS, sesje VPN, dostęp administracyjny, zmiany polityk,
   2) przełączników sieciowych (poz. 3.4 i 4.2) – dostęp administracyjny i zmiany konfiguracji,
   3) serwera NAS (poz. 3.7) i macierzy dyskowych (poz. 3.2 i 3.3 A) – uwierzytelnienia, zmiany konfiguracji, zdarzenia sprzętowe,
   4) kontrolerów zarządzania serwerów (BMC) – uwierzytelnienia i zdarzenia sprzętowe.

5) Dla źródeł, dla których system nie posiada predefiniowanych parserów, Wykonawca przygotuje parsery oraz co najmniej podstawowe reguły detekcyjne.

5. Konfiguracja reguł i powiadomień, w tym reguł o wysokim poziomie istotności dla co najmniej:
   1) nieudanych prób logowania do kont uprzywilejowanych, kontrolerów BMC i interfejsów zarządzania macierzy,
   2) usunięcia zadań lub zbiorów kopii zapasowych oraz zmian polityk retencji,
   3) masowej modyfikacji lub szyfrowania plików na udziałach sieciowych,
   4) zaniku komunikacji z agentem lub źródłem zdarzeń.
6. Uruchomienie modułów badania integralności plików, oceny konfiguracji i identyfikacji podatności oraz konfiguracja akcji reagowania (blokada adresu IP, blokada konta) – w trybie uzgodnionym z Zamawiającym.
7. Przygotowanie pulpitu bezpieczeństwa oraz raportu cyklicznego (miesięcznego) w formacie PDF wysyłanego pocztą elektroniczną.
8. Konfiguracja kopii zapasowej konfiguracji systemu (reguły, parsery, ustawienia).
9. Testy odbiorowe obejmujące co najmniej: napływ zdarzeń z każdego podłączonego źródła, zadziałanie wybranych reguł i powiadomień, wykonanie i wycofanie akcji reagowania na systemie testowym, ponowne wczytanie danych z archiwum oraz odtworzenie konfiguracji z kopii zapasowej.

3.13. Wdrożenie domeny Active Directory – 1 usł.

Przedmiotem usługi jest wdrożenie usług katalogowych Active Directory dla wszystkich pracowników Zamawiającego korzystających z systemów IT i OT (ok. 31 użytkowników), z wykorzystaniem serwerowego systemu operacyjnego z poz. 3.11 uruchomionego w klastrze HA (pkt W.2).

1. Instalacja i konfiguracja usług katalogowych:
   1) instalacja roli Active Directory Domain Services (AD DS) na dwóch maszynach wirtualnych w klastrze HA,
   2) promocja serwerów do roli kontrolerów domeny – Domain Controller 1 i Domain Controller 2, z replikacją pomiędzy nimi,
   3) konfiguracja usług DNS zintegrowanych z Active Directory oraz – w uzgodnieniu z Zamawiającym – usługi DHCP,
   4) konfiguracja synchronizacji czasu w domenie,
   5) włączenie kosza Active Directory (AD Recycle Bin) oraz konfiguracja kopii zapasowych kontrolerów domeny w systemie z poz. 3.3.
2. Struktura domeny i konta:
   1) utworzenie jednostek organizacyjnych (OU) dla użytkowników, grup, komputerów i serwerów, z uwzględnieniem podziału na obszar IT i obszar OT (lokalizacje SUW i oczyszczalnia ścieków),

2) utworzenie kont użytkowników – ok. 35 kont (31 użytkowników oraz konta techniczne i administracyjne),
3) utworzenie grup zabezpieczeń zgodnie z uzgodnioną z Zamawiającym strukturą organizacyjną,
4) utworzenie odrębnych kont administracyjnych dla administratorów oraz ograniczenie członkostwa w grupach uprzywilejowanych.

3. Zasoby i uprawnienia:
1) utworzenie folderów udostępnionych,
2) nadanie uprawnień do folderów po wcześniejszym uzgodnieniu z Zamawiającym macierzy uprawnień,
3) instalacja drukarek – dostosowanie obecnie użytkowanych drukarek do współpracy ze środowiskiem domenowym.

4. Polityki zabezpieczeń:
1) opracowanie i konfiguracja polityk zabezpieczeń (GPO) – ok. 20 polityk, obejmujących co najmniej: politykę haseł i blokady kont, politykę inspekcji (audytu) zdarzeń, ustawienia zapory systemowej, ograniczenia nośników wymiennych, blokadę ekranu, zarządzanie lokalnymi kontami administratorów, ustawienia aktualizacji systemów oraz mapowanie dysków i drukarek,
2) przygotowanie odrębnych polityk dla stacji roboczych OT, uwzględniających wymagania ciągłości pracy systemów sterowania.

5. Przyłączenie stacji i migracja danych:
1) podłączenie komputerów do utworzonej domeny – proces wykonywany etapowo, przy wsparciu pracowników Zamawiającego (podłączenie nowych urządzeń oraz zmiana konfiguracji obecnie użytkowanych w celu dołączenia do domeny), w tym stacji roboczych w lokalizacjach OT w uzgodnionych oknach serwisowych,
2) migracja profili użytkowników i danych do nowego środowiska.

6. Integracja z wdrażanymi systemami:
1) integracja domeny z urządzeniami UTM (poz. 3.8 i 4.1) w zakresie identyfikacji i uwierzytelniania użytkowników,
2) integracja z systemem SIEM/XDR (poz. 3.12) w zakresie przekazywania dzienników zdarzeń kontrolerów domeny,
3) integracja z serwerem NAS (poz. 3.7) i systemem kopii zapasowych (poz. 3.3).

7. Wykonawca przeprowadzi testy poprawności działania domeny (logowanie, replikacja, działanie polityk, dostęp do zasobów).

3.14. Wdrożenie oprogramowania do monitorowania infrastruktury informatycznej – 1 usł.

A. Wymagania dotyczące systemu

Obszar wymagań	Wymagania minimalne
Przeznaczenie	System do monitorowania dostępności, wydajności i stanu technicznego urządzeń, systemów i usług w obszarze IT i OT Zamawiającego, z alarmowaniem o awariach i przekroczeniach progów. Dopuszcza się rozwiązanie o otwartym kodzie źródłowym.
Licencjonowanie	Licencja nieograniczona czasowo albo rozwiązanie open source, bez ograniczeń liczby monitorowanych urządzeń, parametrów i kont użytkowników. Dostęp do aktualizacji oprogramowania bez dodatkowych opłat.
Architektura	Możliwość uruchomienia na maszynie wirtualnej w klastrze HA Zamawiającego (pkt W.2), z wykorzystaniem bazy danych o otwartym kodzie źródłowym. Możliwość zbierania danych z lokalizacji zdalnych za pośrednictwem komponentu pośredniczącego (proxy) lub przez szyfrowane tunele VPN. Udokumentowany interfejs programistyczny (API).
Metody zbierania danych	Agenci dla systemów Windows i Linux. SNMP v1/v2c/v3 oraz odbiór pułapek SNMP. IPMI i/lub Redfish dla kontrolerów zarządzania serwerów. ICMP (ping), sprawdzanie portów i usług sieciowych (TCP, HTTP/HTTPS, DNS), zapytania do API urządzeń i aplikacji.
Zakres monitorowania	Dostępność urządzeń i usług. Wykorzystanie procesora, pamięci, przestrzeni dyskowej i interfejsów sieciowych (ruch, błędy, stan portów). Stan podzespołów sprzętowych: dysków, zasilaczy, wentylatorów, temperatur. Stan zasilaczy UPS: praca na baterii, stan i poziom naładowania baterii, obciążenie. Stan usług i procesów systemowych oraz termin ważności certyfikatów SSL/TLS.
Szablony i wykrywanie	Gotowe szablony monitorowania dla popularnych systemów operacyjnych, urządzeń sieciowych, serwerów i platform wirtualizacji. Możliwość tworzenia i modyfikacji własnych szablonów. Automatyczne wykrywanie urządzeń w sieci oraz ich elementów (interfejsów, dysków, systemów plików).
Alarmowanie	Definiowanie progów i poziomów istotności alarmów. Definiowanie zależności pomiędzy urządzeniami (np. wstrzymanie alarmów dla urządzeń za niedostępnym urządzeniem sieciowym). Powiadomienia co najmniej pocztą elektroniczną, z możliwością eskalacji. Potwierdzanie alarmów przez operatora oraz definiowanie okien serwisowych.
Wizualizacja i raporty	Pulpity, wykresy historyczne oraz mapy sieci z prezentacją stanu urządzeń. Raporty dostępności (SLA). Cykliczne raporty w formacie PDF wysyłane pocztą elektroniczną.

Obszar wymagań	Wymagania minimalne
Retencja danych	Przechowywanie danych szczegółowych przez co najmniej 90 dni oraz danych zagregowanych (trendów) przez co najmniej 12 miesięcy.
Bezpieczeństwo i dostęp	Interfejs WWW w języku polskim lub angielskim, dostępny przez HTTPS. Szyfrowanie komunikacji pomiędzy agentami a serwerem (TLS lub klucz współdzielony PSK). Uwierzytelnianie użytkowników z wykorzystaniem Active Directory (LDAP) oraz uwierzytelnianie dwuskładnikowe. Role i uprawnienia użytkowników z ograniczeniem dostępu do wybranych grup urządzeń. Rejestrowanie działań użytkowników (dziennik audytu).
Dokumentacja producenta	Dokumentacja techniczna dostępna w języku polskim lub angielskim.

B. Zakres wdrożenia

1. Analiza przedwdrożeniowa: wykaz monitorowanych urządzeń i usług, progi alarmowe, lista odbiorców powiadomień – do akceptacji Zamawiającego.
2. Instalacja systemu na maszynie wirtualnej w klastrze HA (pkt W.2), konfiguracja bazy danych, dostępu HTTPS, integracji z Active Directory (poz. 3.13), ról i uprawnień oraz kopii zapasowej systemu w systemie kopii zapasowych (poz. 3.3).
3. Objęcie monitorowaniem co najmniej:
   1) serwerów klastra HA (poz. 3.1) – system operacyjny platformy wirtualizacji, maszyny wirtualne oraz stan sprzętu przez kontrolery zarządzania (BMC),
   2) maszyn wirtualnych Windows i Linux (w tym kontrolerów domeny, systemu SIEM) – z wykorzystaniem agentów,
   3) macierzy dyskowych (poz. 3.2 i 3.3 A), serwera NAS (poz. 3.7) i biblioteki taśmowej (poz. 3.5),
   4) systemu kopii zapasowych (poz. 3.3 B) – w zakresie stanu zadań kopii zapasowych i zajętości repozytoriów,
   5) przełączników sieciowych (poz. 3.4 i 4.2), urządzeń UTM (poz. 3.8 i 4.1) oraz punktów dostępowych i kontrolera (poz. 3.10),
   6) zasilaczy UPS (poz. 3.6 i 4.4),
   7) łączy i tuneli VPN do lokalizacji OT oraz dostępności urządzeń w lokalizacjach OT.
4. Konfiguracja szablonów, progów alarmowych, zależności pomiędzy urządzeniami oraz mapy sieci obejmującej siedzibę Zamawiającego i lokalizacje OT.
5. Konfiguracja powiadomień e-mail, w tym co najmniej dla zdarzeń:
   1) niedostępności urządzenia, usługi lub łącza,
   2) awarii dysku, zasilacza lub wentylatora,
   3) przejścia zasilacza UPS na pracę bateryjną i niskiego poziomu naładowania baterii,

4) przekroczenia progów zajętości przestrzeni dyskowej,

5) nieudanego zadania kopii zapasowej,

6) zbliżającego się terminu wygaśnięcia certyfikatów.

6. Przygotowanie pulpitu stanu infrastruktury oraz miesięcznego raportu dostępności w formacie PDF wysyłanego pocztą elektroniczną.
7. Testy odbiorowe obejmujące co najmniej: zbieranie danych ze wszystkich monitorowanych urządzeń, wyzwolenie wybranych alarmów (np. odłączenie łącza, symulacja pracy UPS na baterii) i doręczenie powiadomień.

Obszar techniczny OT

4.1. Urządzenie UTM dla sieci OT – 3 szt.

Urządzenia muszą współpracować z urządzeniem UTM dostarczanym w ramach poz. 3.8 w zakresie zestawiania tuneli IPSec VPN oraz funkcji SD-WAN, a także umożliwiać centralne zarządzanie i monitorowanie wszystkich urządzeń UTM z jednej konsoli.

Pkt	Wymagania minimalne
1	**Funkcje modułu Firewall**
1.1	Musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2).
1.2	Możliwość uruchomienia w formie klastra wysokiej dostępności (HA) – co najmniej Active-Passive.
1.3	Musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP) lub jako bridge (transparent mode).
1.4	Musi obsługiwać protokoły dynamicznego routingu: RIP v1/v2, OSPF i BGP4.
1.5	Musi obsługiwać Multicast routing.
1.6	Musi obsługiwać Policy Based routing.
1.7	Musi umożliwiać znakowanie QoS w oparciu o ToS (Type of Service) lub DSCP (Differentiated Service Code Point) w ramach zapewnienia jakości usług.
1.8	Musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPPoE) na zewnętrznym interfejsie.
1.9	Musi obsługiwać DHCPv6 na zewnętrznym interfejsie.
1.10	Musi obsługiwać funkcję agregacji linków (802.3ad dynamic, static, active/backup).
1.11	Musi obsługiwać Dynamic DNS.
1.12	Musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1.
1.13	Musi obsługiwać translację portów: PAT.
1.14	Musi obsługiwać IPSec NAT traversal.
1.15	Musi obsługiwać mechanizm Policy Based NAT.
1.16	Musi obsługiwać VLAN 802.1Q.

Pkt	Wymagania minimalne
1.17	Musi zapewniać funkcję serwera DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.
1.18	Musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP.
1.19	Musi mieć możliwość obsługi zapasowego łącza typu 4G LTE/5G poprzez podłączenie zewnętrznego modemu USB.
1.20	Musi mieć możliwość automatycznego przełączania ruchu pomiędzy interfejsami zewnętrznymi w przypadku awarii jednego z nich.
1.21	Musi zapewniać funkcję równoważenia obciążenia pomiędzy interfejsami zewnętrznymi.
1.22	Musi zapewniać funkcjonalność SD-WAN w ramach automatycznej dystrybucji ruchu na podstawie jakości łącza, minimum dla wartości: utrata pakietów, opóźnienie, jitter.
1.23	Musi zapewniać funkcję równoważenia obciążenia w ramach połączeń do wewnętrznych serwerów.
1.24	Musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.
1.25	Musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: Active Directory, LDAP, RADIUS, SecurID, VASCO oraz wewnętrznej bazy użytkowników.
1.26	Musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z Active Directory.
1.27	Musi posiadać co najmniej dwie metody transparentnej autoryzacji nie wymagające instalacji dedykowanego agenta na stacjach roboczych użytkowników.
1.28	Musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z usług terminalowych Microsoft oraz Citrix.
1.29	Nie może ograniczać ilości urządzeń, adresów IP czy użytkowników sieci wewnętrznej.
1.30	Musi dostarczać mechanizm identyfikacji urządzeń w sieci w tym co najmniej identyfikację systemu operacyjnego, otwartych portów i usług.
1.31	Musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.
1.32	Musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.
1.33	Musi posiadać mechanizmy rozpoznawania anomalii w protokołach sieciowych – dla najpopularniejszych protokołów.
1.34	Musi umożliwiać sterowanie przepustowością w oparciu o politykę zapory sieciowej oraz wybraną aplikację.
1.35	Musi dostarczać mechanizmów limitowania dostępu do sieci użytkownikom w oparciu o quoty czasowe lub transferu danych, co najmniej dla komunikacji http.
1.36	Musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMTPS, POP3S, IMAPS, H.323, SIP.
1.37	Musi zapewniać funkcjonalność Content Routing w ramach protokołu HTTP/HTTPS na podstawie co najmniej nagłówka hosta HTTP i żądania HTTP.

Pkt	Wymagania minimalne
1.38	Musi zapewniać funkcjonalność TLS/SSL Offloading dla protokołu HTTPS w ramach połączeń do wewnętrznych serwerów.
1.39	Musi ochraniać przed minimum: atakami DoS, pofragmentowanymi i zniekształconymi pakietami, zagrożeniami mieszanymi (Blended threats).
1.40	Musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site.
1.41	VPN site-to-site musi wspierać minimum: IKEv2, IPSec, tunele oparte na politykach i routingu, TLS hub and spoke.
1.42	VPN client-to-site musi wspierać minimum: IKEv2, IPSec, L2TP, TLS
2	**Specyfikacja UTM**
2.1	Firewall musi zapewnić obsługę na poziomie minimalnym: – 2.28 Gbps dla pracy w trybie firewall dla pakietów UDP 1518, – 510 Mbps dla pracy w trybie full scan (włączone mechanizmy bezpieczeństwa takie jak: AV, IPS), – 1.44 Gbps dla pracy w trybie VPN dla pakietów UDP 1518, – 725 Mbps dla modułu IPS w trybie full scan, – 880 Mbps dla skanowań antywirusa – 270 Mbps dla protokołu HTTPS z włączonym IPS oraz pełnym skanowaniem
2.2	Nielimitowana sprzętowo ilość obsługi VLAN
2.3	Firewall musi obsługiwać 3 850 000 jednoczesnych połączeń TCP oraz przyjmować nowe połączenia z wydajnością minimalną 26 500 połączeń na sekundę.
2.4	Minimalna ilość portów 10/100/1000 BaseT: 4
2.5	Minimalna ilość portów 2.5 GbE: 1
2.6	Wsparcie połączeń VPN site-to-site lub client-to-site dla minimum 10 użytkowników.
2.7	Sieć bezprzewodowa (interfejs bezprzewodowy musi być wyłączony w konfiguracji produkcyjnej): a. Urządzenie musi wspierać Wi-Fi 7 b. Urządzenie musi posiadać minimum 3 anteny zewnętrzne SMA o częstotliwościach: – 2x 2,4 GHz i 5 GHz – 1x 5 GHz c. Bezprzewodowe radia muszą spełniać poniższe parametry: d. Radio 1 (2,4 GHz) e. Wi-Fi 7 2x2 802.11be/ax/b/g/n f. Prędkość transmisji danych do 688 Mb/s g. Radio 2 (5 GHz) h. Wi-Fi 7 3x3 802.11be/ax/ac/a/n i. Prędkość transmisji danych do 4323 Mb/s
3	**Dostarczony system bezpieczeństwa (UTM) musi zapewniać**
3.1	Ochronę z wykorzystaniem mechanizmów IPS.
3.2	Ochronę antywirusową opartą na sygnaturach.
3.3	Ochronę przed niechcianą pocztą.

Pkt	Wymagania minimalne
3.4	Kontrolę wykorzystywanych aplikacji.
3.5	Możliwość filtrowania URL.
3.6	Ochronę przed Advanced Persistent Threat.
3.7	Ochronę antywirusową opartą na sztucznej inteligencji i uczenia maszynowego.
4	**W ramach ochrony przed atakami system musi zapewniać**
4.1	Automatyczną aktualizację bazy sygnatur IPS. Powinna ona zawierać co najmniej 8000 definicji sygnatur.
4.2	Automatyczne blokowanie znanych źródeł ataków.
4.3	Ochronę przed lukami w zabezpieczeniach w aplikacjach, bazach danych, systemach operacyjnych.
4.4	Mechanizmy ochrony przed atakami typu DoS i DDoS co najmniej (IPsec Flood, IKE Flood, ICMP Flood, Syn Flood, UDP Flood, IP Scan, Ilość połączeń, Port Scan, IP Source Route, ARP/IP Spoofing).
4.5	Mechanizmy blokowania przed atakami typu: SQL Injection, Cross-Site-Scripting, Buffer Overflow, Remote File Inclusions.
4.6	Mechanizm, który pozwoli generować alarmy – dla wskazanego poziomu nasilenia ataku.
5	**W ramach kontroli antywirusowej system musi zapewniać**
5.1	Możliwość rozbudowy (np. w oparciu o licencję) o możliwość uruchomienia co najmniej 2 skanerów antywirusowych opartych na analizie sygnaturowej oraz bezsygnaturowej lokalnie
5.2	Automatyczną aktualizację baz sygnatur, nie rzadziej niż co 12 godzin.
5.3	Możliwość skanowania plików o rozmiarze co najmniej 10MB.
5.4	Możliwość zdefiniowania rozmiaru skanowanego pliku.
5.5	Możliwość skanowania plików w wielokrotnie skompresowanych archiwach.
5.6	Możliwość tworzenia wyjątków (biała lista) dla określonych adresów URL, typów plików, sygnatury pliku MD5.
5.7	Wykrywanie i blokowanie złośliwego oprogramowania typu: Virus, Trojan, Worms, Spyware, Rogueware, Malware.
5.8	Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS.
5.9	Minimum jeden silnik ochronny oparty na sztucznej inteligencji i uczeniu maszynowym, w tym: – nie może się on opierać na sygnaturach – musi skanować pliki typu: dokumenty Microsoft Office (doc, docx, xls, xlsx), pliki wykonywalne Windows (exe, dll), dokumenty PDF, formaty Mach-O, pliki binarne ELF
6	**W ramach kontroli antyspamowej system musi zapewniać**
6.1	Analizę wiadomości pocztowych w oparciu o technologię Recurrent Pattern Detection.
6.2	Możliwość oznaczania wiadomości e-mail określonych jako spam poprzez dodanie informacji do tematu wiadomości e-mail.

Pkt	Wymagania minimalne
6.3	Blokowanie spamu w oparciu o język, format i zawartość wiadomości e-mail.
6.4	Możliwość usuwania złośliwego oprogramowania z wiadomości e-mail.
7	**W ramach filtrowania zawartości URL system musi zapewniać**
7.1	Filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji.
7.2	Baza filtra URL musi zawierać co najmniej 130 kategorii stron, w tym kategorie istotne z punktu widzenia bezpieczeństwa: Command&Control, Proxy Avoidance, Bot Networks, Malicious sites, Phishing, Spyware.
7.3	Odpytywanie bazy on-line w czasie rzeczywistym.
7.4	Możliwość wysłania modyfikowalnej notyfikacji do użytkownika o tym, dlaczego dostęp do strony www został zablokowany.
7.5	Możliwość uzyskania dostępu do zablokowanych stron www na podstawie grupy użytkownika lub hasła.
7.6	Możliwość określenia różnego rodzaju akcji dla nieskategoryzowanych stron www.
7.7	Możliwość tworzenia białych/czarnych list wyjątków dla filtrowania zawartości URL.
7.8	Możliwość określenia różnego rodzaju akcji dla połączeń do wybranych adresów URL na podstawie reputacji.
7.9	Możliwość filtrowania treści w oparciu o typy MIME.
7.10	Możliwość blokowania plików cookies dla określonych domen.
7.11	Możliwość filtrowania metod żądań i odpowiedzi protokołu HTTP.
7.12	Analizę treści dla protokołu https.
7.13	Wyłączenie inspekcji https dla wybranych kategorii stron www.
8	**W ramach ochrony przed Advanced Persistent Threat system musi zapewniać**
8.1	Oparty na chmurze silnik ochronny, wykorzystujący pełną analizę emulacji systemu w celu identyfikacji cech i zachowania złośliwego oprogramowania.
8.2	Zabezpieczenie przed plikami i załącznikami wiadomości e-mail, które wchodzą do sieci.
8.3	Ochronę nie opartą na sygnaturach.
8.4	Wsparcie dla plików: windows PE, PDF, dokumenty Microsoft Office, dokumenty RTF, pliki .apk, pliki .app, pliki .js w załącznikach e-mail, pliki .hwp, pliki .iso.
8.5	Wsparcie dla plików archiwalnych: gzip, tar, zip, rar, 7z.
8.6	Kategoryzację aktywności APT w oparciu o stopień zagrożenia: wysokie, średnie, niskie, czyste.
9	**W ramach kontroli aplikacyjnej system musi zapewniać**
9.1	Rozpoznawanie aplikacji oraz kategorii aplikacji w oparciu o analizę ruchu a nie przez porty i protokoły.
9.2	Ilość rozpoznawanych aplikacji: nie mniej niż 1000, podzielonych na kategorie.
9.3	W ramach konkretnych aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w

Pkt	Wymagania minimalne
	komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe, blokować wysyłanie plików).
9.4	Rozpoznawanie aplikacji co najmniej: Tor, CryptoAdmin, Proxy, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online.
10	**Wymagane funkcje VPN systemu**
10.1	Musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz IPSec over GRE.
10.2	W zakresie IPSec site-to-site VPN musi współpracować z rozwiązaniami innych producentów.
10.3	Musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256.
10.4	Musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, certyfikaty.
10.5	Obsługa Dead Peer Detection (DPD).
10.6	Wsparcie dla IKEv1 i IKEv2.
10.7	Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman.
10.8	Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego).
10.9	Musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu.
10.10	Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP, IKEv2.
10.11	Połączenia client-to-site muszą być możliwe z systemów: Windows 10 i 11, MacOS, iOS i Android.
10.12	Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu Windows.
11	**Zarządzanie**
11.1	Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) oraz za pomocą wbudowanego interfejsu www.
11.2	Interfejs www do zarządzania musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.
11.3	Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.
11.4	W ramach dostarczonego rozwiązania musi istnieć możliwość wyświetlenia mapy sieci wewnętrznej zawierającej szczegółowe dane na temat urządzeń (MAC, IP, System operacyjny).
11.5	Elementy systemu bezpieczeństwa pełniące funkcje: Firewall, VPN, Ochrona przed atakami, Kontrola Aplikacji – muszą integrować się z dedykowaną aplikacją lub platformą centralnego zarządzania instalowaną lokalnie.
11.6	Elementy systemu bezpieczeństwa muszą zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania.
11.7	Komunikacja do systemów logowania i raportowania musi być szyfrowana.
11.8	W ramach postępowania koniecznym jest dostarczenie dedykowanej aplikacji lub platformy centralnego

Pkt	Wymagania minimalne
	zarządzania, logowania, raportowania.
12	**Wymagania dotyczące systemu centralnego zarządzania, logowania, raportowania**
12.1	Musi zapewniać możliwość zarządzania elementami systemu jednocześnie przez wielu administratorów.
12.2	Musi zapewniać zarządzanie w oparciu o role przypisywane dla poszczególnych administratorów.
12.3	Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online
12.4	Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline
12.5	Musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.
12.6	Możliwość rozbudowy (np. w oparciu o licencję) o graficzną konsolę do zarządzania połączeniami VPN. W ramach postępowania muszą zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.
12.7	System musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi.
12.8	Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
12.9	System musi umożliwiać zbieranie i przechowywanie logów oraz generowanie raportów.
12.10	Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.
12.11	Umożliwia przeglądanie logów ruchu w czasie rzeczywistym.
12.12	Rozwiązanie musi udostępniać narzędzie analizy całości ruchu.
12.13	Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa.
12.14	Rozwiązanie musi posiadać zestaw predefiniowanych typów raportów.
12.15	Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie.
12.16	System ma mieć możliwość generowania raportów w formacie PDF oraz opcję eksportowania szczegółowych informacji do pliku CSV.
12.17	System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania ich pocztą e-mail.
12.18	Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.
12.19	System musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów.
12.20	System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.
12.21	Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.
12.22	Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów.
12.23	W ramach licencji, musi zostać dostarczony system XDR dla produktów producenta.
12.24	XDR musi zapewniać rozszerzone możliwości wykrywania poprzez korelację danych z różnych produktów zabezpieczających od producenta, które wskazują na obecność zagrożeń.

Pkt	Wymagania minimalne
12.25	XDR musi być hostowany w chmurze producenta.
12.26	XDR musi zapewniać informację, ze wszystkich produktów producenta z wymaganą licencją.
12.27	XDR musi posiadać tworzenie automatycznych polityk.
12.28	Automatyczna polityka, musi zawierać minimum: zakres ryzyka, typ incydentu, typ urządzenia, zablokowanie adresu IP zagrożenia, usunięcie pliku, wyizolowanie urządzenia, zatrzymanie złośliwego procesu.
13	**Ochrona stacji końcowych**
13.1	Licencja musi obejmować dodatkową ochronę stacji końcowych w formie agentów (minimum 5).
13.2	Rozwiązanie musi pochodzić od producenta rozwiązania.
13.3	Rozwiązanie musi minimum: ochraniać przed oprogramowaniem ransomware, posiadać zaawansowane techniki ochrony przed złośliwym oprogramowaniem, posiadać ochronę antytamperową, aktualizować sygnatury i heurystykę.
14	**Gwarancja**
14.1	Gwarancja na urządzenie musi obejmować wszystkie wymienione powyżej funkcjonalności, które muszą działać (wraz z aktualizacjami sygnatur, baz i oprogramowania) przez okres co najmniej 36 miesięcy od dnia odbioru.
14.2	Gwarancja musi być świadczona przez producenta lub autoryzowanego przez producenta partnera serwisowego, na terenie Rzeczypospolitej Polskiej, z przyjmowaniem zgłoszeń i komunikacją w języku polskim.

4.2. Przełącznik dystrybucyjny 24-portowy PoE – sieć OT – 3 szt.

Obszar wymagań	Wymagania minimalne
Obudowa	Obudowa urządzenia musi być przystosowana do montażu w standardowej szafie 19” i zajmować maksymalnie 1U.
Interfejsy	Minimum 24 gigabitowe interfejsy RJ-45 100/1000 Mbps, 4 interfejsy 10 Gigabit SFP+ Wszystkie porty SFP+ muszą być dostarczone z wkładami SFP+ Budżet mocy PoE nie mniejszy niż 370 W.
Wydajność i funkcjonalności	– Potencjał przełączania nie mniejszy niż 128 Gbps – Wydajność przekazywania pakietów nie mniejsza niż 95,2 Mpps – Bufor pakietu nie mniejszy niż 1500 KB – Tabela adresów MAC nie mniejsza niż 16K – Jumbo frame (byte) – 9K – Flash/RAM (MB): 32/512 – L3 forwarding table: Max. 512 IPv4 entries; Max. 512 IPv6 entries – Routing table: 32 – VLAN routing – IP interface (IPv4/IPv6): 32/32

Obszar wymagań	Wymagania minimalne
Tryby pracy	– Urządzenie musi umożliwiać zdalną konfigurację i monitorowanie poprzez panel sterowania dostępny w technologii chmurowej, dostarczony bezpłatnie przez producenta urządzenia
Zgodność ze standardami	– IEEE 802.3 10BASE-T Ethernet – IEEE 802.3u 100BASE-TX Ethernet – IEEE 802.3ab 1000BASE-T Ethernet – IEEE 802.3z 1000BASE-X – IEEE 802.3af PoE – IEEE 802.3at PoE Plus – IEEE 802.3az EEE – IEEE 802.3x flow control – IEEE 802.3ad LACP aggregation – IEEE 802.1D Spanning Tree Protocol (STP) – IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) – IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) – IEEE 802.1p Class of Service (CoS) prioritization – IEEE 802.1X port authentication
Odporność i dostępność	– IEEE 802.1D Spanning Tree Protocol (STP) – IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) – IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) – IEEE 802.3ad LACP. Max # Trunks/ Links per Trunk: 24/8
Kontrola ruchu	– 802.1Q static VLANs/dynamic VLANs: 1 K/4 K – Support up to 4K VLAN ID – Independent VLAN Learning (IVL) – L2TP – Port-based VLAN – Voice VLAN – VLAN trunking – GVRP
Bezpieczeństwo	– 802.1X – Port security – MAC authentication – Static MAC forwarding – SSL – Static ARP – Policy-based security filtering – Port isolation – MAC search – Guest VLAN – PPPoE relay agent

Obszar wymagań	Wymagania minimalne
	– PPPoE option 82 – PPPoE IA – Interface related trap enable/ disable (by port) – CPU protection – SHA2 HTTPS certification – Login authentication by RADIUS – RADIUS accounting – Authorization on RADIUS – Multiple RADIUS servers – 802.1x VLAN and bandwidth assignment by RADIUS – ACL packet filtering (IPv4)
QoS	– No. of hardware queues per port: 8 – 802.1p queuing methods: SPQ, WRR, WFQ – Storm control: broadcast, unknown L2MC, unknown unicast (DLF) – Rate limiting per port – Policy-based rate limiting – Policy-based prioritization
Layer 2 Multicast	– L2 multicast group: 1K – IGMP snooping (v1, v2, v3) – Configurable IGMP snooping timer and priority – IGMP snooping statistics – IGMP throttling – IGMP filtering – Static multicast
Zarządzanie	– SNMP v1, v2c, v3 – SNMP trap group – RMON (1, 2, 3, 9) – Syslog ((IPv4/v6) – IEEE 802.1AB LLDP – IEEE 802.1AB LLDP-MED
Zarządzanie IPv6	– IPv6 over Ethernet (RFC 2464) – IPv6 addressing architecture (RFC 4291) – Dual stack (RFC 4213) – ICMPv6 (RFC4884) – Path MTU (RFC 1981) – Minimum path MTU size of 1280 (RFC 5095) – Encapsulation for maximum PMTU of 1500 – Neighbor discovery (RFC 4861) – DHCPv6 relay – Default DHCP client mode

Obszar wymagań	Wymagania minimalne
	– Duplicated Address Detection (DAD)
Zarządzanie urządzeniem	– Standalone management by Web interface – Setup Wizard – Management through Telnet – Management through Web, SNMP – Firmware upgrade by FTP/Web – Configuration saving and retrieving – Multiple logins supported – Configure clone – DHCP relay per VLAN – DHCP client IPv4 – DHCP client IPv6 – DHCP option 82 – Daylight saving – NTP Server (IPv4/IPv6) Support DNS format – Display port utilization – Port mirroring – Scheduled PoE – PoE default consumption mode – PoE power management extended configuration – Web login warning page – Restore to last custom default
MIB	– RFC 1213, 1157 SNMPv2c/v3 MIB – RFC 1493 bridge MIB – RFC 1643 Ethernet MIB – RFC 1757 RMON group 1, 2, 3, 9 – RFC 2011, 2012, 2013 SNMPv2 MIB – RFC 2233 SMIv2 MIB – RFC 2819, 2925 remote management MIB – RFC 4292 IP forwarding table MIB – RFC 4293 Management Information Base (MIB) for IP
Gwarancja	Gwarancja producenta na okres co najmniej 24 miesięcy od dnia odbioru. Gwarancja musi być świadczona przez producenta lub autoryzowanego przez producenta partnera serwisowego, na terenie Rzeczypospolitej Polskiej, z przyjmowaniem zgłoszeń i komunikacją w języku polskim.
Serwis	W przypadku awarii urządzenia, wysyłka zastępczego produktu następuje w następnym dniu roboczym, po którym zgłoszona zostanie awaria. Urządzenie musi być objęte ww. opcją serwisową przez cały okres gwarancji.
Wymagane Certyfikaty	Bezpieczeństwo – LVD

Obszar wymagań	Wymagania minimalne
	– CE – RoHS
Pozostałe	Sprzęt musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE.

4.3. Szafa rack wisząca 12U – 3 szt.

Obszar wymagań	Wymagania minimalne
Typ urządzenia	Szafa teleinformatyczna 19" wisząca, przeznaczona do montażu na ścianie.
Wymiary	Wysokość: co najmniej 12U. Szerokość zewnętrzna: 600 mm. Głębokość zewnętrzna: co najmniej 600 mm. Konstrukcja umożliwiająca montaż urządzeń o głębokości co najmniej 480 mm (w tym zasilacza UPS w wersji rack).
Konstrukcja	Nośność co najmniej 60 kg. 4 szyny montażowe 19" z pełną regulacją głębokości. Otwory umożliwiające montaż szafy na ścianie. Otwory w dachu i podłodze umożliwiające wprowadzenie okablowania.
Drzwi i panele	Drzwi przednie przeszklone (szkło hartowane) z zamkiem na klucz, z możliwością montażu z prawej lub lewej strony. Zdejmowane panele boczne z możliwością zamknięcia. Tylna ściana zamknięta.
Wentylacja	Otwory wentylacyjne w dachu i podłodze zapewniające wentylację naturalną. Możliwość montażu wentylatora w dachu szafy.
Wyposażenie	Komplet śrub montażowych z nakrętkami koszykowymi (co najmniej 15 kompletów). Co najmniej 1 półka 19" dopasowana do głębokości szafy, przeznaczona do instalacji urządzenia UTM. Komplet elementów montażowych umożliwiających instalację w szafie urządzeń będących przedmiotem zamówienia dla danej lokalizacji.
Zgodność ze standardami	ANSI/EIA RS-310-D, DIN 41491 cz. 1, IEC 297-2, DIN 41494 cz. 7 lub równoważne.
Gwarancja	Gwarancja co najmniej 24 miesiące. Gwarancja musi być świadczona przez producenta lub autoryzowanego przez producenta partnera serwisowego, na terenie Rzeczypospolitej Polskiej, z przyjmowaniem zgłoszeń i komunikacją w języku polskim.

4.4. Zasilacz UPS z monitoringiem – 3 szt.

Obszar wymagań	Wymagania minimalne

Obszar wymagań	Wymagania minimalne
Moc	Moc pozorna: min. 1500 VA. Moc czynna: min. 1000 W.
Technologia	Line-interactive z automatyczną regulacją napięcia (AVR). Napięcie wyjściowe o przebiegu sinusoidalnym, również podczas pracy z baterii. Czas przełączenia na pracę bateryjną nie dłuższy niż 4 ms.
Wejście	Napięcie znamionowe 230 V, częstotliwość 50/60 Hz z automatycznym rozpoznawaniem. Zakres napięcia wejściowego bez przechodzenia na pracę bateryjną co najmniej 160–286 V, z możliwością regulacji czułości. Gniazdo wejściowe IEC C14 wraz z przewodem zasilającym.
Wyjście	Napięcie znamionowe 230 V (z możliwością ustawienia 220/240 V). Co najmniej 4 gniazda IEC C13 wraz z przewodami połączeniowymi do zasilanych urządzeń.
Akumulatory	Bezobsługowe akumulatory kwasowo-ołowiowe (VRLA). Wymiana akumulatorów przez użytkownika, bez konieczności wyłączania zasilania odbiorów (hot-swap). Czas ładowania akumulatorów nie dłuższy niż 3 godziny. Automatyczny test akumulatorów oraz sygnalizacja konieczności ich wymiany.
Funkcje	Możliwość uruchomienia z akumulatorów bez obecności napięcia sieciowego (zimny start). Panel LCD prezentujący co najmniej stan pracy, obciążenie, poziom naładowania akumulatorów i szacowany czas podtrzymania. Sygnalizacja dźwiękowa stanów alarmowych, w tym niskiego poziomu naładowania akumulatorów. Ochrona przeciwprzepięciowa.
Komunikacja i zarządzanie	Port USB oraz port szeregowy RS-232. Zainstalowana karta sieciowa z portem RJ-45 umożliwiająca co najmniej: zarządzanie przez przeglądarkę WWW z obsługą HTTPS, monitorowanie przez SNMP (w tym SNMP v3), powiadomienia e-mail oraz przesyłanie zdarzeń do serwera syslog. Czujnik temperatury otoczenia podłączany do karty sieciowej, dostarczony w komplecie. Oprogramowanie umożliwiające bezpieczne, automatyczne zamykanie systemów operacyjnych zasilanych urządzeń w przypadku długotrwałego zaniku zasilania. Możliwość monitorowania w systemie z poz. 3.14.
Obudowa	Do montażu w szafie rack 19", wysokość maks. 2U, wraz z kompletem szyn montażowych. Głębokość umożliwiająca montaż w szafie z poz. 4.3.
Normy	Deklaracja zgodności CE. Zgodność z normami EN/IEC 62040-1 (bezpieczeństwo) oraz EN/IEC 62040-2 (kompatybilność elektromagnetyczna) lub równoważnymi.
Gwarancja	Co najmniej 36 miesięcy gwarancji producenta na urządzenie oraz co najmniej 24

Obszar wymagań	Wymagania minimalne
	miesiące na akumulatory. Gwarancja musi być świadczona przez producenta lub autoryzowanego przez producenta partnera serwisowego, na terenie Rzeczypospolitej Polskiej, z przyjmowaniem zgłoszeń i komunikacją w języku polskim.

Wymagania dotyczące wdrożenia infrastruktury

Wymagania niniejszego rozdziału dotyczą instalacji, konfiguracji i zabezpieczenia całości sprzętu i oprogramowania dostarczanego w ramach obszaru technicznego IT oraz obszaru technicznego OT. Koszt usług wdrożeniowych Wykonawca uwzględni w cenach poszczególnych pozycji. Szczegółowe wymagania dotyczące wdrożenia systemu SIEM/XDR, domeny Active Directory oraz oprogramowania do monitorowania infrastruktury określono odpowiednio w poz. 3.12, 3.13 i 3.14.

W.1. Instalacja i konfiguracja sprzętu i oprogramowania – obszar IT

1. Wykonawca przeprowadzi dostawę, montaż, instalację, uruchomienie oraz konfigurację urządzeń i oprogramowania dostarczanych w ramach obszaru technicznego IT w siedzibie Zamawiającego (a w przypadku serwera NAS – w odseparowanej lokalizacji wskazanej przez Zamawiającego), obejmującą co najmniej:
   1) szafę rack (poz. 3.9),
   2) zasilacz UPS dla klastra HA (poz. 3.6),
   3) serwery klastra HA (poz. 3.1) wraz z licencjami serwerowego systemu operacyjnego i CAL (poz. 3.11),
   4) macierz dyskową (poz. 3.2),
   5) serwer kopii zapasowych wraz z oprogramowaniem (poz. 3.3) oraz bibliotekę taśmową (poz. 3.5),
   6) serwer NAS na odmiejscowione kopie zapasowe (poz. 3.7),
   7) przełączniki sieciowe (poz. 3.4),
   8) urządzenie UTM dla sieci IT (poz. 3.8),
   9) punkty dostępowe sieci bezprzewodowej wraz z kontrolerem (poz. 3.10).
2. W zakresie instalacji fizycznej Wykonawca:
   1) złoży, ustawi, wypoziomuje i uziemi szafę rack w miejscu wskazanym przez Zamawiającego,
   2) zamontuje urządzenia w szafie rack lub w miejscach wskazanych przez Zamawiającego (punkty dostępowe – na suficie lub ścianie),
   3) dostarczy i wykona połączenia zasilające i logiczne niezbędne do uruchomienia dostarczanych urządzeń (kable zasilające, patchcordy, kable DAC lub wkładki światłowodowe),

4) podłączy zasilacz UPS do instalacji elektrycznej Zamawiającego (w tym ewentualne podłączenie stałe) przez osobę posiadającą odpowiednie uprawnienia elektryczne oraz rozdzieli zasilanie urządzeń w sposób wykorzystujący redundantne zasilacze,
5) uporządkuje i trwale oznaczy wykonane okablowanie i urządzenia,
6) zaktualizuje firmware i oprogramowanie wszystkich urządzeń do wersji aktualnych na dzień wdrożenia.

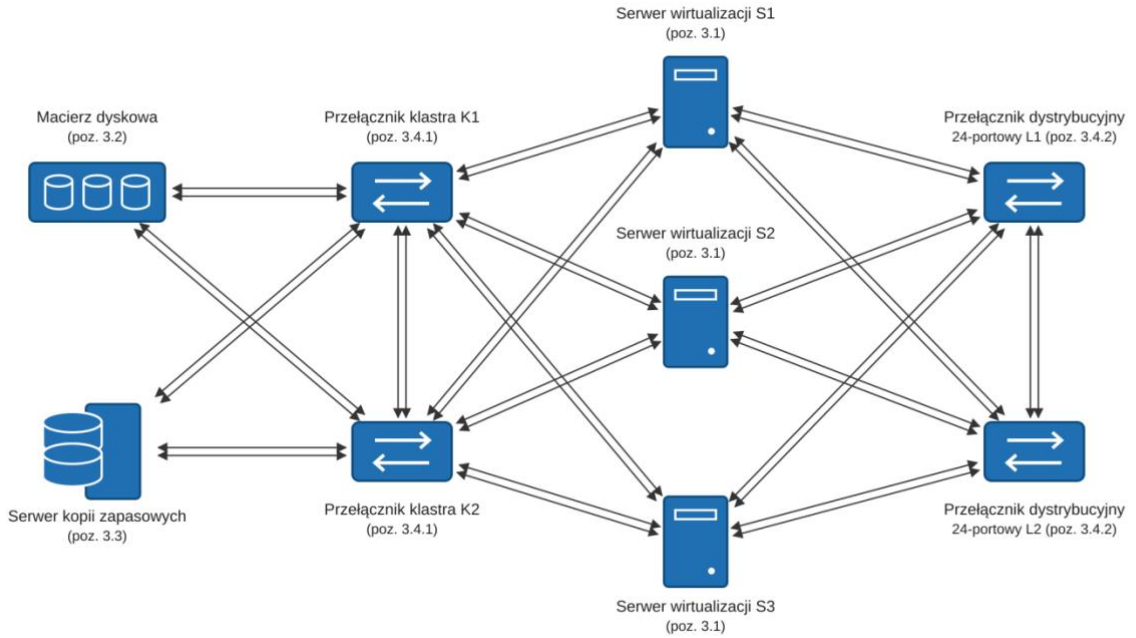
3. Budowę klastra wysokiej dostępności (serwery z poz. 3.1, macierz dyskowa z poz. 3.2, przełączniki z poz. 3.4.1 i 3.4.2) Wykonawca zrealizuje zgodnie z pkt W.2.
4. W zakresie sieci LAN i WLAN Wykonawca:
   1) na podstawie uzgodnień z Zamawiającym opracuje i wdroży podział sieci na segmenty (VLAN), obejmujący co najmniej: serwery, drukarki, system wizyjny, zarządzanie urządzeniami, użytkowników LAN, sieć WLAN Spółki, sieć WLAN dla gości, VLAN izolacyjny oraz VLAN OT,
   2) skonfiguruje VLAN izolacyjny bez dostępu do pozostałych sieci, przypisany do wszystkich nieużywanych portów przełączników i wykorzystywany do ręcznej izolacji urządzeń w przypadku incydentu, a procedurę izolacji opisze w dokumentacji powdrożeniowej (pkt W.7),
   3) skonfiguruje przełączniki dystrybucyjne, w tym: VLAN, łącza trunk, agregację łączy, protokół RSTP/MSTP, DHCP snooping, ochronę portów i zasilanie PoE,
   4) skonfiguruje kontroler i punkty dostępowe, w tym: sieć Spółki z zabezpieczeniem WPA3, sieć dla gości odseparowaną od sieci wewnętrznej z izolacją klientów, przypisanie sieci do odpowiednich VLAN oraz roaming między punktami dostępowymi.
5. W zakresie urządzenia UTM dla sieci IT Wykonawca:
   1) skonfiguruje interfejsy, strefy bezpieczeństwa, routing oraz translację adresów NAT, w tym routing i kontrolę ruchu pomiędzy segmentami sieci,
   2) skonfiguruje polityki bezpieczeństwa firewall w oparciu o zasadę minimalnych uprawnień (domyślne blokowanie ruchu),
   3) uruchomi i skonfiguruje funkcje ochronne: IPS, ochronę antywirusową, filtrowanie WWW i DNS, kontrolę aplikacji, inspekcję ruchu HTTPS, ochronę przed nieznanym złośliwym oprogramowaniem (sandbox) oraz ochronę przed phishingiem,
   4) skonfiguruje integrację z domeną Active Directory w zakresie identyfikacji i uwierzytelniania użytkowników,
   5) skonfiguruje zdalny dostęp VPN dla wskazanych użytkowników z uwierzytelnianiem dwuskładnikowym,
   6) skonfiguruje tunele VPN (IPSec lub SD-WAN) do urządzeń UTM w lokalizacjach OT (poz. 4.1),
   7) wdroży agentów ochrony stacji roboczych i serwerów (EDR) dostępnych w ramach licencji urządzenia na stanowiskach wskazanych przez Zamawiającego oraz skonfiguruje korelację zdarzeń,

8) skonfiguruje przekazywanie logów do systemu SIEM (poz. 3.12) oraz monitorowanie urządzenia w systemie z poz. 3.14.

6. W zakresie systemu kopii zapasowych Wykonawca:
   1) zainstaluje i skonfiguruje oprogramowanie do tworzenia kopii zapasowych (poz. 3.3 B) wykorzystujące macierz z poz. 3.3 A jako repozytorium kopii oraz zintegruje je ze środowiskiem wirtualizacyjnym, biblioteką taśmową z poz. 3.5 i serwerem NAS z poz. 3.7; sposób uruchomienia oprogramowania (maszyna wirtualna lub instalacja na serwerze) oraz serwer z poz. 3.1, w którym zostanie zainstalowany kontroler HBA SAS do obsługi biblioteki taśmowej, Wykonawca wskaże w projekcie klastra (pkt W.2) do akceptacji Zamawiającego,
   2) skonfiguruje zadania kopii zapasowych co najmniej dla: maszyn wirtualnych, serwerów, wskazanych komputerów użytkowników oraz konfiguracji urządzeń IT i OT,
   3) skonfiguruje harmonogramy, retencję, deduplikację, kompresję i szyfrowanie kopii,
   4) wdroży zasadę 3-2-1, w tym: kopie na serwerze kopii zapasowych, kopie na nośnikach taśmowych przechowywanych offline (air-gap) wraz z procedurą rotacji taśm oraz kopie odmiejscowione na serwerze NAS w odseparowanej lokalizacji,
   5) skonfiguruje mechanizmy ochrony kopii przed modyfikacją lub usunięciem (np. WORM, kopie niemodyfikowalne, migawki) oraz monitorowanie i powiadamianie o wyniku zadań,
   6) skonfiguruje serwer NAS, w tym: wolumeny i poziom RAID, szyfrowanie, migawki, integrację z domeną oraz bezpieczne połączenie z siedzibą Zamawiającego.

W.2. Budowa klastra wysokiej dostępności (HA) – obszar IT

1. W ramach budowy klastra wysokiej dostępności Wykonawca uruchomi i skonfiguruje środowisko składające się z:
   1) trzech serwerów wirtualizacji S1, S2, S3 (poz. 3.1) wraz z licencjami z poz. 3.11,
   2) macierzy dyskowej (poz. 3.2),
   3) dwóch przełączników klastra K1 i K2 (poz. 3.4.1),
   4) dwóch przełączników dystrybucyjnych 24-portowych L1 i L2 (poz. 3.4.2) zapewniających dostęp maszyn wirtualnych do sieci LAN,
   5) serwera kopii zapasowych (poz. 3.3) oraz biblioteki taśmowej (poz. 3.5),
   6) zasilacza UPS (poz. 3.6).
2. Wykonawca przygotuje projekt budowanego klastra wysokiej dostępności i przedłoży go Zamawiającemu do akceptacji w terminie 3 dni od dnia przekazania przez Zamawiającego dokumentacji sieci lub od dnia przeprowadzenia wizji lokalnej, w zależności od tego, które z tych zdarzeń nastąpi później. Projekt należy przygotować zgodnie z ideą przedstawioną na schemacie poglądowym (Rysunek 1), z uwzględnieniem dokumentacji sieci przekazanej przez Zamawiającego (adresacja, VLAN, mechanizmy zabezpieczeń). Wszystkie nowe zagadnienia dotyczące konfiguracji sieci Wykonawca uzgodni z Zamawiającym.



Rysunek 1. Schemat poglądowy klastra HA

3. Zamawiający wymaga pełnej redundancji klastra na poziomie:
   1) serwerów – awaria jednego z trzech serwerów nie może powodować niedostępności maszyn wirtualnych dłuższej niż czas ich automatycznego ponownego uruchomienia na pozostałych węzłach,
   2) kontrolerów macierzy dyskowej,
   3) przełączników sieciowych – każde urządzenie klastra (serwery, macierz, serwer kopii zapasowych) musi być podłączone do obu przełączników klastra K1 i K2, a serwery dodatkowo do obu przełączników L1 i L2,
   4) łączy pomiędzy urządzeniami – połączenia K1–K2 oraz L1–L2 muszą być zrealizowane co najmniej dwoma łączami z agregacją,
   5) zasilania – urządzenia z redundantnymi zasilaczami należy podłączyć w sposób zapewniający ciągłość pracy przy awarii pojedynczego obwodu.
4. W zakresie serwerów wirtualizacji Wykonawca:
   1) zaktualizuje firmware serwerów i ich podzespołów,
   2) skonfiguruje macierz RAID dysków systemowych,
   3) skonfiguruje kontrolery zarządzania (BMC) wraz z monitorowaniem stanu podzespołów i powiadomieniami, w wydzielonej sieci zarządzającej,
   4) zainstaluje na każdym z serwerów platformę wirtualizacyjną Proxmox VE w najnowszej dostępnej wersji wraz ze wszystkimi poprawkami dostępnymi na dzień odbioru (maszyny wirtualne z serwerowym systemem operacyjnym uruchamiane zgodnie z warunkami licencyjnymi oprogramowania z poz. 3.11),

5) skonfiguruje nadmiarowe połączenia sieciowe (agregacja lub teaming kart sieciowych) z podziałem na sieci: zarządzającą, pamięci masowej (iSCSI), migracji maszyn wirtualnych, komunikacji wewnątrzklastrowej oraz sieci maszyn wirtualnych.

5. W zakresie macierzy dyskowej Wykonawca:
   1) zaktualizuje firmware macierzy,
   2) skonfiguruje grupy RAID oraz pule dyskowe,
   3) utworzy jednostki logiczne (LUN) i przypisze je do serwerów klastra,
   4) skonfiguruje połączenie iSCSI z wykorzystaniem obu przełączników klastra oraz mechanizmu wielościeżkowego dostępu (multipath) na serwerach,
   5) skonfiguruje powiadomienia o stanie macierzy.
6. W zakresie przełączników klastra (K1, K2) i przełączników dystrybucyjnych (L1, L2) Wykonawca:
   1) zaktualizuje firmware przełączników,
   2) utworzy i skonfiguruje sieci VLAN na potrzeby klastra (pamięć masowa, migracja, komunikacja wewnątrzklastrowa, zarządzanie) oraz sieci VLAN wskazane przez Zamawiającego,
   3) skonfiguruje ramki Jumbo dla sieci pamięci masowej,
   4) skonfiguruje redundantne połączenia pomiędzy przełącznikami oraz ze wszystkimi urządzeniami klastra,
   5) skonfiguruje połączenie przełączników L1 i L2 z pozostałą siecią LAN Zamawiającego oraz z urządzeniem UTM (poz. 3.8), które będzie pełniło funkcję routingu pomiędzy sieciami VLAN.
7. W zakresie klastra Wykonawca:
   1) utworzy klaster Proxmox VE ze wszystkich trzech serwerów, z zapewnieniem kworum oraz wydzieloną, redundantną siecią komunikacji wewnątrzklastrowej,
   2) skonfiguruje połączenie klastra z macierzą z poz. 3.2 (iSCSI z multipath) oraz współdzieloną przestrzeń dyskową dla maszyn wirtualnych,
   3) zainstaluje i skonfiguruje mechanizmy wysokiej dostępności (HA) – automatyczne uruchamianie maszyn wirtualnych na pozostałych węzłach po awarii węzła – oraz migrację maszyn wirtualnych bez przerywania ich pracy,
   4) utworzy maszyny wirtualne wymagane do uruchomienia systemów wdrażanych w ramach zamówienia (w tym kontrolerów domeny, systemu SIEM/XDR oraz systemu monitorowania infrastruktury),
   5) przeniesie do środowiska wirtualnego istniejące systemy i aplikacje Zamawiającego z dotychczasowego serwera, w zakresie uzgodnionym z Zamawiającym, wraz z niezbędną zmianą konfiguracji urządzenia UTM,
   6) skonfiguruje kartę zarządzającą zasilacza UPS (poz. 3.6) wraz z automatycznym, bezpiecznym wyłączaniem maszyn wirtualnych i serwerów klastra po zaniku zasilania,

7) zintegruje klaster z systemem kopii zapasowych (poz. 3.3) i biblioteką taśmową (poz. 3.5) oraz skonfiguruje kopie zapasowe wszystkich maszyn wirtualnych.

8. Przed zgłoszeniem prac do odbioru Wykonawca, w obecności przedstawiciela Zamawiającego, przeprowadzi testy niezawodności klastra polegające co najmniej na:
   1) symulacji awarii pojedynczych łączy pomiędzy urządzeniami a przełącznikami sieciowymi,
   2) symulacji awarii jednego z przełączników klastra (K1 lub K2) oraz jednego z przełączników dystrybucyjnych (L1 lub L2),
   3) symulacji awarii jednego z węzłów klastra HA,
   4) migracji maszyny wirtualnej pomiędzy węzłami bez przerywania jej pracy,
   5) weryfikacji wydajności sieci pamięci masowej oraz poprawności wykonywania i odtwarzania kopii zapasowych maszyn wirtualnych.

W.3. Konfiguracja bezpieczeństwa i hardening – obszar IT

1. Wykonawca przeprowadzi konfigurację bezpieczeństwa oraz hardening wdrażanych urządzeń i systemów w obszarze IT, zgodnie z dobrymi praktykami producentów oraz uznanymi wytycznymi bezpieczeństwa (np. CIS Benchmarks, zalecenia producenta systemu operacyjnego). Zakres obejmuje co najmniej:
   1) urządzenie UTM,
   2) przełączniki sieciowe,
   3) punkty dostępowe i kontroler sieci bezprzewodowej,
   4) serwery klastra HA, ich kontrolery zarządzania (BMC) oraz środowisko wirtualizacyjne,
   5) maszyny wirtualne uruchamiane w ramach wdrożenia,
   6) macierz dyskową,
   7) serwer i oprogramowanie kopii zapasowych oraz bibliotekę taśmową,
   8) serwer NAS,
   9) kartę zarządzającą zasilacza UPS.
2. W ramach hardeningu urządzeń i systemów Wykonawca wykona co najmniej:
   1) zmianę domyślnych ustawień bezpieczeństwa i danych dostępowych,
   2) ograniczenie lub wyłączenie zbędnych usług, protokołów oraz interfejsów administracyjnych (w tym nieużywanych portów przełączników),
   3) konfigurację bezpiecznych metod dostępu administracyjnego (HTTPS, SSH, SNMPv3) wyłącznie z wydzielonej sieci zarządzającej lub wskazanych adresów,
   4) konfigurację mechanizmów uwierzytelniania i autoryzacji, w tym ról administracyjnych i uwierzytelniania dwuskładnikowego tam, gdzie pozwala na to rozwiązanie,
   5) konfigurację polityk haseł zgodnych z dobrymi praktykami bezpieczeństwa,
   6) konfigurację synchronizacji czasu z wykorzystaniem protokołu NTP,
   7) konfigurację rejestrowania zdarzeń, retencji logów oraz ich przekazywania do systemu SIEM,

8) konfigurację bezpiecznych parametrów komunikacji szyfrowanej,

9) konfigurację mechanizmów lub procedur aktualizacji,

10) wykonanie kopii zapasowych konfiguracji urządzeń.

3. W zakresie środowiska serwerowego i wirtualizacyjnego Wykonawca dodatkowo zastosuje zalecane przez producenta systemu operacyjnego ustawienia bezpieczeństwa (security baseline), skonfiguruje zaporę systemową, ograniczy uprawnienia kont uprzywilejowanych oraz włączy szyfrowanie dysków tam, gdzie jest to uzasadnione.
4. W zakresie systemu kopii zapasowych Wykonawca zapewni odrębne poświadczenia administracyjne niezależne od domeny produkcyjnej, uwierzytelnianie dwuskładnikowe dla konsoli zarządzającej (jeżeli dostępne) oraz ochronę repozytoriów przed nieautoryzowanym dostępem.
5. Wykonawca przeprowadzi weryfikację poprawności zastosowanych ustawień bezpieczeństwa oraz testy funkcjonalne potwierdzające poprawność działania wdrożonych usług po wykonaniu hardeningu.

W.4. Instalacja i konfiguracja sprzętu – obszar OT

1. Wykonawca przeprowadzi dostawę, montaż, instalację, uruchomienie oraz konfigurację urządzeń dostarczanych w ramach obszaru technicznego OT w każdej z trzech lokalizacji OT (stacje uzdatniania wody oraz oczyszczalnia ścieków), obejmującą:

   1) szafę rack wiszącą (poz. 4.3),

   2) zasilacz UPS (poz. 4.4),

   3) urządzenie UTM dla sieci OT (poz. 4.1),

   4) przełącznik dystrybucyjny PoE (poz. 4.2).
2. W zakresie instalacji fizycznej Wykonawca:

   1) zamontuje i uziemi szafy wiszące w miejscach wskazanych przez Zamawiającego,

   2) zamontuje urządzenia w szafach, w tym urządzenie UTM na półce,

   3) wykona połączenia zasilające z zasilaczem UPS oraz połączenia logiczne pomiędzy dostarczanymi urządzeniami i istniejącą infrastrukturą OT oraz łączem dostępu do Internetu,

   4) uporządkuje i trwale oznaczy wykonane okablowanie i urządzenia,

   5) zaktualizuje firmware urządzeń do wersji aktualnych na dzień wdrożenia.
3. W zakresie sieci OT Wykonawca:

   1) na podstawie inwentaryzacji wykonanej wspólnie z Zamawiającym wdroży segmentację sieci lokalnej w każdej lokalizacji (VLAN), obejmującą co najmniej: systemy sterowania i wizualizacji (SCADA/PLC), stacje robocze OT, komputery biurowe obsługi obiektu, system wizyjny oraz zarządzanie urządzeniami,

   2) skonfiguruje urządzenia UTM jako urządzenia brzegowe, w tym polityki firewall dopuszczające wyłącznie niezbędną komunikację (zasada domyślnego blokowania), z zablokowaniem bezpośredniego dostępu systemów sterowania do Internetu,

3) skonfiguruje szyfrowane tunele VPN (IPSec lub SD-WAN) pomiędzy lokalizacjami OT a urządzeniem UTM w siedzibie Zamawiającego (poz. 3.8), z mechanizmem przełączania na łącze zapasowe, o ile Zamawiający takie udostępni, oraz z zachowaniem ochrony sieci lokalnej w przypadku utraty połączenia z siedzibą,
4) uruchomi funkcje IPS, ochrony antywirusowej, filtrowania WWW i DNS oraz kontroli aplikacji w zakresie nieblokującym pracy systemów sterowania,
5) skonfiguruje bezpieczny zdalny dostęp serwisowy do systemów OT wyłącznie przez VPN z uwierzytelnianiem dwuskładnikowym i rejestrowaniem sesji,
6) skonfiguruje przełączniki PoE, w tym: VLAN, ochronę portów, uwierzytelnianie urządzeń tam, gdzie pozwala na to infrastruktura, oraz zasilanie PoE urządzeń wskazanych przez Zamawiającego,
7) skonfiguruje zasilacze UPS wraz z monitorowaniem i powiadomieniami.

4. W zakresie integracji z systemami centralnymi Wykonawca:
1) obejmie stacje robocze OT oraz komputery biurowe w lokalizacjach OT agentami systemu SIEM (poz. 3.12), a w uzgodnieniu z Zamawiającym przyłączy je do domeny Active Directory (poz. 3.13) i obejmie agentami ochrony (EDR),
2) włączy urządzenia UTM, przełączniki i zasilacze UPS do systemu monitorowania infrastruktury (poz. 3.14) oraz skonfiguruje przekazywanie ich logów do systemu SIEM,
3) obejmie konfiguracje urządzeń OT oraz wskazane stacje robocze OT systemem kopii zapasowych (poz. 3.3).

5. Prace w obszarze OT Wykonawca zrealizuje według harmonogramu i w oknach serwisowych uzgodnionych z Zamawiającym, w sposób niezakłócający ciągłości dostaw wody i odbioru ścieków. Wykonawca nie będzie ingerował w konfigurację sterowników i aplikacji systemów sterowania bez zgody Zamawiającego, a prace wymagające takiej ingerencji uzgodni z Zamawiającym i dostawcą systemu SCADA.

W.5. Konfiguracja bezpieczeństwa i hardening – obszar OT

1. Wykonawca przeprowadzi konfigurację bezpieczeństwa oraz hardening rozwiązań wdrażanych w obszarze OT, z uwzględnieniem specyfiki środowisk przemysłowych oraz konieczności zapewnienia ciągłości działania systemów sterowania. Zakres obejmuje co najmniej:
1) urządzenia UTM w lokalizacjach OT,
2) przełączniki PoE,
3) karty zarządzające zasilaczy UPS,
4) interfejsy administracyjne urządzeń objętych wdrożeniem,
5) w uzgodnieniu z Zamawiającym – stacje robocze OT przyłączane do domeny.

2. W ramach hardeningu Wykonawca wykona co najmniej:
1) zmianę domyślnych danych dostępowych i ustawień bezpieczeństwa,
2) ograniczenie lub wyłączenie zbędnych usług, funkcjonalności i nieużywanych portów,

3) konfigurację bezpiecznych metod dostępu administracyjnego wyłącznie z sieci zarządzającej lub przez tunel VPN,
4) konfigurację polityk haseł i zasad uwierzytelniania, w tym uwierzytelniania dwuskładnikowego dla dostępu zdalnego,
5) konfigurację synchronizacji czasu z wykorzystaniem NTP,
6) konfigurację rejestrowania zdarzeń i działań administracyjnych oraz przekazywania logów do systemu SIEM,
7) konfigurację bezpiecznych parametrów komunikacji szyfrowanej,
8) ograniczenie dostępu administracyjnego do wskazanych kont, adresów lub segmentów sieciowych,
9) wykonanie kopii konfiguracji urządzeń objętych wdrożeniem.

3. Wykonawca przeprowadzi weryfikację poprawności zastosowanych ustawień bezpieczeństwa oraz testy funkcjonalne potwierdzające poprawną pracę systemów sterowania i komunikacji pomiędzy lokalizacjami po wykonaniu hardeningu.

W.6. Testy i wsparcie (obszar IT i OT)

1. Po zakończeniu wdrożenia Wykonawca przeprowadzi w obecności Zamawiającego testy obejmujące co najmniej:
   1) weryfikację komunikacji sieciowej i segmentacji (dozwolony i blokowany ruch pomiędzy VLAN oraz pomiędzy IT i OT),
   2) test przełączenia awaryjnego klastra HA oraz migracji maszyn wirtualnych,
   3) test działania zasilaczy UPS, w tym automatycznego wyłączania serwerów,
   4) wykonanie kopii zapasowej i testowe odtworzenie maszyny wirtualnej oraz pojedynczych plików, w tym z nośnika taśmowego i z serwera NAS,
   5) test dostępu do sieci bezprzewodowej oraz dostępu VPN z uwierzytelnianiem dwuskładnikowym,
   6) test tuneli VPN do lokalizacji OT, w tym zachowania przy utracie łącza,
   7) weryfikację rejestrowania zdarzeń w systemie SIEM oraz monitorowania urządzeń.
2. Wykonawca zapewni wsparcie techniczne (zdalna pomoc w przypadku problemów z działaniem wdrożonych rozwiązań, pomoc w aktualizacjach) w okresie 12 miesięcy od dnia odbioru, w dni robocze w godzinach pracy Zamawiającego, z wykorzystaniem wskazanego przez Wykonawcę kanału zgłoszeń (e-mail lub system zgłoszeń).

W.7. Dokumentacja powdrożeniowa (wszystkie wdrożenia)

1. Wykonawca przekaże Zamawiającemu jedną, wspólną dokumentację powdrożeniową dla wszystkich wdrożeń realizowanych w ramach zamówienia (obszar techniczny IT i OT), w języku polskim, w formie elektronicznej, obejmującą co najmniej:
   1) wykaz dostarczonych urządzeń i oprogramowania wraz z numerami seryjnymi, wersjami i licencjami,

2) schematy fizyczne i logiczne sieci IT i OT oraz zestawienie adresacji IP i VLAN,
3) projekt i opis konfiguracji klastra HA (serwery, macierz, przełączniki, połączenia, mechanizmy wysokiej dostępności),
4) opis konfiguracji urządzeń sieciowych, urządzeń UTM, tuneli VPN i sieci bezprzewodowej,
5) opis zastosowanych mechanizmów bezpieczeństwa oraz wykonanych działań hardeningowych w obszarze IT i OT,
6) opis polityk i procedur wykonywania i odtwarzania kopii zapasowych, w tym rotacji taśm i kopii odmiejscowionych,
7) opis domeny Active Directory: struktura jednostek organizacyjnych, wykaz polityk GPO, macierz uprawnień,
8) opis systemu SIEM: architektura, wykaz podłączonych źródeł, utworzonych reguł i parserów, procedura przywracania danych z archiwum,
9) opis systemu monitorowania: wykaz monitorowanych urządzeń i parametrów, progi alarmowe, odbiorcy powiadomień,
10) procedurę izolacji urządzeń z wykorzystaniem VLAN izolacyjnego (pkt W.1),
11) dane dostępowe przekazane zgodnie z procedurą ustaloną z Zamawiającym,
12) procedury utrzymaniowe (aktualizacje, kopie zapasowe konfiguracji, odtworzenie po awarii) oraz instrukcje uruchamiania, wyłączania i podstawowej obsługi wdrożonych rozwiązań, wraz z rekomendacjami utrzymania bezpiecznej konfiguracji.

W.8. Szkolenie administratorów (wszystkie wdrożenia)

1. Wykonawca przeprowadzi jedno szkolenie administracyjne obejmujące całość wdrożonych rozwiązań, dla 3 administratorów wskazanych przez Zamawiającego.
2. Wymiar szkolenia: 2 dni po 8 godzin.
3. Zakres szkolenia obejmie co najmniej:
   1) administrację klastrem HA i platformą wirtualizacji oraz macierzą dyskową,
   2) obsługę systemu kopii zapasowych, biblioteki taśmowej i serwera NAS, w tym procedury odtwarzania danych i maszyn wirtualnych,
   3) administrację urządzeniami UTM (IT i OT), tunelami VPN, przełącznikami sieciowymi i siecią bezprzewodową,
   4) administrację domeną Active Directory i politykami GPO,
   5) obsługę systemu SIEM (analiza alarmów, reguły, raporty) oraz systemu monitorowania infrastruktury,
   6) procedury postępowania w przypadku awarii i incydentu bezpieczeństwa.
4. Szkolenie zostanie przeprowadzone w języku polskim, w siedzibie Zamawiającego, na wdrożonym środowisku Zamawiającego, w terminie uzgodnionym z Zamawiającym. Uczestnicy otrzymają materiały szkoleniowe w formie elektronicznej oraz zaświadczenia ukończenia szkolenia.

Wymagania wspólne dla obszaru organizacyjnego i kompetencyjnego

1. Usługi z obszaru organizacyjnego i kompetencyjnego dotyczą całej organizacji Zamawiającego, tj. siedziby oraz obiektów infrastruktury wodno-kanalizacyjnej (stacje uzdatniania wody, przepompownie, oczyszczalnia ścieków), i obejmują zarówno obszar IT, jak i obszar OT (systemy sterowania i nadzoru SCADA/ICS).
2. Dokumentacja musi być opracowana indywidualnie dla Zamawiającego i odzwierciedlać jego stan faktyczny, strukturę organizacyjną, procesy i zasoby. Zamawiający nie dopuszcza przekazania dokumentacji ogólnodostępnej ani wzorów niedostosowanych do jego organizacji.
3. Dokumentacja musi uwzględniać infrastrukturę dostarczaną i wdrażaną w ramach obszaru technicznego IT i OT (m.in. klaster HA, system kopii zapasowych, urządzenia UTM, system SIEM, domenę Active Directory, system monitorowania).
4. Dokumentacja i szkolenia muszą być zgodne z obowiązującymi przepisami i normami, w zakresie mającym zastosowanie do Zamawiającego, w szczególności:
   a) ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa wraz z aktami wykonawczymi,
   b) PN-EN ISO/IEC 27001:2023, PN-EN ISO/IEC 27002:2023 oraz ISO/IEC 27005 lub normami równoważnymi,
   c) ISO 22301 lub normą równoważną (system zarządzania ciągłością działania),
   d) rozporządzeniem (UE) 2016/679 (RODO) – w zakresie powiązań z ochroną danych osobowych,
   e) dyrektywą (UE) 2022/2555 (NIS2) – w zakresie przygotowania do jej wymagań,
   f) w obszarze OT – z uwzględnieniem dobrych praktyk serii norm IEC 62443 lub norm równoważnych.
5. Prace analityczne, wywiady i warsztaty będą realizowane w siedzibie Zamawiającego oraz – w zakresie obiektów OT – w tych obiektach, w terminach uzgodnionych z Zamawiającym. Wykonawca przeprowadzi odrębne spotkania z kierownikami komórek organizacyjnych Zamawiającego.
6. Wszystkie dokumenty, materiały i szkolenia muszą być w języku polskim. Dokumenty Wykonawca przekaże w formie elektronicznej edytowalnej (DOCX/XLSX) oraz w formacie PDF.
7. Zamawiający ma prawo wnosić uwagi do przekazanych dokumentów w terminie 5 dni roboczych od ich przekazania. Wykonawca uwzględni uwagi i przekaże poprawione dokumenty w terminie 5 dni roboczych.
8. Jeżeli w trakcie realizacji umowy zmienią się przepisy dotyczące przedmiotu zamówienia, Wykonawca dostosuje do nich dokumentację bez dodatkowego wynagrodzenia.
9. Wykonawca przeniesie na Zamawiającego autorskie prawa majątkowe do wytworzonej dokumentacji i materiałów szkoleniowych.

10. Przed rozpoczęciem prac Wykonawca podpisze umowę o zachowaniu poufności. Wyniki audytów i testów stanowią informacje chronione i mogą być przekazywane wyłącznie Zamawiającemu.
11. Wszystkie dokumenty i materiały szkoleniowe muszą być oznakowane zgodnie z zasadami informacji i promocji obowiązującymi dla projektów finansowanych z Krajowego Planu Odbudowy i Zwiększania Odporności oraz spełniać wymagania dostępności cyfrowej.
12. Wykonawca skieruje do realizacji zamówienia osoby posiadające kwalifikacje odpowiednie do zakresu prac, co najmniej:
    a) do poz. 1.1, 1.4 i 1.5 – osobę posiadającą certyfikat audytora wiodącego ISO/IEC 27001 lub równoważny oraz – dla poz. 1.4 i 1.5 – certyfikat audytora ISO 22301 lub równoważne kwalifikacje,
    b) do poz. 1.3 – osobę posiadającą doświadczenie w audytach bezpieczeństwa systemów przemysłowych OT/ICS (np. certyfikat GICSP, ISA/IEC 62443 lub równoważny) oraz osobę przeprowadzającą testy penetracyjne posiadającą certyfikat z tego zakresu (np. OSCP, CEH Practical, PNPT lub równoważny),
    c) do poz. 2.1–2.3 – trenerów posiadających doświadczenie w prowadzeniu szkoleń z cyberbezpieczeństwa i bezpieczeństwa informacji.

Obszar organizacyjny

1.1. Opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Przedmiotem usługi jest ustanowienie, opracowanie dokumentacji i wdrożenie SZBI zgodnego z wymaganiami PN-EN ISO/IEC 27001:2023 lub normy równoważnej, obejmującego całą organizację Zamawiającego, w tym obszar IT i OT, w sposób umożliwiający jego późniejszą certyfikację.

1. Analiza luk (audyt zerowy):
    a) analiza istniejących regulacji wewnętrznych Zamawiającego dotyczących bezpieczeństwa informacji,
    b) ocena zgodności z wymaganiami ISO/IEC 27001:2023 lub normy równoważnej oraz ustawy o krajowym systemie cyberbezpieczeństwa,
    c) analiza struktury organizacyjnej pod kątem ról i odpowiedzialności w SZBI,
    d) raport z analizy luk zawierający zidentyfikowane niezgodności i rekomendacje z priorytetyzacją, omówiony z Zamawiającym.
2. Ustanowienie SZBI:
    a) określenie kontekstu organizacji, stron zainteresowanych i ich wymagań,
    b) określenie zakresu SZBI,
    c) opracowanie polityki bezpieczeństwa informacji oraz celów i mierników bezpieczeństwa,
    d) określenie ról, odpowiedzialności i uprawnień, w tym Pełnomocnika ds. SZBI,

e) opracowanie mapy dokumentów SZBI do akceptacji Zamawiającego.

3. Zarządzanie aktywami:
   a) opracowanie metodyki identyfikacji i klasyfikacji aktywów informacyjnych,
   b) przeprowadzenie inwentaryzacji i klasyfikacji aktywów IT i OT wraz z przypisaniem właścicieli,
   c) opracowanie rejestru aktywów.
4. Zarządzanie ryzykiem:
   a) opracowanie metodyki szacowania ryzyka zgodnej z ISO/IEC 27005 lub normą równoważną,
   b) przeprowadzenie szacowania ryzyka dla aktywów IT i OT,
   c) opracowanie rejestru ryzyk, planu postępowania z ryzykiem oraz deklaracji stosowania (SoA) dla zabezpieczeń z załącznika A normy ISO/IEC 27001:2023 lub normy równoważnej.
5. Dokumentacja SZBI:
   a) opracowanie polityk dziedzinowych, procedur i instrukcji – łącznie co najmniej 15 procedur, w zakresie wynikającym z deklaracji stosowania, w tym co najmniej: kontroli dostępu i zarządzania uprawnieniami, zarządzania hasłami i uwierzytelnianiem, kopii zapasowych, zarządzania zmianą i podatnościami, bezpieczeństwa sieci i zdalnego dostępu, bezpieczeństwa systemów OT, bezpiecznego korzystania z nośników i urządzeń mobilnych, pracy zdalnej, współpracy z dostawcami, bezpieczeństwa fizycznego, monitorowania i rejestrowania zdarzeń,
   b) opracowanie procedury zarządzania incydentami bezpieczeństwa, z uwzględnieniem obowiązków zgłaszania incydentów do właściwego zespołu CSIRT i organu właściwego wynikających z ustawy o krajowym systemie cyberbezpieczeństwa oraz obowiązków wynikających z RODO,
   c) opracowanie programu audytów wewnętrznych oraz procedury przeglądu zarządzania.
6. Wdrożenie SZBI:
   a) przekazanie dokumentacji do zatwierdzenia przez Zamawiającego,
   b) opracowanie materiałów informacyjnych dla kierownictwa i pracowników dotyczących wprowadzenia SZBI,
   c) wsparcie konsultacyjne Zamawiającego we wdrażaniu dokumentacji,
   d) przeprowadzenie pierwszego audytu wewnętrznego SZBI wraz z raportem oraz wsparcie Zamawiającego w przeprowadzeniu pierwszego przeglądu zarządzania.
7. Szacowany wymiar prac Zamawiający określa na 220–300 roboczogodzin.

1.2. Wdrożenie narzędzia do zarządzania SZBI, BCP i DRP (open source)

Przedmiotem usługi jest konfiguracja i wdrożenie narzędzia wspierającego Zamawiającego w samodzielnym utrzymaniu, zarządzaniu i doskonaleniu SZBI, SZCD oraz planów BCP i DRP, opartego wyłącznie na oprogramowaniu o otwartym kodzie źródłowym, bez opłat licencyjnych. Podstawą jest system GLPI, który Zamawiający uruchamia we własnym zakresie na maszynie wirtualnej w klastrze HA i do którego zapewni Wykonawcy dostęp z uprawnieniami administratora.

Wykonawca może uzupełnić GLPI o wtyczki open source lub, w uzgodnieniu z Zamawiającym, o dodatkowe narzędzie klasy GRC open source (np. CISO Assistant Community lub równoważne) zintegrowane z GLPI w zakresie rejestru aktywów, uruchomione na maszynie wirtualnej udostępnionej przez Zamawiającego.

A. Wymagania funkcjonalne (minimalne)

1. Repozytorium dokumentacji SZBI, SZCD, BCP i DRP z wersjonowaniem, statusem dokumentu (projekt, obowiązujący, archiwalny), wskazaniem właściciela i terminem kolejnego przeglądu.
2. Dostęp do dokumentów według ról, z uwierzytelnianiem przez Active Directory (LDAP): dokumenty przeznaczone do publikacji dostępne dla wszystkich pracowników, pełna dokumentacja dla Pełnomocnika ds. SZBI i osób wskazanych przez Zamawiającego.
3. Publikacja dokumentów pracownikom wraz z ewidencją potwierdzeń zapoznania się z nimi.
4. Rejestr aktywów IT i OT powiązany z inwentarzem GLPI, z przypisaniem właściciela i klasyfikacji.
5. Rejestr ryzyk, plan postępowania z ryzykiem i deklaracja stosowania (SoA) - w narzędziu lub jako wersjonowane dokumenty w repozytorium, powiązane z aktywami.
6. Rejestr incydentów bezpieczeństwa obsługiwanych jako zgłoszenia, z kategoriami i polami umożliwiającymi kontrolę terminów zgłoszeń wynikających z ustawy o krajowym systemie cyberbezpieczeństwa i RODO.
7. Harmonogram przeglądów dokumentów, audytów wewnętrznych oraz testów BCP i DRP w postaci zadań z przypomnieniami.
8. Interfejs w języku polskim, eksport danych co najmniej do PDF, XLSX lub CSV, dane przechowywane wyłącznie w infrastrukturze Zamawiającego.

B. Zakres wdrożenia

1. Analiza przedwdrożeniowa i projekt konfiguracji (struktura dokumentów, kategorie, role i uprawnienia, pola dodatkowe, ewentualne wtyczki lub dodatkowe narzędzie open source) - do akceptacji Zamawiającego.
2. Konfiguracja GLPI (oraz ewentualnych wtyczek lub dodatkowego narzędzia) zgodnie z zatwierdzonym projektem i metodykami opracowanymi w poz. 1.1, 1.4 i 1.5 (klasyfikacja aktywów, skale szacowania ryzyka, kategorie incydentów).
3. Wprowadzenie do narzędzia całej dokumentacji i rejestrów opracowanych w ramach poz. 1.1, 1.3, 1.4 i 1.5 (dokumenty SZBI i SZCD, rejestr aktywów, rejestr ryzyk, deklaracja stosowania, BIA, plany BCP i DRP), z oznaczeniem wersji i właścicieli.
4. Instrukcja użytkownika i administratora w języku polskim oraz szkolenie w siedzibie Zamawiającego dla administratorów (co najmniej 3 godziny) i dla Pełnomocnika ds. SZBI i właścicieli aktywów (co najmniej 2 godziny).
5. Testy odbiorowe obejmujące co najmniej: dostęp użytkowników o różnych rolach, publikację dokumentu i potwierdzenie zapoznania, rejestrację incydentu, przypomnienie o przeglądzie dokumentu oraz eksport rejestrów.

1.3. Audyt sieci OT – inwentaryzacja, opis stanu aktualnego, analiza potrzeb modernizacji zabezpieczeń

Przedmiotem usługi jest kompleksowy audyt cyberbezpieczeństwa środowiska IT oraz OT/ICS Zamawiającego, obejmujący siedzibę, stacje uzdatniania wody, przepompownie i oczyszczalnię ścieków, wraz z testami penetracyjnymi środowiska IT oraz analizą potrzeb modernizacji zabezpieczeń.

1. Inwentaryzacja i opis stanu aktualnego:
   a) inwentaryzacja urządzeń i systemów IT i OT, w tym sterowników PLC, paneli HMI, stacji operatorskich i serwerów SCADA, urządzeń sieciowych, urządzeń komunikacji i telemetrii oraz łączy z obiektami,
   b) opracowanie schematów sieci IT i OT oraz przepływów danych pomiędzy strefami, w tym połączeń z siecią IT, Internetem i dostawcami zewnętrznymi,
   c) identyfikacja wersji oprogramowania i oprogramowania układowego (firmware) urządzeń OT.
2. Audyt środowiska OT/ICS:
   a) ocena architektury i segmentacji sieci OT, z odniesieniem do modelu stref i kanałów komunikacji (IEC 62443 lub norm równoważnych),
   b) analiza konfiguracji sterowników PLC, HMI i systemów SCADA pod kątem bezpieczeństwa (m.in. kontrola dostępu, hasła domyślne, zabezpieczenie programów, wykorzystywane protokoły komunikacyjne),
   c) ocena zdalnego dostępu serwisowego do systemów OT, w tym dostępu dostawców,
   d) ocena zabezpieczeń stacji operatorskich (aktualizacje, ochrona przed złośliwym oprogramowaniem, kopie zapasowe konfiguracji i programów),
   e) ocena zabezpieczeń fizycznych szaf i pomieszczeń z urządzeniami OT,
   f) identyfikacja podatności z wykorzystaniem metod pasywnych (analiza ruchu sieciowego, przegląd konfiguracji, wywiady). Aktywne skanowanie urządzeń OT jest dopuszczalne wyłącznie za zgodą Zamawiającego, w uzgodnionych oknach serwisowych i w sposób niezakłócający pracy procesu technologicznego.
3. Testy penetracyjne IT:
   a) test zewnętrzny – usług i adresów IP Zamawiającego dostępnych z Internetu,
   b) test wewnętrzny – sieci biurowej Zamawiającego, z oceną możliwości przedostania się do sieci OT,
   c) testy prowadzone zgodnie z uznaną metodyką (np. OWASP, PTES, NIST SP 800-115), według zakresu i harmonogramu uzgodnionego z Zamawiającym, z zachowaniem zasad bezpieczeństwa i możliwością natychmiastowego wstrzymania testów na żądanie Zamawiającego.
4. Raport z audytu, zawierający co najmniej:
   a) streszczenie dla kierownictwa,

b) opis stanu aktualnego i inwentaryzację wraz ze schematami sieci,

c) wykaz zidentyfikowanych podatności i niezgodności z oceną poziomu ryzyka,

d) wyniki testów penetracyjnych wraz z opisem sposobu odtworzenia podatności,

e) analizę potrzeb modernizacji zabezpieczeń z rekomendacjami uszeregowanymi według priorytetów,

f) omówienie raportu z Zamawiającym.

5. Po wdrożeniu rekomendacji o najwyższym priorytecie Wykonawca przeprowadzi na wniosek Zamawiającego jednokrotny retest podatności o krytycznym i wysokim poziomie ryzyka.
6. Wyniki audytu zostaną wykorzystane w szacowaniu ryzyka SZBI (poz. 1.1).

1.4. Opracowanie i wdrożenie Systemu Zarządzania Ciągłością Działania (SZCD)

Przedmiotem usługi jest opracowanie i wdrożenie Systemu Zarządzania Ciągłością Działania zgodnego z wymaganiami ISO 22301 lub normy równoważnej, komplementarnego do SZBI (poz. 1.1).

1. Określenie kontekstu, zakresu i polityki zarządzania ciągłością działania oraz celów ciągłości działania, spójnych z SZBI.
2. Określenie ról i odpowiedzialności w SZCD, w tym składu i zadań zespołu zarządzania kryzysowego.
3. Opracowanie procedur nadzoru nad dokumentacją i politykami SZCD, w tym zasad przeglądu i aktualizacji planów.
4. Opracowanie zasad komunikacji w sytuacji kryzysowej (wewnętrznej i zewnętrznej, w tym z organami, CSIRT i odbiorcami usług).
5. Opracowanie programu ćwiczeń i testów ciągłości działania.
6. Wsparcie Zamawiającego we wdrożeniu SZCD oraz włączenie SZCD do programu audytów wewnętrznych i przeglądów zarządzania.
7. Szacowany wymiar prac Zamawiający określa na 150–180 roboczogodzin.

1.5. Opracowanie i wdrożenie planów ciągłości działania (BCP) i odtwarzania po awarii (DRP)

Przedmiotem usługi jest opracowanie planów ciągłości działania (BCP) oraz planów odtwarzania po awarii (DRP) dla systemów teleinformatycznych Zamawiającego, w ramach SZCD (poz. 1.4).

1. Analiza wpływu na działalność (BIA):
   a) identyfikacja kluczowych procesów Zamawiającego (w szczególności uzdatnianie i dostarczanie wody, odbiór i oczyszczanie ścieków, obsługa klientów i rozliczenia) oraz wspierających je systemów IT i OT,
   b) określenie dopuszczalnego czasu niedostępności (MTPD), docelowego czasu odtworzenia (RTO) i dopuszczalnej utraty danych (RPO),

c) opracowanie rejestru usług IT i ich zależności.

2. Plany BCP dla kluczowych procesów, zawierające co najmniej: kryteria aktywacji, role i odpowiedzialności, rozwiązania obejściowe (w tym ręczne prowadzenie procesów technologicznych przy niedostępności systemów sterowania), komunikację oraz powrót do normalnej pracy.
3. Plany DRP dla systemów teleinformatycznych, zawierające co najmniej:
   a) procedury odtwarzania infrastruktury klastra HA, macierzy dyskowych, maszyn wirtualnych i usług (w tym Active Directory) z kopii zapasowych z systemu z poz. 3.3, serwera NAS z poz. 3.7 oraz nośników taśmowych z poz. 3.5,
   b) procedury odtwarzania konfiguracji urządzeń sieciowych i UTM,
   c) procedury odtwarzania stacji operatorskich, programów sterowników i systemów SCADA,
   d) kolejność odtwarzania zgodną z wynikami BIA oraz listy kontaktowe.
4. Przeprowadzenie, wspólnie z Zamawiającym, co najmniej jednego ćwiczenia sztabowego (tabletop) BCP oraz jednego testu odtworzenia wybranego systemu wg DRP, wraz z raportem z wnioskami i aktualizacją planów.
5. Szacowany wymiar prac Zamawiający określa na 140–190 roboczogodzin.

Obszar kompetencyjny

Wymagania wspólne dla szkoleń (poz. 2.1–2.3):

1. Program każdego szkolenia oraz scenariusze testów socjotechnicznych Wykonawca przedstawi do akceptacji Zamawiającego co najmniej 10 dni roboczych przed ich realizacją.
2. Treść szkoleń musi uwzględniać specyfikę przedsiębiorstwa wodociągowo-kanalizacyjnego, w tym zagrożenia dla systemów OT, oraz – po ich opracowaniu – dokumentację SZBI, SZCD i plany BCP/DRP Zamawiającego (poz. 1.1, 1.4 i 1.5).
3. Szkolenia stacjonarne odbędą się w siedzibie Zamawiającego, w dni robocze, w godzinach pracy Zamawiającego. Zamawiający zapewni salę z ekranem lub rzutnikiem.
4. Materiały szkoleniowe w języku polskim, zrozumiałe dla osób bez przygotowania technicznego, Wykonawca przekaże każdemu uczestnikowi najpóźniej w dniu szkolenia (dopuszczalna forma elektroniczna PDF), a Zamawiającemu – również prezentacje wykorzystane w trakcie szkolenia.
5. Każdy uczestnik otrzyma imienny certyfikat lub zaświadczenie ukończenia szkolenia. Wykonawca prowadzi dokumentację szkoleń: listy obecności oraz listy odbioru certyfikatów.
6. Szkolenia muszą być realizowane z poszanowaniem zasad równości szans i niedyskryminacji, w tym dostępności dla osób z niepełnosprawnościami.
7. Zamawiający nie ponosi kosztów dojazdu, zakwaterowania i wyżywienia Wykonawcy.

2.1. Podstawowe szkolenia z cyberbezpieczeństwa dla pracowników IT/OT

Przedmiotem usługi jest przeprowadzenie podstawowych szkoleń budujących świadomość cyberzagrożeń dla wszystkich pracowników Zamawiającego obsługujących systemy IT i OT (31 osób), w formie szkoleń stacjonarnych w siedzibie Zamawiającego.

Zakres i organizacja szkoleń

1. Zakres tematyczny co najmniej:
   a) podstawowe pojęcia cyberbezpieczeństwa i rodzaje ataków: phishing, malware i ransomware, socjotechnika, spoofing, ataki telefoniczne i SMS,
   b) bezpieczna praca z pocztą elektroniczną, hasłami i uwierzytelnianiem wieloskładnikowym, urządzeniami mobilnymi, nośnikami wymiennymi oraz praca zdalna,
   c) cyberhigiena i bezpieczne korzystanie z Internetu,
   d) ochrona danych osobowych – obowiązki pracownika,
   e) zagrożenia dla systemów sterowania (OT) w przedsiębiorstwie wodociągowym i zasady bezpiecznej pracy na stacjach operatorskich,
   f) rozpoznawanie i zgłaszanie incydentów bezpieczeństwa,
   g) obowiązki pracowników wynikające z wdrożonego SZBI (polityki, procedury, klasyfikacja informacji).
2. Szkolenie stacjonarne w siedzibie Zamawiającego, przeprowadzone jednorazowo dla każdej grupy uczestników (w grupach liczących nie więcej niż 15 osób), w wymiarze co najmniej 4 godzin zegarowych, po przekazaniu Wykonawcy przez Zamawiającego projektu dokumentacji SZBI. Szkolenie obejmuje zakres z pkt 1 oraz ćwiczenia praktyczne z rozpoznawania phishingu i zgłaszania incydentów zgodnie z wdrażanymi procedurami, zakończone testem wiedzy.
3. Opracowanie i przekazanie Zamawiającemu planu regularnych szkoleń z cyberbezpieczeństwa na kolejne 2 lata, w tym dla nowo zatrudnianych pracowników.
4. Wskaźnikiem realizacji jest liczba przeszkolonych użytkowników (31 osób), potwierdzona certyfikatami ukończenia szkolenia.

2.2. Szkolenie wraz z testami socjotechnicznymi (phishing)

Przedmiotem usługi jest przeprowadzenie testów socjotechnicznych weryfikujących świadomość zagrożeń i reakcje personelu Zamawiającego oraz szkoleń powiązanych z ich wynikami.

1. Przeprowadzenie co najmniej 4 kampanii phishingowych skierowanych do wszystkich pracowników posiadających konto poczty elektronicznej, w odstępach czasowych uzgodnionych z Zamawiającym, o zróżnicowanym poziomie trudności i scenariuszach dostosowanych do specyfiki Zamawiającego.
2. Przeprowadzenie testów vishing (próby wyłudzenia informacji drogą telefoniczną) oraz smishing (wiadomości SMS) wobec grupy pracowników wskazanej przez Zamawiającego.
3. Scenariusze, listy odbiorców i harmonogram testów wymagają uprzedniej akceptacji Zamawiającego. Testy nie mogą powodować instalacji złośliwego oprogramowania, pozyskiwania rzeczywistych haseł ani przetwarzania danych w zakresie wykraczającym poza niezbędny do analizy wyników.
4. Po każdej kampanii Wykonawca przekaże raport zawierający co najmniej: liczbę wysłanych wiadomości, otwarć, kliknięć, wprowadzonych danych oraz zgłoszeń podejrzanej wiadomości,

z porównaniem wyników kolejnych kampanii. Raporty prezentują wyniki w sposób zbiorczy, bez publicznego wskazywania poszczególnych pracowników.

5. Osoby, które uległy atakowi testowemu, otrzymają od Wykonawcy krótki materiał doszkalający (np. instrukcję lub nagranie), a zastosowane techniki zostaną omówione na szkoleniu podsumowującym z pkt 6.
6. Po zakończeniu testów Wykonawca przeprowadzi w siedzibie Zamawiającego szkolenie (co najmniej 2 godziny zegarowe) omawiające wyniki testów, zastosowane techniki socjotechniczne i sposoby ich rozpoznawania, oraz przekaże raport końcowy z rekomendacjami.

2.3. Szkolenie kadry zarządzającej z SZBI i świadomości cyberbezpieczeństwa

Przedmiotem usługi jest przeprowadzenie dwudniowych warsztatów dla kadry zarządzającej Zamawiającego (maks. 10 osób), w siedzibie Zamawiającego, w wymiarze co najmniej 6 godzin zegarowych dziennie.

1. Zakres tematyczny co najmniej:
   a) znaczenie cyberbezpieczeństwa w przedsiębiorstwie wodociągowo-kanalizacyjnym – zagrożenia i ryzyka dla obszaru IT i OT, przykłady incydentów w sektorze wodnym,
   b) obowiązki podmiotu i kierownictwa wynikające z ustawy o krajowym systemie cyberbezpieczeństwa i dyrektywy NIS2, w tym odpowiedzialność kierownictwa,
   c) SZBI wg ISO/IEC 27001:2023 lub normy równoważnej – cykl PDCA, role i odpowiedzialność kierownictwa w ustanawianiu, utrzymaniu i przeglądzie systemu,
   d) zarządzanie ryzykiem – akceptacja ryzyka i decyzje dotyczące postępowania z ryzykiem,
   e) zarządzanie dokumentacją SZBI, SZCD oraz planami BCP i DRP – nadzór, przeglądy i doskonalenie, z wykorzystaniem aplikacji z poz. 1.2,
   f) reagowanie na incydenty i współpraca z CSIRT – ścieżki decyzyjne i komunikacja,
   g) ćwiczenie sztabowe (tabletop) – scenariusz incydentu dotyczącego systemów OT lub ataku ransomware, z podejmowaniem decyzji zarządczych.
2. Warsztaty zostaną przeprowadzone po opracowaniu dokumentacji SZBI (poz. 1.1), tak aby co najmniej połowa programu odnosiła się do dokumentacji Zamawiającego.

Rozwiązania równoważne

1. Zamawiający dopuszcza rozwiązania równoważne. Ogólne zasady równoważności rozwiązań:
   a. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
   b. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.

c. Użycie w opisie przedmiotu zamówienia nazw rozwiązań, materiałów i urządzeń służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań.

d. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne.

e. Brak określenia „minimum" oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.

f. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.

g. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.

h. Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic niewpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane.

Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.

i. Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych (zwana dalej ustawą), Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych takich samych lub lepszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów / produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia,

dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania.