Zamawiający: Gmina Lubartów

ul. Lubelska 18A, 21-100 Lubartów, NIP: 7141996904 REGON: 431019951 tel.: 81 855 35 86, email: ug@gmina-lubartow.pl

Numer sprawy: ZP.271.7.2027.RF

ZAŁĄCZNIK 1B DO SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI 2

dla zamówienia o wartości nieprzekraczającej 216 000,00 euro, co stanowi równowartość kwoty 930 960,00 złotych pod nazwą

„ZWIĘKSZENIE POZIOMU CYBERBEZPIECZEŃSTWA WODOCIĄGÓW W GMINIE LUBARTÓW”

Zamówienie realizowane jest w ramach projektu grantowego pod nazwą „Cyberbezpieczne Wodociągi” – Krajowy Plan Odbudowy i Zwiększania Odporności finansowany ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności, Inwestycja C3.1.1. Cyberbezpieczńsowto – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Cyberbezpieczeństwo – Cyberbezpieczne Wodociągi.

Podpisane elektronicznie przez Marek Adam Woźniak (Certyfikat kwalifikowany) w dniu 2026-11-09.

Zamawiający określa, że przedmiotem niniejszego postępowania w części 2 o udzielenie zamówienia jest realizacja dostawa sprzętów oraz oprogramowania. Zamówienie realizowane jest zgodnie założeniami projektu grantowego pod nazwą „Cyberbezpieczne Wodociągi" – Krajowy Plan Odbudowy i Zwiększania Odporności finansowany ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności, Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Cyberbezpieczeństwo – Cyberbezpieczne Wodociągi.

Niniejszy dokument obejmuje wymagania dotyczące serwera, pamięci masowej, sieci LAN i WiFi, zabezpieczeń sieciowych, zasilania awaryjnego, oprogramowania bezpieczeństwa oraz szafy rack. Szczegółowy zakres dostawy i wymagania minimalne określono w rozdziałach poniżej.

Zakres dokumentu

Rozdział	Przedmiot zamówienia
1	Serwer fizyczny z oprogramowaniem do wirtualizacji
2	Serwer NAS z dyskami
3	Zestaw sieciowy LAN i WiFi
4	System bezpieczeństwa sieciowego
5	Zasilacze awaryjne UPS 3000 VA i 3000 W
6	Zasilacze awaryjne UPS 900 VA i 480 W
7	Skanowanie podatności systemów i sieci
8	Ochrona urządzeń końcowych z EDR i zarządzaniem poprawkami
9	Centralny system zarządzania i analizy logów wraz z usługą wdrożenia

1. Serwer fizyczny z oprogramowaniem do wirtualizacji

Zamawiający wymaga dostawy serwera fizycznego do zainstalowania rozwiązań z zakresu bezpieczeństwa wraz z oprogramowaniem do wirtualizacji, spełniającego wszystkie poniższe wymagania.

Parametr lub funkcja	Wymagania minimalne
Obudowa	• Rack o wysokości max 1U lub wersja tower lub rack • Min. 8 slotów na dyski 2.5” • Możliwość wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne – serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android / Apple iOS) przy użyciu jednego z protokołów BLE / WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania jednego procesora. • Obsługa procesorów 144 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. • Płyta główna powinna obsługiwać do 4TB pamięci RAM.
Procesor	• Zainstalowany jeden procesor min. 16-rdzeniowe, min. 2.3GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 199 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji jednoprocesorowej.
Pamięć RAM	• 64 GB DDR5 RDIMM 6400MT/s
Kontroler RAID	• Sprzętowy kontroler dyskowy • Możliwość konfiguracji poziomów RAID: 0, 1, 10 (oraz tryb Non-RAID). • Wsparcie dla dysków samoszyfrujących • Obsługa dysków 12Gbps SAS3, 6Gbps SATA3/SAS2 oraz NVMe (Gen3 i Gen4)
Pamięć masowa	• Możliwość instalacji dysków SATA/SAS. • Zainstalowane 4 dyski SAS o pojemności min. 2.4 TB każdy, 12Gbps, 2,5“ Hot-Plug.
Gniazda rozszerzeń	• Minimum 2x slot PCIe x16 generacji 5. Dodatkowo min. 1 sloty w standardzie OCP 3.0 (x16) przeznaczone dla kart sieciowych.
Interfejsy sieciowe/FC/SAS	• 4 interfejsy sieciowe 10/25 GbE SFP28 (porty nie mogą być osiągnięte poprzez zainstalowanie karty w wymaganych slotach PCIe). • 1 przewód typu DAC, SFP+ to SFP+, 10GbE 3 m

Wbudowane porty	• 4 porty USB w tym min:
	  • 1 port USB 2.0 Type-C dostępne z przodu obudowy
	  • 2 porty USB 3.1 typ A dostępne z tyłu obudowy
	  • 1 port USB 3.0 dostępne wewnątrz obudowy
	• Port VGA z tyłu obudowy
	Nie dopuszcza się stosowania kart PCIe.

Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200.
Zasilanie	• Redundantne, Hot-Plug min. 800W klasy Titanium
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych (dotyczy wyłącznie obudowy typu rack)

Parametr lub funkcja	Wymagania minimalne
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 V3 • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Bezpieczeństwo — ciąg dalszy	• Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).

Diagnostyka	• System powiadomień LED o funkcjonalności:
	  • Informacji o statusie zasilania serwera
	  • Pomocy w zlokalizowaniu serwera
	  • Informacji o błędach, powiązanej z logami systemowymi.

Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer • integracja z Active Directory • możliwość obsługi przez sześciu administratorów jednocześnie • Wsparcie dla automatycznej rejestracji DNS • wsparcie dla LLDP • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. • Monitorowanie zużycia dysków SSD • Automatyczne zgłaszanie alertów do centrum serwisowego producenta
Karta Zarządzania — ciąg dalszy	• Automatyczne update firmware dla wszystkich komponentów serwera • Możliwość przywrócenia poprzednich wersji firmware • Możliwość eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON

Parametr lub funkcja	Wymagania minimalne
	• Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych • Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram. • Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera • kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania • możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień • możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera • możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer • możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe Możliwość rozszerzenia funkcjonalności o: • możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych jak Splunk, Grafana, ElasticSearch
Karta Zarządzania — ciąg dalszy	• możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej • Automatyczne odświeżanie certyfikatów SSL • monitorowanie przepływu powietrza na bieżąco (w CFM)
Oprogramowanie do zarządzania	Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: Zainstalowane oprogramowanie producenta do zarządzania, spełniające poniższe wymagania: • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF • Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. • Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska
Oprogramowanie do zarządzania — ciąg dalszy	• Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB • Przesyłanie alertów „as-is” do innych konsol firm trzecich

Parametr lub funkcja	Wymagania minimalne
	• Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
Oprogramowanie do zarządzania — ciąg dalszy	• Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. • Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • Zdalne uruchamianie diagnostyki serwera. • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.
Oprogramowanie do zarządzania — ciąg dalszy	Oprogramowanie dostarczone jako wirtualny appliance dla KVM, ESXi i Hyper-V.

Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:
	• Monitoring:
	  • ilość podłączonych oraz rozłączonych systemów
	  • stan podłączonych urządzeń
	  • informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów
	  • Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia
	  • informacje o statusie gwarancji dla poszczególnych urządzeń
	  • informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń
	  • informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.
	  • Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych

Oprogramowanie do monitorowania — ciąg dalszy	• Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. • Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. • Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. • Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. • Monitoring parametrów serwerów z informacją o minimum:

Parametr lub funkcja	Wymagania minimalne
	• Obciążeniu procesora • Zużyciu pamięci RAM • Temperaturze procesorów • Temperaturze powietrza wlotowego • Zużyciu prądu • Zmianach w fizycznej konfiguracji serwera • Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Monitoring parametrów pamięci masowych z informacją o minimum: • Opóźnieniach • IOPS • Przepustowości • Utylizacji kontrolerów • Pojemność całkowita i dostępna
Oprogramowanie do monitorowania — ciąg dalszy	• Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. • Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata • Informacje o poziomie redukcji danych • Informacje o statusie replikacji oraz snapshotów • Monitoring parametrów przełączników sieciowych z informacją o minimum: • Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny • Stanie komponentów: zasilacze, wentylatory • Podłączonych hostach • Ilości i statusu portów • Utylizacji procesora • Utylizacji poszczególnych portów • Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware • możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania
Oprogramowanie do monitorowania — ciąg dalszy	• możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania • możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania • możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania • możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty • Możliwość generowania raportów dla serwerów zawierających informację o: • Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej • Średnim obciążeniu: procesorów, pamięci RAM, IO, • Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:

Parametr lub funkcja	Wymagania minimalne
	• Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji
Oprogramowanie do monitorowania — ciąg dalszy	• Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo • Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. • Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. • Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. • Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia • Urządzenie Producenta dostarczane w ramach postępowania • Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent
Oprogramowanie do monitorowania — ciąg dalszy	• Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności • Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne • Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
System operacyjny/dodatkowe oprogramowanie	• Dostarczony system operacyjny przez wzgląd na kompatybilność z obecnie posiadaną infrastrukturą. • Licencja na Windows Server 2025 Standard, licencja pokrywająca wszystkie fizyczne rdzenie w serwerze, pozwalająca na uruchomienie oprogramowania na minimum 2 maszynach wirtualnych. • Nośnik CD/DVD umożliwiający downgrade do wersji Windows Server 2022 Stadnard; • Licencje User Call 2025 – 10 sztuk
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE.
Certyfikaty — ciąg dalszy	• Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku.

Parametr lub funkcja	Wymagania minimalne
Certyfikaty — ciąg dalszy	• Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.
Dokumentacja	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. • Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.

Warunki gwarancji — ciąg dalszy	• Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
	• Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:
	  • Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.
	  • Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.
	  • Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.

Warunki gwarancji — ciąg dalszy	• Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. • Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty

2. Serwer NAS z dyskami

2.1 Parametry sprzętowe

Parametr lub funkcja	Wymagania minimalne
Typ urządzenia	Serwer NAS w obudowie wolnostojącej (Tower).
Procesor	Procesor x86-64, co najmniej 4 rdzenie i 8 wątków, taktowanie co najmniej 2,2 GHz.
Szyfrowanie sprzętowe	Sprzętowe przyspieszanie szyfrowania AES.
Pamięć RAM	Co najmniej 8 GB pamięci DDR4 ECC SODIMM, z możliwością rozbudowy do co najmniej 32 GB.
Zatoki na dyski	Co najmniej 5 zatok na dyski SATA 3,5 cala HDD lub 2,5 cala SSD, z obsługą hot-swap.
Rozbudowa liczby zatok	Możliwość rozbudowy do co najmniej 15 zatok łącznie przez podłączenie maksymalnie dwóch kompatybilnych jednostek rozszerzających.
Gniazda M.2	Co najmniej 2 gniazda M.2 2280 NVMe do tworzenia pamięci podręcznej SSD lub puli pamięci masowej, zgodnie z listą kompatybilności i warunkami producenta.
Dyski SSD w zestawie	2 dyski SSD M.2 2280 NVMe o pojemności co najmniej 400 GB każdy, zgodne z listą kompatybilności producenta dla oferowanego NAS i przeznaczonego zastosowania.
Dyski HDD w zestawie	3 dyski HDD SATA 3,5 cala o pojemności co najmniej 16 TB każdy, przeznaczone do pracy w serwerach NAS i zgodne z listą kompatybilności producenta dla oferowanego NAS.
Porty USB	Co najmniej 2 porty USB 3.2 Gen 1.
Porty rozszerzeń	Co najmniej 2 dedykowane porty rozszerzeń w formacie USB Type-C do podłączania kompatybilnych jednostek rozszerzających.
Porty sieciowe	Co najmniej 2 porty RJ45 2,5 GbE.
Funkcje zasilania	Wake on LAN oraz możliwość zaplanowanego włączania i wyłączania urządzenia.
Chłodzenie	Co najmniej 2 wentylatory o wymiarach 92 × 92 mm.
Zasilacz	Zasilacz o mocy znamionowej nie większej niż 120 W, dostarczony wraz z urządzeniem.

2.2 Serwer NAS – oprogramowanie i gwarancja

Parametr lub funkcja	Wymagania minimalne
System plików	Obsługa Btrfs oraz ext4 dla dysków wewnętrznych.
Macierze dyskowe	Obsługa co najmniej Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 oraz elastycznej macierzy umożliwiającej wykorzystanie dysków o różnej pojemności.
Pamięć masowa	Obsługa pojedynczego wolumenu do co najmniej 108 TB. Możliwość udostępniania zasobów blokowych iSCSI oraz wykonywania migawek i klonowania obsługiwanych jednostek LUN.
Usługi plikowe	Obsługa SMB2/SMB3, NFS, FTP, SFTP, WebDAV i rsync. Integracja z listami kontroli dostępu Windows ACL.
Użytkownicy i zasoby	Obsługa co najmniej 1024 kont użytkowników, 256 grup oraz 256 folderów współdzielonych.
Bezpieczeństwo	Zapora sieciowa, szyfrowanie folderów współdzielonych, połączenia HTTPS oraz automatyczne blokowanie prób nieautoryzowanego logowania.

Parametr lub funkcja	Wymagania minimalne
Ochrona danych	Obsługa migawek Btrfs, niezmiennych migawek oraz folderów WORM (Write Once, Read Many), zgodnie z warunkami producenta.
Kopie zapasowe	Dostępne bez dodatkowych opłat licencyjnych oprogramowanie do centralnego tworzenia kopii zapasowych komputerów, serwerów i maszyn wirtualnych, w środowiskach wspieranych przez producenta.
Kopie danych NAS	Możliwość tworzenia kopii danych na nośnikach lokalnych, innych serwerach i w obsługiwanych chmurach publicznych. Oprogramowanie bez dodatkowych opłat licencyjnych; koszt usług chmurowych nie jest objęty tym wymogiem.
Synchronizacja i współpraca	Dostępne bez opłat cyklicznych aplikacje do synchronizacji i wersjonowania plików oraz współpracy nad dokumentami, arkuszami i prezentacjami przez przeglądarkę. Obsługa klientów Windows i macOS oraz dostępu mobilnego Android/iOS.
Wysoka dostępność	Możliwość utworzenia klastra HA z dwóch identycznych, zgodnie skonfigurowanych urządzeń, z replikacją danych i automatycznym przełączeniem usług w przypadku awarii, zgodnie z warunkami producenta. Wymóg dotyczy obsługi funkcji, a nie dostawy drugiego urządzenia ani uruchomienia klastra.
Dokumentacja i gwarancja	Dokumentacja w języku polskim lub angielskim. Gwarancja na jednostkę NAS przez co najmniej 3 lata.

Wymagania określają obsługiwane możliwości urządzenia. Nie oznaczają jednoczesnego uruchomienia wszystkich funkcji. Zestaw musi obejmować 2 dyski SSD M.2 NVMe po co najmniej 400 GB oraz 3 dyski HDD SATA po co najmniej 16 TB. Rozbudowa pamięci RAM i dodatkowe jednostki rozszerzające nie są wymagane w ramach powyższych zapisów.

3. Zestaw sieciowy LAN i WiFi

Zamawiający wymaga dostawy urządzeń spełniających poniższe wymagania minimalne.

Parametr lub funkcja	Wymagania minimalne
Przedmiot dostawy	1 zestaw sieciowy obejmujący: 1 przełącznik zarządzalny PoE+, 1 kontroler sprzętowy, 10 wewnętrznych punktów dostępowych oraz 2 zewnętrzne punkty dostępowe. Łącznie 14 urządzeń.
Kompletność i współpraca	Wszystkie urządzenia muszą być fabrycznie nowe, kompletne i wzajemnie kompatybilne. Kontroler musi umożliwiać centralne zarządzanie dostarczonym przełącznikiem oraz wszystkimi 12 punktami dostępowymi.
Oprogramowanie	Należy dostarczyć oprogramowanie i uprawnienia niezbędne do lokalnego korzystania z wymaganych funkcji bez obowiązkowej subskrypcji. Dostęp chmurowy nie może być warunkiem zarządzania lokalnego.
Wyposażenie	Należy dostarczyć przewód zasilający przełącznik, uchwyty do jego montażu w szafie rack oraz zestawy montażowe punktów dostępowych. Kontroler i punkty dostępowe muszą umożliwiać zasilanie z dostarczonego przełącznika.
Dokumentacja i identyfikacja	Instrukcje w języku polskim lub angielskim, dostęp do aktualizacji producenta oraz wykaz modeli i wersji sprzętowych. Urządzenia przeznaczone do użytkowania w Polsce, z oznakowaniem CE i deklaracją zgodności UE.
Gwarancja	Wymagany okres gwarancji: 12 miesięcy.

3.1 Przełącznik zarządzalny PoE+ – 1 sztuka

Parametr lub funkcja	Wymagania minimalne
Liczba	1 sztuka.
Porty dostępowe	Co najmniej 48 portów RJ45 10/100/1000 Mb/s, wszystkie z obsługą PoE IEEE 802.3af/at.
Porty uplink	Co najmniej 4 niezależne sloty SFP+ 10 Gb/s, dodatkowe względem portów RJ45.
Zasilanie PoE	Łączny budżet co najmniej 500 W; do 30 W na pojedynczym porcie zgodnie z IEEE 802.3at. Możliwość jednoczesnego zasilania wszystkich dostarczonych punktów dostępowych i kontrolera.
Wydajność	Przepustowość przełączania co najmniej 176 Gb/s; szybkość przekazywania pakietów co najmniej 130,9 mln pakietów/s; tablica MAC co najmniej 16 tys. wpisów.
Funkcje sieciowe	VLAN IEEE 802.1Q, agregacja łączy LACP, STP/RSTP/MSTP, IGMP Snooping, routing statyczny, QoS z priorytetyzacją 802.1p/DSCP.
Bezpieczeństwo	Listy ACL dla MAC i IP, uwierzytelnianie 802.1X, Port Security, DHCP Snooping oraz ograniczanie ruchu rozgłoszeniowego (Storm Control).
Zarządzanie	Lokalny interfejs WWW, CLI przez SSH, SNMP oraz centralne zarządzanie z dostarczonego kontrolera. Kopia zapasowa i odtwarzanie konfiguracji.
Obudowa i zasilanie	Obudowa do szafy rack 19 cali, wysokość maksymalnie 1U. Zasilanie sieciowe 100–240 V AC, 50/60 Hz.

3.2 Kontroler sprzętowy – 1 sztuka

Parametr lub funkcja	Wymagania minimalne
Liczba i typ	1 sztuka. Dedykowany kontroler sprzętowy z wbudowanym oprogramowaniem; praca bez dodatkowego komputera lub serwera.
Skala zarządzania	Obsługa co najmniej 100 punktów dostępowych oraz 20 kompatybilnych przełączników. Centralne zarządzanie całym dostarczonym zestawem.
Interfejsy	Co najmniej 2 porty Ethernet 10/100 Mb/s lub szybsze oraz 1 port USB do wykonywania kopii zapasowych na nośniku zewnętrznym.
Zasilanie	Zasilanie PoE zgodne z IEEE 802.3af lub IEEE 802.3at, kompatybilne z dostarczonym przełącznikiem.
Konfiguracja	Wykrywanie i przyłączanie urządzeń, konfiguracja grupowa, grupowe aktualizacje firmware oraz zarządzanie wieloma lokalizacjami.
Monitorowanie	Podgląd stanu urządzeń i klientów, statystyki ruchu, zdarzenia i alarmy oraz prezentacja topologii sieci.
Dostęp administracyjny	Lokalne zarządzanie przez przeglądarkę, konta administratorów z przydziałem uprawnień; możliwość zdalnego dostępu przez usługę producenta i aplikację mobilną.
Utrzymanie	Wykonywanie i odtwarzanie kopii konfiguracji; harmonogram kopii zapasowych oraz restartów. Wymagane funkcje muszą działać z oferowanymi wersjami sprzętu i firmware.

3.3 Wewnętrzne punkty dostępowe – 10 sztuk

Parametr lub funkcja	Wymagania minimalne
Liczba i przeznaczenie	10 sztuk. Punkty dostępowe do pracy wewnątrz budynków, z antenami wewnętrznymi i zestawem do montażu na suficie lub ścianie.
Standard i pasma	Wi-Fi 6 (IEEE 802.11ax), jednoczesna praca w pasmach 2,4 GHz i 5 GHz; zgodność z 802.11a/b/g/n/ac.
Parametry radiowe	Co najmniej 2×2 MIMO w każdym paśmie; nominalna szybkość PHY co najmniej 574 Mb/s w paśmie 2,4 GHz i 1201 Mb/s w paśmie 5 GHz. Obsługa OFDMA i MU-MIMO.
Port sieciowy	Co najmniej 1 port RJ45 10/100/1000 Mb/s, wykorzystywany do transmisji danych i zasilania PoE.
Funkcje Wi-Fi	Co najmniej 16 SSID łącznie, w tym 8 na każde pasmo; mapowanie SSID do VLAN, izolacja klientów, sterowanie pasmem, regulacja mocy i wybór kanału.
Bezpieczeństwo	WPA2 i WPA3, uwierzytelnianie 802.1X oraz obsługa zewnętrznego serwera RADIUS.
Zarządzanie i mobilność	Centralne zarządzanie z dostarczonego kontrolera, monitoring klientów i statystyk; obsługa roamingu wspomaganego przez kontroler oraz bezprzewodowej sieci mesh.
Zasilanie	PoE IEEE 802.3af lub IEEE 802.3at.
Warunki pracy	Zakres temperatur pracy obejmujący co najmniej 0°C do +40°C.

3.4 Zewnętrzne punkty dostępowe – 2 sztuki

Parametr lub funkcja	Wymagania minimalne
Liczba i przeznaczenie	2 sztuki. Punkty dostępowe do pracy na zewnątrz, z zestawami do montażu na ścianie lub słupie.

Parametr lub funkcja	Wymagania minimalne
Standard i pasma	Wi-Fi 6 (IEEE 802.11ax), jednoczesna praca w pasmach 2,4 GHz i 5 GHz; zgodność z 802.11a/b/g/n/ac.
Parametry radiowe	Co najmniej 2×2 MIMO w każdym paśmie; nominalna szybkość PHY co najmniej 574 Mb/s w paśmie 2,4 GHz i 1201 Mb/s w paśmie 5 GHz. Obsługa OFDMA i MU-MIMO.
Port sieciowy	Co najmniej 1 port RJ45 10/100/1000 Mb/s, wykorzystywany do transmisji danych i zasilania PoE.
Funkcje Wi-Fi	Co najmniej 16 SSID łącznie, w tym 8 na każde pasmo; mapowanie SSID do VLAN, izolacja klientów, sterowanie pasmem, regulacja mocy i wybór kanału.
Bezpieczeństwo	WPA2 i WPA3, uwierzytelnianie 802.1X oraz obsługa zewnętrznego serwera RADIUS.
Zarządzanie i mobilność	Centralne zarządzanie z dostarczonego kontrolera, monitoring klientów i statystyk; obsługa roamingu wspomaganego przez kontroler oraz bezprzewodowej sieci mesh.
Zasilanie	PoE IEEE 802.3at.
Odporność i warunki pracy	Obudowa o klasie szczelności co najmniej IP67. Zakres temperatur pracy obejmujący co najmniej −30°C do +70°C.

4. System bezpieczeństwa sieciowego

Ilość: 4 sztuki.

Parametr lub funkcja	Wymagania minimalne
Wymagania Ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. 1. Ochrony w warstwie aplikacji. 1. Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie:	1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: 1. 5 portami Gigabit Ethernet RJ-45. 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie AC.
Parametry wydajnościowe:	1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 1 Gbps. 6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

Parametr lub funkcja	Wymagania minimalne
Funkcje Systemu Bezpieczeństwa:	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN . 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 11. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.
Funkcje Systemu Bezpieczeństwa: — ciąg dalszy	12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
Polityki, Firewall	1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: 1. Translację jeden do jeden oraz jeden do wielu. 1. Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 2. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 3. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP. 4. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 5. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 6. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. 1. Amazon Web Services (AWS).
Polityki, Firewall — ciąg dalszy	1. Microsoft Azure. 1. Cisco ACI. 1. Google Cloud Platform (GCP). 1. OpenStack. 1. VMware NSX. 1. Kubernetes.
Połączenia VPN	1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: 1. Wsparcie dla IKE v1 oraz v2. 1. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). 1. Obsługa protokołu Diffie-Hellman grup 19, 20.

Parametr lub funkcja	Wymagania minimalne
	1. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. 1. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. 1. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. 1. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. 1. Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. 1. Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. 1. Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. 1. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. 1. Mechanizm „Split tunneling" dla połączeń Client-to-Site.
Połączenia VPN — ciąg dalszy	2. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

Parametr lub funkcja	Wymagania minimalne
Ochrona przed malware — ciąg dalszy	7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej. 8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
Ochrona przed atakami	1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
Kontrola WWW	1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.

Parametr lub funkcja	Wymagania minimalne
Kontrola WWW — ciąg dalszy	8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: 1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. 1. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. 1. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. 3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
Zarządzanie — ciąg dalszy	7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Parametr lub funkcja	Wymagania minimalne
Testy wydajnościowe oraz funkcjonalne	1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni.)
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, Weryfikacja zgodności konfiguracji z dobrymi praktykami producenta (audyt konfiguracji i polityk urządzenia) na okres do 31.12.2026 r.
Gwarancja oraz wsparcie	1. Dostarczone rozwiązanie musi być objęte rozszerzonym wsparciem technicznym gwarantującym - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres wymaganej gwarancji.

5. Zasilacze awaryjne UPS (min. 3000 VA i 1950 W)

Przedmiotem zamówienia jest dostawa 2 sztuk jednofazowych zasilaczy awaryjnych UPS o mocy co najmniej 3000 VA i 1950 W, w obudowie wolnostojącej Tower, z akumulatorami wewnętrznymi.

Parametr lub funkcja	Wymagania minimalne
Typ i technologia	Jednofazowy UPS na wejściu i wyjściu, line-interactive (VI), z układem automatycznej regulacji napięcia AVR.
Moc wyjściowa	Co najmniej 3000 VA i 1950 W.
Obudowa	Wolnostojąca typu Tower, przeznaczona do pracy w pozycji pionowej.
Napięcie wejściowe	Znamionowe 230 V AC. Zakres 160–264 V AC, z możliwością rozszerzenia programowego do 145–280 V AC; tolerancja ±2%.
Częstotliwość wejściowa	Znamionowa 50 Hz; zakres 45–55 Hz z tolerancją ±1 Hz.
Napięcie wyjściowe	Znamionowe 230 V AC. Przy pracy bateryjnej: 230 V AC ±5%, przebieg sinusoidalny. Przy pracy sieciowej: kształt przebiegu zgodny z wejściowym.
Przełączenie na baterie	Czas przełączenia na pracę bateryjną poniżej 3 ms.
Gniazda wyjściowe	Co najmniej 4 gniazda PN-E-93201 z podtrzymaniem bateryjnym.
Akumulatory wewnętrzne	W zestawie 4 akumulatory VRLA, każdy o napięciu 12 V i pojemności 7 Ah.
Czas podtrzymania	Z baterii wewnętrznych: co najmniej 3 min przy 1950 W, 4 min przy 1560 W i 8 min przy 975 W, w warunkach określonych przez producenta.
Wymiary obudowy	Nie więcej niż 190 × 165 × 575 mm (wysokość × szerokość × głębokość).

5.1 UPS funkcje oprogramowanie i gwarancja

Parametr lub funkcja	Wymagania minimalne
Zabezpieczenia	Zabezpieczenie przeciwprzepięciowe oraz elektroniczne zabezpieczenia przeciwzwarciowe i przeciążeniowe na wyjściu.
Sygnalizacja	Optyczna, za pomocą diod LED, oraz akustyczna.
Komunikacja	Interfejs USB HID.
Oprogramowanie	Oprogramowanie producenta UPS do monitorowania pracy zasilacza i kontrolowanego zamykania systemu, dostępne do pobrania ze strony producenta.
Zgodność	Oznakowanie CE i dostarczenie deklaracji zgodności UE dla oferowanego urządzenia.
Serwis i gwarancja	Wykonawca zapewni gwarancję co najmniej 24 miesiące na urządzenie i akumulatory oraz obsługę napraw na terenie Polski. Wraz z dostawą przekaże dokument gwarancyjny i informacje o sposobie zgłaszania oraz realizacji napraw.
Dokumentacja	Instrukcja obsługi w języku polskim oraz dostęp do dokumentacji technicznej i oprogramowania producenta.
Identyfikacja produktu	Wykonawca wskaże w ofercie producenta, model i symbol oferowanego UPS oraz przedstawi dokumentację umożliwiającą potwierdzenie wymaganych parametrów.

Zakres dostawy

Dostawa obejmuje 2 kompletne, fabrycznie nowe zasilacze UPS z akumulatorami wewnętrznymi oraz standardowym wyposażeniem producenta niezbędnym do ich uruchomienia i użytkowania.

6. Zasilacze awaryjne UPS (min. 900 VA i 480 W)

Ilość: 2 sztuki.

Parametr lub funkcja	Wymagania minimalne
Przedmiot i ilość	Dostawa 2 sztuk zasilaczy awaryjnych UPS. Poniższe parametry dotyczą każdej sztuki.
Technologia	Line-interactive z automatyczną regulacją napięcia AVR.
Moc wyjściowa	Co najmniej 900 VA mocy pozornej oraz 480 W mocy czynnej.
Obudowa	Wolnostojąca (Tower).
Zasilanie	Jednofazowe, napięcie znamionowe 230 V AC, obsługa częstotliwości 50/60 Hz.
Zakres wejściowy	Praca bez wykorzystania baterii w zakresie napięcia wejściowego co najmniej 140–300 V AC, zgodnie z warunkami producenta.
Przyłącze wejściowe	Gniazdo IEC C14.
Gniazda wyjściowe	Co najmniej 4 gniazda IEC C13 z podtrzymaniem bateryjnym.
Akumulator	Wbudowany, szczelny akumulator kwasowo-ołowiowy VRLA; dostarczony wraz z UPS.
Funkcje baterii	Zimny start, automatyczny test akumulatora oraz zabezpieczenie przed głębokim rozładowaniem.
Komunikacja	Port USB zgodny z HID, umożliwiający komunikację z komputerem i kontrolowane zamknięcie systemu.
Współpraca z systemami	Integracja z mechanizmami zarządzania zasilaniem systemów Windows, macOS i Linux przez USB HID, zgodnie z dokumentacją producenta.
Sygnalizacja	Sygnalizacja stanu pracy diodami LED oraz alarmy dźwiękowe.
Ochrona	Ochrona przeciwprzepięciowa oraz regulacja AVR ograniczająca konieczność użycia baterii przy wahaniach napięcia sieciowego.
Warunki pracy	Praca w pomieszczeniach, w temperaturze od 0°C do +40°C.
Wyposażenie	Każdy UPS z akumulatorem, co najmniej 2 przewodami wyjściowymi IEC–IEC oraz instrukcją instalacji i informacjami bezpieczeństwa.
Zgodność	Oznakowanie CE; zgodność z normami bezpieczeństwa i kompatybilności elektromagnetycznej dla UPS, w szczególności IEC/EN 62040-1 i IEC/EN 62040-2.
Gwarancja	Co najmniej 24 miesiące gwarancji na urządzenie, zgodnie z warunkami producenta.
Stan i identyfikacja	Urządzenia fabrycznie nowe, kompletne. Wykonawca wskaże producenta oraz dokładny model oferowanego UPS.

7. Skanowanie podatności systemów i sieci

7.1 Przedmiot zamówienia i wymagania ogólne

Parametr lub funkcja	Wymagania minimalne
Przedmiot zamówienia	Dostawa subskrypcji systemu do skanowania podatności systemów i urządzeń sieciowych oraz zarządzania wykrytymi podatnościami.
Liczba licencji	22 licencje zasobowe, obejmujące łącznie 22 zasoby sieciowe (hosty/IP), rozliczane zgodnie z zasadami licencjonowania oferowanego rozwiązania.
Okres subskrypcji	Subskrypcja do 31.12.2026 r. Wykonawca przekaże potwierdzenie liczby licencji oraz dat rozpoczęcia i zakończenia subskrypcji.
Zakres funkcjonalny	Skanowanie systemów i urządzeń sieciowych, ewidencja zasobów, zarządzanie podatnościami, obsługa zgłoszeń naprawczych i raportowanie opisane w niniejszym dokumencie.
Model udostępnienia	Usługa chmurowa (SaaS), z centrum danych na terenie Unii Europejskiej oraz dostępem do centralnej konsoli administracyjnej.
Uprawnienia i aktualizacje	Dostęp do konsoli i wszystkich wymaganych funkcji oraz aktualizacje bazy testów podatności przez cały okres subskrypcji.
Sondy skanujące	Możliwość wdrożenia lokalnych sond jako maszyn wirtualnych, dostępnych w formacie OVA lub VHDX. Rejestracja sondy w konsoli centralnej za pomocą tokena administratora.
Konta i role	Możliwość dodawania użytkowników administracyjnych, definiowania ról i przypisywania uprawnień. Obsługa uwierzytelniania dwuskładnikowego.
Integracje	Możliwość integracji z zewnętrznymi systemami obsługi zgłoszeń oraz wysyłania powiadomień przez e-mail, webhooki i integracje z komunikatorami zespołowymi.
Interfejs API	Możliwość zarządzania systemem i integracji z innymi narzędziami za pomocą API.

7.2 Skanowanie systemów i sieci

Parametr lub funkcja	Wymagania minimalne
Liczba skanów	Nieograniczona liczba skanów na żądanie i według harmonogramu w ramach zakupionej liczby licencji; powiadomienia o skanowaniu.
Sondy i lokalizacje	Możliwość wdrażania sond bez odrębnego licencjonowania każdej sondy. Obsługa skanowania licencjonowanych zasobów w wielu segmentach i lokalizacjach z wykorzystaniem wielu sond.
Wybór źródła skanowania	Wybór lokalnej sondy, grupy sond lub zewnętrznej sondy hostowanej w chmurze dostawcy rozwiązania.
Adresacja i wykrywanie	Obsługa IPv6; wykrywanie urządzeń z wyborem portów domyślnych i dodatkowych oraz metod TCP SYN, TCP SYN ACK i ICMP Ping.
Profile	Tworzenie własnych profili i import profili predefiniowanych. Tryby skanowania pełnego, podstawowego oraz wykrywania zasobów.
Zakres testów	Co najmniej 130 tys. testów podatności, aktualizowanych na bieżąco. Możliwość wyboru testów i intensywności skanowania.
Testy opcjonalne	Możliwość uwzględniania wyników o niskim prawdopodobieństwie wystąpienia, hostów nieodpowiadających oraz opcjonalnego skanowania drukarek. Możliwość włączania i wyłączania potencjalnie niebezpiecznych testów oraz testów haseł typu brute force.

Parametr lub funkcja	Wymagania minimalne
Uwierzytelnianie	Możliwość skanowania uwierzytelnionego systemów z rodziny Windows oraz Linux.
Harmonogram	Uruchamianie skanów jednorazowo lub cyklicznie, według harmonogramu administratora.
Wyniki i ewidencja	Automatyczne dodawanie wykrytych urządzeń do ewidencji i przypisywanie tagów na podstawie wykrytych usług, portów i systemu operacyjnego.
Rejestr podatności	Automatyczne przekazywanie wykrytych podatności do centralnego menedżera podatności.
Eksport zadań	Eksport listy zadań skanowania do pliku CSV.

7.3 Zarządzanie zasobami sieciowymi

Parametr lub funkcja	Wymagania minimalne
Dodawanie zasobów	Ręczne dodawanie urządzeń, import z CSV oraz wskazywanie pojedynczych adresów IP, zakresów adresów lub podsieci z maską.
Klasyfikacja biznesowa	Przypisywanie zasobom poziomu wpływu biznesowego: neutralnego, niskiego, średniego lub wysokiego.
Tagi statyczne	Tworzenie tagów statycznych, nadawanie im kolorów i przypisywanie ich do zasobów.
Tagi dynamiczne	Automatyczne przypisywanie tagów na podstawie nazwy grupy zasobów, zakresu IP, otwartych portów lub systemu operacyjnego.
Lista zasobów	Widok obejmujący nazwę zasobu, grupy i tagi, liczbę podatności, najwyższą ważność podatności, wpływ biznesowy, system operacyjny oraz datę dodania i ostatniego wykrycia.
Szczegóły zasobu	Podgląd otwartych portów oraz podatności: aktywnych, ignorowanych i wyłączonych, ze statusem nowa, aktywna, ponownie otwarta lub naprawiona.
Trendy	Prezentacja zmian podatności zasobu według ważności i stanu, z możliwością wyboru okresu i przedziału czasu.
Edycja danych	Edycja nazwy, opisu i wpływu biznesowego zasobu oraz informacji, czy zasób przechowuje dane osobowe.

7.4 Zarządzanie podatnościami i naprawą

Parametr lub funkcja	Wymagania minimalne
Panel główny	Konfigurowalny panel prezentujący podatności sieciowe i zgłoszenia według ważności, także na wykresach słupkowych i kołowych; 10 najważniejszych wyników, ostatnie i nadchodzące skany oraz ostatnie 10 raportów.
Historia i alerty	Prezentacja liczby podatności w czasie dla wszystkich lub wybranych zasobów i tagów, z wyborem okresu i interwału. Monitorowanie zmian oraz powiadomienia i alarmy.
Filtrowanie i widoki	Sortowanie, grupowanie i priorytetyzacja. Własne widoki oraz filtrowanie według stanu, statusu, ważności, tagów, pierwszego i ostatniego wykrycia, kategorii podatności i hosta.
Wyjątki	Wyłączanie i ignorowanie podatności, określanie powodu (wynik fałszywie dodatni, zaakceptowane ryzyko lub brak istotności) oraz terminu wygaśnięcia wyjątku.
Opis podatności	Informacje o wpływie, rozwiązaniu, podsumowaniu, szczegółach technicznych i sposobie wykrycia, odniesieniach, dostępnych poprawkach oraz środkach zaradczych.
Współpraca	Notatki widoczne w raportach oraz możliwość prowadzenia dyskusji między użytkownikami przy obsłudze podatności.

Parametr lub funkcja	Wymagania minimalne
Raport z podatności	Tworzenie raportów bezpośrednio z menedżera podatności po wybraniu jednej lub wielu pozycji.
Zgłoszenia naprawcze	Wbudowany system zgłoszeń. Tworzenie zgłoszenia z podatności, numerowanie, powiadomienia e-mail oraz statusy: otwarte, zamknięte i rozwiązane.
Odpowiedzialność	Powiązanie zgłoszenia z podatnością i zasobem, określenie ważności oraz przypisanie właściciela i terminu realizacji.
Widoki zgłoszeń	Filtrowanie i grupowanie według statusu, typu zasobu, kategorii usługi i skanowania, tagów, terminu, istotności, systemu operacyjnego, portów i właściciela.
Automatyzacja	Możliwość automatycznej obsługi zgłoszeń na podstawie zdefiniowanych reguł.

7.5 Raportowanie

Parametr lub funkcja	Wymagania minimalne
Rodzaje raportów	Raporty skanowania sieci, poprawek, środków zaradczych, porównawcze (delta) oraz zgodności dotyczące wyników skanowania systemów i sieci.
Raporty zgodności	Możliwość odniesienia wyników do regulacji i standardów: Sarbanes–Oxley, HIPAA, ochrony danych osobowych, ISO/IEC 27001, RODO, bezpieczeństwa sieci i informacji oraz PCI DSS, w zakresie technicznej oceny podatności obsługiwanym przez rozwiązanie.
Szablony	Tworzenie i dostosowywanie szablonów raportów opartych na wybranym skanie, bieżących podatnościach lub trendach historycznych.
Treść raportu	Szczegóły i podsumowanie raportu, przegląd podatności oraz lista według podatności i hosta. Wybór szczegółów technicznych, podsumowania, sposobu wykrycia i odniesień; możliwość ograniczenia długości opisu.
Prezentacja wyników	Prezentacja podatności według ważności, statusu i zmian w czasie oraz pięciu najbardziej narażonych kategorii.
Filtry raportów	Selektywny dobór podatności i wykluczeń oraz filtrowanie według systemów operacyjnych, zasobów i podatności.
Raporty okresowe	Możliwość wysyłania pocztą elektroniczną tygodniowych i miesięcznych raportów podsumowujących.

8. Ochrona urządzeń końcowych z EDR i zarządzaniem poprawkami

8.1 Przedmiot zamówienia i licencjonowanie

Parametr lub funkcja	Wymagania minimalne
Przedmiot zamówienia	Dostawa subskrypcji centralnie zarządzanego systemu ochrony urządzeń końcowych EPP z funkcjami wykrywania i reagowania na zagrożenia EDR oraz modułem zarządzania poprawkami systemów operacyjnych i aplikacji (Patch Management).
Liczba licencji	Ochrona 13 urządzeń końcowych. Każde z 13 urządzeń musi być objęte uprawnieniami do EPP, EDR i Patch Management. Jeżeli zarządzanie poprawkami wymaga odrębnej licencji, należy dostarczyć odpowiednie uprawnienia dla wszystkich 13 urządzeń.
Okres subskrypcji	Do 31.12.2026 r. Wszystkie wymagane składniki muszą obowiązywać przez ten sam okres.
Sposób zarządzania	Centralna konsola administracyjna dostępna przez przeglądarkę; wspólne zarządzanie ochroną, incydentami i poprawkami.
Zakres środowiska	Urządzenia końcowe IT oraz stacje robocze i serwery wykorzystywane w OT, wyposażone w system operacyjny i aplikacje wspierane przez oferowane rozwiązanie.
Zgodność systemowa	Obsługa wspieranych przez producenta wersji Windows dla stacji roboczych i serwerów. Dostępność poszczególnych funkcji dla innych systemów operacyjnych musi wynikać z dokumentacji oferowanego rozwiązania.
Prawa i aktualizacje	Prawo do korzystania z wymaganych funkcji, aktualizacji oprogramowania, mechanizmów ochrony i baz sygnatur oraz wsparcia technicznego przez cały okres subskrypcji.

8.2 Ochrona urządzeń końcowych i EDR

Parametr lub funkcja	Wymagania minimalne
Ochrona antymalware	Wykrywanie i blokowanie złośliwego oprogramowania z użyciem sygnatur, analizy zachowania i mechanizmów uczenia maszynowego. Ochrona w czasie rzeczywistym oraz skanowanie na żądanie i według harmonogramu.
Zaawansowane zagrożenia	Mechanizmy wykrywania podejrzanej aktywności procesów, ataków bezplikowych i prób wykorzystania podatności.
Ransomware	Wykrywanie i blokowanie zachowań charakterystycznych dla ransomware.
Polityki ochrony	Centralne tworzenie i przypisywanie polityk do urządzeń i grup, konfigurowanie wykluczeń oraz kontrola stanu agentów i aktualizacji.
Zmniejszanie ryzyka	Ocena podatnych aplikacji i niebezpiecznych konfiguracji oraz priorytetyzacja działań ograniczających ryzyko.
Monitorowanie EDR	Zbieranie i analiza zdarzeń bezpieczeństwa z urządzeń końcowych oraz wykrywanie podejrzanych działań i incydentów.
Analiza incydentów	Prezentacja przebiegu incydentu i powiązań między zdarzeniami; analiza przyczyny źródłowej oraz informacje wspierające ocenę zasięgu ataku.
Korelacja i wyszukiwanie	Korelacja powiązanych zdarzeń z wielu urządzeń oraz wyszukiwanie danych bieżących i historycznych według wskaźników naruszenia bezpieczeństwa (IoC) i kontekstu zdarzeń.
Reakcja	Możliwość izolowania urządzenia od sieci i usuwania izolacji, z zachowaniem komunikacji administracyjnej z systemem ochrony. Blokowanie lub poddawanie kwarantannie wykrytych zagrożeń, zgodnie z możliwościami chronionego systemu operacyjnego.
Raportowanie	Centralny podgląd alertów i incydentów, priorytetyzacja, raporty stanu ochrony oraz informacje o podjętych działaniach.

8.3 Zarządzanie poprawkami

Parametr lub funkcja	Wymagania minimalne
Inwentaryzacja poprawek	Wykrywanie brakujących poprawek systemu operacyjnego i obsługiwanych aplikacji; centralny widok stanu aktualizacji na zarządzanych urządzeniach.
Skanowanie	Skanowanie w poszukiwaniu brakujących poprawek na żądanie oraz według harmonogramu.
Instalacja	Ręczne zlecanie instalacji wybranych poprawek oraz automatyczna instalacja zgodnie z polityką administratora.
Harmonogramy i okna	Możliwość planowania instalacji i stosowania okien serwisowych; dobór terminów osobno dla grup urządzeń.
Kontrola zakresu	Możliwość określania aktualizowanych produktów, wybierania poprawek i stosowania wykluczeń. Zakres obejmuje produkty i wersje znajdujące się na liście wsparcia modułu.
Kontrola restartów	Dla wspieranych urządzeń Windows możliwość zarządzania ponownym uruchomieniem po aktualizacji, w tym odroczenia restartu zgodnie z ustawieniami administratora.

9. Centralny system zarządzania i analizy logów wraz z usługą wdrożenia

9.1 Przedmiot zamówienia i zakres licencji

Parametr lub funkcja	Wymagania minimalne
Przedmiot zamówienia	Dostawa licencji systemu centralnego gromadzenia, analizy, korelacji, wyszukiwania i archiwizacji dzienników zdarzeń z infrastruktury IT oraz źródeł automatyki I SCADA wraz z usługą wdrożenia.
Łączny zakres	Jednoczesne objęcie monitoringiem co najmniej 18 źródeł logów: 10 komputerów PC, 3 serwerów, 4 źródeł automatyki/SCADA oraz 1 dodatkowego stanowiska lub punktu.
Komputery PC	10 stacji roboczych z systemem Windows. Licencja musi uwzględniać kategorię stacji roboczych, jeżeli jest rozliczana oddzielnie.
Serwery	3 serwery jako źródła logów systemowych i aplikacyjnych, w zakresie obsługiwanym przez rozwiązanie.
Automatyka I SCADA	4 źródła logów z urządzeń lub systemów automatyki/SCADA.
Dodatkowy punkt	Uprawnienie do objęcia monitoringiem 1 dodatkowego źródła: stacji roboczej, serwera albo urządzenia/29tanda przekazującego logi. Zestaw licencji ma umożliwiać wykorzystanie tego punktu w odpowiedniej kategorii licencyjnej.
Pakiety licencyjne	Dopuszcza się pakiety o pojemności większej niż wskazany zakres. Suma licencji i ich kategorie muszą pokrywać całą 29 tandardi źródeł bez dodatkowych zakupów. Nie wystarcza sama deklaracja 18 licencji, jeśli nie obejmują one wymaganych typów źródeł.
Okres	Subskrypcja do 31.12.2026 r., obejmująca wszystkie wymagane funkcje, aktualizacje i wsparcie techniczne.
Architektura	Możliwość instalacji centralnego 29tanda w infrastrukturze Zamawiającego, na serwerze fizycznym lub maszynie wirtualnej spełniającej wymagania oprogramowania. Konsola administracyjna dostępna przez przeglądarkę.

9.2 Gromadzenie i analiza logów

Parametr lub funkcja	Wymagania minimalne
Windows Event Log	Centralne zbieranie dzienników bezpieczeństwa, systemowych i aplikacyjnych ze wspieranych stacji i serwerów Windows.
Syslog	Odbiór i analiza komunikatów Syslog z obsługiwanych systemów i urządzeń; obsługa transmisji UDP i TCP.
Kolekcja logów	Obsługa agentowego i bezagentowego zbierania logów, zależnie od rodzaju źródła i udostępnionego mechanizmu.
Logi niestandardowe	Możliwość zbierania lub importu obsługiwanych tekstowych plików dzienników aplikacji oraz definiowania własnych parserów i pól dla niestandardowych formatów.
Normalizacja	Wydobywanie pól umożliwiających analizę m.in. czasu zdarzenia, źródła, hosta, identyfikatora, ważności i użytkownika, jeżeli informacje te występują w logu.
Wyszukiwanie	Wyszukiwanie logów według przedziału czasu, źródła, treści i dostępnych pól; filtrowanie wyników I zapisywanie zapytań.
Korelacja zdarzeń	Wykrywanie powiązań między zdarzeniami na podstawie reguł predefiniowanych i definiowanych przez administratora.
Alerty	Tworzenie alertów na podstawie zdarzeń, progów lub reguł korelacji; powiadomienia e-mail oraz podgląd alertów w konsoli.

Parametr lub funkcja	Wymagania minimalne
Panel monitorowania	Centralny podgląd źródeł, ilości i struktury zdarzeń, alertów oraz stanu odbioru logów.
Analiza incydentów	Możliwość przeglądania zdarzeń w kontekście czasu, użytkownika i źródła oraz przechodzenia do szczegółów zebranych logów.
Raporty	Raporty predefiniowane i własne, harmonogram raportowania oraz eksport co najmniej do PDF I CSV.
Audyt bezpieczeństwa	Raportowanie aktywności użytkowników, prób logowania, zmian i zdarzeń bezpieczeństwa w zakresie informacji udostępnianych przez źródła.

9.3 Archiwizacja, bezpieczeństwo i źródła OT

Parametr lub funkcja	Wymagania minimalne
Archiwizacja	Archiwizacja zebranych logów, konfigurowanie polityk retencji oraz możliwość przywrócenia archiwalnych danych do analizy.
Ochrona archiwów	Możliwość szyfrowania archiwów oraz weryfikacji ich integralności w celu wykrywania zmian.
Dostęp administracyjny	Dostęp do konsoli przez HTTPS, konta administracyjne i role ograniczające dostęp do funkcji lub grup źródeł.
Audyt administratorów	Rejestrowanie działań użytkowników administracyjnych i możliwość przeglądania historii aktywności.
Źródła SCADA	Licencja musi obejmować 4 źródła logów z automatyki/SCADA w ramach łącznej liczby 18 źródeł.

Usługa wdrożenia – wymagana zdalna
usługa wdrożenia centralnego systemu zarządzania i analizy logów – instalacja i konfiguracja systemu, integracja 18 źródeł logów (PC, serwery, automatyka/SCADA), konfiguracja zbierania i archiwizacji zdarzeń, reguł korelacji, al ertów i raportowania oraz weryfikacja poprawności działania system.

Wymagania ogólne dotyczące przedmiotu zamówienia oraz dopuszczalności rozwiązań równoważnych

Wszystkie urządzenia oraz elementy wyposażenia oferowane przez Wykonawcę muszą być fabrycznie nowe, nieużywane oraz pochodzić z autoryzowanych lub oficjalnych kanałów dystrybucji na terenie Polski. Analogiczny wymóg dotyczący legalnego pochodzenia i dystrybucji obowiązuje w odniesieniu do oferowanego oprogramowania, z wyłączeniem rozwiązań udostępnianych na zasadach licencji open source, o ile znajdują one zastosowanie w ramach przedmiotu zamówienia.

Zamawiający dopuszcza możliwość zaoferowania rozwiązań równoważnych względem produktów, technologii i rozwiązań wskazanych w dokumentacji zamówienia.

Wszelkie odniesienia zawarte w opisie przedmiotu zamówienia do określonych producentów, marek, nazw handlowych, modeli, znaków towarowych, patentów, źródeł pochodzenia, dostawców lub konkretnych technologii i procesów należy traktować wyłącznie jako określenie oczekiwanego standardu technicznego, jakościowego i funkcjonalnego, a nie jako obowiązek zastosowania produktów lub rozwiązań konkretnego producenta.

Wskazane w dokumentacji parametry i wymagania stanowią minimalny poziom oczekiwanej jakości, wydajności, funkcjonalności, trwałości oraz bezpieczeństwa oferowanych rozwiązań.

Wykonawca może zaproponować rozwiązania alternatywne, pod warunkiem, że zapewnią one parametry techniczne, jakościowe, funkcjonalne i użytkowe nie gorsze niż określone przez Zamawiającego. Oferowane rozwiązania równoważne muszą zapewniać pełną realizację funkcji przewidzianych dla przedmiotu zamówienia, jego prawidłowe i niezawodne działanie oraz spełnienie wszystkich minimalnych wymagań określonych w dokumentacji postępowania.

Ocena równoważności będzie dokonywana w szczególności z uwzględnieniem parametrów technicznych, wydajności, funkcjonalności, kompatybilności, trwałości, niezawodności, bezpieczeństwa użytkowania oraz możliwości integracji z pozostałymi elementami infrastruktury objętej zamówieniem.

Zamawiający nie ogranicza konkurencji poprzez wskazanie obowiązku stosowania urządzeń, materiałów, oprogramowania lub technologii pochodzących od określonego producenta. Dopuszczalne jest zastosowanie dowolnych rozwiązań spełniających wymagania opisane w specyfikacji, pod warunkiem zachowania oczekiwanego standardu technicznego i jakościowego oraz osiągnięcia zakładanego efektu użytkowego.

W przypadku zaoferowania rozwiązań równoważnych Wykonawca zobowiązany jest wykazać, że proponowane produkty, urządzenia, oprogramowanie lub technologie spełniają wymagania określone przez Zamawiającego. Potwierdzenie równoważności może nastąpić w szczególności poprzez przedstawienie dokumentacji technicznej, kart katalogowych, specyfikacji producenta lub innych dokumentów pozwalających na obiektywną weryfikację zgodności oferowanego rozwiązania z wymaganiami opisu przedmiotu zamówienia.

Zastosowanie rozwiązań równoważnych nie może prowadzić do ograniczenia zakresu zamówienia, obniżenia wymaganych parametrów technicznych lub jakościowych, pogorszenia poziomu bezpieczeństwa ani zmniejszenia funkcjonalności przewidzianej przez Zamawiającego.