

WZP.271.16.2026.AA.MT

Opis przedmiotu zamówienia

Dostawa i wdrożenie sprzętu informatycznego oraz modernizacja istniejącego środowiska informatycznego wraz z podniesieniem poziomu cyberbezpieczeństwa w ramach konkursu grantowego „Cyberbezpieczny Samorząd” w trzech jednostkach Gminy Nowogard

Wstęp

Przedmiotem zamówienia jest wykonanie usług wdrożeniowych oraz konsultacji technicznych w zakresie infrastruktury sieciowej, serwerowej i wirtualizacji, usług katalogowych, migracji systemów, kopii zapasowych oraz systemów bezpieczeństwa, a także przeprowadzenie testów bezpieczeństwa, w środowisku Zamawiającego obejmującym dwie lokalizacje oraz trzy niezależne jednostki organizacyjne (UM, CUS, ZEAS).

1. Sieć i segmentacja (VLAN) — rekonfiguracja

Zakres obejmuje kompleksową analizę istniejącej sieci, zaprojektowanie segmentacji logicznej zgodnej z zasadą minimalnego zaufania i separacji ruchu, oraz rekonfigurację urządzeń sieciowych w obu lokalizacjach. Celem jest wydzielenie ruchu poszczególnych jednostek organizacyjnych oraz klas systemów, ograniczenie powierzchni ataku i umożliwienie kontroli przepływów między segmentami na poziomie zapory.

1.1. Analiza i inwentaryzacja stanu obecnego

- Inwentaryzacja urządzeń sieciowych (przełączniki, routery, punkty dostępowe), ich oprogramowania układowego oraz aktualnej konfiguracji VLAN, trunków i routingu.
- Mapowanie fizycznej i logicznej topologii sieci w obu lokalizacjach, identyfikacja punktów krytycznych i wąskich gardeł.
- Identyfikacja systemów, usług i grup użytkowników wraz z ich wymaganiami komunikacyjnymi (porty, protokoły, zależności).
- Ocena obecnej adresacji IP, wykorzystania podsieci oraz zależności od usług DHCP/DNS.

1.2. Projekt segmentacji i adresacji

- Projekt logiczny segmentacji z wydzieleniem VLAN-ów dla jednostek UM, CUS, ZEAS oraz klas systemów: serwery, stacje robocze, sieć zarządzania (out-of-band), kopie zapasowe, urządzenia drukujące, goście/BYOD, VoIP (jeśli dotyczy).
- Projekt planu adresacji IP (schemat podsieci, maski, bramy, zakresy DHCP, rezerwacje) wraz z konwencją nazewnictwa.
- Projekt routingu inter-VLAN oraz macierzy przepływów dozwolonych/zabronionych między segmentami (reguły zapory).
- Określenie polityki QoS oraz priorytetyzacji ruchu krytycznego, jeśli wymagane.
- Uzgodnienie i pisemna akceptacja projektu przez dział IT Zamawiającego przed wdrożeniem.

1.3. Rekonfiguracja urządzeń i wdrożenie VLAN

- Konfiguracja przełączników w warstwie L2/L3 — porty dostępne (access) i agregujące (trunk 802.1Q), przypisanie VLAN natywnego, ograniczenie zakresu VLAN na trunkach.
- Konfiguracja routingu inter-VLAN (SVI / interfejsy routowane) z zachowaniem redundancji bramy domyślnej, jeśli architektura na to pozwala.
- Konfiguracja usług DHCP (zakresy, rezerwacje, opcje) zintegrowanych z usługą katalogową oraz przekazywania DHCP (relay) między segmentami.
- Integracja segmentacji z zaporą brzegową — definicja stref bezpieczeństwa i reguł przepływu między VLAN-ami zgodnie z macierzą przepływów.
- Wydzielenie i zabezpieczenie VLAN administracyjnego (out-of-band) oraz VLAN kopii zapasowych.
- Wdrożenie mechanizmów ochrony warstwy L2 (DHCP snooping, ochrona przed pętlami, zabezpieczenie portów), w zakresie wspieranym przez sprzęt.

1.4. Migracja ruchu i minimalizacja przerw

- Etapowe przełączanie segmentów w uzgodnionych oknach serwisowych z planem wycofania (rollback) dla każdego etapu.
- Weryfikacja ciągłości usług krytycznych po każdym etapie przełączenia.

1.5. Testy i odbiór

- Testy routingu inter-VLAN, separacji ruchu oraz skuteczności reguł zapory (przepływy dozwolone i zablokowane).
- Testy poprawności działania DHCP/DNS w każdym segmencie oraz dostępu do usług współdzielonych.
- Protokół z testów odbiorowych.

1.6. Dokumentacja

- Schemat logiczny VLAN, tablica adresacji IP, macierz przepływów, kopie konfiguracji urządzeń, procedury administracyjne i utrzymaniowe.

Konsultacje techniczne

- Przed wdrożeniem: konsultacje projektowe dot. modelu segmentacji, doboru liczby i typów VLAN, planu adresacji oraz strategii routingu i polityk zapory; rekomendacje wariantów architektury z uzasadnieniem.
- W trakcie wdrożenia: nadzór techniczny nad rekonfiguracją, bieżące wsparcie decyzyjne przy konfiguracji trunków, routingu i reguł między segmentami, weryfikacja zgodności z projektem.
- Po wdrożeniu: konsultacje stabilizacyjne, analiza ewentualnych problemów komunikacyjnych, dostrojenie reguł i QoS na podstawie obserwowanego ruchu.
- Transfer wiedzy: omówienie z administratorami przyjętej segmentacji, zasad utrzymania VLAN, dodawania nowych segmentów oraz diagnostyki problemów sieciowych.
- Wsparcie powdrożeniowe: konsultacje w uzgodnionym oknie wsparcia w zakresie zmian konfiguracji sieci, rozbudowy o nowe segmenty i rozwiązywania incydentów sieciowych.

2. Serwery, macierz i wirtualizacja, UPS — wdrożenie

Pozycja obejmuje dostawę sprzętu zgodnie ze specyfikacją techniczną oraz komplet usług instalacji, konfiguracji i uruchomienia środowiska wirtualizacji opartego o hypervisor, z zapewnieniem wysokiej dostępności i redundancji dostępu do danych.

2.1. Zakres dostaw

Wykonawca dostarcza sprzęt i oprogramowanie zgodnie z poniższą specyfikacją:

SERWER TYP 1 (2 sztuki)

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	<ul style="list-style-type: none"> Obudowa Rack o wysokości max 2U 16 wnęk na dyski 2.5"
	<ul style="list-style-type: none"> Obudowa z możliwością 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. <p>Kryterium oceny ofert NIE – 0 punktów TAK – 6 punktów</p>
Płyta główna	<ul style="list-style-type: none"> Płyta główna z możliwością zainstalowania do dwóch procesorów. Obsługa procesorów 144 rdzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 8TB pamięci RAM.
Procesor	<ul style="list-style-type: none"> Zainstalowane dwa procesory min. 8-rdzeniowe, min. 3.7GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 170 w teście SPECSpeed®2017_fp_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej oferowanego serwera.
RAM	<ul style="list-style-type: none"> 128GB DDR5 RDIMM 6400MT/s,
Kontroler RAID	<ul style="list-style-type: none"> Sprzętowy kontroler dyskowy, posiadający <ul style="list-style-type: none"> Min. 8GB nieulotnej pamięci cache, Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących Obsługa dysków 22.5 Gbps SAS, 12 Gbps SAS, and 6 Gbps SATA/SAS
Dyski twarde	<ul style="list-style-type: none"> Zainstalowane: <ul style="list-style-type: none"> 2x dysk SSD SATA o pojemności min. 480GB, Hot-Plug Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Gniazda PCI	<ul style="list-style-type: none"> Cztery sloty PCIe Dwa sloty OCP
Interfejsy	<ul style="list-style-type: none"> 4 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte

sieciowe/FC/SAS	<p>poprzez karty w slotach PCIe)</p> <ul style="list-style-type: none"> • Dwuportowa karta sieciowa 25Gb Ethernet w standardzie SFP28 • Dwuportowa karta 32GB FC HBA
Wbudowane porty	<ul style="list-style-type: none"> • 4 porty USB w tym min: <ul style="list-style-type: none"> ○ 1 port USB 2.0 Type-C ○ 2 porty USB 3.1 ○ 1 port USB 3.0 wewnątrz obudowy • Port VGA z tyłu obudowy
Video	<ul style="list-style-type: none"> • Zintegrowana karta graficzna umożliwiającą wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	<ul style="list-style-type: none"> • Redundantne, Hot-Plug min. 1500W klasy Titanium
Elementy montażowe	<ul style="list-style-type: none"> • Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
System operacyjny/ dodatkowe oprogramowanie	<p>Microsoft Windows Server 2025 Datacenter lub rozwiązanie równoważne. Przez rozwiązanie równoważne Zamawiający rozumie system operacyjny zapewniający co najmniej:</p> <ul style="list-style-type: none"> • pełną obsługę usług Active Directory Domain Services (AD DS), • obsługę usług DNS oraz DHCP, • obsługę zasad grup (Group Policy), • możliwość pracy jako kontroler domeny Active Directory, • obsługę środowiska wirtualizacji Hyper-V lub rozwiązania równoważnego, • obsługę funkcji Failover Clustering, • obsługę funkcji Storage Replica, • możliwość uruchamiania nieograniczonej liczby instancji wirtualnych systemu operacyjnego zgodnie z zasadami licencjonowania producenta, • integrację z usługami katalogowymi Active Directory, • współpracę z bazami danych Microsoft SQL Server, • współpracę z systemami SIEM, NAC oraz rozwiązaniami monitoringu przewidzianymi w projekcie, • możliwość centralnego zarządzania aktualizacjami systemowymi, • możliwość integracji z mechanizmami uwierzytelniania wieloskładnikowego (MFA), • możliwość pracy w środowisku kopii zapasowych oraz odtwarzania awaryjnego wdrażanym w ramach projektu. • Licencjonowanie systemu operacyjnego musi zostać dobrane w sposób zapewniający zgodne z warunkami producenta uruchomienie wszystkich maszyn wirtualnych przewidzianych do wdrożenia w środowisku Urzędu Miejskiego.
Bezpieczeństwo	<ul style="list-style-type: none"> • Zatrask 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

	<ul style="list-style-type: none"> Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0 Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem 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).
	<ul style="list-style-type: none"> Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera <p>Kryterium oceny ofert NIE – 0 punktów TAK – 6 punktów</p>
Karta Zarządzania	<ul style="list-style-type: none"> Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające: <ul style="list-style-type: none"> zdalny dostęp do graficznego interfejsu Web karty zarządzającej szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika wsparcie dla IPv6 wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH Wsparcie dla automatycznej rejestracji DNS wsparcie dla LLDP możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. Monitorowanie zużycia dysków SSD Możliwość przywrócenia poprzednich wersji firmware możliwość rozszerzenia funkcjonalności o: <ul style="list-style-type: none"> integracja z Active Directory możliwość podmontowania zdalnych wirtualnych napędów wirtualną konsolę z dostępem do myszy, klawiatury możliwość obsługi przez sześciu administratorów jednocześnie wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer 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 Automatyczne zgłaszanie alertów do centrum serwisowego producenta Automatyczne update firmware dla wszystkich komponentów serwera możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do

	<p>slotów PCIe</p> <ul style="list-style-type: none"> możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. 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 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	<ul style="list-style-type: none"> Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: <ul style="list-style-type: none"> 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 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 Możliwość definiowania ról administratorów Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów

	<ul style="list-style-type: none"> o Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) o Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta o Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów o 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. o Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. o Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile o Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. o Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. o Zdalne uruchamianie diagnostyki serwera. o Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. o Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi. o Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin: <ul style="list-style-type: none"> ▪ wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze Vmware do zdefiniowanej polityki poziomu mikrokodów ▪ wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityką konfiguracji ▪ z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny) ▪ inwentaryzacja komponentów w serwerze i ich mikrokodów ▪ historia poboru mocy i temperatury serwera ▪ zbieranie danych diagnostycznych serwera do paczki serwisowej <p>Kryterium oceny ofert NIE – 0 punktów TAK – 6 punktów</p>
Oprogramowanie do monitorowania	<p>Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:</p> <ul style="list-style-type: none"> • Monitoring: <ul style="list-style-type: none"> o ilość podłączonych oraz rozłączonych systemów o stan podłączonych urządzeń o informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów o Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia o informacje o statusie gwarancji dla poszczególnych urządzeń o informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności

	<p>urządzeń</p> <ul style="list-style-type: none"> ○ 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 ○ 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: <ul style="list-style-type: none"> ▪ 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: <ul style="list-style-type: none"> ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ 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: <ul style="list-style-type: none"> ▪ 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. <p>• Aktualizacja firmware</p>
--	---

	<ul style="list-style-type: none"> ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań 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 <ul style="list-style-type: none"> ○ Możliwość generowania raportów dla serwerów zawierających informację o: <ul style="list-style-type: none"> ▪ 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: <ul style="list-style-type: none"> ▪ 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 ○ Generowanie raportów do plików CSV i PDF ● Cyberbezpieczeństwo <ul style="list-style-type: none"> ○ 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 <ul style="list-style-type: none"> ○ 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 <ul style="list-style-type: none"> ○ 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 <ul style="list-style-type: none"> ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. ● Inne <ul style="list-style-type: none"> ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android <p>Kryterium oceny ofert NIE – 0 punktów</p>
--	--

	TAK – 6 punktów
Certyfikaty	<ul style="list-style-type: none"> Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 Serwer musi posiadać deklaracja CE. 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, dla kraju, w którym produkt będzie użytkowany, według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu. 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 użytkownika	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. Możliwość bezpłatnego pobierania aktualizacji firmware, BIOS i sterowników po wygaśnięciu gwarancji. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. 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

	<p>bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.</p> <ul style="list-style-type: none"> • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: <ul style="list-style-type: none"> ○ 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. ○ 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 przekaze 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.
--	---

SERWER TYP 2 (1 sztuka)

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	<ul style="list-style-type: none"> • Obudowa Rack o wysokości max 2U • 16 wnęk na dyski 2.5"
	<ul style="list-style-type: none"> • Obudowa z możliwością 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. <p>Kryterium oceny ofert NIE – 0 punktów TAK – 3 punkty</p>
Płyta główna	<ul style="list-style-type: none"> • Płyta główna z możliwością zainstalowania do dwóch procesorów. • Obsługa procesorów 144 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci.

	<ul style="list-style-type: none"> Płyta główna powinna obsługiwać do 8TB pamięci RAM.
Procesor	<ul style="list-style-type: none"> Zainstalowane dwa procesory min. 8-rdzeniowe, min. 3.7GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 170 w teście SPECspeed®2017_fp_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej oferowanego serwera.
RAM	<ul style="list-style-type: none"> 128GB DDR5 RDIMM 6400MT/s,
Kontroler RAID	<ul style="list-style-type: none"> Sprzętowy kontroler dyskowy, posiadający <ul style="list-style-type: none"> Min. 8GB nieulotnej pamięci cache, Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących Obsługa dysków 22.5 Gbps SAS, 12 Gbps SAS, and 6 Gbps SATA/SAS
Dyski twarde	<ul style="list-style-type: none"> Zainstalowane: <ul style="list-style-type: none"> 2x dysk SSD SATA o pojemności min. 480GB, Hot-Plug 4x dysk SAS o pojemności min. 2.4TB, Hot-Plug Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Gniazda PCI	<ul style="list-style-type: none"> Cztery sloty PCIe Dwa sloty OCP
Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none"> 4 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) Dwuportowa karta sieciowa 25Gb Ethernet w standardzie SFP28
Wbudowane porty	<ul style="list-style-type: none"> 4 porty USB w tym min: <ul style="list-style-type: none"> 1 port USB 2.0 Type-C 2 porty USB 3.1 1 port USB 3.0 wewnątrz obudowy Port VGA z tyłu obudowy
Video	<ul style="list-style-type: none"> Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	<ul style="list-style-type: none"> Redundantne, Hot-Plug min. 1500W klasy Titanium
Elementy montażowe	<ul style="list-style-type: none"> Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
System operacyjny/ dodatkowe oprogramowanie	<p>Microsoft Windows Server 2025 Standard lub Datacenter lub rozwiązanie równoważne.</p> <p>W przypadku zaoferowania systemu Microsoft Windows Server 2025 Standard liczba dostarczonych licencji musi zostać dobrana w sposób zapewniający, zgodnie z zasadami licencjonowania producenta, możliwość legalnego uruchomienia minimum 8 maszyn wirtualnych w środowisku CUS i ZEAS.</p> <p>W przypadku zaoferowania systemu Microsoft Windows Server 2025 Datacenter liczba dostarczonych licencji musi zostać dobrana w sposób zapewniający zgodne z warunkami producenta uruchomienie wszystkich maszyn wirtualnych przewidzianych do wdrożenia.</p>

	<p>Przez rozwiązanie równoważne Zamawiający rozumie system operacyjny zapewniający co najmniej:</p> <ul style="list-style-type: none"> • pełną obsługę usług Active Directory Domain Services (AD DS), • obsługę usług DNS oraz DHCP, • obsługę zasad grup (Group Policy), • możliwość pracy jako kontroler domeny Active Directory, • obsługę środowiska wirtualizacji Hyper-V lub rozwiązania równoważnego, • obsługę funkcji Failover Clustering, • obsługę funkcji Storage Replica, • integrację z usługami katalogowymi Active Directory, • współpracę z bazami danych Microsoft SQL Server, • współpracę z systemami SIEM, NAC oraz rozwiązaniami monitoringu przewidzianymi w projekcie, • możliwość centralnego zarządzania aktualizacjami systemowymi, • możliwość integracji z mechanizmami uwierzytelniania wieloskładnikowego (MFA), • możliwość pracy w środowisku kopii zapasowych oraz odtwarzania awaryjnego wdrażanym w ramach projektu.
Bezpieczeństwo	<ul style="list-style-type: none"> • Zatrząsek 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 • 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 • 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).
	<ul style="list-style-type: none"> • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera <p>Kryterium oceny ofert NIE – 0 punktów TAK – 3 punkty</p>
Karta Zarządzania	<ul style="list-style-type: none"> • Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające: <ul style="list-style-type: none"> ○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej ○ szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika ○ wsparcie dla IPv6 ○ wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH

	<ul style="list-style-type: none"> ○ Wsparcie dla automatycznej rejestracji DNS ○ wsparcie dla LLDP ○ możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. ○ Monitorowanie zużycia dysków SSD ○ Możliwość przywrócenia poprzednich wersji firmware możliwość rozszerzenia funkcjonalności o: <ul style="list-style-type: none"> ○ integracja z Active Directory ○ możliwość podmontowania zdalnych wirtualnych napędów ○ wirtualną konsolę z dostępem do myszy, klawiatury ○ możliwość obsługi przez sześciu administratorów jednocześnie ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer ○ Możliwość wykrywania odchyłeń 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 ○ Automatyczne zgłaszanie alertów do centrum serwisowego producenta ○ Automatyczne update firmware dla wszystkich komponentów serwera ○ możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer ○ możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer ○ Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON ○ Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych ○ Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. ○ 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 ○ możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielokrotnego przy logowaniu do karty zarządzającej ○ Automatyczne odświeżanie certyfikatów SSL ○ monitorowanie przepływu powietrza na bieżąco (w CFM)
Oprogramowanie do zarządzania	<ul style="list-style-type: none"> • Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: <ul style="list-style-type: none"> ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego

	<p>agenta</p> <ul style="list-style-type: none"> ○ 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 ○ 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 ○ 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 ○ 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 modułarnych 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
--	--

	<p>urządzenia przez serwis producenta.</p> <ul style="list-style-type: none"> ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. ○ Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin: <ul style="list-style-type: none"> ▪ wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze Vmware do zdefiniowanej polityki poziomu mikrokodów ▪ wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityką konfiguracji ▪ z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny) ▪ inwentaryzacja komponentów w serwerze i ich mikrokodów ▪ historia poboru mocy i temperatury serwera ▪ zbieranie danych diagnostycznych serwera do paczki serwisowej <p>Kryterium oceny ofert NIE – 0 punktów TAK – 3 punkty</p>
Oprogramowanie do monitorowania	<p>Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:</p> <ul style="list-style-type: none"> • Monitoring: <ul style="list-style-type: none"> ○ 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 ○ 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: <ul style="list-style-type: none"> ▪ Obciążeniu procesora

	<ul style="list-style-type: none"> ▪ 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: <ul style="list-style-type: none"> ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ 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: <ul style="list-style-type: none"> ▪ 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 <ul style="list-style-type: none"> ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań 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 <ul style="list-style-type: none"> ○ Możliwość generowania raportów dla serwerów zawierających informację o: <ul style="list-style-type: none"> ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej
--	---

	<ul style="list-style-type: none"> ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, ○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: <ul style="list-style-type: none"> ▪ 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 ○ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo <ul style="list-style-type: none"> ○ 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 <ul style="list-style-type: none"> ○ 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 <ul style="list-style-type: none"> ○ 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 <ul style="list-style-type: none"> ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne <ul style="list-style-type: none"> ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android <p>Kryterium oceny ofert NIE – 0 punktów TAK – 3 punkty</p>
Certyfikaty	<ul style="list-style-type: none"> • Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • 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

	<p>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, dla kraju, w którym produkt będzie użytkowany, według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnienie wymogu.</p> <ul style="list-style-type: none"> 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 użytkownika	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. Możliwość bezpłatnego pobierania aktualizacji firmware, BIOS i sterowników po wygaśnięciu gwarancji. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/portał) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. 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. 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: <ul style="list-style-type: none"> Możliwości utworzenia zgłoszenia serwisowego w wyniku, którego proces

	<p>diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.</p> <ul style="list-style-type: none"> o 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. o Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. o 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. o 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 prześle 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. <ul style="list-style-type: none"> • 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.
--	--

MACIERZ DYSKOWA (1 sztuka)

Parametr	Charakterystyka (wymagania minimalne)
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19", o wysokość maksymalnie 2U z możliwością instalacji min. 12 dysków 3.5"
Przestrzeń dyskowa	Zainstalowane: 7x dysk SAS o pojemności min. 12TB, Hot-Plug 4x dysk SSD SAS o pojemności min. 1.92TB, Hot-Plug
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 264 dysków twardych.
Obsługa dysków	Macierz musi mieć możliwość obsługi dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5" jak również 3,5".
Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku). Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.

Tryb pracy kontrolerów w macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
Pamięć cache	Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania baterijnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
Interfejsy	Macierz musi posiadać, co najmniej 8 portów 32Gb FC (4 porty na kontroler)
Kable/wkładki	8x wkładka 32Gb FC
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.
Zarządzanie grupami dyskowymi i dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Tiering	Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Wewnętrzne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach

ne kopie pełne	macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
Zdalna replikacja danych	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.
Podłączani e zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
Redundan cja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.
Monitorin g	Rozwiązanie w obszarze monitoringu musi zapewniać automatyczną ocenę kondycji środowiska macierzy na podstawie wskaźnika health score wraz z prezentacją rekomendowanych działań korygujących, ciągły monitoring konfiguracji bezpieczeństwa (w tym wykrywanie odchyłeń od dobrych praktyk i ocenę ich wpływu na ryzyko), predykcyjne wykrywanie anomalii w teledziennych z wykorzystaniem mechanizmów analitycznych/ML, centralny widok ryzyka dla całej floty macierzy z możliwością rankingu i filtrowania systemów, nadzór nad łącznością oraz integralnością danych teledziennych (z generowaniem alertów przy przerwach lub niekompletności danych), analizę zużycia energii i parametrów środowiskowych pod kątem ryzyka operacyjnego, a także generowanie raportów oceny bezpieczeństwa środowiska, zawierających listę odchyłeń i rekomendowane działania prewencyjne lub naprawcze.
Dodatkow e wymagani a	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.

	Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.
Standardy bezpieczeństwa	Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International). Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające spełnienie powyższych zaleceń.
Inne	<p>Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.</p> <p>Oferowany model macierzy w momencie składania oferty nie może mieć ogłoszonej daty końca sprzedaży. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego urządzenia, potwierdzające brak ogłoszenia takiej daty.</p> <p>Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001.</p> <p>Deklaracja zgodności CE.</p>
Warunki gwarancji	<p>Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat.</p> <p>Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.</p> <p>Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.</p> <p>Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.</p> <p>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.</p> <p>Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</p> <p>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.</p> <p>Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</p> <p>Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:</p> <ul style="list-style-type: none"> • 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. • 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

	<p>pracownik serwisu zamówi nową część i prześle 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.</p> <p>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.</p>
--	--

UPS CENTRALNY (1 sztuka)

Parametr	Charakterystyka (wymagania minimalne)
Opis zasilacza UPS	<p>Projektuje się zasilacz UPS pracujący w topologii on-line VFI-SS-111, wg normy IEC 62040-3, o mocy 20kVA/20kW. UPS będzie wyposażony w wewnętrzny, bezprzerwowy bypass elektroniczny. Bypass wewnętrzny będzie posiadał zabezpieczenie przed zwrotnym podawaniem energii do sieci zasilającej (backfeed protection, zgodnie z normą IEC 62040). UPS będzie zasilany dwutorowo – przez tor główny (układ prostownik-falownik) oraz tor rezerwowy (bypass elektroniczny). Dodatkowo będzie wyposażony w zewnętrzny tor obejściowy (serwisowy, mechaniczny). Baterie akumulatorów, zapewniające czas podtrzymania 6 minut dla obciążenia 20kW, będą umieszczone wewnątrz zasilacza UPS.</p>
Opis techniczny	<ul style="list-style-type: none"> • producent oferowanego urządzenia powinien posiadać certyfikat ISO 9001 w zakresie projektowania, produkcji, sprzedaży i serwisu systemów zasilania gwarantowanego UPS • moc wyjściowa: 20 kVA/20 kW • możliwość pracy równoległej do 4 jednostek • ilość faz 3/3 – trzy fazy wejściowe i trzy fazy wyjściowe • sprawność w trybie on-line: minimum 95,64% w zakresie obciążenia 50-100% (do 99,08% w trybie oszczędzania energii) • tolerancja napięcia wejściowego prostownika, bez przejścia na pracę z baterii: 190/330-276/478 V przy obciążeniu 100%; • częstotliwość wejściowa 50 Hz lub 60 Hz z tolerancją 40 Hz do 72 Hz • $\cos\phi$ wyjściowy = 1 • $\cos\phi$ wejściowy = 0,99 przy 100% obciążenia • współczynnik szczytu: 3:1 • zabezpieczenie przed zwrotnym podaniem energii do sieci zasilającej (backfeed protection, zgodnie z normą IEC 62040) w torze bypassu statycznego UPS • urządzenie powinno być wyposażone w system nieciągłego ładowania baterii. Należy dołączyć opis sposobu zarządzania pracą baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta • wejściowe zniekształcenia THDi < 3% • wyjściowe THDu: <ul style="list-style-type: none"> - dla obciążenia liniowego < 2% - dla obciążenia nieliniowego < 5% • Urządzenie musi posiadać panel komunikacyjny, w którym powinny być zainstalowane: <ul style="list-style-type: none"> - gniazdo komunikacji RS-232 - gniazdo wyłącznika awaryjnego p.poż.

	<ul style="list-style-type: none"> interfejs komunikacyjny SNMP – obsługiwane protokoły: IPv4/v6, TLS, SNMPv1/v3, DHCP, SSH, LDAP prędkość gigabit’owa (half-duplex, full-duplex). Zgodność z normami dot. cyberbezpieczeństwa UL 2900-1 lub IEC62443-4-2. Opcjonalnie: Modbus TCP/RTU graficzny wyświetlacz LCD
Wymiary	Wymiary UPS (szer. x gł. x wys.): 380 x 740 x 1328 mm

2.2. Plan wdrożenia

- Opracowanie planu wdrożenia i migracji: harmonogram, opis działań, kryteria odbioru, procedura odtworzenia środowiska w razie awarii.
- Uzgodnienie projektu architektury środowiska (klastery, sieć, magazyn danych) z Zamawiającym.

2.3. Instalacja i konfiguracja systemowa

- Montaż serwerów i macierzy w szafie rack, podłączenie zasilania redundantnego, sieci LAN/SAN oraz kanałów zarządzania (out-of-band).
- Aktualizacja oprogramowania układowego (firmware) i BIOS/UEFI do wersji zalecanych przez producenta.
- Konfiguracja kontrolerów RAID, woluminów oraz parametrów wydajnościowych i niezawodnościowych.
- Konfiguracja kontrolerów zdalnego zarządzania (alerty SMTP/SNMPv3, Syslog, zdalna konsola).
- Instalacja i aktualizacja systemów operacyjnych oraz hypervisora.

2.4. Wirtualizacja i wysoka dostępność

- Dostarczenie, instalacja oraz konfiguracja środowiska wirtualizacyjnego wysokiej dostępności składającego się z dwóch serwerów klasy rack oraz współdzielonej macierzy dyskowej SAN.
- Utworzenie klastra wysokiej dostępności umożliwiającego centralne zarządzanie środowiskiem, automatyczne przełączanie awaryjne maszyn wirtualnych oraz migrację maszyn pomiędzy węzłami klastra.
- Konfiguracja mechanizmu quorum dedykowanego dla klastra dwuwęzłowego, zapewniającego prawidłowe działanie środowiska podczas awarii jednego z węzłów.
- Konfiguracja współdzielonej pamięci masowej dla maszyn wirtualnych wraz z przygotowaniem odpowiednich woluminów i repozytoriów danych.
- Konfiguracja wielościżkowości (Multipath) dostępu do macierzy dyskowej w celu zapewnienia wysokiej dostępności oraz redundancji połączeń do pamięci masowej.
- Konfiguracja dedykowanych sieci dla ruchu zarządzającego, komunikacji klastrowej, migracji maszyn wirtualnych oraz komunikacji z pamięcią masową.
- Konfiguracja przełączników wirtualnych, sieci maszyn wirtualnych oraz separacji ruchu administracyjnego, produkcyjnego i backupowego.
- Migracja istniejących maszyn wirtualnych Zamawiającego do nowego środowiska wraz z weryfikacją poprawności działania systemów po migracji.
- Konfiguracja automatycznego przełączania awaryjnego (failover) maszyn wirtualnych pomiędzy węzłami klastra w przypadku awarii pojedynczego serwera.

- Konfiguracja migracji online (Live Migration) maszyn wirtualnych pomiędzy węzłami klastra bez przerywania pracy uruchomionych usług.
- Zapewnienie możliwości rozbudowy klastra o kolejne węzły obliczeniowe bez konieczności przebudowy środowiska wirtualizacyjnego.
- Zapewnienie możliwości migracji maszyn wirtualnych pomiędzy serwerami wyposażonymi w procesory różnych generacji tego samego producenta.
- Konfiguracja centralnego monitoringu środowiska obejmującego co najmniej monitorowanie serwerów, pamięci masowej, usług klastra, wykorzystania zasobów CPU, RAM, przestrzeni dyskowej oraz interfejsów sieciowych.
- Konfiguracja mechanizmów alertowania o awariach serwerów, pamięci masowej, utracie komunikacji klastrowej, utracie quorum, przeciążeniu zasobów oraz błędach sprzętowych.
- Konfiguracja mechanizmów rejestracji zdarzeń administracyjnych, operacji wykonywanych na maszynach wirtualnych, migracji, zdarzeń wysokiej dostępności oraz awarii infrastruktury.
- Konfiguracja systemu wykonywania oraz odtwarzania kopii zapasowych maszyn wirtualnych.
- Opracowanie i przekazanie dokumentacji powdrożeniowej obejmującej architekturę rozwiązania, konfigurację środowiska, konfigurację wysokiej dostępności, konfigurację pamięci masowej, procedury administracyjne oraz procedury wykonywania i odtwarzania kopii zapasowych.
- Przeprowadzenie szkolenia administratorów obejmującego obsługę środowiska, zarządzanie maszynami wirtualnymi, wykonywanie kopii zapasowych, procedury awaryjne oraz podstawową diagnostykę systemu.
- Dostarczenie wszelkich licencji, subskrypcji oraz praw do użytkowania wymaganych do uruchomienia i eksploatacji środowiska wirtualizacyjnego wraz z funkcjami wysokiej dostępności, migracji online maszyn wirtualnych, klastrowania, monitoringu i centralnego zarządzania.

2.5. Testy i odbiór

- Testy uruchomienia maszyn wirtualnych, dostępu do zasobów oraz ścieżek SAN (multipath).
- Test przełączania awaryjnego (failover) i powrotu (failback) między węzłami klastra.
- Testy wydajności oraz weryfikacja poprawności konfiguracji redundancji; protokół odbioru.

2.6. Dokumentacja

- Schemat środowiska, konfiguracja klastra wirtualnego, mapowanie zasobów i woluminów, konfiguracja MPIO, procedury administracyjne i utrzymaniowe.

Konsultacje techniczne

- Przed wdrożeniem: konsultacje dot. architektury środowiska wirtualizacji, projektu klastra HA, doboru parametrów magazynu danych, modelu separacji maszyn wirtualnych i strategii licencjonowania; weryfikacja zgodności dostarczonego sprzętu z założeniami projektu.
- W trakcie wdrożenia: nadzór nad konfiguracją klastra, magazynu i sieci wirtualnej, wsparcie decyzyjne przy konfiguracji multipath, parametrów wydajnościowych i polityk wysokiej dostępności.
- Po wdrożeniu: konsultacje stabilizacyjne, analiza wydajności i obciążenia, rekomendacje optymalizacji rozmieszczenia maszyn wirtualnych i wykorzystania zasobów.

- Transfer wiedzy: szkolenie administratorów z obsługi klastra wirtualnego, zarządzania maszynami wirtualnymi, procedur failover/failback oraz monitoringu środowiska.
- Wsparcie powdrożeniowe: konsultacje w oknie wsparcia w zakresie rozbudowy środowiska, dodawania węzłów i maszyn wirtualnych oraz diagnostyki problemów wydajnościowych i awarii.

3. Active Directory — wdrożenie

Zakres obejmuje wdrożenie trzech niezależnych środowisk usług katalogowych (UM, CUS, ZEAS) wraz z usługami towarzyszącymi (DNS, DHCP), kompleksowymi politykami bezpieczeństwa oraz integracją z infrastrukturą sieciową i systemami uwierzytelniania. Każde środowisko projektowane jest z uwzględnieniem redundancji, odporności na awarie i zgodności z dobrymi praktykami zabezpieczania usług katalogowych.

3.1. Projekt usług katalogowych

- Projekt struktury lasu i domen dla trzech jednostek, z określeniem poziomu funkcjonalnego oraz zasad separacji.
- Projekt struktury jednostek organizacyjnych (OU), modelu kont, grup zabezpieczeń i grup dystrybucyjnych.
- Projekt konwencji nazewnictwa, schematu delegacji uprawnień i modelu kont uprzywilejowanych.

3.2. Wdrożenie kontrolerów domeny i usług towarzyszących

- Instalacja i konfiguracja AD DS / DNS / DHCP dla jednostki UM, z kontrolerami w układzie redundantnym (co najmniej dwa kontrolery domeny).
- Instalacja i konfiguracja AD DS / DNS / DHCP dla jednostki CUS.
- Instalacja i konfiguracja AD DS / DNS / DHCP dla jednostki ZEAS.
- Konfiguracja replikacji, ról FSMO, stref DNS (z DNSSEC, jeśli wymagane) oraz integracji DHCP z usługą katalogową.
- Konfiguracja synchronizacji czasu (hierarchia NTP) w obrębie każdej domeny.

3.3. Polityki bezpieczeństwa (GPO)

- Wdrożenie polityk haseł, blokady kont oraz polityk uwierzytelniania zgodnych z wymaganiami KRI.
- Polityki zabezpieczeń stacji roboczych i serwerów (konfiguracja zabezpieczeń systemu, zapory, ograniczeń lokalnych).
- Polityki konfiguracji środowiska użytkownika, mapowania zasobów, drukarek i przekierowania folderów (jeśli dotyczy).
- Polityki ograniczania uprawnień administracyjnych oraz zabezpieczenia kont uprzywilejowanych.

3.4. Integracja i uwierzytelnianie

- Wdrożenie usługi uwierzytelniania sieciowego (NPS/RADIUS) i integracja z mechanizmami dostępu do sieci oraz zaporą.
- Integracja usług katalogowych z segmentacją VLAN, usługami sieciowymi oraz przygotowanie pod integrację z systemem NAC (poz. 7).
- Konfiguracja logowania i autoryzacji stacji roboczych oraz przyłączania stacji do domen.

3.5. Testy i dokumentacja

- Testy logowania, autoryzacji, replikacji między kontrolerami oraz rozwiązywania nazw (DNS).
- Testy stosowania polityk GPO na obiektach testowych przed wdrożeniem produkcyjnym.
- Dokumentacja struktury OU, wykazu polityk GPO, modelu uprawnień oraz procedur administracyjnych.

Konsultacje techniczne

- Przed wdrożeniem: konsultacje dot. projektu struktury lasu/domen, modelu OU i grup, strategii polityk GPO oraz modelu kont uprzywilejowanych i delegacji uprawnień; rekomendacje w zakresie zabezpieczania usług katalogowych.
- W trakcie wdrożenia: nadzór nad konfiguracją kontrolerów, replikacji i polityk, wsparcie decyzyjne przy projektowaniu i testowaniu GPO oraz integracji z RADIUS.
- Po wdrożeniu: konsultacje stabilizacyjne, weryfikacja skuteczności polityk, analiza zdarzeń logowania i replikacji, dostrojenie konfiguracji.
- Transfer wiedzy: szkolenie administratorów z zarządzania usługami katalogowymi, tworzenia i modyfikacji GPO, zarządzania kontami i grupami oraz diagnostyki replikacji i uwierzytelniania.
- Wsparcie powdrożeniowe: konsultacje w oknie wsparcia w zakresie modyfikacji polityk, rozbudowy struktury i rozwiązywania problemów z usługami katalogowymi.

4. Migracja systemów do nowej infrastruktury

Zakres obejmuje przeniesienie usług, danych, baz danych i maszyn wirtualnych z dotychczasowego środowiska do nowo wdrożonej infrastruktury, z zachowaniem ciągłości działania, integralności danych i minimalizacją przerw w pracy jednostek. Migracja prowadzona jest etapowo, z procedurą wycofania na każdym etapie.

4.1. Analiza i planowanie migracji

- Inwentaryzacja systemów, aplikacji, baz danych, udziałów i powiązań aplikacyjnych przeznaczonych do migracji.
- Analiza zależności między systemami oraz określenie kolejności migracji minimalizującej ryzyko przestoju.
- Opracowanie planu migracji: harmonogram, okna serwisowe, kryteria sukcesu, procedura wycofania (rollback) i kryteria jej uruchomienia.
- Uzgodnienie planu z Zamawiającym oraz przygotowanie kopii zabezpieczających przed migracją.

4.2. Migracja usług i danych

- Migracja usług katalogowych, DNS, DHCP, profili użytkowników oraz udziałów sieciowych z zachowaniem uprawnień (ACL).
- Migracja maszyn wirtualnych (w tym z dotychczasowych zasobów, np. NAS) z zachowaniem konfiguracji, parametrów sieciowych i przestrzeni dyskowych.
- Migracja baz danych (m.in. MS SQL Server, Firebird) z weryfikacją spójności i integralności po przeniesieniu.
- Migracja systemów dziedzinowych wraz z ich komponentami i konfiguracją.
- Aktualizacja powiązań aplikacyjnych, parametrów połączeń i punktów integracji po migracji.

4.3. Testy powdrożeniowe i walidacja

- Testy logowania, dostępu do zasobów, komunikacji inter-VLAN oraz poprawności usług katalogowych.
- Testy funkcjonalne aplikacji i baz danych oraz potwierdzenie ich pełnej dostępności i wydajności.
- Weryfikacja integralności danych po migracji oraz testy wydajności w nowym środowisku.
- Protokół odbioru migracji oraz dokumentacja powykonawcza (wykaz przeniesionych systemów, zmiany konfiguracji).

Konsultacje techniczne

- Przed wdrożeniem: konsultacje dot. strategii migracji, analizy zależności systemów, kolejności przenoszenia, doboru metody migracji baz danych i maszyn wirtualnych oraz projektu procedury wycofania.
- W trakcie wdrożenia: nadzór techniczny nad procesem migracji, bieżące wsparcie decyzyjne przy nieprzewidzianych zależnościach i problemach z danymi, weryfikacja kompletności przenoszenia.
- Po wdrożeniu: konsultacje stabilizacyjne, analiza wydajności systemów po migracji, wsparcie przy dostrajaniu konfiguracji aplikacji i baz danych.
- Transfer wiedzy: omówienie z administratorami zmian w środowisku, nowej lokalizacji systemów i danych oraz zaktualizowanych procedur eksploatacyjnych.
- Wsparcie powdrożeniowe: konsultacje w oknie wsparcia w zakresie problemów ujawniających się po migracji oraz dalszych przeniesień systemów.

5. Wdrożenie systemu backup

Zakres obejmuje wdrożenie systemu kopii zapasowych w modelu 3-2-1 z replikacją między lokalizacjami oraz mechanizmami ochrony przed modyfikacją i usunięciem (immutable), wraz z politykami retencji, monitoringiem i regularnymi testami odtwarzania. System projektowany jest z myślą o odporności na ransomware oraz zapewnieniu odtwarzalności danych w wymaganych oknach czasowych.

5.1. Projekt systemu kopii zapasowych

- Analiza danych i systemów objętych ochroną, określenie wymaganych parametrów RPO (dopuszczalna utrata danych) i RTO (czas odtworzenia).
- Projekt architektury kopii w modelu 3-2-1 (wiele kopii, różne nośniki, kopia poza lokalizacją) z uwzględnieniem mechanizmu immutable.
- Projekt polityk retencji (np. kopie codzienne, tygodniowe, miesięczne) oraz harmonogramu kopii pełnych i przyrostowych.

5.2. Wdrożenie i konfiguracja repozytoriów

- Wdrożenie oprogramowania kopii zapasowych oraz konfiguracja repozytorium kopii jako zasobu wydzielonego i odseparowanego od środowiska produkcyjnego.
- Integracja z istniejącą infrastrukturą składowania (np. NAS) jako dodatkowy nośnik kopii. (Wdrożenie musi uwzględniać integrację z istniejącą infrastrukturą NAS Synology wykorzystywaną przez Zamawiającego do backupu, replikacji oraz archiwizacji danych.)

- Konfiguracja repozytorium z ochroną immutable (WORM / niezmiennie migawki) jako zabezpieczenie przed ransomware i nieautoryzowanym usunięciem.

5.3. Zakres backupu i replikacja

- Konfiguracja kopii maszyn wirtualnych, usług katalogowych, baz danych i plików, z zapewnieniem spójności aplikacyjnej (mechanizmy migawek i spójności).
- Konfiguracja kopii baz danych (m.in. MS SQL, Firebird) zgodnie z dobrymi praktykami dla danego silnika.
- Replikacja kopii między lokalizacjami przez szyfrowany kanał (VPN/IPSec) z wykorzystaniem wydzielonego VLAN-u backupowego.
- Konfiguracja szyfrowania kopii w spoczynku i w transmisji.

5.4. Monitoring, testy odtwarzania i dokumentacja

- Konfiguracja monitoringu zadań kopii zapasowych oraz alertów o błędach i nieukończonych zadaniach.
- Przeprowadzenie testów odtwarzania obejmujących co najmniej maszyny wirtualne, usługi katalogowe Active Directory, bazy danych oraz pliki użytkowników, zakończonych sporządzeniem raportu z testów.
- W ramach testów odbiorowych Wykonawca przeprowadzi test odtworzenia usług Active Directory.
- Wykonawca odpowiada za zapewnienie możliwości skutecznego odtworzenia danych i usług z kopii zapasowych, w tym w scenariuszu całkowitej utraty jednej z lokalizacji.
- W ramach odbioru Wykonawca zweryfikuje zgodność rzeczywistych czasów odtworzenia z założonymi parametrami RTO i przedstawi raport z przeprowadzonych testów.
- Dokumentacja: schemat systemu kopii, polityki retencji, harmonogram, procedury backupu i odtwarzania awaryjnego.

Konsultacje techniczne

- Przed wdrożeniem: konsultacje dot. strategii kopii zapasowych, ustalenia parametrów RPO/RTO, projektu modelu 3-2-1, doboru mechanizmu immutable oraz polityk retencji adekwatnych do wymagań prawnych i operacyjnych.
- W trakcie wdrożenia: nadzór nad konfiguracją repozytoriów, replikacji i harmonogramów, wsparcie decyzyjne przy konfiguracji spójności aplikacyjnej i szyfrowania.
- Po wdrożeniu: konsultacje stabilizacyjne, analiza skuteczności kopii i czasów odtwarzania, rekomendacje optymalizacji harmonogramów i wykorzystania przestrzeni.
- Transfer wiedzy: szkolenie administratorów z obsługi systemu kopii, monitorowania zadań, wykonywania odtworzeń oraz procedur reagowania w sytuacji utraty danych.
- Wsparcie powdrożeniowe: konsultacje w oknie wsparcia w zakresie rozbudowy ochrony o nowe systemy, modyfikacji polityk oraz wsparcia przy odtwarzaniu awaryjnym.

6. Dostawa i wdrożenie SIEM

Zakres obejmuje dostarczenie i wdrożenie systemu klasy SIEM (z funkcjami XDR) do centralnego zbierania, normalizacji, korelacji i analizy logów oraz wykrywania i reagowania na incydenty bezpieczeństwa w środowisku Zamawiającego. System stanowi podstawę monitorowania bezpieczeństwa i wsparcia obowiązków raportowych.

6.1. Projekt i dostawa

- Analiza środowiska i źródeł logów, projekt architektury SIEM (rozmieszczenie kolektorów, retencja, przepustowość).
- Dostarczenie systemu SIEM/XDR wraz z niezbędnymi licencjami, zgodnie ze specyfikacją zamówienia.
- Określenie polityki retencji logów oraz wymagań pojemnościowych repozytorium zdarzeń.

6.2. Wymagania minimalne dla systemu SIEM/XDR

Dostarczony system musi spełniać co najmniej poniższe wymagania funkcjonalne i techniczne. Zamawiający dopuszcza rozwiązania równoważne, tj. dowolny system spełniający wszystkie wymienione wymagania. Wymagania sformułowano w sposób neutralny technologicznie i niewskazujący konkretnego producenta.

Architektura i licencjonowanie

- Architektura oparta o centralny serwer (zarządzający) oraz lekkich agentów instalowanych na monitorowanych hostach, z możliwością zbierania zdarzeń również w trybie bezagentowym (syslog, API) z urządzeń sieciowych i bezpieczeństwa.
- Brak ograniczeń licencyjnych na liczbę monitorowanych hostów (agentów), liczbę użytkowników oraz dobową ilość przetwarzanych zdarzeń (EPS) lub dobowy wolumen danych; dopuszcza się model bezpłatny bądź oparty wyłącznie o opcjonalne wsparcie producenta.
- Możliwość instalacji w środowisku wirtualnym na systemie operacyjnym z rodziny Linux, z możliwością wdrożenia w architekturze rozproszonej/klastrowej zapewniającej skalowalność i wysoką dostępność.
- Agenci dostępni co najmniej dla systemów Windows, Linux oraz macOS; centralne zarządzanie agentami (wdrażanie, grupowanie, aktualizacja konfiguracji) z poziomu serwera.
- Szyfrowana i uwierzytelniana komunikacja pomiędzy agentami a serwerem.

Zbieranie, normalizacja i przechowywanie zdarzeń

- Centralne zbieranie i normalizacja logów z wielu typów źródeł: systemy operacyjne, dziennik zdarzeń Windows, usługi katalogowe, hypervisor, przełączniki, zapory sieciowe, system NAC oraz aplikacje (poprzez agenta, syslog lub API).
- Mechanizm parsowania i dekodowania zdarzeń z możliwością tworzenia własnych dekodowników i reguł dla nietypowych źródeł.
- Indeksowanie i przechowywanie zdarzeń z możliwością pełnotekstowego przeszukiwania oraz definiowania polityk retencji i archiwizacji.
- Zapewnienie integralności gromadzonych logów (ochrona przed modyfikacją) na potrzeby dowodowe i zgodności.

Detekcja, analiza i zgodność

- Wbudowany mechanizm wykrywania włamań na hoście (HIDS) oraz analiza logów w czasie zbliżonym do rzeczywistego.
- Monitorowanie integralności plików (FIM) z wykrywaniem zmian w plikach i kluczach rejestru oraz rejestrowaniem informacji kto i kiedy dokonał zmiany.
- Wykrywanie podatności na monitorowanych hostach poprzez korelację zainstalowanego oprogramowania z bazami znanych podatności (CVE).

- Ocena konfiguracji bezpieczeństwa hostów (audyt zgodności konfiguracji, hardening) względem uznanych standardów oraz dobrych praktyk.
- Mapowanie wykrytych zdarzeń i reguł na uznaną macierz technik ataku (np. MITRE ATT&CK) oraz mechanizm korelacji zdarzeń z wielu źródeł.
- Wykrywanie złośliwego oprogramowania oraz anomalii (m.in. wykrywanie nieznanych procesów, nietypowych połączeń) oraz możliwość integracji ze źródłami informacji o zagrożeniach (threat intelligence).
- Predefiniowane zestawy reguł oraz raportów wspierających zgodność z uznanymi normami i regulacjami (m.in. zarządzanie bezpieczeństwem informacji, ochrona danych), z możliwością rozbudowy o własne reguły.

Reagowanie (XDR), wizualizacja i integracja

- Mechanizm aktywnego reagowania umożliwiający automatyczne działania na hoście w odpowiedzi na zdarzenie (m.in. blokada adresu IP, izolacja hosta, zatrzymanie procesu lub uruchomienie skryptu).
- Graficzna konsola webowa z konfigurowalnymi pulpitemi, wyszukiwaniem i analizą zdarzeń oraz generowaniem raportów; interfejs w języku polskim lub angielskim.
- Kontrola dostępu do konsoli oparta o role (RBAC) oraz możliwość integracji uwierzytelniania z usługą katalogową lub innym zewnętrznym dostawcą tożsamości.
- Mechanizm alertów i powiadomień (m.in. poczta elektroniczna) oraz interfejs programistyczny (API) i wsparcie integracji z zewnętrznymi systemami (m.in. zgłoszeniowymi, powiadomień, SOAR).
- Dostępna publicznie dokumentacja techniczna oraz regularnie aktualizowane reguły detekcji i sygnatury.

6.3. Instalacja i konfiguracja platformy

- Instalacja serwera/serwerów SIEM (fizycznych lub wirtualnych) oraz przygotowanie repozytorium logów i indeksów.
- Konfiguracja ról, kont administracyjnych i dostępu opartego o role (RBAC).
- Konfiguracja retencji, archiwizacji oraz zabezpieczenia integralności gromadzonych logów.

6.4. Integracja źródeł i detekcja

- Podłączenie źródeł logów: serwery, hypervisor, usługi katalogowe, przełączniki, zaporę, system NAC, stacje robocze, urządzenia kluczowe.
- Konfiguracja agentów/kolektorów oraz normalizacji i parsowania zdarzeń z poszczególnych źródeł.
- Wdrożenie reguł korelacji i scenariuszy detekcji (use case) dostosowanych do środowiska oraz typowych technik ataku.
- Konfiguracja funkcji detekcji i reagowania (XDR) na stacjach i serwerach, w zakresie wspieranym przez rozwiązanie.
- Konfiguracja alertów, powiadomień i klasyfikacji incydentów.

6.5. Dostrojenie, testy i dokumentacja

- Dostrojenie reguł w celu ograniczenia liczby fałszywych alarmów (false-positive) oraz kalibracja progów.
- Konfiguracja pulpitu (dashboardów), widoków operacyjnych i raportów (w tym raportów na potrzeby zgodności).

- Testy detekcji wybranych scenariuszy oraz weryfikacja kompletności i poprawności zbieranych logów.
- Dokumentacja konfiguracji, wykazu źródeł logów, reguł korelacji oraz procedur obsługi alertów.

Konsultacje techniczne

- Przed wdrożeniem: konsultacje dot. architektury SIEM/XDR, doboru źródeł logów, projektowania scenariuszy detekcji (use case), polityki retencji oraz wymagań pojemnościowych i wydajnościowych.
- W trakcie wdrożenia: nadzór nad integracją źródeł i konfiguracją reguł, wsparcie decyzyjne przy projektowaniu korelacji i progów alertowania, weryfikacja kompletności zbieranych danych.
- Po wdrożeniu: konsultacje stabilizacyjne, dostrajanie reguł na podstawie rzeczywistego ruchu, ograniczanie fałszywych alarmów, rozwój scenariuszy detekcji.
- Transfer wiedzy: szkolenie administratorów z obsługi konsoli SIEM, analizy alertów i incydentów, tworzenia reguł i raportów oraz procedur reagowania na zdarzenia bezpieczeństwa.
- Wsparcie powdrożeniowe: konsultacje w oknie wsparcia w zakresie podłączania nowych źródeł logów, rozwoju reguł korelacji oraz wsparcia analitycznego przy incydentach.

7. Dostawa i wdrożenie NAC

Zakres obejmuje dostarczenie i wdrożenie systemu kontroli dostępu do sieci (NAC), umożliwiającego uwierzytelnianie i autoryzację urządzeń przyłączanych do sieci, profilowanie urządzeń oraz egzekwowanie polityk dostępu w oparciu o tożsamość i stan urządzenia. Wdrożenie prowadzone jest etapowo — od trybu monitorującego do egzekwowania — w celu minimalizacji ryzyka zakłóceń.

7.1. Projekt i dostawa

- Analiza środowiska sieciowego, urządzeń końcowych i wymagań dostępu, projekt polityk i scenariuszy uwierzytelniania.
- Dostarczenie systemu NAC wraz z licencjami, zgodnie ze specyfikacją zamówienia.
- Projekt integracji z usługą katalogową, RADIUS oraz segmentacją VLAN.

7.2. Wymagania minimalne dla systemu NAC

Dostarczony system musi spełniać co najmniej poniższe wymagania funkcjonalne i techniczne. Zamawiający dopuszcza rozwiązania równoważne, tj. dowolny system spełniający wszystkie wymienione wymagania. Wymagania sformułowano w sposób neutralny technologicznie i niewskazujący konkretnego producenta.

Architektura i licencjonowanie

- Scentralizowany system kontroli dostępu do sieci (NAC), możliwy do wdrożenia w środowisku wirtualnym na systemie operacyjnym z rodziny Linux.
- Brak ograniczeń licencyjnych na liczbę obsługiwanych urządzeń końcowych (endpointów) oraz portów przełączników; dopuszcza się model bezpłatny bądź oparty wyłącznie o opcjonalne wsparcie producenta.
- Możliwość wdrożenia w trybie wysokiej dostępności (klaster) oraz obsługa wielu lokalizacji z jednego systemu zarządzającego.
- Wbudowany serwer RADIUS realizujący uwierzytelnianie i autoryzację dostępu do sieci, bez konieczności zakupu dodatkowych komponentów.

Uwierzytelnianie i kontrola dostępu

- Obsługa uwierzytelniania portów w standardzie 802.1X (przewodowo i bezprzewodowo) oraz uwierzytelniania w oparciu o adres MAC (MAB) dla urządzeń nieobsługujących 802.1X.
- Integracja ze źródłami tożsamości: usługa katalogowa (Active Directory), LDAP oraz zewnętrzny RADIUS, na potrzeby uwierzytelniania użytkowników i urządzeń.
- Dynamiczne przypisywanie sieci VLAN do urządzenia/użytkownika w wyniku uwierzytelnienia (enforcement na przełączniku), z wykorzystaniem mechanizmów RADIUS (m.in. atrybuty VLAN, RADIUS CoA — zmiana autoryzacji w trakcie sesji).
- Współpraca z przełącznikami i punktami dostępowymi różnych producentów (wsparcie dla wielu modeli/dostawców urządzeń sieciowych), zapewniająca niezależność od pojedynczego producenta infrastruktury.
- Portal przechwytyjący (captive portal) dla rejestracji i uwierzytelniania urządzeń (m.in. sieć gości) z możliwością dostosowania wyglądu oraz samodzielnej rejestracji.

Profilowanie, segmentacja i reagowanie

- Automatyczne wykrywanie i profilowanie (fingerprinting) urządzeń przyłączanych do sieci oraz ich klasyfikacja (m.in. komputery, urządzenia mobilne, drukarki, urządzenia sieciowe, IoT).
- Definiowanie polityk dostępu na podstawie tożsamości, typu i stanu urządzenia oraz przypisywanie urządzeń do odpowiednich segmentów (VLAN) zgodnie z polityką.
- Mechanizm izolacji/kwarantanny urządzeń nieautoryzowanych lub niezgodnych z polityką, z możliwością automatycznego przeniesienia do sieci ograniczonej.
- Możliwość weryfikacji stanu urządzenia końcowego (m.in. zgodność z politykami bezpieczeństwa) w trybie z agentem lub bezagentowym.
- Wdrożenie etapowe: możliwość pracy w trybie wyłącznie monitorującym (bez egzekwowania) przed przełączeniem w tryb egzekwowania polityk.

Zarządzanie i integracja

- Graficzna konsola webowa do zarządzania politykami, urządzeniami i użytkownikami, z kontrolą dostępu opartą o role (RBAC); interfejs w języku polskim lub angielskim.
- Rejestrowanie zdarzeń dostępu do sieci oraz możliwość przekazywania logów do zewnętrznego systemu SIEM (m.in. przez syslog) na potrzeby korelacji.
- Interfejs programistyczny (API) umożliwiający integrację z innymi systemami oraz automatyzację działań.
- Dostępna publicznie dokumentacja techniczna oraz regularne aktualizacje (m.in. baz profili urządzeń).

7.3. Instalacja i integracja

- Instalacja serwera/serwerów NAC (wirtualnych) oraz konfiguracja wysokiej dostępności, jeśli dotyczy.
- Integracja z usługą katalogową i serwerem RADIUS (NPS) na potrzeby uwierzytelniania użytkowników i urządzeń.
- Integracja z przełącznikami i infrastrukturą sieciową (przypisywanie VLAN, dynamiczna autoryzacja).
- Integracja obejmuje również istniejącą infrastrukturę firewall Stormshield wykorzystywaną przez Zamawiającego, w zakresie niezbędnym do prawidłowego działania wdrażanego rozwiązania, w tym polityk bezpieczeństwa, segmentacji sieci VLAN oraz komunikacji pomiędzy segmentami sieci.

7.4. Polityki dostępu i profilowanie

- Wdrożenie uwierzytelniania portów 802.1X oraz metody zapasowej opartej o adres MAC (MAB) dla urządzeń bez obsługi 802.1X.
- Konfiguracja profilowania i klasyfikacji urządzeń (komputery, drukarki, urządzenia sieciowe, IoT).
- Definicja polityk dostępu i dynamicznego przypisywania VLAN w zależności od tożsamości i typu urządzenia.
- Konfiguracja sieci kwarantanny i sieci gości oraz reguł postępowania z urządzeniami niezgodnymi z polityką.

7.5. Wdrożenie etapowe, testy i dokumentacja

- Uruchomienie w trybie monitorującym (bez egzekwowania) w celu identyfikacji urządzeń i weryfikacji polityk.
- Stopniowe przełączanie segmentów w tryb egzekwowania polityk, z monitorowaniem wpływu na użytkowników.
- Testy scenariuszy dostępu (urządzenie autoryzowane, nieautoryzowane, gość, urządzenie niezgodne).
- Dokumentacja polityk dostępu, integracji, scenariuszy uwierzytelniania oraz procedur obsługi.

Konsultacje techniczne

- Przed wdrożeniem: konsultacje dot. architektury NAC, strategii uwierzytelniania (802.1X / MAB), modelu polityk dostępu, profilowania urządzeń oraz planu wdrożenia etapowego minimalizującego ryzyko.
- W trakcie wdrożenia: nadzór nad integracją z RADIUS i przełącznikami, wsparcie decyzyjne przy definiowaniu polityk i obsłudze urządzeń problematycznych, kontrola przejścia w tryb egzekwowania.
- Po wdrożeniu: konsultacje stabilizacyjne, dostrajanie polityk na podstawie zaobserwowanych urządzeń i zdarzeń, ograniczanie wpływu na użytkowników.
- Transfer wiedzy: szkolenie administratorów z obsługi systemu NAC, zarządzania politykami, obsługi nowych urządzeń oraz diagnostyki problemów z dostępem do sieci.
- Wsparcie powdrożeniowe: konsultacje w oknie wsparcia w zakresie modyfikacji polityk, obsługi nowych typów urządzeń oraz rozwiązywania incydentów dostępu.

8. Testy podatności i testy socjotechniczne

Zakres obejmuje przeprowadzenie testów podatności infrastruktury oraz kontrolowanych testów socjotechnicznych, zakończonych raportem z oceną ryzyka i rekomendacjami naprawczymi. Testy realizowane są wyłącznie w zakresie, terminach i na warunkach uzgodnionych z Zamawiającym, na podstawie pisemnej autoryzacji, z zachowaniem zasad etyki, poufności i ochrony danych osobowych.

8.1. Przygotowanie i uzgodnienia

- Ustalenie zakresu testów (systemy, segmenty, grupy odbiorców), reguł postępowania (rules of engagement) oraz okien czasowych.
- Uzyskanie pisemnej autoryzacji oraz uzgodnienie kanałów komunikacji i procedury wstrzymania testów.

8.2. Testy podatności

- Skanowanie podatności infrastruktury sieciowej i serwerowej z perspektywy wewnętrznej (oraz zewnętrznej, jeśli dotyczy).
- Identyfikacja i klasyfikacja podatności wraz z oceną istotności (np. wg CVSS) i potencjalnego wpływu.

- Weryfikacja konfiguracji urządzeń, serwerów i usług pod kątem dobrych praktyk oraz wymagań KRI.
- Eliminacja wyników fałszywie dodatnich i potwierdzenie istotnych podatności (bez działań destrukcyjnych).

8.3. Testy socjotechniczne

- Przygotowanie i przeprowadzenie kontrolowanej kampanii phishingowej wśród uzgodnionej grupy pracowników.
- Pomiar wskaźników reakcji (otwarcia, kliknięcia, podanie danych, zgłoszenia do działu IT) bez gromadzenia danych wrażliwych poza zakresem testu.
- Zachowanie zasad etyki, proporcjonalności i ochrony danych osobowych przez cały czas trwania testów.

8.4. Raport, rekomendacje i omówienie

- Raport zbiorczy z wynikami testów podatności i socjotechnicznych, oceną ryzyka oraz priorytetyzacją działań naprawczych.
- Rekomendacje techniczne (naprawa podatności, twardnienie konfiguracji) oraz organizacyjne (procedury, podnoszenie świadomości).
- Omówienie wyników z Zamawiającym oraz wskazanie kierunków dalszego podnoszenia poziomu bezpieczeństwa.

Konsultacje techniczne

- Przed testami: konsultacje dot. zakresu i metodyki testów, reguł postępowania, doboru scenariuszy socjotechnicznych oraz aspektów prawnych i ochrony danych osobowych.
- W trakcie testów: bieżąca komunikacja o istotnych ustaleniach, konsultacje przy podatnościach krytycznych wymagających pilnej reakcji, koordynacja z zespołem Zamawiającego.
- Po testach: szczegółowe omówienie wyników, konsultacje przy planowaniu działań naprawczych oraz wsparcie w ustaleniu priorytetów remediacji.
- Transfer wiedzy: przekazanie zespołowi Zamawiającego wniosków z testów, dobrych praktyk w zakresie twardnienia i reagowania oraz rekomendacji dot. programu podnoszenia świadomości.
- Wsparcie powdrożeniowe: konsultacje w oknie wsparcia przy weryfikacji skuteczności wdrożonych działań naprawczych oraz planowaniu kolejnych cykli testów.

9. Dokumentacja, szkolenia i odbiór

Zakres obejmuje opracowanie kompletnej dokumentacji powykonawczej dla wszystkich wdrożonych obszarów, przeprowadzenie szkoleń administratorów oraz formalny odbiór całości wdrożenia, z weryfikacją zgodności z wymaganiami KRI / ISO 27001.

9.1. Dokumentacja powdrożeniowa

- Dokumentacja techniczna środowiska: schematy logiczne i fizyczne (sieć/VLAN, środowisko serwerowe i klastry, system kopii zapasowych, SIEM, NAC).
- Tablica adresacji IP, wykaz VLAN-ów, macierz przepływów, konfiguracje urządzeń i systemów.

- Procedury bezpieczeństwa: zarządzanie użytkownikami i uprawnieniami, obsługa incydentów, backup i odtwarzanie, zarządzanie zmianą.
- Dokumentacja eksploatacyjna i utrzymaniowa, w tym procedury monitorowania i reagowania na awarie.

9.2. Szkolenia administratorów

- Szkolenie z obsługi wdrożonych obszarów: sieć/VLAN, usługi katalogowe, wirtualizacja i klaster, system kopii zapasowych, SIEM, NAC.
- Szkolenie z procedur monitorowania, diagnostyki oraz reagowania na awarie i incydenty bezpieczeństwa.
- Przekazanie materiałów szkoleniowych oraz dokumentacji procedur.

9.3. Odbiór końcowy

- Testy odbiorowe per lokalizacja oraz odbiór końcowy całości wdrożenia, potwierdzony protokołem.
- Weryfikacja zgodności konfiguracji środowiska z wymaganiami KRI / ISO 27001.
- Przekazanie kompletu dokumentacji powykonawczej oraz potwierdzenie realizacji transferu wiedzy.
- Dostawa sprzętu bez jego pełnej konfiguracji, integracji, migracji danych oraz uruchomienia wszystkich wymaganych usług nie będzie uznana za realizację zamówienia.

Konsultacje techniczne

- Przed odbiorem: konsultacje dot. zakresu i struktury dokumentacji powykonawczej, kryteriów odbioru oraz przygotowania środowiska do weryfikacji zgodności z KRI / ISO 27001.
- W trakcie: wsparcie przy weryfikacji kompletności dokumentacji i procedur, konsultacje przy testach odbiorowych poszczególnych obszarów.
- Po odbiorze: konsultacje dot. utrzymania i aktualizacji dokumentacji oraz dalszego rozwoju procedur bezpieczeństwa i eksploatacji.
- Transfer wiedzy: kompleksowe przekazanie wiedzy o całości wdrożonego środowiska, wzajemnych zależnościach obszarów oraz dobrych praktykach eksploatacji.
- Wsparcie powdrożeniowe: konsultacje w uzgodnionym oknie wsparcia obejmujące całość wdrożonego środowiska, w tym wsparcie przy incydentach, zmianach konfiguracji i planowaniu rozwoju.

Uwagi końcowe

- Prace należy realizować w sposób minimalizujący przerwy w pracy Zamawiającego, w uzgodnionych oknach serwisowych, z procedurą wycofania dla działań krytycznych.
- Po każdym etapie Wykonawca przekazuje dokumentację powykonawczą oraz przeprowadza testy odbiorowe potwierdzone protokołem.
- Konsultacje techniczne stanowią integralny element każdej pozycji zamówienia i obejmują fazę przed wdrożeniem, w jego trakcie, po wdrożeniu, transfer wiedzy oraz wsparcie w uzgodnionym oknie powdrożeniowym.
- Konfiguracje urządzeń i systemów muszą być zgodne z politykami bezpieczeństwa Zamawiającego.