

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Zadanie 1 - Szkolenie pracowników - socjotechniki - 20 osób

Szkolenia z zakresu cyberbezpieczeństwa

Przedmiot zamówienia

Przedmiotem zamówienia jest:

- przeprowadzenie szkolenia zwiększającego świadomość pracowników Zamawiającego w dziedzinie cyberbezpieczeństwa;
- wykonanie testów socjotechnicznych na wybranej grupie kontrolnej pracowników Zamawiającego.

Szczegółowe wymagania

1. Szkolenie - minimalne wymagania:

- a. Szkolenie zamknięte
- b. Szkolenie musi być przeprowadzone w języku polskim;
- c. szkolenie musi odbyć się w formie zdalnej poprzez udostępniony przez Wykonawcę kanał elektroniczny lub dedykowaną aplikację, z możliwością późniejszego odtworzenia spotkania (nagranie szkolenia), z zastrzeżeniem nierozpowszechniania nagrania poza obszar organizacji Zamawiającego;
- d. Czas trwania szkolenia minimum 2 godziny
- e. Zamawiający dopuszcza udział uczestników szkolenia w ramach większej grupy szkoleniowej
- f. agenda szkoleń musi dotyczyć tematyki cyberbezpieczeństwa, w tym przynajmniej: socjotechniki, phishingu, ransomware, bezpieczeństwa poczty elektronicznej oraz korzystania z urządzeń mobilnych, sieci Wi-Fi, bezpieczeństwa nośników danych;
- g. wykonawca gwarantuje, że osoba prowadząca szkolenia posiada odpowiednie predyspozycje do prowadzenia szkoleń oraz wyczerpującą wiedzę, popartą 2-letnim doświadczeniem
- h. wykonawca zobowiązany jest w porozumieniu z Zamawiającym ustalić dokładną datę przeprowadzenia szkoleń.
- i. po ukończeniu szkolenia uczestnicy otrzymają zaświadczenie lub certyfikat ukończenia szkolenia w formie papierowej bądź elektronicznej. Zaświadczenia zostaną przesłane na wskazany przez Zamawiającego adres fizyczny lub adres skrzynki poczty elektronicznej.

2. Etap II (testy socjotechniczne) - minimalne wymagania:

- a. wykonanie testu weryfikacyjnego poziomu świadomości cyberzagrożeń Pracowników Zamawiającego poprzez nakłanianie ich do niestosowania się do obowiązujących zasad i procedur bezpieczeństwa obowiązujących u Zamawiającego;
- b. przygotowanie i wdrożenie indywidualnych scenariuszy kontrolowanego ataku hakerskiego, na wybraną grupę Pracowników Zamawiającego;
- c. opracowanie raportu po realizacyjnego zawierającego:
- d. wyniki przeprowadzonych testów oraz stan poziomu zabezpieczenia zasobów systemu informatycznego Zamawiającego;
- e. rekomendacje oraz zalecenia dla posiadanego środowiska;
- f. propozycje modernizacji środowiska lub jego zabezpieczeń;
- g. spotkanie organizacyjne pomiędzy Zleceniodawcą a Wykonawcą, mające na celu omówienie wyników testów socjotechnicznych oraz zaleceń i rekomendacji zawartych w raporcie po realizacyjnym.

Zadanie 2 - Szkolenia dla Administratorów

Przedmiot zamówienia

Przedmiotem zamówienia jest:

- Przeprowadzenie szkolenia z zakresu rozwiązań technicznych takich jak: Microsoft Active Directory, rozwiązania Fortinet Fortigate, rozwiązań kopii zapasowych dedykowanych środowiskom zwirtualizowanym, bezpieczeństwa sieci.

Szczegółowe wymagania

1. Szkolenie - minimalne wymagania:
 - a. szkolenia będą zrealizowane jako szkolenia zamknięte;
 - b. szkolenia będą przeprowadzone w języku polskim;
 - c. szkolenia muszą odbyć się w formie zdalnej poprzez udostępniony przez Wykonawcę kanał elektroniczny lub dedykowaną aplikację, z możliwością późniejszego odtworzenia spotkania (nagranie szkolenia), z zastrzeżeniem nierozpowszechniania nagrania poza obszar organizacji Zamawiającego;
 - d. Musi tworzyć cykl 3 (słownie trzech) szkoleń, trwających minimum 1 godzinę każde, gdzie łączna liczba godzin poświęcona na szkolenia nie może być mniejsza niż 10 godzin
 - e. Zamawiający dopuszcza udział uczestników szkolenia w ramach większej grupy szkoleniowej
 - f. agenda szkoleń musi dotyczyć tematyki technologicznej, w tym przynajmniej: Microsoft Active Directory, rozwiązania Fortinet Fortigate, rozwiązań kopii zapasowych dedykowanych środowiskom zwirtualizowanym, bezpieczeństwa sieci, rozwiązań klasy xDR/EDR.
 - g. obowiązek sprawdzania obecności w trakcie każdego ze szkoleń np. w postaci zrzutów ekranowych listy zalogowanych uczestników szkolenia pozwalającej potwierdzić obecność uczestników. Oryginalne wersje list obecności zostaną przekazane Zamawiającemu po zakończeniu każdej edycji szkolenia;

- h. wykonawca gwarantuje, że osoba prowadząca szkolenia posiada odpowiednie predyspozycje do prowadzenia szkoleń oraz wyczerpującą wiedzę, popartą 2-letnim doświadczeniem w obszarze technologicznym
- i. wykonawca zobowiązany jest w porozumieniu z Zamawiającym ustalić dokładną datę przeprowadzenia szkoleń
- j. po ukończeniu szkolenia uczestnicy otrzymają zaświadczenie lub certyfikat ukończenia szkolenia w formie papierowej bądź elektronicznej. Zaświadczenia zostaną przesłane na wskazany przez Zamawiającego adres fizyczny lub adres skrzynki poczty elektronicznej.

Zadanie 3 - Backup

Przedmiot zamówienia

Przedmiotem zamówienia jest:

1. dostawa serwera fabrycznie nowego, nie finansowanego wcześniej z krajowych lub unijnych funduszy projektowych,
2. dostawa macierzy NAS fabrycznie nowej, nie finansowanej wcześniej z krajowych lub unijnych funduszy projektowych,
3. dostawa streamera LTO fabrycznie nowego, nie finansowanego wcześniej z krajowych lub unijnych funduszy projektowych,
4. konfiguracja, instalacja serwera,
5. konfiguracja, instalacja macierzy NAS,
6. konfiguracja, instalacja streamera LTO,
7. dostawa sytemu kopii zapasowych – licencja wieczysta z dwuletnim wsparciem umożliwiającą kopie minimum 10 VM,
8. wdrożenie oraz konfiguracja systemu kopii zapasowych w środowisku IT Zamawiającego,
9. dostarczenie przez Wykonawcę dokumentacji konfiguracji wdrożonego rozwiązania.

Zestawienie wymaganych parametrów technicznych – serwer (1 sztuka)

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji 4 dysków 3.5"
Płyta główna	Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych
Procesor	Jeden procesor 8-rdzeniowy, min. 3.2GHz, umożliwiający osiągnięcie wyniku osiągający wynik w teście PassMark minimum 31200 punktów (Multithread Rating), wynik publikowany na stronie https://www.cpubenchmark.net/
Pamięć RAM	2x16GB pamięci RAM DDR5 UDIMM kompatybilnych z procesorem
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający Min. 8GB nieulotnej pamięci cache, Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.

	Wsparcie dla dysków samoszyfrujących
Dyski twarde	Zainstalowane 4x dysk 8TB SATA 6Gb/s 512e 7,2tys. obr./min 3,5-calowy, Hot-Plug. Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480 GB każdy, Hot-Plug z możliwością konfiguracji RAID 1.
Sloty PCIe	Dwa sloty PCIe
Interfejsy sieciowe/FC/SAS	min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz min. 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT Zainstalowana kompatybilna karta rozszerzeń HBA SAS (4 Ports Quad), 12 Gb/s
Wbudowane porty	Przynajmniej: 1 port USB 3.0 1 port USB 2.0 1 port VGA
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Zasilacze	Redundantne, o mocy maks. 800W
Elementy montażowe	Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
System operacyjny/dodat kowe oprogramowanie	Microsoft Windows Server 2025 Essentials - Licencja - 10 rdzeni
Bezpieczeństwo	Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardech. Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0 V3 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. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą: zdalny dostęp do graficznego interfejsu Web karty zarządzającej; zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; możliwość podmontowania zdalnych wirtualnych napędów (ISO/IMG); wirtualną konsolę z dostępem do myszy, klawiatury; wsparcie dla IPv6; wsparcie dla SNMP; IPMI2.0, SSH; możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; integracja z Active Directory/LDAP; możliwość obsługi przez dwóch administratorów jednocześnie; wsparcie dla automatycznej rejestracji DNS wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. możliwość bezpośredniego zarządzania poprzez dedykowany port USB
Oprogramowanie do zarządzania	wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych; integracja z usługą katalogową (LDAP/Active Directory); zarządzanie dostarczonymi serwerami bez udziału dedykowanego agenta zainstalowanego



	na zarządzanym hoście; wsparcie dla protokołów SNMP, IPMI, SSH, Redfish; możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram lub ręcznie; szczegółowy opis wykrytych systemów oraz ich komponentów; możliwość eksportu danych inwentaryzacyjnych i dzienników zdarzeń do pliku CSV lub HTML; możliwość filtrowania i tworzenia widoków inwentarza w oparciu o dowolne atrybuty zarządzanych urządzeń; grupowanie urządzeń w oparciu o kryteria użytkownika, w tym automatyczne grupowanie według elementów konfiguracji serwera (np. nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, stan gwarancji); możliwość uruchamiania narzędzi zarządzających dla poszczególnych urządzeń; przegląd stanu środowiska na jednym pulpicie nawigacyjnym; podsumowanie i szczegółowy status każdego urządzenia i jego komponentów; generowanie alertów przy zmianie stanu urządzenia; filtrowanie zdarzeń i alertów; integracja z centrum serwisowym producenta dostarczonej platformy sprzętowej (automatyczne zgłaszanie incydentów i wysyłanie danych diagnostycznych); możliwość przejęcia zdalnego pulpitu serwera; możliwość podmontowania wirtualnego napędu; możliwość definiowania akcji dla wybranych alertów i zdarzeń; przekazywanie alertów i zdarzeń do zewnętrznych systemów firm trzecich (poprzez SNMP lub Syslog); możliwość definiowania ról i uprawnień administratorów; zdalna aktualizacja oprogramowania wewnętrznego (firmware) serwerów bez udziału agenta, z możliwością wyboru źródła aktualizacji (lokalne repozytorium lub repozytorium on-line producenta); automatyczne generowanie i zgłaszanie incydentów awarii do centrum serwisowego producenta serwerów; moduł raportujący obejmujący co najmniej: numery seryjne sprzętu, konfigurację urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCIe i gniazd pamięci, adresy IP i MAC kart sieciowych, stan gwarancji, aktywne alerty oraz stan komponentów serwera; możliwość tworzenia sprzętowej konfiguracji bazowej i weryfikacji środowiska pod kątem rozbieżności; wdrażanie serwerów i przełączników sieciowych w oparciu o profile konfiguracyjne; możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami; tworzenie paczek danych diagnostycznych do diagnozy awarii przez serwis producenta; zdalne uruchamianie diagnostyki serwera; dedykowana aplikacja mobilna (Android/iOS) integrująca się z oprogramowaniem zarządzającym; oprogramowanie dostarczane jako wirtualny appliance dla środowisk KVM, VMware ESXi oraz Microsoft Hyper-V.
Oprogramowanie do monitorowania	Monitoring: stan i liczba podłączonych urządzeń (serwery, urządzenia sieciowe, pamięci masowe); alerty z podziałem na co najmniej: krytyczne, błędy, ostrzeżenia; status gwarancji dla poszczególnych urządzeń; informacje o stanie licencji oprogramowania rozszerzającego funkcjonalności urządzeń; monitoring parametrów serwerów (procesor, pamięć RAM, temperatura, pobór prądu, zmiany konfiguracji fizycznej) wraz z danymi historycznymi i wykrywaniem anomalii; monitorowanie wydajności pamięci masowych (opóźnienia, IOPS, przepustowość, pojemność) wraz z danymi historycznymi;



	dane historyczne o wykorzystaniu przestrzeni pamięci masowej przechowywane co najmniej 2 lata; monitoring parametrów przełączników sieciowych (model, firmware, IP, MAC, nr seryjny, komponenty, porty, obciążenie) wraz z danymi historycznymi; analityka predykcyjna i wykrywanie anomalii wydajnościowych w oparciu o dane historyczne. Aktualizacja firmware: możliwość aktualizacji firmware serwerów i systemów pamięci masowych wraz z informacją o zalecanych wersjach. Raporty: generowanie raportów dla serwerów i pamięci masowych (m.in. model, nr seryjny, konfiguracja, wersje firmware, stan gwarancji, alerty); eksport raportów do pliku CSV. Cyberbezpieczeństwo: analiza środowiska pod kątem najlepszych praktyk bezpieczeństwa z przypisaniem oceny bezpieczeństwa dla urządzeń i wskazaniem sposobu usunięcia wykrytych luk; możliwość definiowania ról administratorów.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 Serwer musi posiadać deklarację 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 według normy wprowadzonej w 2019 roku Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2025.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. Wymagana możliwość zachowania dysku twardego w ramach świadczonej usługi wsparcia serwisowego dla sprzętu, obejmująca 3-letni okres wsparcia serwisowego z gwarancją producenta. Usługa ma na celu umożliwienie zamawiającemu zachowania nośników danych (dysków twardych) po ich awarii. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. 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: 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. Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń
--	---

Zestawienie wymaganych parametrów technicznych – macierz NAS (1 sztuka)

Typ urządzenia	Serwer NAS
Obudowa	Rack 2U
Procesor	Czterordzeniowy procesor o taktowaniu 2,2 GHz osiągający w teście PassMark na lipiec 2025 co najmniej 4 550 punktów
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 4 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 32 GB
Możliwości rozbudowy	Sprzęt powinien być wyposażony w min. 8 kieszeni na dyski twarde typu hot-swap z możliwością rozszerzenia do 12 dysków łącznie przy użyciu dodatkowej jednostki rozszerzającej podłączanej do jednostki głównej za pomocą portu eSATA.
Porty zewnętrzne	Minimum:

Porty sieciowe	• 2 porty USB 3.2.1 • 1 port eSATA (jako gniazdo rozszerzenia)
Funkcja Wake on LAN/WAN	Minimum:
Gniazdo rozszerzeń PCIe 2.0	• 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)
Wentylator obudowy	Tak
System plików	Min. 1x 4-liniowe gniazdo x8 gen. 3 Min. 2 wentylatory (80 × 80 × 25 mm) Min.: • Wewnętrzny: Btrfs, ext4 • Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
Obsługiwane typy macierzy RAID	Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 • Maksymalny rozmiar pojedynczego wolumenu: 108 TB • Minimalny liczba wewnętrznych wolumenów: 64
Zarządzanie pamięcią masową	• Minimalny liczba obiektów iSCSI Target: 64 • Minimalny liczba jednostek iSCSI LUN: 128 • Obsługa klonowania/migawek jednostek iSCSI LUN
Obsługiwane protokoły	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, sesje Kerberized NFS, iSCSI, HTTP, HTTPS, FTP, SNMP, LDAP, CalDAV • Minimalna liczba kont użytkowników: 1 024 • Minimalna liczba grup użytkowników: 256
Konto i folder współdzielony	• Minimalna liczba folderów współdzielonych: 256 • Minimalna liczba zadań synchronizacji folderów współdzielonych: 8
Usługi plików	• Protokół plików: SMB, AFP, NFS, FTP, WebDAV, Rsync • Minimalna liczba połączeń SMB (oparta na FSCT): 180 • Integracja z listą kontroli dostępu Windows (ACL) • Uwierzytelnianie Kerberos NFS
Wirtualizacja	Obsługa VMware vSphere with VAAI, Windows Server 2022, Citrix Ready, OpenStack
Bezpieczeństwo	Zapora, szyfrowanie folderów współdzielonych, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, wsparcie Let's Encrypt, HTTPS (konfigurowalny zestaw szyfrów) • Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów współdzielonych • Urządzenie musi wspierać funkcję WORM (Write Once, Read Many) oraz migawki niezmiennie
Oprogramowanie	

Konserwacja

Zasilanie

Gwarancja

- Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów
 - Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym.
 - Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia.
 - Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwanych szyn rack
 - Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz
- Wykonawca udzieli gwarancji:
- 3 lata na urządzenia główne
 - 1 rok na dodatkowe akcesoria montażowe w postaci przesuwanych szyn rack

Zestawienie wymaganych parametrów technicznych – Dysk Typ1 - (8 sztuk)

Parametr	Wartość
Pojemność	4 TB
Format	3.5"
Interfejs	SATA 6 Gb/s
Prędkość obrotowa	5,400 obr./min
Maks. prędkość przesyłu danych	202 MB/s
Gwarancja	3 lata
Zużycie energii w trybie aktywnego bezczynności (typowe)	3.96 W
Zakres temperatury podczas pracy	0°C do 65°C (32°F do 149°F)
Zakre tempreatury podczas spoczynku	-40°C do 70°C (-40°F do 158°F)

Zestawienie wymaganych parametrów technicznych – biblioteka LTO (1 sztuka)

L.p.	Element konfiguracji	Wymagane minimalne parametry techniczne
1.	Wykorzystana technologia	LTO Ultrium wspierająca technologię partycjonowania nośników.
2.	Obudowa	Typu rack 19". Wysokość maksymalnie 1U - wszystkie elementy do montażu muszą być dostarczone wraz z urządzeniem. Urządzenie musi mieć możliwość instalowania w tej samej obudowie różnych generacji napędów LTO (minimum od LTO-6 wzwyż).
3.	Wbudowany napęd	LTO-8 wyposażony w dwa złącza mSAS SFF-8088. Urządzenie musi mieć możliwość instalowania w tej samej obudowie także napędów LTO z interfejsem FC oraz wspierać technologię LTFS (Linear Tape File System) umożliwiającą kopiowanie danych na taśmę bez konieczności użycia oprogramowania do backupu kompatybilną z systemami Linux, MAC OS i Microsoft. Prędkość zapisu pojedynczego napędu bez kompresji – minimum 300 MB/sek. Zainstalowany napęd musi mieć możliwość dynamicznego i płynnego dopasowania prędkości do napływających danych (speed matching) w przedziale od 100 do 300 MB/sek. oferować funkcję SkipSync zapewniającą dużą szybkość zapisu małych plików bez konieczności zatrzymywania i przewijania kasety oraz stosować szyfrowanie danych metodą AES 256-bit zgodną ze standardem FIPS 140-2
4.	Ilość slotów i magazynki	Minimum 8 kieszeni na taśmy podzielone na dwa magazynki (urządzenie musi być dostarczone z kompletem magazynków). Wymagana ilość mail slot (I/E): min. 1. Wymiana taśm przez MailSlot musi odbywać się bez konieczności wysuwania całego magazynka.
5.	Pojemność	Pojemność bez kompresji – minimum 96TB przy obsadzeniu wszystkich slotów na taśmy wyłącznie nośnikami LTO-8
6.	Zarządzanie	Za pomocą panelu kontrolnego znajdującego się na froncie urządzenia oraz zdalnie przez sieć poprzez przeglądarkę internetową (web GUI) za pomocą interfejsu FastEthernet. Wymagane wsparcie SNMP, protokołów SSL/TLS i IPv6 oraz definiowanie minimum 4 poziomów zarządzania urządzeniem i dostępem do niego. Urządzenie musi mieć możliwość zabezpieczania swojej konfiguracji na podłączony, poprzez slot USB, PenDrive. Operacja powinna być możliwa zarówno poprzez web GUI jak i poprzez panel kontrolny urządzenia. Wymagana możliwość zdalnego wysuwania magazynków, restartowania biblioteki oraz wyłączania zasilania napędów poprzez webGUI.
7.	Dodatkowe	Biblioteka musi być wyposażone w interfejs sieciowy, interfejs USB oraz

	interfejsy	interfejs ADI
8.	Obsługa urządzenia	Wymagana możliwość wymiany napędu, zasilacza, modułu portów zarządzania u użytkownika bez konieczności demontażu urządzenia z szafy przemysłowej oraz bez konieczności zdejmowania pokrywy głównej. Możliwość wyjmowania magazynków z urządzenia nawet przy braku zasilania. Zarówno napęd jak i zasilacz oraz moduł portów zarządzania powinny być wyposażone w lamki kontrolne, informujące o stanie technicznym i widoczne na tylnej stronie biblioteki. Wsparcie funkcjonalności Air Gap (izolacji powietrznej)
9.	Wyposażenie	Urządzenie musi być standardowo wyposażone w czytnik kodów kreskowych, zestaw kabli: 1x zasilając, 1x komunikacyjny konieczny do podłączenia urządzenia do odpowiedniego kontrolera serwera i umożliwiającego komunikację z urządzeniem – długość kabla min. 2m. W przypadku, gdyby serwer nie dysponował odpowiednim kontrolerem, należy taki dostarczyć wraz z urządzeniem – interfejs kontrolera: dual SAS 12Gb). Wraz z urządzeniem należy dostarczyć także zestaw 10-ciu identycznych nośników na dane o pojemności natywnej pojedynczego nośnika min. 12TB oraz jeden nośnik czyszczący wyposażonych w unikalne naklejki z kodem kreskowym. Wszystkie dostarczone nośniki muszą być kompatybilne i dedykowane do współpracy z oferowanym urządzeniem, co należy potwierdzić odpowiednim oświadczeniem producenta urządzenia dołączonym do oferty.
10.	Kompatybilność	Urządzenie musi być w pełni kompatybilne z aplikacją Veeam Backup and Replication, która będzie wykorzystywana do backupu danych – kompatybilność musi być potwierdzona odpowiednim oświadczeniem producenta urządzenia dołączonym do oferty
11.	Gwarancja	36 miesięcy z szybkiej wymiany całego urządzenia lub komponentów w czasie do 48 godz. (dni robocze) od momentu zgłoszenia uszkodzenia. Czas przyjmowania zgłoszeń serwisowych w trybie 5x9 z czasem reakcji do 12 godzin od zgłoszenia. Gwarantowana możliwość rozszerzenia oferowanego serwisu do 84 miesięcy. Do oferty należy dołączyć pisemne oświadczenia wystawione przez producenta o gwarancji świadczonej w rygorze 5x9xNBD realizowanej przez producenta wraz z potwierdzeniem możliwości przedłużenia gwarancji do 84 miesięcy.

Zestawienie wymaganych parametrów technicznych – system do Backupu

1. Wymagania ogólne

a. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter, posiadającym co najmniej 150 recenzji i średnią ocenę minimum 4,5 na platformie Gartner Peer Insights w kategorii Enterprise Backup and Recovery Software Solutions (<https://www.gartner.com/reviews/market/enterprise-backup-and-recovery-software-solutions>).

b. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba że wyszczególniono inaczej.

c. Oprogramowanie musi współpracować z infrastrukturą Nutanix AHV w wersji 6.5.x–6.7.x oraz Proxmox VE 8.2 lub nowszy.

d. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB/CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure Blob, Amazon S3 i urządzeń kompatybilnych z protokołem S3, oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

2. Całkowite koszty posiadania

- a. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.
- b. Oprogramowanie musi tworzyć samowystarczalne archiwa, do odtworzenia których nie jest wymagana osobna baza danych z metadanymi deduplikowanych bloków.
- c. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.
- d. Oprogramowanie musi posiadać mechanizmy zapewniające, że utrata bazy danych używanej przez oprogramowanie nie prowadzi do utraty możliwości odtworzenia backupu.
- e. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe, z wsparciem dla wielu pamięci masowych w tej puli.
- f. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Amazon S3, Wasabi Cloud Storage oraz innych kompatybilnych z S3 przestrzeniach obiektowych. Oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
- g. Oprogramowanie musi wspierać niezmienność kopii zapasowych (immutability) chroniącą przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
- h. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia wewnątrz maszyny wirtualnej dla funkcjonalności backupu lub odtwarzania maszyn wirtualnych.
- i. Oprogramowanie musi oferować portal samoobsługowy umożliwiający odtwarzanie przez użytkowników maszyn wirtualnych, obiektów MS Exchange, baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time).
- j. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu.
- k. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.
- l. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
- m. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami, jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiegokolwiek funkcjonalności wymienionej w tej specyfikacji.
- n. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.
- o. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
- p. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej.
- q. Oprogramowanie musi posiadać kontrolę dostępu opartą o role (RBAC) umożliwiającą definiowanie uprawnień poszczególnych administratorów.

3. Wymagania RPO

- a. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking (CBT) na wszystkich wspieranych platformach wirtualizacyjnych, certyfikowane przez dostawcę platformy.
- b. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.

- c. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak, aby nie przekraczane były skonfigurowane poziomy latencji.
- d. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych oraz odtwarzanie maszyn wirtualnych z takich snapshotów w środowisku VMware.
- e. Oprogramowanie musi posiadać wsparcie dla VMware vSAN.
- f. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO).
- g. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).
- h. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi, w tym co najmniej: Dell DataDomain, HPE StoreOnce oraz Quantum DXi.
- i. Oprogramowanie musi wspierać mechanizmy szybkiego klonowania bloków danych przy przechowywaniu kopii zapasowych na systemach plików Windows Server (ReFS) lub Linux (XFS).
- j. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji maszyn wirtualnych z wykorzystaniem wbudowanej akceleracji WAN.
- k. Oprogramowanie musi mieć możliwość replikacji asynchronicznej działających maszyn wirtualnych w środowiskach VMware vSphere oraz Hyper-V, zarówno między hostami, jak i z plików kopii zapasowych jako źródła replikacji.
- l. Oprogramowanie musi mieć możliwość replikacji ciągłej działających maszyn wirtualnych w środowisku VMware vSphere z RPO co najmniej 1 sekundy, z możliwością zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu w zadanym oknie RPO.
- m. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.
- n. Oprogramowanie musi umożliwiać wykorzystanie istniejących maszyn wirtualnych jako źródła do dalszej replikacji (replica seeding).
- o. Oprogramowanie musi wykorzystywać dostępne tryby transportu danych: sieć (LAN), hot-add oraz LAN-Free (SAN).

4. Wymagania RTO

- a. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze skompresowanego i zdeduplikowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania na storage produkcyjny — dla środowisk VMware, Hyper-V oraz Nutanix AHV.
- b. Powyższa funkcjonalność powinna umożliwiać uruchamianie backupów z innych platform (inne wirtualizatory, maszyny fizyczne).
- c. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny.
- d. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.
- e. Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego pliku backupu, z możliwością migracji on-line na środowisko produkcyjne.
- f. Oprogramowanie musi umożliwiać pełne odtworzenie maszyny wirtualnej, plików konfiguracji i dysków.
- g. Oprogramowanie musi umożliwiać pełne odtworzenie maszyny wirtualnej bezpośrednio do Microsoft Azure, Amazon EC2 oraz Google Cloud Platform.
- h. Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora lub serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz maszyny wirtualnej.

- i. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware oraz PowerShell Direct dla platformy Hyper-V.
- j. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, Mac.
- k. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM.
- l. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia agenta zainstalowanego wewnątrz maszyny wirtualnej.
- m. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory (konta użytkowników, konta komputerów, rekordy DNS, atrybuty, certyfikaty).
- n. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013 SP1 i nowszych, włącznie z obiektami z folderu „Permanently Deleted Objects”, bezpośrednio do środowiska produkcyjnego.
- o. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych, bezpośrednio do środowiska produkcyjnego, dla odzysku point-in-time oraz całych baz danych.
- p. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SharePoint 2013 i nowszych (całe witryny, biblioteki i dokumenty).
- q. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzania point-in-time, dla baz uruchomionych w środowiskach Windows oraz Linux, realizowane przez integrację z Oracle RMAN.
- r. Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzania point-in-time dla baz uruchomionych w środowiskach Linux.
- s. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN.
- t. Oprogramowanie musi posiadać natywną integrację dla backupów Microsoft SQL przez VSS/VDI.

5. Ograniczenie ryzyka

- a. Oprogramowanie musi dawać możliwość stworzenia izolowanego laboratorium dla vSphere i Hyper-V używając maszyn wirtualnych uruchamianych bezpośrednio z plików backupu, z możliwością uruchamiania backupów z innych platform.
- b. Dla VMware oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych.
- c. Oprogramowanie musi umożliwiać automatyczną weryfikację odtwarzalności wielu maszyn wirtualnych jednocześnie z dowolnego backupu według harmonogramu, w izolowanym środowisku, z możliwością uruchomienia skryptów testujących, bez interakcji z administratorem.
- d. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem, co najmniej dla Windows Defender.
- e. Oprogramowanie musi analizować zawartość zabezpieczanych maszyn w poszukiwaniu oznak obecności ransomware/malware (rozszerzenia plików, notatki żądania okupu).
- f. Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania.
- g. Oprogramowanie musi wykrywać oznaki złośliwego oprogramowania (malware, ransomware) na podstawie analizy anomalii w danych.
- h. Oprogramowanie musi umożliwiać automatyczne, dwuetapowe odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia skryptu przed odtworzeniem danych do środowiska produkcyjnego.

Wymagane prace wdrożeniowe

1. Dostarczenie sprzętu wraz z konfiguracją
 - a. Zinwentaryzowanie i walidacja aktualnego środowiska serwerowego
 - b. Podłączenie serwera, macierzy, biblioteki LTO do infrastruktury elektrycznej i sieciowej Zamawiającego, z zastrzeżeniem, że pasywna część teletechniczna leży w gestii Wykonawcy tj. szafa rack oraz okablowanie sieci komputerowej
 - c. Wstępna konfiguracja serwera, macierzy, biblioteki LTO polegająca na nadaniu dostępów, adresacji oraz aktualizacji oprogramowaniu sprzętowego do najnowszej zalecanej przez producenta wersji
 - d. Przekazanie dostępów Zamawiającemu
 - e. Testy po uruchomieniu środowiska polegające na sprawdzeniu poprawności uruchamiania się środowiska systemowego
 - f. Przygotowanie dokumentacji powdrożeniowej zawierającej opis wdrożonej konfiguracji wirtualizacji zasobów
2. Wdrożenie backup
 - a. instalacja oprogramowania do kopii zapasowych na zasobie wskazanym przez Zamawiającego;
 - b. skonfigurowanie repozytorium kopii zapasowych wskazanego przez Klienta
 - c. zaprojektowanie i wdrożenie polityki tworzenia kopii zapasowych z wykorzystaniem dostarczonego oprogramowania do kopii zapasowych dla przynajmniej 2 maszyn wirtualnych i 2 stacji roboczych;
 - d. przeprowadzenie testów akceptacyjnych poprawności działania operacji, kopii zapasowych i odzyskiwania danych;
 - e. konfiguracja powiadomień systemu kopii zapasowej oraz weryfikacja ich działania;

Zadanie 4 - Modernizacja DC

Przedmiot zamówienia

Przedmiotem zamówienia jest:

- a. Dostawa serwera fabrycznie nowego, nie finansowanego wcześniej z krajowych lub unijnych funduszy projektowych;
- b. Dostawa wymaganego oprogramowania
- c. Konfiguracja, instalacja serwera;
- d. Wdrożenie oraz konfiguracja środowiska wirtualizacji w środowisku IT Zamawiającego
- e. Wsparcie w migracji obecnie posiadanych systemów
- f. Dostarczenie przez Wykonawcę dokumentacji konfiguracji wdrożonego systemu

Wymagania szczegółowe Zamawiającego:

Zestawienie wymaganych parametrów technicznych – serwer

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 1U, 8 slotów na dyski 2.5" Hot-Swap. Obudowa z

	możliwością wyposażenia w panel wyświetlający informacje o stanie serwera (procesor, pamięć, dyski, BIOS, zasilanie, temperatura). Obudowa z możliwością wyposażenia w moduł umożliwiający bezpośredni dostęp z urządzenia mobilnego (Android/iOS) do konfiguracji i monitorowania kluczowych komponentów serwera za pośrednictwem dedykowanej aplikacji mobilnej, z wykorzystaniem połączenia USB lub Wi-Fi.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Obsługa procesorów 56 rdzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Na płycie głównej powinny znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 8TB pamięci RAM.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowany Jeden procesor min. 16-rdzeniowy, min. 2.0GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 266 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	128GB DDR5 RDIMM 5600MT/s, (8x16GB)
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający Min. 8GB nieulotnej pamięci cache, Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących
Dyski twarde	Zainstalowane: 5x 960 GB SSD SATA 6 Gb/s 512 2.5" do intensywnego odczytu, Hot-Plug. Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480 GB każdy z możliwością konfiguracji RAID 1.
Gniazda PCI	Trzy sloty PCIe LP
Interfejsy sieciowe/F C/SAS	min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz min. 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT
Wbudowane porty	Przynajmniej: 1 port USB 3.0 1 port USB 2.0 1 port VGA Możliwość rozbudowy o port RS232
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	Redundantne, Hot-Plug min. 1100W klasy Titanium
Elementy montażowe	Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
System operacyjny /dodatkowe oprogramowanie	Windows Server 2025 Standard w ilości umożliwiającej utworzenie 4 VM (z systemem z rodzinny Windows) zgodnie z licencją producenta.
Bezpieczeństwo	Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Możliwość wyłączenia w BIOS/UEFI funkcji przycisku zasilania oraz przejście do



	bezpiecznego trybu rozruchowego z zarządzaniem blokadą zasilania, panelem sterowania i zmianą hasła. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0. Możliwość dynamicznego włączania i wyłączania portów USB bez potrzeby restartu serwera. Możliwość bezpiecznego wymazania danych z dysków wewnętrznych serwera niezależnie od zainstalowanego systemu operacyjnego, uruchamiana z poziomu zarządzania serwerem. Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania zgodnie z zaleceniami NIST SP 800-147B. Serwer musi posiadać zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (sprzętowy Root of Trust).
Karta Zarządzania	zdalny dostęp do graficznego interfejsu Web karty zarządzającej; zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); szyfrowane połączenie (TLS) oraz uwierzytelnianie i autoryzację użytkowników; możliwość podmontowania zdalnych wirtualnych napędów; wirtualną konsolę z dostępem do myszy i klawiatury; wsparcie dla IPv6; wsparcie dla protokołów: SNMP, IPMI 2.0, SSH, Redfish oraz CIM-XML; zdalne monitorowanie poboru prądu w czasie rzeczywistym; zdalne ustawianie limitu poboru prądu serwera; integrację z Active Directory/LDAP; jednoczesną obsługę przez co najmniej dwóch administratorów; wsparcie dla automatycznej rejestracji DNS; wysyłanie powiadomień e-mail do administratora w przypadku awarii lub zmiany konfiguracji sprzętowej; lokalne zarządzanie przez dedykowany port USB na przednim panelu serwera; zarządzanie wieloma serwerami bezpośrednio z konsoli karty zarządzającej
Oprogramowanie do zarządzania	wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych; integracja z usługą katalogową (LDAP/Active Directory); zarządzanie serwerami bez udziału dedykowanego agenta; wsparcie dla protokołów SNMP, IPMI, SSH, Redfish; możliwość uruchamiania wykrywania urządzeń w oparciu o harmonogram lub ręcznie; szczegółowy opis wykrytych systemów i ich komponentów; możliwość eksportu danych inwentaryzacyjnych i dzienników zdarzeń do CSV lub HTML; filtrowanie i grupowanie urządzeń według kryteriów użytkownika (m.in. nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, stan gwarancji); przegląd stanu środowiska na pulpicie nawigacyjnym oraz szczegółowy status każdego urządzenia; generowanie alertów i filtrowanie zdarzeń; integracja z centrum serwisowym producenta (automatyczne zgłaszanie incydentów); możliwość przejęcia zdalnego pulpitu serwera oraz podmontowania wirtualnego napędu; możliwość definiowania akcji dla alertów, ról i uprawnień administratorów; przekazywanie alertów do zewnętrznych systemów przez SNMP lub Syslog; zdalna aktualizacja firmware bez agenta, z wyborem źródła (lokalne lub online producenta); moduł raportujący: numery seryjne, konfiguracja, wersje firmware, obsadzenie slotów PCIe i pamięci, adresy IP i MAC, stan gwarancji, alerty, stan komponentów; tworzenie konfiguracji bazowej i weryfikacja środowiska pod kątem rozbieżności;

	wdrażanie serwerów i przełączników w oparciu o profile konfiguracyjne; migracja ustawień serwera z wirtualnymi adresami sieciowymi (MAC, WWN, IQN); tworzenie paczek diagnostycznych i zdalne uruchamianie diagnostyki; dedykowana aplikacja mobilna (Android/iOS); oprogramowanie jako wirtualny appliance dla KVM, VMware ESXi i Microsoft Hyper-V.
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: Monitoring: stan i liczba podłączonych urządzeń; alerty z podziałem na co najmniej: krytyczne, błędy, ostrzeżenia; status gwarancji i licencji; monitoring parametrów serwerów (procesor, RAM, temperatura, pobór prądu, zmiany konfiguracji fizycznej) wraz z danymi historycznymi i wykrywaniem anomalii; monitorowanie wydajności pamięci masowych (opóźnienia, IOPS, przepustowość, pojemność) wraz z danymi historycznymi; dane historyczne o wykorzystaniu przestrzeni pamięci masowej przechowywane co najmniej 2 lata; monitoring parametrów przełączników sieciowych wraz z danymi historycznymi; analityka predykcyjna i wykrywanie anomalii wydajnościowych. Aktualizacja firmware: możliwość aktualizacji firmware serwerów i systemów pamięci masowych wraz z informacją o zalecanych wersjach. Raporty: generowanie raportów dla serwerów i pamięci masowych (model, nr seryjny, konfiguracja, wersje firmware, stan gwarancji, alerty); eksport raportów do pliku CSV. Cyberbezpieczeństwo: analiza środowiska według najlepszych praktyk bezpieczeństwa z oceną urządzeń i wskazaniem sposobu usunięcia wykrytych luk; możliwość definiowania ról administratorów.
Certyfikaty	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 według normy wprowadzonej w 2019 roku Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2025
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. Wymagana możliwość zachowania dysku twardego w ramach świadczonej usługi wsparcia serwisowego dla sprzętu, obejmująca 3-letni okres wsparcia serwisowego z gwarancją producenta. Usługa ma na celu umożliwienie zamawiającemu zachowania nośników danych (dysków twardych) po ich awarii. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.



	Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. 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 wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.
--	---

Wymagane prace wdrożeniowe

1. Dostarczenie sprzętu wraz z konfiguracją
 - a. Zinwentaryzowanie i walidacja aktualnego środowiska serwerowego
 - b. Zamawiający zobowiązuje się do wskazania osób kontaktowych, świadczących wsparcie dla aplikacji dziedzinowych, celem ich migracji do nowego środowiska serwerowego.
 - c. Dedykowane wsparcie aplikacji dziedzinowych realizuje migrację aplikacji do nowego środowiska na wniosek Zamawiającego

- d. Podłączenie serwera do infrastruktury elektrycznej i sieciowej Zamawiającego
- e. Konfiguracja serwera, polegająca na nadaniu dostępów, adresacji oraz aktualizacji oprogramowaniu sprzętowego do najnowszej zalecanej przez producenta wersji
- f. Konfiguracja środowiska wirtualizacji wraz z replikacją aktualnych VM
- g. Przekazanie dostępów Zamawiającemu
- h. Testy po uruchomieniu środowiska wirtualnego polegające na sprawdzeniu poprawności uruchamiania się środowiska systemowego
- i. Przygotowanie dokumentacji powdrożeniowej zawierającej opis wdrożonej konfiguracji wirtualizacji zasobów

Zadanie 5 - Sieć

Modernizacja sieci LAN

Przedmiot zamówienia

Przedmiotem zamówienia jest:

1. dostawa fabrycznie nowego Sprzętu, nie używanego w innych środowiskach ani projektach, w ilościach:
 - a. Przełącznik sieciowy 52p – 2 sztuki
 - b. Przełącznik sieciowy 10p – 10 sztuk
 - c. UTM z dwuletnim wsparciem – 1 sztuka
2. konfiguracja urządzeń oraz fizyczna instalacja w infrastrukturze IT Zamawiającego;
3. udzielenie przez Wykonawcę gwarancji i zapewnienie w jej ramach serwisu gwarancyjnego oraz wsparcia technicznego na dostarczony Sprzęt;
4. dostarczenie przez Wykonawcę dokumentacji dostarczonego Sprzętu;

Wymagania szczegółowe Zamawiającego

Zestawienie wymaganych parametrów technicznych dla przełączników sieciowych - 52P (2 sztuki)

Interfejs sieciowy	48x 1Gb Ethernet (10/100/1000 Mbps) 4x SFP+ (1/10 Gbps)
Interfejs zarządzania	Ethernet, In-Band
Łączna przepustowość (non-blocking)	Minimum 88 Gbps
Przepustowość przełączania	Minimum 176 Gbps
Prędkość przekazywania	Minimum 130 Mpps
Sposób zasilania	Uniwersalny: 100 - 240 V AC / 50 - 60 Hz USP RPS DC: 11.5 VDC, 5.22A
Zasilacz	Wbudowany, AC/DC Moc minimum 60 W
Maksymalny pobór mocy	60 W
Diody LED	System: Status RJ45: Speed / Link / Activity SFP+: Link / Activity RPS: Status
Waga	Z uchwytyami montażowymi: maksymalnie 4,15 kg Bez uchwytów montażowych: maksymalnie 4,10kg

Dopuszczalna temperatura pracy	Od -5 do 45 st. C
Certyfikaty	IC, FCC, CE
Możliwość montażu w szafie RACK	Tak, maksymalnie 1U

Zestawienie wymaganych parametrów technicznych dla przełączników sieciowych - 10P (10 sztuk)

Parametr	Wartość
Standardy i protokoły	IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE802.3z, IEEE 802.3ad, IEEE 802.3x, IEEE 802.3af, IEEE 802.3at, IEEE 802.3az, IEEE 802.1d, IEEE 802.1s, IEEE 802.1w, IEEE 802.1q, IEEE 802.1x, IEEE 802.1p
Porty	8 x RJ45 10/100/1000 Mbps PoE+ (autonegocjacja MDI/MDIX), 2 x SFP 100/1000 Mbps
Okablowanie sieciowe	10BASE-T: kategoria 3, 4, 5 (do 100 m), 100BASE-TX/1000Base-T: kategoria 5, 5e (do 100 m), 100BASE-FX: MMF, SMF, 1000BASE-X: MMF, SMF
Wentylator	1 wentylator
Zabezpieczenia fizyczne	Tak
Zasilanie	100-240V AC, 50/60Hz
Porty PoE (RJ45)	8 portów PoE+ (802.3at/af), łączne zasilanie 150W
Wymiary (S x G x W)	294 x 180 x 44 mm (11.6 x 7.1 x 1.7 cali)
Montaż	Szafa Rack, Biurko
Wydajność przełączania	20 Gbps
Szybkość przekierowań pakietów	14.9 Mpps
Tablica adresów MAC	8K
Bufor pakietów	4.1 Mbit
Ramki jumbo	9 KB
QoS	Priorytetowanie 802.1p CoS/DSCP, 8 kolejek priorytetów
Funkcje L2 i L2+	DHCP relay, LACP, STP, Spanning Tree, Port Mirroring, Link Aggregation
VLAN	Max 4K grup VLAN, VLAN 802.1Q, GVRP, VLAN głosowy
ACL	Do 230 wpisów ACL, wsparcie dla ACL na IP, MAC, czasie
Bezpieczeństwo transmisji	AAA, 802.1X, IP/IPv6-MAC Binding, DHCP Snooping, DoS Defend
Zawartość opakowania	Przełącznik, kabel zasilający, instrukcja, elementy montażowe, gumowe podstawki
Środowisko pracy	Temperatura: 0–50 °C, wilgotność: 10–90% RH bez kondensacji
Certyfikaty	CE, FCC, RoHS

Wymagania ogólne dla wszystkich typów przełączników sieciowych oraz wykonywanych prac:

1. Dostarczone urządzenia muszą pochodzić z autoryzowanego kanału sprzedaży producentów na rynek polski – do oferty należy dołączyć odpowiednie oświadczenie producenta sprzętu
2. Dostarczone urządzenia muszą być objęte gwarancją opartą o świadczenia gwarancyjne producenta sprzętu, niezależnie od statusu partnerskiego Wykonawcy przez okres co najmniej 12 miesięcy
3. Urządzenie musi mieć możliwość zarządzania i konfigurowania poprzez dedykowane rozwiązanie zarządzające, posiadające funkcje takie jak:
 - a. podgląd statusu urządzeń w czasie rzeczywistym
 - b. centralne zarządzanie wieloma sieciami z poziomu interfejsu graficznego
 - c. możliwość zdalnej aktualizacji oprogramowania urządzeń
 - d. wersję mobilną aplikacji
4. Przełączniki 52p muszą posiadać możliwość zarządzania konfiguracją w warstwach 2 oraz 3 modelu OSI
5. Dostarczający jest zobowiązany do podłączenia urządzeń sieciowych w infrastrukturze Zamawiającego do wskazanych miejsc połączeń sieciowych i elektrycznych
6. Dostarczający jest zobowiązany do aktualizacji oprogramowania sprzętowego dostarczonych urządzeń do najnowszej dostępnej i zalecanej przez producenta wersji
7. Dostarczający musi utworzyć dostępy administracyjne do urządzeń oraz przekazać je Zamawiającemu
8. W ramach przekazanych urządzeń, Wykonawca zobowiązuje się - na wskazanych przez Zamawiającego interfejsach - zdefiniować do 5 VLAN-ów
9. Na wskazanym przez Zamawiającego zasobie serwerowym, Wykonawca zobowiązany jest do instalacji, konfiguracji i dodania urządzeń sieciowych do dedykowanego centralnego rozwiązania zarządzającego.

Wymagania ogólne dla zakupu urządzenia UTM wraz z wdrożeniem klastra HA

1. Dostarczone urządzenia muszą pochodzić z autoryzowanego kanału sprzedaży producentów na rynek polski – do oferty należy dołączyć odpowiednie oświadczenie producenta sprzętu
2. Zapewnienie dwuletniej subskrypcji licencji UTP do urządzenia
3. Zakres prac:
 - a. Audyt istniejącej konfiguracji urządzenia
 - b. Aktualizacja oprogramowania na nowym urządzeniu UTM
 - c. Wyrównanie wersji oprogramowania na istniejącym urządzeniu
 - d. Wdrożenie urządzenia UTM - Podstawowa konfiguracja urządzenia: przypisanie adresacji IP, ustawienie interfejsów sieciowych, konfiguracja dostępu do panelu administracyjnego.
 - e. Konfiguracja klastra HA (High Availability) z istniejącym urządzeniem Fortigate FG 60F

- f. Testowanie i weryfikacja nowej konfiguracji
- 4. Dostarczający musi utworzyć dostępy administracyjne do urządzeń oraz przekazać je Zamawiającemu

Zadanie 6 - Dostawa i wdrożenie systemu klasy DLP

Wdrożenie DLP oraz konfiguracja polityk bezpieczeństwa.

Przedmiot zamówienia

- a. Dostarczenie oprogramowania klasy DLP
- b. Implementacja rozwiązania w środowisku zamawiającego
- c. Konfiguracja oprogramowania

Wymagania szczegółowe Zamawiającego

- 1. System operacyjny:
 - a. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
 - b. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
 - c. MacOS 12 lub nowszy.
- 2. Serwer administracyjny musi obsługiwać instalację na systemach:
 - a. Windows Server 2016 (64-bit) i nowszych.
- 3. Serwer administracyjny musi obsługiwać bazy danych:
 - a. MS SQL Server 2016 lub nowsze,
 - b. MS SQL Express,
 - c. AzureSQL S3 lub nowsze.
- 4. Pomoc i dokumentacja programu dostępne w języku angielskim.
- 5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.
- 6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
- 7. Serwer administracyjny musi umożliwiać instalację/deinstalację zdalnego klienta na stacjach roboczych.
- 8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.
- 9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.
- 10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.
- 11. System musi posiadać mechanizm usuwający najstarsze informacje, gdy rozmiar bazy osiągnie domyślny limit.
- 12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.
- 13. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.
- 14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).
- 15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.
- 16. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.
- 17. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.

18. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, połączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości e-mail oraz czynności na plikach.
19. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.
20. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.
21. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.
22. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.
23. Serwer administracyjny musi posiadać możliwość połączenia z serwerem SMTP udostępnianym przez producenta.
24. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików.
25. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.
26. Administrator musi mieć możliwość tworzenia kategorii danych dla plików zaszyfrowanych lub dla takich gdzie zawartość pliku jest niemożliwa do odczytania.
27. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.
28. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, numer REGON, NIP, wyrażenia regularne, określone ciągi znaków i numer IBAN.
29. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
30. Administrator musi mieć możliwość wyszukiwania danych wrażliwych w zasobach lokalnych
31. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.
32. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.
33. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
34. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365.
35. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.
36. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach.
37. System musi umożliwiać synchronizacji grup bezpieczeństwa z Active Directory na potrzeby logowania do konsoli zarządzającej.
38. System musi umożliwiać administratorowi nadanie użytkownikowi uprzywilejowanego dostępu, przez co nie będzie obejmowany politykami przez określony czas – 1 godzinę, 6 godzin lub do końca dnia.

39. System musi posiadać możliwość tworzenia polityk dynamicznych, pozwalających na dostosowywanie się akcji (takich jak zapisywanie logu, powiadomienie użytkownika, blokowanie lub blokowanie z możliwością zastąpienia przez użytkownika) w zależności od profilu pracy użytkownika wykonującego daną czynność, gdzie akcja dobierana jest w zależności od wyniku systemu uczenia maszynowego.

40. System musi umożliwiać dostosowanie polityk dynamicznych do dwóch trybów: standardowy oraz łagodny. Możliwość taka musi istnieć per użytkownik.

41. System musi umożliwiać tworzenie raportów na podstawie logów zebranych w układach danych z możliwością dostosowania filtrów, użytkowników oraz zakresu czasu objętych raportowaniem.

42. System musi umożliwiać utworzenie raportu, który będzie zawierał podsumowanie stanu zabezpieczenia danych wraz z rekomendacjami w formie cyklicznej.

43. System musi zbierać informacje na temat podłączanych urządzeń do komputera, odwiedzanych domen internetowych, ścieżek sieciowych, drukarek lokalnych oraz sieciowych, umożliwiając jednocześnie przypisanie takowych wpisów do bezpiecznych lub niezaufanych lokalizacji bez potrzeby manualnego wpisywania ścieżek lub numerów seryjnych urządzeń.

44. Dla każdej z wyżej wymienionych lokalizacji system powinien umożliwiać przypisanie indywidualnej polityki dostępu – np. umożliwiając przesyłanie danych do lokalizacji oznaczonej jako bezpieczna, jednocześnie blokując wysyłkę do lokalizacji oznaczonej jako niezaufana lub nieprzypisana.

45. System musi umożliwiać audyt operacji wykonywanych przez administratora w obszarze konsoli DLP.

46. System musi umożliwiać podłączenie archiwa logów w formacie plików o rozszerzeniu mdf

Wymagane prace wdrożeniowe

1. Dostarczenie oprogramowania klasy DLP
 - a. 30 bezterminowych licencji on-prem, licencja zawierająca rok wsparcia producenta
2. Implementacja rozwiązania w środowisku zamawiającego
 - a. Utworzenie i podstawowa konfiguracja VM
 - b. Instalacja konsoli centralnej
 - c. Wdrożenie agentów na wskazanych komputerach zamawiającego
 - d. Konfiguracja integracji dla Microsoft MS365
3. Konfiguracja oprogramowania
 - a. Utworzenie do 5 reguł DLP
 - b. Utworzenie do 5 kategorii danych
 - c. Przygotowanie danych i oraz do 2 raportów, omówienie raportów i zebranych danych

Zadanie 7 - Dostawa zasilacza awaryjnego UPS

Przedmiot zamówienia

Przedmiotem zamówienia jest:

1. dostawa fabrycznie nowych sprzętów, nie używanych w innych środowiskach ani projektach;
2. udzielenie przez Wykonawcę gwarancji i zapewnienie w jej ramach serwisu gwarancyjnego oraz wsparcia technicznego na dostarczony Sprzęt;
3. dostarczenie przez Wykonawcę dokumentacji dostarczonego Sprzętu;

Wymagania szczegółowe Zamawiającego

Zestawienie wymaganych parametrów technicznych systemu podtrzymania bateryjnego - Typ 1 – 1 sztuka

Nazwa komponentu	Wymagane minimalne parametry techniczne
Topologia	Line interactive
Typ przebiegu	Sinusoida
Liczba szaf rackowych	2U
Moc znamionowa w W	minimum 2700 W
Moc znamionowa w VA	minimum 3000 VA
Typowy czas ładowania do 90%	3 godziny
Rodzaj akumulatora	Akumulator kwasowo-ołowiowy
Masa produktu	Maksymalnie 37,5 kg
Sposób montażu	Montaż w szafie RACK (zestaw musi zawierać elementy montażowe)
Komunikacja i zarządzanie	Wielofunkcyjna konsola sterownicza i informacyjna LCD Wyświetlacz stanu LED ze wskaźnikiem zasilania Gniazdo karty zarządzania
Dostarczone wyposażenie	CD z oprogramowaniem Wsporniki montażowe do szaf przemysłowych Kabel do sygnalizacji RS-232 do Smart-UPS Czujnik temperatury podręcznik użytkownika Karta do zdalnego zarządzania Web SNMP Management Card
Certyfikaty produktu	C-Tick, CE, EAC, GOST, IRAM, VDE, UK PSTI
Normy	EN/IEC 62040-1:2019/A11:2021 EN/IEC 62040-2:2006/AC:2006 EN/IEC 62040-2:2018
Gwarancja	3 lata gwarancji naprawy lub wymiany (bez akumulatora) i 2 lata na akumulator

Zestawienie wymaganych parametrów technicznych systemu podtrzymania bateryjnego - Typ 2 - 25 sztuki

Nazwa komponentu	Wymagane minimalne parametry techniczne
Topologia	Line interactive
Moc znamionowa w W	minimum 650 W
Moc znamionowa w VA	minimum 1200 VA
Typ przebiegu	Schodkowa aproksymacja sinusiody
Typowy czas ładowania do 90%	8 godziny
Napięcie akumulatora	12 V
Masa produktu	Maksymalnie 8 kg

Sposób montażu	Wolnostojący
Rodzaj akumulatora	Akumulator kwasowo-ołowiowy
Typ połączenia wyjściowego	4 Schuko
Elementy zestawu	Podręcznik użytkownika
Komunikacja i zarządzanie	Dioda led wskazująca na status zasilania: zasilanie z sieci energetycznej: zasilanie z akumulatora
Certyfikaty produktu	CE, CB, EAC
Normy	EN/IEC 62040-1:2019/A11:2021 EN/IEC 62040-2:2006/AC:2006 EN/IEC 62040-2:2018
Gwarancja	2 lata na naprawę lub wymianę

Zadanie 8 - System rejestracji incydentów

Zapewnienie systemu rejestracji i zarządzania incydentami

Przedmiot zamówienia

Przedmiotem zamówienia jest:

1. dostawa oprogramowania do rejestrowania i zarządzania incydentów w infrastrukturze IT Zamawiającego;
2. przeprowadzenie szkolenia z posługiwania się dostarczonym rozwiązaniem.

Szczegółowe wymagania rozwiązania

Integracja z posiadanym rozwiązaniem ochrony endpoint

Zamawiający posiada aktywną licencję na rozwiązanie ochrony endpoint Eset o kluczu publicznym: 33B-TK5-BT.

Oferowane rozwiązanie musi zapewniać pełną kompatybilność i integrację z posiadaną infrastrukturą ochrony, umożliwiającą rozszerzenie zakresu ochrony bez konieczności wymiany dotychczasowo wdrożonego oprogramowania.

Konsola zarządzająca

1. Rozwiązanie musi być dostępne w modelu chmurowym zarządzanym przez producenta oprogramowania, bez konieczności utrzymania dodatkowej infrastruktury serwerowej po stronie Zamawiającego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu przeglądarki internetowej (interfejs WWW), bez konieczności instalowania dodatkowego oprogramowania klienckiego.
3. Dostęp do konsoli zarządzającej musi być chroniony z wykorzystaniem protokołu szyfrowania SSL/TLS.
4. Rozwiązanie musi posiadać mechanizm wykrywania sklonowanych maszyn na podstawie unikalnego identyfikatora sprzętowego stacji roboczej, zapobiegający powstawaniu zduplikowanych wpisów w konsoli.
5. Rozwiązanie musi umożliwiać komunikację agenta zarządzającego z serwerem centralnym za pośrednictwem serwera proxy HTTP.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi (MDM) z poziomu konsoli centralnej.
7. Rozwiązanie musi posiadać mechanizm wymuszenia uwierzytelnienia wieloskładnikowego (MFA) przy logowaniu do konsoli administracyjnej.

8. Rozwiązanie musi posiadać granularny model uprawnień dla użytkowników konsoli, umożliwiający przypisanie uprawnień co najmniej w zakresie: zarządzania politykami, raportowaniem, zarządzaniem licencjami oraz zadaniami administracyjnymi. Każda z funkcji musi obsługiwać co najmniej następujące poziomy dostępu: odczyt, użycie, zapis oraz brak dostępu.
9. Rozwiązanie musi posiadać co najmniej 80 predefiniowanych szablonów raportów dostarczonych przez producenta.
10. Rozwiązanie musi umożliwiać tworzenie statycznych i dynamicznych grup urządzeń.
11. Dynamiczne grupy urządzeń muszą być tworzone w oparciu o szablony definiujące warunki kwalifikacji, obejmujące co najmniej: zakresy adresów IP, obecność aktywnych zagrożeń, stan ochrony i działania agenta, wersję systemu operacyjnego oraz parametry sprzętowe stacji.
12. Rozwiązanie musi umożliwiać uruchamianie zadań automatycznych z co najmniej następującymi wyzwalaczami: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia w dzienniku oraz po przypisaniu urządzenia do grupy dynamicznej.

Funkcjonalności rozwiązania

1. Wykrywanie i rejestrowanie incydentów bezpieczeństwa na serwerach i stacjach roboczych z systemem operacyjnym Windows.
2. Wykrywanie i rejestrowanie incydentów bezpieczeństwa na zarządzanych urządzeniach mobilnych.
3. Wykrywanie i rejestrowanie incydentów bezpieczeństwa w usługach Microsoft 365 (w tym Exchange Online, SharePoint Online, OneDrive).
4. Wykrywanie podatności w zainstalowanych aplikacjach i systemach operacyjnych zarządzanych urządzeń.
5. Możliwość zabezpieczenia dostępu do systemów operacyjnych i aplikacji z wykorzystaniem dodatkowego składnika uwierzytelnienia (MFA).

Monitorowanie i korelacja incydentów

1. Dostęp do konsoli centralnego zarządzania incydentami musi odbywać się z poziomu przeglądarki internetowej (interfejs WWW).
2. Serwer administracyjny musi posiadać natywny mechanizm przekazywania zdarzeń do konsoli zarządzającej tego samego producenta, umożliwiający scentralizowany podgląd wykrytych zagrożeń.
3. Interfejs konsoli musi być chroniony z wykorzystaniem protokołu szyfrowania SSL/TLS.
4. Serwer administracyjny musi umożliwiać definiowanie wykluczeń, których spełnienie zapobiega generowaniu alarmu bezpieczeństwa.
5. Wykluczenia muszą dotyczyć zarówno procesu będącego bezpośrednim źródłem zdarzenia, jak i procesu nadrzędnego (procesu „rodzica”).
6. Utworzenie wykluczenia musi skutkować automatycznym rozwiązaniem istniejących alarmów spełniających kryteria tego wykluczenia.
7. Kryteria definiowania wykluczeń muszą obejmować co najmniej: nazwę procesu, ścieżkę procesu, parametry wiersza polecenia, wydawcę (sygnatariusza), typ podpisu cyfrowego, wartość skrótu SHA-1, nazwę komputera, grupę urządzeń oraz nazwę użytkownika.
8. Serwer administracyjny musi posiadać zestaw wbudowanych reguł detekcji dostarczonych przez producenta, wyzwalających alarmy bezpieczeństwa po ich

- spełnieniu. Liczba wbudowanych reguł dostarczanych przez producenta musi wynosić co najmniej 500. Administrator musi posiadać możliwość tworzenia własnych reguł detekcji oraz modyfikacji reguł dostarczonych przez producenta.
9. Serwer administracyjny musi umożliwiać blokowanie plików na podstawie ich sumy kontrolnej (hash). Mechanizm blokowania musi umożliwiać dodanie komentarza do wpisu oraz konfigurację akcji wykonywanej po wykryciu zablokowanej sumy kontrolnej.
 10. Administrator musi posiadać możliwość przeglądania listy plików wykonywalnych uruchomionych na stacjach roboczych wraz ze szczegółami wybranego procesu, obejmującymi co najmniej: wartość SHA-1, typ podpisu cyfrowego, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz wskaźniki reputacji i popularności.
 11. Administrator musi posiadać możliwość oznaczenia plików wykonywalnych oraz bibliotek DLL jako bezpieczne lub niebezpieczne, pobrania ich do analizy oraz ich zablokowania — bezpośrednio z poziomu konsoli.
 12. Administrator musi posiadać możliwość przeglądania listy skryptów uruchomionych na stacjach roboczych wraz z informacją o parametrach ich uruchomienia oraz możliwość oznaczenia każdego skryptu jako bezpieczny lub niebezpieczny.
 13. W ramach podglądu wykonanego skryptu administrator musi mieć możliwość przeglądania szczegółowych informacji o czynnościach wykonanych przez skrypt w formie tekstowej.
 14. W ramach analizy skryptu lub pliku wykonywalnego administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń, obejmujących co najmniej: modyfikacje plików i rejestru systemowego, nawiązane połączenia sieciowe oraz utworzone procesy potomne.
 15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktem ochrony endpoint tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. Konsola zarządzająca musi umożliwiać podgląd co najmniej: szczegółów sprzętowych zarządzanego komputera (producent, model, numer seryjny, dane systemu operacyjnego, procesor, pamięć RAM, dyski, wyświetlacz, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz listy zainstalowanego oprogramowania firm trzecich.
 16. Konsola administracyjna musi umożliwiać tagowanie obiektów (urządzeń, procesów, zdarzeń, incydentów) w celu ich kategoryzowania i filtrowania.
 17. Konsola administracyjna musi umożliwiać zdalne połączenie ze stacją roboczą i wykonywanie poleceń z poziomu interfejsu wiersza poleceń lub sesji PowerShell.

Wymagane prace wdrożeniowe

1. Uruchomienie konsoli do Zarządzania wraz z integracją z istniejącym rozwiązaniem
2. konfiguracja wstępna i nadanie dostępu do logowania dla Zamawiającego;
3. przygotowanie po konsultacji z Zamawiającym definicji incydentów
4. konfiguracja 5 szablonów raportów zgodnych z wymogami Zamawiającego
5. konfiguracja powiadomień na wskazaną przez Zamawiającego skrzynkę pocztową za pośrednictwem dedykowanej skrzynki technicznej dostarczonej przez Zamawiającego.

Informacje dodatkowe:

Zamawiający wymaga, aby elementy przedmiotu zamówienia przeznaczone do użytku osób fizycznych, w tym pracowników Zamawiającego, były wykonane z uwzględnieniem wymagań dostępności dla osób z niepełnosprawnościami oraz projektowania z przeznaczeniem dla wszystkich użytkowników, zgodnie z art. 100 ustawy Prawo zamówień publicznych oraz ustawą o zapewnianiu dostępności osobom ze szczególnymi potrzebami. W szczególności Wykonawca zapewni dostępność cyfrową materiałów szkoleniowych, nagrań, dokumentacji, raportów, instrukcji, formularzy, komunikatów użytkownika, certyfikatów elektronicznych oraz interfejsów WWW/aplikacyjnych dostarczanych lub konfigurowanych w ramach zamówienia, w zakresie adekwatnym do ich przeznaczenia. Materiały i dokumenty elektroniczne powinny być przekazane w formatach umożliwiającym odczyt maszynowy, posiadać logiczną strukturę nagłówków, poprawne tabele, teksty alternatywne dla istotnych elementów graficznych, odpowiedni kontrast, możliwość powiększania treści oraz obsługę przez technologie wspomagające. Nagrania szkoleń powinny posiadać co najmniej transkrypcję albo napisy, a platforma szkoleniowa powinna umożliwiać udział osobom korzystającym z klawiatury i technologii wspomagających. Interfejsy systemów, konsol administracyjnych i portali WWW powinny być możliwe do obsługi z klawiatury, współpracować z aktualnymi przeglądarkami i technologiami wspomagającymi, posiadać czytelne komunikaty błędów, dostępne formularze, odpowiedni kontrast, skalowalność tekstu oraz dostępne mechanizmy uwierzytelniania, w tym MFA. Jeżeli ze względu na charakter danego elementu przedmiotu zamówienia pełne zapewnienie dostępności nie jest możliwe albo nie jest uzasadnione, Wykonawca wskaże ograniczenie i zaproponuje rozwiązanie alternatywne, a Zamawiający odnotuje uzasadnienie ograniczenia.