Załącznik nr 7 do SWZ

Szczegółowy opis przedmiotu zamówienia

Przedmiot zamówienia:

Część 1:

Zakup i dostawa serwera z oprogramowaniem – 2 szt.

|  |  |
| --- | --- |
|  | Serwer – 2 sztuki |
|  | WYMAGANIA MINIMALNE |
| Obudowa | * Obudowa Rack o wysokości max 1U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych, oraz organizatorem do kabli. * 8 wnęk na dyski 2.5” * Obudowa wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |
| Płyta główna | * Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| Chipset | * Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |
| Procesor | * Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 165 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |
| RAM | * Minimum 128GB, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać maksymalnie minimum 1TB pamięci RAM. |
| Kontroler RAID | * Sprzętowy kontroler dyskowy, posiadający   + Min. 8GB nieulotnej pamięci cache,   + Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. |
| Dyski | * Zainstalowany 1x dysk SAS o pojemności min. 1.2TB Hot-Plug. * Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480GB z możliwością konfiguracji RAID 1. |
| Gniazda PCI | * Trzy sloty PCIe LP |
| Interfejsy sieciowe /FC/SAS | * Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (w slocie OCP) * Zainstalowane dodatkowe: dwuportowa karta sieciowa 25Gb Ethernet   w standardzie SFP28 oraz dwuportowa karta sieciowa 10Gb Ethernet  w standardzie Base-T   * 2 wkładki 25GbE SFP28 SR (dual rate – 10/25GbE) |
| Wbudowane porty | * 3 x USB z czego nie mniej niż 1x USB 3.0, 1x VGA |
| Video | * Zintegrowana karta graficzna |
| Zasilacze | * Redundantne, Hot-Plug min. 700W każdy |
| System operacyjny | Zainstalowany system operacyjny posiadający następujące, wbudowane cechy (licencja systemu musi uprawniać do uruchamiania systemu w środowisku fizycznym oraz sześciu wirtualnych środowisk systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji):  a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym  b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny,  c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych,  d) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci,  e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,  f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,  g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading),  i) wbudowane wsparcie instalacji i pracy na wolumenach, które:  - pozwalają na zmianę rozmiaru w czasie pracy systemu;  - umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów;  - umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów;  - umożliwiają zdefiniowanie list kontroli dostępu (ACL).  j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów)  w oparciu o ich zawartość;  k) wbudowane szyfrowanie dysków;  l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET;  m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów;  n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych;  o) graficzny interfejs użytkownika;  p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe;  r) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play);  s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu;  t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa;  u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  II. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji  roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach,  pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały  sieciowe), z możliwością wykorzystania następujących funkcji:  1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,  III. zdalna dystrybucja oprogramowania na stacje robocze,  IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,  V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:  1) dystrybucję certyfikatów poprzez http,  2) konsolidację CA dla wielu lasów domeny,  3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  VI. szyfrowanie plików i folderów,  VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),  VIII. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,  IX. serwis udostępniania stron WWW,  X. wsparcie dla protokołu IP w wersji 6 (IPv6),  XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:  1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  2) obsługi ramek typu jumbo frames dla maszyn wirtualnych,  3) obsługi 4-KB sektorów dysków,  4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,  5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,  6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),  v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet,  w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath),  x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,  y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,  z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |
| Bezpieczeństwo | Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.  Moduł TPM 2.0 |
| Karta Zarządzania | * Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   + 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 autentykacje i autoryzację użytkownika;   + możliwość podmontowania zdalnych wirtualnych napędów;   + wirtualną konsolę z dostępem do myszy, klawiatury;   + wsparcie dla IPv6;   + wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;   + możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;   + możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;   + integracja z Active Directory;   + możliwość obsługi przez dwóch administratorów jednocześnie;   + wsparcie dla automatycznej rejestracji DNS   + wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. |
| Oprogramowanie do zarządzania | * Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:   + Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych   + integracja z Active Directory   + Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta   + Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish   + Możliwość uruchamiania procesu wykrywania urządzeń  w oparciu o harmonogram   + Szczegółowy opis wykrytych systemów oraz ich komponentów   + Możliwość eksportu raportu do CSV, HTML, XLS, PDF   + Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.   + Grupowanie urządzeń w oparciu o kryteria użytkownika   + Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji   + Możliwość uruchamiania narzędzi zarządzających  w poszczególnych urządzeniach   + Szybki podgląd stanu środowiska   + 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.   + Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.   + Zdalne uruchamianie diagnostyki serwera. |
| Certyfikaty | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. * Serwer musi posiadać deklaracja CE. * Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022, Microsoft Windows Server 2025 |
| Warunki gwarancji | 5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.  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.  Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.  Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera |

Zamawiający wymaga, aby do oferowanych serwerów (2 szt.) dostarczono licencje dostępowe dla 30 użytkowników.

Zakup i dostawa macierzy z oprogramowaniem – 1 szt.

|  |  |
| --- | --- |
| Macierz – 1 sztuka | |
| PARAMETR | WYMAGANIA MINIMALNE |
| Obudowa | Do instalacji w standardowej szafie RACK 19” rozwiązanie może zajmować maksymalnie 2U i pozwalać na instalacje 24 dysków 2.5”. |
| Kontrolery | Dwa kontrolery RAID pracujące w układzie active-active posiadające łącznie minimum osiem portów iSCSI 25Gb/s. |
| Cache | 16GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami |
| Dyski | Zainstalowane 10 dysków 2,5” Hot-Plug SAS SSD 24Gbps o pojemności min. 1.92TB każdy.  Możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych do łącznie minimum 276 dysków. Możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki. |
| Oprogramowanie/  Funkcjonalności | Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5.  Macierz musi umożliwiać utworzenie minimum 500 LUN’ów oraz 500 kopii migawkowych na całą macierz. Macierz musi umożliwiać podłączanie minimum 8 hostów.  Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między rożnymi typami dysków.  Możliwość wykorzystania dysków SSD jako cache macierzy.  Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym. |
| Wsparcie dla systemów operacyjnych | Windows Server 2022, Windows Server 2019, Windows Server 2016, Red Hat Enterprise Linux (RHEL), SLES, Vmware ESXi. |
| Bezpieczeństwo | Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne. |
| Warunki gwarancji dla macierzy | 5 lat gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7, poprzez ogólnopolską linię telefoniczną producenta.  Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń. W razie awarii dyski pozostają w siedzibie Zamawiającego (usługa pozostawienia dysków) – dokumenty potwierdzające należy załączyć do oferty.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy. |
| Okablowanie sygnałowe | Należy dostarczyć minimum 4 kable DAC SFP28 do SFP28 o długości 3m. |
| Certyfikaty | Macierz musi być wyprodukowana zgodnie z normą ISO 9001 |

|  |
| --- |
| Wymagane prace/usługi wdrożeniowe dotyczące serwerów, macierzy oraz sieci Zamawiającego |
| 1. Montaż serwerów i macierzy w szafie serwerowej na szynach lub półkach 2. Aktualizacja firmware /BIOS serwerów 3. Stworzenie klastra HA składającego się z nodów i macierzy 4. Konfiguracja macierzy dyskowej na potrzeby klastra 5. Konfiguracja serwerów pełniących rolę nodów klastra i będących członkiem AD 6. Instalacja sprzętowa RAID 7. Instalacja i aktywacja systemu operacyjnego 8. Przygotowanie serwerów do wirtualizacji 9. Wsparcie przy wdrożeniu domeny Active Directory:   - Utworzenie przykładowych kont użytkowników  - Utworzenie przykładowych kont stacji roboczych  - Utworzenie przykładowych polityk GPO  - Utworzenie przykładowych zasobów współdzielonych.   1. Przygotowanie warstwy sieciowej na potrzeby współpracy klastra HA 2. Dostosowanie klastra do istniejących vlanów i polityk przepływu ruchu     Prace / usługi wdrożeniowe muszą być wykonywane w siedzibie Urzędu Gminy Dygowo przy współpracy z obsługą informatyczną urzędu. Powinny obejmować szkolenie stanowiskowe z wdrożonych rozwiązań w wymiarze minimum 3 dni roboczych. |

Zakup i dostawa przełącznika sieciowego zarządzalnego – 2 szt.

|  |
| --- |
| Przełącznik sieciowy zarządzalny – 2 sztuki |
| Wymaga się aby urządzenie było objęte ograniczoną gwarancją producenta – 5 lat, realizowaną minimum w systemie „door-to-door” przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji. |
| • Ilość portów 12 portów SFP+ oraz 12 portów 1/2,5/5/10G niezależne |
| • Chłodzenie od przodu do tyłu obudowy |
| • Tablica MAC min. 16K |
| • Tablica 4K ARP/ 512 NDP |
| • Bufor 32Mb |
| • MTBF min. 780202 godzin |
| • Wydajność min. 357 Mp/s |
| • Przepustowość min. 480 Gb/s |
| • Port USB-C |
| • Port zarządzania Out-of-band; |
| • Web GUI |
| • HTTPs |
| • CLI |
| • Telnet |
| • SSH |
| • SNMP |
| • MIB RSPAN |
| • Radius |
| • TACACS+ |
| • DiffServ |
| • Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram |
| • Interfejs web umożliwiający automatyczne przypisanie konfiguracji do portów właściwej dla protokołów czy też producenta: NVX, AMX, NDI, ZeeVee, Aurora, Kramer, LibAV, Dante Video, SDVoE, AES67, Q-SYS, Audio Dante, AVB, Crestron DigitalMedia AV, NUCLEUS Converged AV, Shure, Sonos, Visionary AV |
| • Wymaga się aby powyższe szablony konfiguracji były stworzone przez producenta przełącznika a interfejs web w sposób jednoznaczny wskazywał że dany producent AV czy protokół jest obsługiwany przez dany szablon. |
| • Wymaga się aby producent dostarczył kontroler w formie aplikacji umożlwiający przypisanie profilu AV do grupy przełączników w sposób automatyczny |
| • Wymaga się aby interfejs web miał możliwość wykonywania poleceń tekstowych CLI bez potrzeby tworzenia oddzielnego połączenia Telnet lub SSH. |
| • IPv4/IPv6 Multicast filtering |
| • IGMPv3 MLDv2 Snooping |
| • ASM & SSM |
| • IGMPv1,v2 Querier |
| • Policy-based routing (PBR) |
| • LLDP-MED |
| • Spanning Tree |
| • Green Ethernet |
| • STP |
| • MTP |
| • RSTP |
| • EEE (802.3az) |
| • GVRP/GMRP |
| • Q in Q, |
| • Private VLAN |
| • DOT1X |
| • MAB |
| • Captive Portal |
| • DHCP Snooping |
| • Dynamic ARP |
| • Inspection |
| • IP Source Guard |
| • CPU min ARMv8 1.8Ghz |
| • Min 2GB RAM |
| • Min 512MB Flash |
| • Min ilość obsługiwanych VLAN 4K |
| • DHCP Server min 2K rezerwacji |
| • sFlow |
| • Minimalna ilość przełączników w stosie: 8 |
| • Możliwość łączenia w stos za pomocą interfejsów 10Gb/s |
| • Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh |
| • Distributed Link Aggregation (LAGs across the stack) |
| • Ilość interfejsów IP 128 |
| • Double VLAN Tagging (QoQ) |
| • Yes |
| • PIM-DM (Multicast Routing - dense mode) |
| • PIM-DM (IPv6) |
| • PIM-SM (Multicast Routing - sparse mode) |
| • PIM-SM (IPv6) |
| • RIPv1 |
| • RIPv2 |
| • OSPFv2 |
| • RFC 2328 |
| • RFC 1583 |
| • OSPFv3 |
| • OSPFv2 min. sąsiadów 400 |
| • OSPFv3 min. sąsiadów 400 |
| • OSPFv3 min. sąsiadów na interfejs 100 |
| • UDLD |
| • LLPF |
| • DHCPv6 Snooping |
| • wysyłanie alertów na email |
| • MMRP |
| • Ilość ACL min. 100 |
| • Ilość reguł na listę min. 1023 na wejściu i 511 na wyjściu |

Cześć 2:

Zakup i dostawa serwera plików NAS z oprogramowaniem – 1 szt.

|  |  |
| --- | --- |
| Serwer plików NAS – 1 sztuka | |
| PARAMETR | WYMAGANIA MINIMALNE |
| Procesor | 8-rdzeniowy/16-wątkowy, taktowanie do 5,3 GHz |
| Obudowa | Rack 2U wraz z kompletem szyn do montażu w szafie rack |
| Pamięć RAM | 32 GB UDIMM DDR5, maks. 192 GB |
| Ilość obsługiwanych dysków | 12 dysków 3,5-calowych SATA 6 Gb/s, 3 Gb/s 2 x M.2 2280 PCIe |
| Ilość dysków zamontowanych | 9 dysków HDD o parametrach: Rozmiar: 3,5 cala Pojemność: 16TB Interfejs: SATA 6Gb/s Pamięć podręczna: 512 MB Prędkość obrotowa: 7200 RPM MTBF: 2 500 000 h Szybkość transmisji: min. 250 MB/s Gwarancja: 5 lat  2 dyski SSD o parametrach: Pojemność: 2TB Interfejs: M.2 Odczyt losowy IOPS do: min. 480K IOPS Zapis losowy do: min. 540K IOPS TBW: min. 2500 MTTF: min. 1750000 h Gwarancja: 5 lat  3 dyski SSD o parametrach: Rozmiar: 2,5 cala Pojemność: 3.84TB Interfejs: SATA 6Gb/s Prędkość odczytu losowego: min. 94K IOPS Prędkość zapisu losowego: min. 59K IOPS TBW: 7008 MTBF: 2000 000h Gwarancja: 5 lat |
| Porty sieciowe | 2 x 2,5 Gigabit Ethernet RJ-45 2 x 10 Gigabit Ethernet RJ-45 |
| Porty USB | 2 x USB 3.2 Gen 2 |
| Porty PCIe | 3 x Gen 4 x 4 |
| Wskaźniki LED | HDD 1–12, LAN, M.2 SSD 1-2, Zasilanie |
| Obsługa RAID | RAID 0, 1, 5, 6, 10, 50, 60 |
| Funkcje RAID | Dodanie grupy RAID do puli magazynu, wymiana wszystkich dysków w danej grupie RAID na większe, podłączanie jednostek rozszerzających JBOD. |
| Obsługiwane Systemy Operacyjne | Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 or later Linux Microsoft Windows 7, 8, 10, and 11 Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, and 2022 |
| Stacja monitoringu | Tak |
| Protokoły | CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP |
| Usługi | Stacja monitoringu, Windows ACL, Serwer plików, Manager plików przez WWW,  Serwer RADIUS, LDAP |
| Zarządzanie dyskami | SMART |
| Gwarancja i serwis | - Serwis świadczony przez producenta oferowanego sprzętu - 5 lat gwarancji NBD ON-SITE producenta - gwarancja w tym trybie świadczona również na dyski - wsparcie przez cały okres gwarancji: pomoc zdalna i telefoniczna przy konfiguracji i problemach z urządzeniem, w dni robocze (w godz. 8:00 – 16:00) |
| System plików | Dyski wewnętrzne ZFS lub EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+ |
| iSCSI Service | Tak |
| Liczba kont użytkowników | 4096 |
| Liczba grup | 512 |
| Liczba udziałów | 128 |
| Max ilość połączeń (CIFS) | 5000 |
| Zasilanie | 2 x 550W, 100-240V |
| Wentylatory | 3 x 60 mm, 12VDC |

Zakup i dostawa urządzeń w celu stworzenie bezpiecznego WiFi

Przedmiotem zamówienia jest dostawa urządzeń WiFi firmy Ubiquiti w celu rozbudowy istniejącej infrastruktury.

Wykaz urządzeń:

U7-Pro - 9 szt.

UCK-G2-SSD - 1 szt.

CKG2-RM - 1 szt.

USW-Pro-24-POE - 1 szt.

Zakup i dostawa zasilacza awaryjnego UPS wraz z dodatkowym modułem bateryjnym – 1 szt.

|  |  |
| --- | --- |
| Zasilacz awaryjny UPS wraz z dodatkowym modułem bateryjnym – 1 sztuka | |
| PARAMETR | WYMAGANIA MINIMALNE |
| Technologia | Online |
| Moc wyjściowa (pozorna / czynna) | 3000 VA / 3000 W |
| Obudowa | Rack/Tower (Zestaw do montażu w szafie rack na wyposażeniu) |
| Napięcie wejściowe | 110 ÷ 300 V AC ± 2 % |
| Napięcie wyjściowe znamionowe (wartość skuteczna) | 230V AC |
| Częstotliwość znamionowa napięcia wejściowego | 50Hz / 60Hz |
| Zakres napięcia wyjściowego | 200/208/220/230/240V AC ± 2 %  konfigurowalne z poziomu oprogramowania  oraz z menu zasilacza na wyświetlaczu LCD (domyślnie 230V AC) |
| Gniazda wyjściowe | 4x IEC320 C13 (10A) sterowalne + 4x IEC320 C13 (10A) + 1x IEC320 C19 (16A) |
| Moduły bateryjne | Możliwość podpięcia do 4 szt. modułów |
| Wymagany czas podtrzymania dla obciążenia 3kW/2,4kW/1,5kW (dla zasilacza z 1 dodatkowym modułem bateryjnym) | 15 / 22 / 38 min |
| EPO | Wymagane |
| Sygnalizacja | Akustyczno-diodowa, wyświetlacz LCD oraz diody sygnalizujące usterkę, pracę bateryjną, pracę w trybie online, obejście bypass |
| Język oprogramowania | Polski i angielski do wyboru z poziomu interfejsu użytkownika |
| Wymagane certyfikaty | Deklaracja CE, ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisu |
| Komunikacja z urządzeniem | RS232, USB HID, styki bezpotencjałowe 1-wejście;  1-wyjście; karta sieciowa NMC RJ-45 SNMP – wymagana na wyposażeniu |
| Oprogramowanie do monitorowania pracy zasilacza UPS | Tego samego producenta co UPS, bez dodatkowych opłat. |
| Oprogramowanie - funkcjonalność | - Konfiguracja minimalnego poziomu naładowania baterii.  - Możliwość nadawania unikalnych nazw dla kilku tych samych modeli UPS’ów w oprogramowaniu  - Uruchom poprzez Bypass – Funkcja umożliwiająca załączenie urządzeń o zwiększonym prądzie rozruchowym bez przeciążania falownika UPS |
| Serwis producenta | Wymagany, zlokalizowany na terenie Polski – oświadczenie producenta załączyć do oferty |
| Gwarancja | Minimum 60 miesięcy elektronika, 60 miesięcy akumulatory, serwis door to door |

Część 3:

Zakup i dostawa licencji przedłużających produkt Axence nVision będących w posiadaniu Zamawiającego – 45 szt. oraz usługi wsparcia obejmującą 45 agentów

Przedmiotem zamówienia jest dostawa 45 licencji przedłużający produkt Axence nVision będący w posiadaniu Zamawiającego tj. Urząd Gminy Dygowo oraz usługi wsparcia obejmującą 45 agentów.

1. Przedmiot zamówienia obejmuje rozszerzenie licencji w zakresie liczby obsługiwanych agentów zgodnie z pkt. 1.2.
   1. Aktualnie Zamawiający posiada następujące licencje:
      1. liczba obsługiwanych agentów: 40;
      2. moduły: Network, Inventory, Users, Helpdesk, DataGuard, SmartTime
   2. Wymagane jest rozszerzenie powyższych licencji do następujących (zwanych dalej Oprogramowaniem):
      1. Liczba obsługiwanych agentów: 45;
      2. moduły: Network, Inventory, Users, Helpdesk, DataGuard, SmartTime
   3. Dostarczone rozwiązane powinno mieć zapewnione wsparcie producenta przez okres 60 miesięcy od dnia aktywacji usługi. Aktualne wsparcie producenta (40 agentów) kończy się 22.02.2024r.
   4. W ramach świadczenia wsparcia producenta Zamawiający wymaga zapewnienia:
      1. możliwość instalowania wszelkich aktualizacji oprogramowania Axence nVision®, które będą miały miejsce w czasie obowiązywania Umowy Serwisowej, w tym aktualizacji obejmujących przejście na kolejną wersję oprogramowania;
      2. aktualizacje wzorców oprogramowania;
      3. telefoniczne i mailowe wsparcie techniczne dla oprogramowania Axence nVision®;
      4. dokonywanie przez AXENCE szczegółowej analizy zgłoszonych przypadków (*logów*);
      5. świadczenie przez AXENCE pomocy w formie sesji zdalnych;
      6. czas reakcji na zgłoszenie nie dłuższy niż następny dzień roboczy.
2. Dopuszczalne są licencje równoważne, przy czym:
   1. Zamawiający przez „licencje równoważne” rozumie licencje zapewniające bez dodatkowych nakładów finansowych bezkonfliktowe działanie posiadanego Środowiska zbudowanego w oparciu o Oprogramowanie wymienione w pkt. 1.2 oraz spełniające wszystkie funkcje licencji z pkt. 1.1.
   2. W przypadku dostarczenia licencji równoważnych Wykonawca wdroży w pełni rozwiązanie zastępujące obecnie, na swój koszt oraz przeszkoli z zakresu zaawansowanej administracji wyznaczonych pracowników Urzędu Gminy w terminie do 7 dni kalendarzowych od wdrożenia rozwiązania.
   3. Dodatkowo w przypadku błędnego działania rozwiązania, po instalacji licencji równoważnych, Wykonawca zobowiązany będzie na własny koszt przywrócić Środowisko do stanu poprawnego funkcjonowania w przeciągu 24h od stwierdzenia przez Zamawiającego niepoprawnego funkcjonowania, a w przypadku braku takiej możliwości do stanu pierwotnego oraz dostarczenia innego rozwiązania spełniającego wymagania OPZ w terminie do 3 dni kalendarzowych. Ponadto poniesie wszelkie koszty związane z poniesionymi stratami biznesowymi w związku z brakiem działania rozwiązania.

Część 4

Zakup i dostawa systemu (oprogramowania) do tworzenia kopii zapasowych (backup) – 1 szt.

|  |
| --- |
| System (oprogramowanie)  do tworzenia kopii zapasowych (backup) |
| WYMAGANIA MINIMALNE (MOŻLIWOŚCI SYSTEMU) |
| Zarządzanie i magazyny:  1. Produkt dostępny w polskiej wersji językowej.  2. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej  3. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków  4. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików  i folderów  5. System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych  6. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT  7. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft  8. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe  9. System zarządzania nie może być oparty o relacyjne bazy danych.  10. Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).  11. Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).  12. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.  13. Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.  14. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.  15. Rozwiązanie w warstwie sprzętowej powinno bazować na standardowych komponentach architektury x86, bez powiązania i poleganiu na komponentach wyłącznie jednego dostawy (tzw. "no propietary vendor lock").  16. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.  17. System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.  18. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.  19. Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.  20. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.  21. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych  22. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.  23. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.  24. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).  25. Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.  26. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.  27. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,  28. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.  29. Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym.  30. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).  31. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.  32. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.  33. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych zdeduplikowanych  34. Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie.  35. Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.  36. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.  37. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.  38. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.  39. System musi pozwalać na automatyczne aktualizacje oprogramowania.  40. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.  41. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS w celu ich zabezpieczenia.  42. System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.  43. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.  44. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.  45. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.  46. System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.  47. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.  48. W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.  49. Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego.  50. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.  51. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.  52. System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych: Custom, Basic, G-F-S, Forever incremental,  53. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).  54. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3.  55. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb, nfs, iscsi, katalog lokalny  56. Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS).  57. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniami zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu.  58. Możliwość generowania raportów dobowych w oparciu o harmonogram  59. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter musi być zlokalizowane na terenie Polski)  60. Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna)  61. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP.  62. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail. (poziom definiowany indywidualnie dla każdego magazynu) |
| Wspierane systemy:  Możliwość instalacji oraz uruchomienia agenta backupowego na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych  o systemy:  Alpine 3.10+,  Debian: 9+,  Ubuntu: 16.04+,  Fedora: 29+,  centOS: 7+,  RHEL: 6+,  openSUSE: 15+,  SUSE Enterprise Linux(SLES): 12 SP2+,  macOS: 10.13+,  Windows: 7, 8.1, 10(1607+),  Windows Server: 2008 R2+,  Środowisk wirtualnych:  Hyper-V 2016+,  VMware: 6.7+.  Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych  o systemy:  Debian: 9+  Ubuntu: 16.04+  Fedora: 29+  centOS: 7+  RHEL: 6+  openSUSE: 15+  SUSE Enterprise Linux (SLES): 12 SP2+  Windows Client: 7, 8.1, 10 (1607+)  Windows Server: 2012 R2+, |
| Środowiska fizyczne i bazy danych:  1. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami.  2. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń.  3. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej.  4. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption.  5. System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.  6. System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego scalania danych.  7. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux.  8. W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem.  9. Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.  10. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych.  11. Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V.  12. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).  13. Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych.  14. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows). |
| Środowiska wirtualne:  1. System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów.  2. System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowanie zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych.  3. System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych.  4. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner.  5. System kopii zapasowej musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych.  6. Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).  7. System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.  8. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku. |
| Aplikacje SaaS:  1. Ochrona z tej samej konsoli dla Microsoft 365 minimum na poziomie, skrzynek pocztowych, onedrive, kontaktów, kalendarza.  2. Rozwiązanie musi umożliwiać przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst oraz do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji)  3. System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365.  4. System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket wraz z metadanymi  5. System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe.  6. System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git.  7. System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium.  8. System musi umożliwiać zabezpieczenie środowisk Jira  9. System musi umożliwiać odtworzenie środowiska Jira do chmury lub środowiska lokalnego.  10. System musi umożliwiać zabezpieczenie środowisk Jira |
| Anty-ransomware i bezpieczeństwo:  1. System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików").  2. System powinien umożliwiać wykorzystanie wbudowanego menedżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System  3. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.  4. W ramach systemu, komunikacja pomiędzy hostem źródłowym,  a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu, ani żaden inny komponent, którego awaria sparaliżowały by działanie Systemu. System nie może posiadać pojedynczego punktu awarii.  5. System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczonym urządzeniu. |
| **Licencjonowanie i wsparcie techniczne:**  1. Wszystkie linie supportu muszą być obsługiwane w języku polskim.  2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta.  3. Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu.  4. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów)  5. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego.  6. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie określonej przez Zamawiającego ilości hostów w obrębie wspieranych przez System środowisk.  7. Licencje powinny być dostępne w opcji wieczystej .  8. Dostęp do wsparcia technicznego producenta powinno obowiązywać przez okres min. **60** miesięcy  9. Sposób licencjonowania opiera się na:  - ilości serwerów/endpointów - dla fizycznych urządzeń,  - ilości socketów w hostach - dla środowisk wirtualnych lub ilości maszyn wirtualnych,  - ilość repozytoriów - dla GIT.  **10. Licencje powinny umożliwiać zabezpieczenie w wersji wieczystej:**  **- 35 Endpointów - dla fizycznych urządzeń,**  **- 4 Socketów w hostach maszyn wirtualnych oraz 8 maszyn wirtualnych** |

Część 5:

Zakup usługi wdrożenia rozwiązania do centralnego składowania dzienników zdarzeń w opcji Open Source – 1 szt.

Usługa wdrożenia rozwiązania do centralnego składowania dzienników zdarzeń w opcji Open Source

1. Wymagania związane z rozwiązaniem centralnego składowania dzienników zdarzeń:
   1. System operacyjny powinien być na licencji Open Source.
   2. Platformą sprzętowa dla rozwiązania centralnego składowania dzienników jest w sieci Zamawiającego wirtualna maszyna w środowisku Hyper-V.
   3. Architektura systemu powinna bazować na komponentach o licencjonowaniu Open Source
   4. Zamawiający na wyżej wymieniony cel planuje przeznaczyć maszynę wirtualną o parametrach procesor (CPU) 8 rdzeni, pamięć RAM 16 GB oraz dysk twardy (HDD) 2TB.
   5. Tworzenie użytkowników w systemie centralnego składowania logów może odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (Active Directory) lub ręcznie przez definiowanie kont w samym rozwiązaniu.
   6. System centralnego składowania dzienników zdarzeń powinien mieć możliwość zdefiniowania dowolnie wielu i dowolnie skonfigurowanych źródeł danych, wśród których znajdują się m.in.: Sysloga UDP/TCP, Plaintext UDP/TCP, RAW UDP/TCP, NetFlow UDP, JSON, Beat, CEF UDP/TCP. Konfiguracja źródeł danych powinna pozwalać na zdefiniowanie dowolnego portu komunikacji, np. Syslog UDP 514 lub/i Syslog UDP 10514.
   7. System centralnego składowania dzienników zdarzeń powinien mieć możliwość ekstrakcji fragmentów wpisów logów z możliwością wykorzystania ich do filtrowania danych, budowania zapytań dla powiadomień i alarmów czy widoków w ramach dashboardów oraz ich import jak i eksport.
   8. System centralnego składowania dzienników zdarzeń powinien udostępniać możliwość budowania widoków w formie dashboardów, które w łatwy sposób można udostępnić w trypie ReadOnly (tylko do odczytu) na urządzeniach z funkcją SMART-TV czy urządzeniach z dowolną przeglądarką WWW.
   9. System centralnego składowania dzienników zdarzeń powinien pozwalać na budowanie powiadomień (alarmów) w oparciu o reguły, które uwzględniają napływające dane z dzienników systemowych w sieci Zamawiającego.
   10. System centralnego składowania dzienników zdarzeń powinien mieć możliwość tworzenia paczek składających się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe i pulpitów nawigacyjnych (dashboardów).
2. W zakresie wdrożenie proponowanego rozwiązania wykonawca wykona następujące czynności opisujące zarówno konfigurację rozwiązania jak i szkolenie z codziennego wykorzystania systemu centralnego składowania dzienników zdarzeń:
   1. Instalacja systemu operacyjnego na wybranych przez Zamawiającego maszynie wirtualnej.
   2. Weryfikacja źródła czasu na wszystkich urządzeniach/systemach wysyłających logi do Centralnego systemu centralnego składowania dzienników zdarzeń. Jeśli urządzenia nie mają wspólnego zegara czasu Wykonawca zaproponuje rozwiązanie pozwalające na uspójnienie zegarów czasów sieci Zamawiającego.
   3. Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracją parametrów podstawowej pracy, w tym polityki dostępu dla pracowników zespołu IT Zamawiającego.
   4. Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów aktyw prawnych i dobrych praktyk występujących w środowisku Zamawiającego.
   5. Konfiguracja na urządzeniach i systemach w sieci Zamawiającego usługi wysyłania dzienników zdarzeń (logów) do wdrażanego systemu. Zamawiający wymaga, aby w zakresie minimalnym prace objęły:
      * (1x) Urządzenie klasy UTM firmy Fortinet
      * (2x) Przełączniki zarządzalne firmy HP
      * (2x) Przełączniki zarządzalne firmy Netgear
      * (8x) Serwery Windows
      * (2x) Serwery Linux
      * (30x) stacji roboczych Windows 10 i 11
      * (1x) Aplikację centralnego zarządzania ESET
      * (1x) Klaster serwerów wirtualizacji Hyper-V (2 serwery Hyper-V w klastrze)
      * (1x (Serwer zarządzania wirtualizacją Hyper-V
      * (6x) Urządzenia drukujące
      * (3x) Urządzenia NAS firmy QNAP
      * (1x) Kontroler WiFI Ubiquiti
      * (3x) UPS
      * Inne urządzenia (RCP, NVR) – 8 urządzeń

* 1. Zdefiniowanie portów nasłuchu logów w oparciu o segmentację nasłuchu pozwalającej odseparować dane napływające z różnych typów urządzeń i systemów w sieci Zamawiającego.
  2. Wykonanie wstępnej analizy napływających logów w celu zdefiniowania odpowiednich ekstraktorów wydzielających wybrane segmenty danych z napływających strumieni logów.
  3. Automatyzacja analizy napływających logów poprzez zbudowanie Dashboardów generujących i prezentujących dane w postaci tabelarycznej i lub graficznej.
  4. Konfiguracja mechanizmów alarmowania i powiadomień oparta o analizę napływających i przeanalizowanych logów.
  5. Konfiguracja wysyłania powiadomień poprzez maila lub Microsoft Teams w przypadku stwierdzenia przez system niepokojącej sytuacji zgodnie z wcześniej ustawionymi alarmami.
  6. Wprowadzenie pracowników działu IT do obsługi wdrożonego systemu.

1. Szkolenie w formie warsztatu:
   1. Zamawiający wymaga aby Wykonawca zorganizował i przeprowadził w swojej siedzibie lub innym miejscu nie zależnym od Zmawiającego warsztaty techniczne z zarządzenia i administracji wdrożonego systemu.
   2. Zamawiający wymaga aby usługa została zrealizowana w terminie do 6 miesięcy od zamówienia usługi.
   3. Zamawiający wymaga przeszkolenia w formie warsztatów 1 uczestnika.
   4. Zamawiający wymaga aby w trakcie warsztatów realizowane były ćwiczenia opisujące codzienną pracę administracyjną z wdrożonym systemem, rozwiązywaniem problemów, procedurę aktualizacji rozwiązania oraz rozbudowy o dodatkowe widoki i kanały napływu danych.
   5. Wymagana agenda warsztatów:
      * Wstęp do zarządzania logami
      * Wymagania oraz architektura wdrożonego rozwiązania
      * Instalacja i konfiguracja ogólnych ustawień
      * Zbieranie logów, czyli konfiguracja metod pozyskiwania dzienników zdarzeń.
      * Przetwarzanie dzienników zdarzeń, czyli tworzenie strumieni logów, ich parsowanie oraz filtrowanie
      * Wizualizacja logów czyli tworzenie czytelnych zestawień tabelarycznych i graficznych
      * Konfiguracja alertów i powiadomień.
      * Administracja i utrzymanie wdrożonego rozwiązania
      * Case Study czyli praktyczne przykłady użycia
   6. Zamawiający wymaga aby warsztaty zamykały się w ramach czasowych 2 dni roboczych (2x 7 godz.)
   7. Zamawiający wymaga aby wykonawca pokrył koszty pełnego wyżywienia i zakwaterowania uczestnika w czasie warsztatów.
   8. Zamawiający wymaga aby warsztaty kończyły się potwierdzeniem uczestnictwa w formie certyfikatu.
2. Gwarancja i asysta techniczne:
   1. Zamawiający wymaga aby Wykonawca w czasie do 24 miesięcy od wdrożenia rozwiązania zapewnił wsparcie techniczne polegające na zdalnej pomocy w przypadku wystąpienia problemów z działaniem systemu.
   2. Zamawiający wymaga aby Wykonawca w okresie do 24 miesięcy od wdrożenia rozwiązania świadczył asystę w zakresie aktualizacji zarówno systemu, jak i jego komponentów.
   3. Zamawiający wymaga aby w/w usługi były świadczone od poniedziałku do piątku między godzinami 8.00 a 16.00.
   4. Zamawiający akceptuje fakt, ze każda interwencja wymagać będzie od niego zgłoszenia potrzeby pomocy drogą elektroniczną, a wskazany kanał komunikacji będzie wyznaczony przez Wykonawcę, i może to być system zgłoszeń elektronicznych lub komunikacja mailowa.
3. Wymagania dotyczące doświadczenia wykonawcy:
   1. Zamawiający wymaga aby Wykonawca w okresie ostatnich 12 miesięcy przed przystąpieniem do realizacji zadania był wstanie wykazać się minimum 5 wdrożeniami proponowanego rozwiązania w jednostkach publicznych o podobnej wielkości do Zamawiającego.
   2. Zamawiający wymaga aby Wykonawca posiadał certyfikaty producenta potwierdzające ukończone szkolenia z proponowanego rozwiązania.
   3. Zamawiający wymaga aby Wykonawca był ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia na sumę gwarancyjną min. 450 000,00 PLN (słownie złotych: czterysta pięćdziesiąt tysięcy 00/100).

Część 6

Zakup usługi skanowania podatności urządzeń w sieci Zamawiającego – 1 szt.

|  |
| --- |
| Usługa skanowania podatności urządzeń w sieci Zamawiającego |
| WYMAGANIA MINIMALNE |
| Skanowanie podatności musi być wykonane za pomocą skanera w wersji komercyjnej – nie dopuszcza się skanerów w wersji open. Należy podać producenta i nazwę skanera |
| Skanowanie podatności musi być wykonane lokalnie w siedzibie Zamawiającego |
| Skanowanie podatności należy wykonać w oparciu o zaktualizowaną bazę wiedzy podatności (plug’inów) na dzień skanowania. |
| Ocenę wykrytych podatności należy wykonać w oparciu o system oceny podatności oprogramowania na zagrożenia – Common Vulnerability Scoring System |
| Urządzenia, które mają być objęte skanowaniem:  - Komputery stacjonarne / laptopy – 30 sztuk  - Urządzenia drukujące pracujące w sieci – 6 sztuk  - Serwery fizyczne – 3 sztuki (10 maszyn wirtualnych)  - Serwer typu NAS – 3 sztuka  - Macierz – 1 sztuka  - Urządzenia sieciowe – 5 sztuk (UTM – 1 sztuka, Switche – 4 sztuki)  - Zasilacz awaryjny z karta sieciową – 3 sztuka  - Inne urządzenia: RCP, terminale płatnicze, NVR, kontroler WiFi –10 sztuk  Zakres skanowania:  Wykrycie i analiza podatności, a w szczególności:  - Detekcja nieaktualnego oprogramowania  - Analiza portów  - Wykrywanie luk bezpieczeństwa  - Wykrywanie podatności umieszczonych w bazach CVE/CVS  - Identyfikacja błędów konfiguracji |
| Wymagany jest raport końcowy po wykonaniu skanowania zawierający co najmniej  zestawienie znalezionych podatności wraz z proponowanymi rozwiązaniami w celu ich usunięcia (dla podatności o charakterze wysokim i krytycznym), wnioski końcowe dotyczące skanowania zawierające rekomendacje dotyczące bezpieczeństwa urządzeń pracujących w sieci Zamawiającego |
| Wymagana minimalna funkcjonalność skanera podatności stosowanego przez Wykonawcę:  Raportowanie i monitorowanie:   * Celowane powiadomienia o wynikach skanowania, wysyłane e-mailem, zalecenia działań naprawczych i usprawnień dotyczących konfiguracji skanów * Dostosowanie raportów według podatności lub urządzeń, możliwość wygenerowania streszczenia lub porównania wyników różnych skanów  w celu wyróżnienia zmian, format standardowy .html, .csv   Możliwości skanowania:   * Precyzyjne i efektywne wykrywanie zasobów * Skanowanie podatności (w tym IPv4, IPv6, sieci hybrydowe) * Wykrywanie podatności bez uwierzytelnienia * Skanowanie z uwierzytelnieniem * Szeroki zakres zasobów i możliwości profilowania:   - urządzenia sieciowe: firewall'e, routery, switche, drukarki, dyski sieciowe  - wirtualizacja: Vmware ESX, ESXi, vSphere, vCenter, Microsoft, Hyper-V  - systemy operacyjne: Windows, OS X, Linux, FreeBSD, Cisco iOS  - bazy danych: Oracle, SQL Server, MySQL, DB2, PostgreSQL, Firebird   * Wykrywane Zagrożenia:   - znajdowanie złośliwego oprogramowania  - znajdowanie luk w zabezpieczeniach, komunikacji urządzeń z zainfekowanymi systemami  Zarządzanie:   * Skanowanie bez uwierzytelnienia lub z uwierzytelnieniem * Konfiguracja i polityki skanowania - predefiniowane polityki i wzorce konfiguracji * Ocena ryzyka - ranking oceny podatności w oparciu o CVSS (Common Vulnerability Scoring System), co najmniej cztery poziomy dotkliwości (Krytyczny, Wysoki, Średni, Niski) |