Załącznik nr 3 do SWZ

**Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym. Zamawiający zaleca zapisanie dokumentów w formacie PDF.**

**OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)**

dotyczący realizacji zadania pn.:

***„Dostawa urządzeń i oprogramowania dla Gminy Rogów zwiększających odporność na cyberataki***

***i wycieki danych w ramach realizacji projektu grantowego***

***Cyberbezpieczny Samorząd w Gminie Rogów”***

**Wykaz sprzętu (spis)**

[I. Serwer NAS z oprogramowaniem i dyskami - 1 Kpl. 2](#_Toc203562240)

[II. Serwer do instalacji usług podnoszących cyberbezpieczeństwo – 1 Kpl. 5](#_Toc203562241)

[III. System NAC do izolacji sieci LAN w siedzibie zamawiającego – 80 IP 21](#_Toc203562242)

[IV. System do kategoryzacji i archiwizacji logów 27](#_Toc203562243)

[V. System do utrzymywania aktualności inwentaryzacji sprzętu i DLP 28](#_Toc203562244)

[VI. Wdrożenia i szkolenie 36](#_Toc203562245)

[A. Wdrożenie serwera 36](#_Toc203562246)

[B. Wdrożenie serwera NAS z oprogramowaniem i dyskami 39](#_Toc203562247)

[C. Wdrożenie systemu NAC do izolacji sieci LAN w siedzibie zamawiającego 46](#_Toc203562248)

[D. Wdrożenie systemu do utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania 46](#_Toc203562249)

**Ograniczenia w zakresie wypełniania OPZ**

**Zamawiający zastrzega, że Wykonawca nie jest uprawniony do dokonywania jakichkolwiek modyfikacji, dopisków ani zmian w treści OPZ, z wyjątkiem miejsc wyraźnie oznaczonych do wypełnienia: dot. danych producenta/modelu oferowanego sprzętu oraz miejsc w których należy jednoznacznie wskazać, czy oferowany sprzęt lub usługa spełnia wymagania minimalne określone w tabeli stanowiącej opis przedmiotu zamówienia – poprzez wpisanie lub wyraźne zaznaczenie (pogrubienie i wykreślenie) odpowiednio: TAK/NIE.**

**Opis Przedmiotu Zamówienia stanowi integralną część umowy i obowiązuje Wykonawcę w brzmieniu opublikowanym przez Zamawiającego na etapie prowadzenia postępowania.**

# **Serwer NAS z oprogramowaniem i dyskami - 1 Kpl.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
| **CZY SPEŁNIAJĄ WYMAGANIA?** |
| 1. | Dane producenta /model | Producent oferowanego rozwiązania /model i wersja modelu  …………………………………………………..………/……………………………………………. \* | |
| 2. | Procesor | Procesor o architekturze 64-bit. | (TAK / NIE)\* |
| 3. | Obudowa | Typu rack o wysokości maksymalnej 2U z szynami przesuwnymi do instalacji w szafie rack w zestawie. | (TAK / NIE)\* |
| 4. | Pamięć RAM | Minimum 8GB DDR4 ECC. | (TAK / NIE)\* |
| 5. | Interfejsy sieciowe | Minimum 2 porty 1GbE RJ-45, Minimum 1 port 10GbE RJ-45,  Obsługa agregacji łączy. | (TAK / NIE)\* |
| 6. | Ilość obsługiwanych dysków | Minimum 12 dysków o maksymalnej pojemności 18TB każdy, po podłączeniu modułów rozszerzających minimum 24 dyski. | (TAK / NIE)\* |
| 7. | Zainstalowane dyski | 6 dysków o pojemności 8TB każdy zgodnych z listą kompatybilności oferowanego serwera NAS oraz charakteryzujących się następującymi parametrami: - prędkość obrotowa: minimum 7200 RPM,  - pamięć cache: minimum 256MB,  - MTBF: minimum 1 milion,  - możliwość aktualizowania oprogramowania dysków w czasie rzeczywistym podczas pracy serwera bez potrzeby demontażu dysków. | (TAK / NIE)\* |
| 8. | Gniazda rozszerzeń | 1 slot PCIe 3.0 x8 (x4 link) | (TAK / NIE)\* |
| 9. | Wskaźniki LED | Status, HDD 1-12, zasilanie, LAN 1-3 | (TAK / NIE)\* |
| 10. | Obsługa RAID | Pojedynczy, JBOD, RAID 0, 1, 5, 6, 10, SHR wraz z obsługa dysków typu hot spare. | (TAK / NIE)\* |
| 11. | Funkcje RAID | Możliwość zwiększania pojemności i migracja między poziomami RAID online. | (TAK / NIE)\* |
| 12. | Szyfrowanie | Możliwość szyfrowania wybranych udziałów sieciowych. | (TAK / NIE)\* |
| 13. | Protokoły | SMB, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP | (TAK / NIE)\* |
| 14. | Usługi | 1. Serwer VPN, Serwer pocztowy dla kilku domen, Stacja monitoringu, Windows ACL, Integracja z Windows ADS, Firewall, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Antyvirus, Klient VPN, Usługa DDNS, Zarządzanie przez komórkę, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, migawki (min. 65 tys. w cały systemie), możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów.  2. Wykonywanie kopii zapasowych typu bare-metal komputerów lokalnych z systemem Windows 7 lub nowszym według harmonogramu z centralnej konsoli zarządzania dostępnej lokalnie oraz zdalnie, z możliwością przywracania pojedynczych plików, folderów oraz całych obrazów dysku. Kopia musi być wykonywana w trybie przyrostowym z możliwością przechowywania minimum 32 wersji i zarządzania ich przechowywaniem w sposób automatyczny poprzez dedykowany algorytm. Bez ograniczenia liczby podłączanych komputerów do systemu kopii zapasowej.  3. Możliwość utworzenia klastra wysokiej dostępności (HA) z dwóch identycznych urządzeń pracującego minimum w trybie aktywny-pasywny. Wymagane jest, aby klaster obsługiwał w pełni automatyczne przełączanie awaryjne bez ingerencji administratora. | (TAK / NIE)\* |
| 15. | Zarządzanie dyskami | SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów, | (TAK / NIE)\* |
| 16. | Język GUI | Polski | (TAK / NIE)\* |
| 17. | Gwarancja i serwis | Minimum 12 miesięcy gwarancji producenta działającej w trybie 5/13 NBD na cały system złożony z serwera, dysków i akcesoriówz opcją pozostawienia uszkodzonego nośnika u Zgłaszającego. Dostawa sprzętu zastępczego na następny dzień roboczy po wystąpieniu awarii sprzętowej, obowiązuje od poniedziałku do piątku w dni robocze. | (TAK / NIE)\* |
| 18. | Pobór mocy | Maksymalnie 125W w trybie pracy. Maksymalnie 50W w trybie hibernacja dysków. | (TAK / NIE)\* |
| 19. | Certyfikaty | FCC, CE | (TAK / NIE)\* |
| 20. | System plików | Dyski wewnętrzne BTRFS. Dyski zewnętrzne BTRFS, FAT, NTFS, EXT3, EXT4, HFS+. | (TAK / NIE)\* |
| 21. | Zasilanie | Redundantny zasilacz o mocy minimum 300W | (TAK / NIE)\* |
| 22. | **Dodatkowe Wsparcie techniczne** | **Zakres dodatkowego wsparcia**  Wsparcie techniczne musi być świadczone przez wykwalifikowanych inżynierów Producenta oferowanego rozwiązania lub certyfikowanych inżynierów dystrybutora oferowanego rozwiązania na terenie Polski posiadającego autoryzację producenta od minimum 10 lat. Wymagane jest, aby osoby te posiadały odpowiednie kompetencje techniczne i doświadczenie w obsłudze oraz serwisowaniu urządzeń objętych niniejszą dostawą, co zapewni najwyższy poziom jakości usług oraz bezpieczeństwo danych Zamawiającego.   1. **Proaktywne monitorowanie infrastruktury**    * Ciągłe monitorowanie pracy urządzeń, obejmujące:      + Stan techniczny nośników danych, w tym parametry SMART, zużycie i temperaturę.      + Wykorzystanie zasobów systemowych, takich jak procesor, pamięć i przestrzeń dyskowa.      + Analizę logów systemowych pod kątem potencjalnych zagrożeń i anomalii.    * Automatyczne powiadomienia o wykrytych problemach technicznych przesyłane do administratora Zamawiającego oraz zespołu wsparcia. 2. **Kwartalne raportowanie stanu infrastruktury**    * Przygotowywanie szczegółowych raportów technicznych zawierających:      + Stan urządzeń, w tym status macierzy dyskowych oraz aktualną konfigurację systemową.      + Wykorzystanie zasobów i ich dynamikę w okresie sprawozdawczym.      + Informacje o liczbie zgłoszeń serwisowych, podejmowanych działaniach oraz ich wynikach.      + Rekomendacje dotyczące optymalizacji wydajności i planowania przyszłych działań.    * Raporty dostarczane w formie elektronicznej oraz omawiane podczas cyklicznych spotkań technicznych z przedstawicielami Zamawiającego. 3. **Reakcja serwisowa i wsparcie w sytuacjach krytycznych**    * Gwarantowany czas reakcji na zgłoszenia:      + Krytyczne awarie: **maksymalnie 1 godzina** od zgłoszenia.      + Problemy o wysokim priorytecie: **do 4 godzin roboczych**.      + Problemy o niskim priorytecie: **do 1 dnia roboczego**. 4. **Przeglądy techniczne i diagnostyka**    * Realizacja kwartalnych przeglądów technicznych obejmujących:      + Weryfikację stanu nośników danych i macierzy RAID.      + Aktualizację systemów operacyjnych oraz aplikacji zainstalowanych na urządzeniach.      + Testowanie procedur odzyskiwania danych z kopii zapasowych.      + Sprawdzanie konfiguracji systemów zabezpieczeń oraz logów w celu identyfikacji potencjalnych zagrożeń.    * Każdy przegląd kończy się sporządzeniem szczegółowego raportu dla Zamawiającego wraz z rekomendacjami. 5. **Analiza ryzyk i doradztwo techniczne**    * Regularne identyfikowanie potencjalnych zagrożeń dla działania urządzeń oraz opracowanie planów zapobiegawczych.    * Bieżąca analiza wydajności oraz analiza ryzyk związanych z przetwarzaniem danych.    * Proponowanie działań optymalizacyjnych, dostosowanych do zmieniających się potrzeb Zamawiającego. 6. **Wsparcie w integracji i optymalizacji infrastruktury**    * Pomoc techniczna przy integracji urządzeń z istniejącą infrastrukturą sieciową i systemami informatycznymi Zamawiającego.    * Konfiguracja i utrzymanie mechanizmów zabezpieczeń danych, w tym systemów tworzenia kopii zapasowych oraz ich odtwarzania.   Dostosowanie konfiguracji urządzeń do zmieniających się wymagań operacyjnych, zapewniające optymalne wykorzystanie zasobów  **Oferent winien przedłożyć dokumenty:**  Dokument potwierdzony przez Producenta lub Autoryzowanego Dystrybutora producenta o gotowości świadczenia na rzecz Zamawiającego wymaganego wsparcia (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). | (TAK / NIE)\* |

**\* określić czy oferowany sprzęt/usługa spełnia/ją wymagania minimalne określone w tabeli stanowiącej opis przedmiotu zamówienia (wypełnić/zaznaczyć odpowiednio TAK/NIE).**

# **Serwer do instalacji usług podnoszących cyberbezpieczeństwo – 1 Kpl.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
| **CZY SPEŁNIAJĄ WYMAGANIA?** |
| 1. | Dane producenta /model | Producent oferowanego rozwiązania /model i wersja modelu  ………………………………………………………/…………………………………. \* | |
| 2. | Przeznaczenie | Serwer będzie przeznaczony do instalacji oprogramowania zwiększającego poziom cyberbezpieczeństwa w środowisku Zamawiającego. Na serwerze zostanie zainstalowany system wirtualizacji Proxmox VE, a następnie uruchomione maszyny wirtualne z oprogramowaniem takimi jak: system NAC, systemy DLP, narzędzia do monitorowania i analizy ruchu sieciowego, narzędzia do kategoryzacji i składowania logów oraz inne systemy zwiększające bezpieczeństwo sieci. Serwer będzie pełnił rolę węzła klastra Proxmox oraz współdzielonego storage CEPH. | (TAK / NIE)\* |
| 3. | Obudowa | * Obudowa Rack o wysokości 2U. * 24 slotów na dyski 2.5”, obsługa do 16 dysków NVMe. * Możliwość instalacji dysków SAS/SATA/NVMe – fabryczna blokada demontowania dysków twardych za pomocą zamka lub linki zabezpieczającej lub innego podobnego zabezpieczenia. * LCD na froncie obudowy lub diody LED informujące o stanie komponentów np. CPU, RAM, SSD, zasilanie. | (TAK / NIE)\* |
| 4. | Płyta główna | * Płyta główna w architekturze dwuprocesorowej z możliwością zainstalowania procesorów 64 rdzeniowych. * Płyta główna musi umożliwiać instalacje minimum 32 kości DDR5 z możliwością wyskalowania pamięci do minimum 8TB. | (TAK / NIE)\* |
| 5. | Procesor | Zainstalowane dwa procesory, dedykowane do pracy z zaoferowanym serwerem, umożliwiający osiągnięcie wyniku min. 294 w teście SPECrate2017\_int\_base w konfiguracji dwuprocesorowej, dostępnym na stronie [www.spec.org](http://www.spec.org) – wyniki załączyć na wezwanie Zamawiającego do oferty. | (TAK / NIE)\* |
| 6. | RAM | * 256GB DDR5 RDIMM. * Pamięć RAM musi wspierać wczesne wykrywanie błędów poprawialnych (CE) w pamięci i przeprowadzanie operacji izolacji. Pamięć musi wspierać typowe technologie ochrony m.in. ECC, Address/Command Parity, PPR, Write Data CRC Protection, ADC-SR, ADDDC-MR, SDDC. | (TAK / NIE)\* |
| 7. | Kontroler RAID | **Zamawiający wymaga, aby kontroler dysków w oferowanym serwerze spełniał następujące warunki:**   1. **Wspierał tryb JBOD** (Just a Bunch of Disks) – umożliwiając bezpośrednią, niezależną widoczność każdego nośnika danych przez system operacyjny 2. **Nie zawierał pamięci cache RAID** – wykluczając tym samym ingerencję w integralność zapisu/odczytu na poziomie sprzętowym (wymagane przez systemy SDS). 3. **Umożliwiał pracę dysków NVMe w trybie passtrough / direct attach** – co jest wymagane dla środowisk wirtualizacyjnych (np. Proxmox VE) oraz rozwiązań typu Ceph. 4. **Obsługiwał co najmniej RAID 0, RAID 1 oraz JBOD** – w odniesieniu do dysków M.2 SATA lub NVMe. | (TAK / NIE)\* |
| 8. | Dyski twarde | * Zainstalowane:   + 8x dysk SSD NVMe o pojemności min. 1.92TB   + Dwa dyski M.2 SSD o pojemności 480GB Hot-Plug z możliwością konfiguracji RAID 0 lub 1. | (TAK / NIE)\* |
| 9. | Gniazda PCIe | * 1× PCIe5 x16 * 2× PCIe4 x8 | (TAK / NIE)\* |
| 10. | Interfejsy sieciowe/FC/SAS | * Min. 4 interfejsy sieciowe 10 GbE SFP+ * Min. 2 interfejsy sieciowe 25 GbE SFP28 * Min. 1 interfejs sieciowy 1 GbE RJ-45 (inny niż port zarządzający / iBMC) | (TAK / NIE)\* |
| 11. | Wbudowane porty oraz wskaźniki | * 5 portów USB w tym min:   + 2 porty USB 3.0 z tyłu obudowy,   + 2 port USB 3.0 z przodu obudowy   + 1 port USB 2.0 zainstalowany wewnętrznie * 2 porty VGA * 3 dedykowane, wbudowane poty umożliwiające zarządzanie serwerem, z czego co najmniej jeden umożliwiający połączenie z graficznym interfejsem zarządzającym, przynajmniej jeden port na przodzie obudowy umożliwiający połączenie za pomocą USB Type-C. * Przyciski i wskaźniki:   + Diagnostyczny panel LED – panel musi wyświetlać informacje na temat aktualnego stanu serwera. W przypadku awarii, panel LED musi wskazywać odpowiedni kod błędu, a w sytuacji wystąpienia więcej niż jednego błędu, system musi wyświetlać odpowiednie kody błędów w pętli.   + Wskaźnik aktualnego stanu urządzenia – wskaźnik musi za pomocą stosownego koloru oraz określonej częstotliwości odświeżania wyświetlać w jakim stanie znajduje się urządzenie.   + Wskaźnik stanu karty OCP NIC. Wskaźnik musi informować czy:     - Karta została wykryta     - Karta została wykryta ale nie jest włączona     - Karta została zainstalowana, wykryta i działa poprawnie   + Wskaźnik stanu zasilania zintegrowany z przyciskiem zasilania informujący czy:     - Urządzenie jest włączone.     - Urządzenie jest wyłączone.     - Urządzenie zostało uruchomione, a moduł zarządzania się uruchamia. W tej sytuacji wciśnięcie przycisku zasilania nie może spowodować wyłączenia serwera.   + Wskaźnik UID zintegrowany z przyciskiem, umożliwiający zlokalizowanie urządzenia, udostępniający następujące funkcje:     - Przycisk migający lub świecący ciągłym światłem niebieskim umożliwia zlokalizowanie serwera.     - Włączenie/wyłączenie funkcji lokalizacji urządzenia musi być możliwe zarówno z poziomu przycisku jak i z poziomu interfejsu zarządzania.   Wskaźnik statusu bezpośredniego połączenia z interfejsem zarządzania. Musi informować o aktualnym stanie połączenia z interfejsem zarządzania umieszczonym na przednim panelu urządzenia.   Wszystkie wskaźniki oraz porty muszą znajdować się na przodzie urządzenia co znacząco ułatwi analizę wyświetlanych komunikatów. Sam sposób wyświetlania informacji musi być opisany w dokumentacji, a ich funkcje muszą być zgodnie z obowiązującymi praktykami w tym zakresie. | (TAK / NIE)\* |
| 12. | Video | Zintegrowana karta graficzna z minimum 32MB pamięci osiągająca rozdzielczość 1920x1200 60Hz | (TAK / NIE)\* |
| 13. | Wentylatory | Redundantne | (TAK / NIE)\* |
| 14. | Zasilacze | Minimum dwa redundantne zasilacze o mocy minimum 900W z certyfikatem minimum Titanium. | (TAK / NIE)\* |
| 15. | System operacyjny/System wirtualizacji | Oferowany serwer musi umożliwiać instalację systemu operacyjnego klasy Microsoft Windows Server 2025 Standard lub równoważnego, spełniającego poniższe wymagania funkcjonalne:  Licencja musi umożliwiać uruchomienie systemu w środowisku fizycznym oraz maksymalnie czterech środowiskach wirtualnych przy użyciu wbudowanego mechanizmu wirtualizacji.  Każda maszyna wirtualna musi móc wykorzystywać do 64 wirtualnych procesorów, 1 TB pamięci RAM i 64 TB przestrzeni dyskowej.  Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy (live migration) między serwerami fizycznymi za pośrednictwem sieci Ethernet, bez konieczności stosowania zewnętrznych rozwiązań współdzielenia pamięci.  Wsparcie (przy odpowiednim sprzęcie) dla wymiany i dodawania pamięci RAM oraz procesorów bez przerywania pracy systemu.  Weryfikacja cyfrowych sygnatur sterowników – system musi umożliwiać sprawdzenie, czy sterownik przeszedł testy jakości producenta.  Obsługa dynamicznego zarządzania poborem mocy przez rdzenie CPU, w tym obsługa Hyper-Threading.  Mechanizm klasyfikowania i indeksowania plików na podstawie zawartości.  Wbudowane szyfrowanie dysków z użyciem mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny.  Obsługa aplikacji internetowych opartych o ASP.NET oraz dystrybucja ruchu HTTP pomiędzy wiele serwerów.  Wbudowana zapora sieciowa (firewall) z możliwością definiowania reguł dostępu.  Interfejs użytkownika oraz elementy systemu (menu, przeglądarka, pomoc, komunikaty) w języku polskim, z możliwością zmiany języka po instalacji (min. 2 języki do wyboru).  Wsparcie dla powszechnie używanych urządzeń peryferyjnych (drukarki, urządzenia sieciowe, standardy USB, Plug & Play).  Możliwość zdalnej konfiguracji, administrowania i aktualizacji systemu.  Obsługa zasobów dyskowych z wieloma ścieżkami dostępu (Multipath I/O).  Możliwość integracji poprawek z obrazem instalacyjnym systemu.  Obsługa administracji zdalnej, w tym przez skrypty i interfejsy tekstowe.  Możliwość migracji konfiguracji systemu z wersji Microsoft Windows Server 2021 oraz 2016. | (TAK / NIE)\* |
| 16. | Licencje dostępowe | 30 szt. licencji dostępowych typu CAL – użytkownicy. Licencje mają umożliwiać dostęp do środowiska domenowego Windows Server w ramach uruchomionych maszyn wirtualnych. | (TAK / NIE)\* |
| 17. | Elementy montażowe | * Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych * Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych | (TAK / NIE)\* |
| 18. | Bezpieczeństwo | * Moduł TPM 2.0 * Secure boot * Ochrona przed atakami. Urządzenie musi udostępniać minimalną wymaganą liczbę portów usług sieciowych. Domyślnie, zbędne usługi muszą być wyłączone, porty usług sieciowych do debugowania i diagnozy muszą być wyłączone podczas normalnej pracy serwera. | (TAK / NIE)\* |
| 19. | Moduł zarządzania | * Niezależny od zainstalowanego na serwerze systemu operacyjnego, moduł zarządzania, posiadająca dedykowany port Gigabit Ethernet RJ45. * NC-SI * Zarządzanie certyfikatami. Moduł musi obsługiwać szyfrowanie i wymianę certyfikatów SSL. Wymiana samych certyfikatów musi być możliwa z poziomu GUI. * Moduł musi umożliwiać import certyfikatu LDAP (Lightweight Directory Access Protocol. * Wsparcie dla DCMI 1.5. * Wsparcie dla IMPI 1.5 oraz 2.0. * Moduł zarządzania musi posiadać certyfikacje CC EAL4+. * Wymagana jest funkcjonalność zarządzania diagnostyką błędów (FDM. Funkcjonalność musi obejmować zbieranie i analizę danych o błędach, diagnozowanie i lokalizowanie błędów, wczesne ostrzeganie o błędach oraz analizę kondycji urządzeń. Podczas rutynowej obsługi i konserwacji można wyświetlać informacje o wadliwych komponentach oraz związanych z nimi zdarzeniami historycznymi. Wymagana funkcjonalność musi być możliwa do włączenia/wyłączenia z poziomu BIOS. * Moduł musi oferować precyzyjne powiadomienia o niekrytycznych, niekorygowalnych błędach (UCE) w pamięci w sposób umożliwiający zlokalizowanie uszkodzonego modułu. * Wymagana jest obsługa szczegółowych alarmów dotyczących dysków twardych, które mogą rozróżniać trzy typy alarmów: oprogramowania układowego dysku twardego, konfigurację i usterki fizyczne. * Musi umożliwiać przeglądanie w formie graficznego modelu 3D rozkładu temperatury. Mapa temperatury musi umożliwić lokalizowanie anomalii związanych z temperaturą wewnątrz urządzenia w dowolnym jego punkcie. * Moduł musi umożliwiać włączenie funkcji szyfrowania KVM i VNC (Virtual Network Console), które szyfrują dane przesyłane do i z zdalnej konsoli wirtualnej. | (TAK / NIE)\* |
| 20. | BIOS | * Oferowany serwer musi być wyposażony w BIOS zapewniający następujące funkcjonalności:   + Inicjalizacja sprzętu: BIOS musi wspierać pełne testowanie i uruchamianie kluczowych komponentów serwera, takich jak procesory, pamięć RAM, dyski twarde oraz interfejsy sieciowe.   + Zarządzanie konfiguracją systemu: BIOS musi umożliwiać konfigurację ustawień systemowych, w tym kolejności bootowania, konfiguracji RAID oraz ustawień zasilania.   + Bezpieczeństwo systemu: BIOS musi wspierać funkcję Secure Boot, chroniącą przed uruchamianiem nieautoryzowanego oprogramowania. Musi również posiadać opcję zabezpieczenia hasłem dostępu. * Aktualizacje oprogramowania: BIOS musi umożliwiać aktualizację firmware’u oraz zapewniać wsparcie dla aktualizacji zdalnych. | (TAK / NIE)\* |
| 21. | System do zarządzania serwerem – w formularzu należy podać pełną nazwę oferowanego oprogramowania | Oferowany serwer musi być wyposażony w zaawansowane oprogramowanie do zarządzania i monitorowania, które umożliwia centralne zarządzanie oraz optymalizację pracy serwera. Oprogramowanie musi spełniać następujące wymagania:  1. Centralne zarządzanie serwerami   * Oprogramowanie do zarządzania serwerami musi zapewniać:   + Monitorowanie infrastruktury w czasie rzeczywistym: Oprogramowanie musi umożliwiać śledzenie wydajności serwerów, stanu komponentów oraz zużycia zasobów, prezentując dane w formie graficznej.   + Automatyzacja aktualizacji: Musi wspierać zdalne i automatyczne aktualizowanie oprogramowania układowego oraz sterowników, z możliwością planowania aktualizacji.   + Diagnostyka i analiza stanu sprzętu: System musi umożliwiać analizę kondycji serwerów, gromadząc dane diagnostyczne i identyfikując potencjalne problemy przed ich wystąpieniem.   + Zarządzanie wieloma serwerami jednocześnie: Oprogramowanie musi umożliwiać zarządzanie co najmniej 50 serwerami z jednej platformy zarządzającej.   2. Moduł zarządzania płytą główną   * Serwer musi być wyposażony w moduł zarządzania, który oferuje następujące funkcjonalności:   + Dostęp do zdalnej konsoli serwera: Moduł musi umożliwiać pełną kontrolę nad serwerem poprzez zdalny dostęp do konsoli, niezależnie od stanu systemu operacyjnego.   + Monitorowanie sprzętu: Moduł musi zapewniać monitorowanie parametrów sprzętowych, takich jak temperatura, prędkość wentylatorów, napięcia oraz stan kluczowych komponentów.   + Obsługa wirtualnych nośników: Moduł musi umożliwiać montowanie obrazów dysków zdalnie, co ułatwia instalację systemów operacyjnych oraz aktualizacje oprogramowania.   + Bezpieczne zarządzanie: Moduł musi wspierać szyfrowanie komunikacji oraz integrację z systemami uwierzytelniania, takimi jak LDAP, oraz zarządzanie certyfikatami.   + Wsparcie dla standardowych protokołów zarządzania: Moduł musi obsługiwać popularne protokoły zarządzania sprzętem, umożliwiając integrację z zewnętrznymi systemami zarządzania.   3. System zarządzania zasobami serwera   * Serwer musi być wyposażony w oprogramowanie do zarządzania zasobami, które zapewnia:   + Monitorowanie obciążenia w czasie rzeczywistym: Oprogramowanie musi umożliwiać śledzenie wykorzystania procesora, pamięci oraz przestrzeni dyskowej, prezentując dane w formie wykresów i raportów.   + Automatyczna optymalizacja zasobów: System musi posiadać funkcję automatycznego dostosowywania przydziału zasobów, aby maksymalizować wydajność serwera.   + Zarządzanie cyklem życia sprzętu: Oprogramowanie musi wspierać planowanie konserwacji, aktualizacje oprogramowania układowego oraz zarządzanie konfiguracją serwera.   + Integracja z zewnętrznymi systemami zarządzania: System musi obsługiwać standardowe interfejsy API, co umożliwia integrację z narzędziami do automatyzacji i zarządzania infrastrukturą.   4. Oprogramowanie do zarządzania serwerem lokalnie i zdalnie   * Oferowane oprogramowanie musi umożliwiać zarządzanie serwerami zarówno lokalnie, jak i zdalnie, zapewniając:   + Automatyzację konfiguracji i monitorowania: Oprogramowanie musi umożliwiać automatyczną konfigurację serwerów, monitorowanie ich stanu oraz zarządzanie zasobami.   + Integrację z popularnymi platformami chmurowymi: Musi wspierać integrację z rozwiązaniami używanymi w środowiskach chmurowych, takimi jak narzędzia do wirtualizacji oraz systemy zarządzania centrami danych.   + Monitorowanie zużycia energii: Oprogramowanie musi oferować funkcje monitorowania zużycia energii oraz zarządzania profilami energetycznymi serwerów, co pozwala na optymalizację kosztów energii.   5. Otwarte standardy zarządzania sprzętem   * Oprogramowanie musi wspierać otwarte standardy zarządzania sprzętem, takie jak nowoczesny interfejs API, który zapewnia:   + Zdalne zarządzanie sprzętem: API musi umożliwiać programistyczne zarządzanie serwerem, monitorowanie jego parametrów oraz automatyzację zadań administracyjnych.   + Bezpieczną komunikację: API musi wspierać szyfrowanie danych oraz integrację z narzędziami do zarządzania certyfikatami. * Integrację z narzędziami do automatyzacji: API musi umożliwiać integrację z popularnymi narzędziami automatyzacji, takimi jak systemy zarządzania konfiguracją i orkiestracji. | (TAK / NIE)\* |
| 22. | Wymagania dotyczące systemu diagnostycznego | Oferowany serwer musi być wyposażony w zaawansowany system diagnostyczny, który zapewnia kompleksowe monitorowanie stanu sprzętu oraz precyzyjną diagnostykę problemów. Wymagane są następujące funkcjonalności:  1. Funkcja diagnostyki błędów   * System musi zapewniać pełną funkcjonalność diagnostyki błędów, obejmującą:   + Zbieranie i analizę danych o błędach: Automatyczne gromadzenie danych diagnostycznych dotyczących kluczowych komponentów serwera, takich jak procesory, pamięć RAM, dyski twarde, zasilacze oraz wentylatory.   + Diagnozowanie i lokalizowanie usterek: System musi umożliwiać automatyczne wykrywanie i lokalizowanie usterek sprzętowych, wskazując precyzyjnie wadliwe komponenty.   + Wczesne ostrzeganie o błędach: Wymagane jest wsparcie dla funkcji wczesnego ostrzegania, które informuje użytkownika o potencjalnych problemach jeszcze przed ich wystąpieniem, co minimalizuje ryzyko awarii.   + Analiza historii zdarzeń: System diagnostyczny musi umożliwiać przeglądanie pełnej historii zdarzeń oraz błędów, co ułatwia analizę przyczyn awarii i planowanie działań naprawczych.   2. Zaawansowane monitorowanie dysków twardych   * System musi oferować szczegółowe monitorowanie stanu dysków twardych z podziałem na:   + Alarmy dotyczące oprogramowania układowego dysku (firmware): Wykrywanie błędów związanych z oprogramowaniem układowym dysków oraz informowanie o konieczności aktualizacji firmware’u.   + Alarmy dotyczące konfiguracji dysków: Monitorowanie nieprawidłowej konfiguracji dysków, takich jak problemy z RAID, oraz informowanie o konieczności interwencji.   + Alarmy dotyczące usterek fizycznych: Wykrywanie błędów fizycznych dysków, takich jak problemy mechaniczne lub sektory uszkodzone, z możliwością precyzyjnego wskazania wadliwego dysku.   3. Monitoring temperatury i zarządzanie termiczne   * System diagnostyczny musi zapewniać:   + Graficzną mapę temperatury: Wymagana jest funkcjonalność przeglądania rozkładu temperatury wewnątrz serwera w formie graficznego modelu 3D. Mapa temperatury musi umożliwiać szybkie lokalizowanie anomalii termicznych.   + Alerty dotyczące przekroczenia temperatur: Automatyczne powiadamianie o przekroczeniu dopuszczalnych wartości temperatury dla kluczowych komponentów, takich jak procesory, pamięć RAM czy zasilacze.   + Dynamiczne zarządzanie chłodzeniem: System musi wspierać dynamiczne dostosowywanie prędkości wentylatorów na podstawie aktualnych odczytów temperatury, co zapewnia optymalną pracę serwera i minimalizuje zużycie energii.   4. Szyfrowane powiadomienia o błędach   * Wymagane jest wsparcie dla szyfrowanych powiadomień o niekrytycznych i niekorygowalnych błędach (UCE), które umożliwiają precyzyjną identyfikację wadliwego modułu pamięci lub dysku. * System musi wspierać funkcję wysyłania powiadomień o błędach do administratora poprzez e-mail oraz protokoły zarządzania (np. SNMP, Redfish API).   5. Integracja z modułem zarządzania   * System diagnostyczny musi być w pełni zintegrowany z modułem zarządzania iBMC, co umożliwia dostęp do danych diagnostycznych z poziomu interfejsu zarządzania.   Wymagana jest możliwość przeglądania szczegółowych raportów diagnostycznych oraz uruchamiania testów diagnostycznych w czasie rzeczywistym z poziomu konsoli zarządzającej. | (TAK / NIE)\* |
| 23. | Certyfikaty (załączyć do oferty) | Oferowany serwer musi być certyfikowany dla następujących środowisk:   * Microsoft Windows Server (wymagana zgodność z HCL Microsoft).   Producent oferowanego serwera musi posiadać certyfikaty jakości i bezpieczeństwa:   * ISO 9001 (System Zarządzania Jakością). * ISO 14001 (System Zarządzania Środowiskowego). * ISO 50 001 (System Zarządzania Energią) * QC 080000 (System Zarządzania Procesami Produktów Niebezpiecznych). * Deklaracja CE dla oferowanego modelu serwera. * Certyfikat EPEAT na poziomie min. Bronze * Serwer musi posiadać deklaracja CE. | (TAK / NIE)\* |
| 24. | Parametry środowiskowe i efektywność energetyczna | * Oferowane urządzenie musi udostępniać narzędzie, które zapewni możliwość bieżącej analizy poboru prądu. * Serwer musi być przystosowany do pracy w temperaturze od 5 do 40 stopni Celsjusza co musi być kompatybilne z wytycznymi ASHRAE A1 do A3. * Oferowane urządzenie musi być przystosowane do pracy w środowisku określonym normą ISO 14644-1. Informacja na ten temat musi znajdować się w oficjalnej dokumentacji dotyczącej oferowanego serwera. * Zasilacze muszą posiadać certyfikat 80 Plus Titanium, zapewniający sprawność energetyczną na poziomie co najmniej 96% przy obciążeniu 50%. | (TAK / NIE)\* |
| 25. | Dokumentacja użytkownika | Zamawiający wymaga dokumentacji w języku polskim lub angielskim oraz dostęp do oprogramowania wymaganego do poprawnego funkcjonowania serwera. | (TAK / NIE)\* |
| 26. | Dodatkowe oprogramowanie zabezpieczające – w formularzu należy podać pełną nazwę oferowanego oprogramowania | System chroniący przed zagrożeniami, posiadający certyfikaty: OPSWAT Platinum, AV-Test ‘Top Product’, AV Comperative Advance +, ISO 27001 .  Szyfrowanie danych:  • Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.  • Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.  Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.  Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.  Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.  Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.  Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.  Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.  Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware.  Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware  Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:  • Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli  • Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory  • Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux  • Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.  • Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich  • Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji  Zarządzanie przez Chmurę:  1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach  2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury  3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur  4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy  5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach  6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń  7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej  Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.  Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.  1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer  2. Oprogramowanie klienckie, zarządzane z poziomu serwera.  System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:  • różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie  • funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD  • funkcje regulowania połączeń WiFi i Bluetooth  • funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe  • funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi  • funkcje blokowania dostępu dowolnemu urządzeniu  • możliwość tymczasowego dodania dostępu do urządzenia przez administratora  • zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu  • możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka  • możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora  • możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry  • możliwość używania tylko zaufanych urządzeń sieciowych,w tym urządzeń wskazanych na końcówkach klienckich  • funkcję wirtualnej klawiatury  • możliwość blokowania każdej aplikacji  • możliwość zablokowania aplikacji w oparciu o kategorie  • możliwość dodania własnych aplikacji do listy zablokowanych  • zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze  • dodawanie innych aplikacji  • dodawanie aplikacji w formie portable  • możliwość wyboru pojedynczej aplikacji w konkretnej wersji  • dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB  • kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool  • możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.  • możliwość zablokowania funkcji Printscreen  • funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx  • funkcje monitorowania i kontroli przepływu poufnych informacji  • możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików  • możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj  • możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe  • ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe  • ochrona zawartości schowka systemu  • ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL  • możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych  • ochrona plików zamkniętych w archiwach  • Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem  • możliwość tworzenia profilu DLP dla każdej polityki  • wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania  • ochrona przez wyciekiem plików poprzez programy typu p2p  Monitorowanie zmian w plikach:  • Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.  • Funkcje monitorowania określonych rodzajów plików.  • Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.  • Generator raportów do funkcjonalności monitora zmian w plikach.  • możliwość śledzenia zmian we wszystkich plikach  • możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach  • możliwość definiowana własnych typów plików  Optymalizacja systemu operacyjnego stacji klienckich:  • usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku  • optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem  • możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich  • instruktaż stanowiskowy pracowników Zamawiającego  • dokumentacja techniczna w języku polskim  Wspierane platformy i systemy operacyjne:  1.Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit)  2.Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit)  3.Mac OS X, Mac OS 10  4.Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat  Platforma do zarządzania dla Android i iOS:  • Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę  • Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej.  Zarządzanie użytkownikiem  • Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email  • Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika  • Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi  • Musi posiadać możliwość eksportu danych użytkownika  Zarządzanie urządzeniem  • Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO  • Musi umożliwiać import listy urządzeń z pliku CSV  • Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych  • Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta  • Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał  • Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres  • Musi zawierać podgląd aktualnie zainstalowanych aplikacji  • Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych,  • Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł  • Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres  Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:  Wymagania dotyczące technologii:  1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową  2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.  3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:  - Microsoft Internet Explorer  - Microsoft Edge  - Mozilla Firefox  - Google Chrome  - Safari  4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących  5 Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie  6. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne:  - Windows 2008 R2  - Windows 2012  - Windows 2012 R2  - Windows 2016  7. Portal zarządzający musi umożliwiać:  a) przegląd wybranych danych na podstawie konfigurowalnych widgetów  b) zablokowania możliwości zmiany konfiguracji widgetów  c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.  d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności  e) eksport wszystkich skanów podatności do pliku CSV   * Backup i przywracanie danych * Deduplikacja danych, * Backup przyrostowy i różnicowy, * Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji, * Backup danych lokalnych – plikowy oraz poczty Outlook, * Backup otwartych plików (VSS), * Filtr plików oraz folderów, * Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.), * Wyłączanie komputera po wykonaniu backupu, * Przywracanie danych do wskazanej lokalizacji, * Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora, * Wyszukiwanie plików w repozytorium użytkownika,   Ustawienia   * Automatyczne logowanie, * Zapamiętywanie danych logowania, * Automatyczne uruchamianie programu przy starcie systemu, * Ustawianie priorytetu dla procesu backupu, * Zmiana klucza szyfrującego, * Ustawienia przepustowości/zajętości pasma, * Konfiguracja wydajności procesu backupu,   Bezpieczeństwo   * Zastępowanie nazwy pliku GUID-em, * Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika, * Kompresja danych, * Transmisja po bezpiecznym protokole TLS, * Deklaracja klucza szyfrującego dane użytkownika, * Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji, * Obliczanie sumy kontrolnej, * Kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center, na terenie Polski.   WSPIERANE SYSTEMY OPERACYJNE Microsoft Windows 7 i nowsze, Mac OS, Licencje przypisywane do jednego urządzenia z limitem pojemności przestrzeni w chmurze – minimum 50 GB. Wsparcie techniczne, świadczone jest bezpośrednio od producenta, w języku polskim, zawarte jest w cenie licencji.   * Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. | (TAK / NIE)\* |
| 27. | Warunki serwisu i gwarancji | * Zamawiający wymaga zapewnienia oficjalnego wsparcia Producenta w ramach oferowanej technologii na okres 5 lat realizowaną na miejscu u Zamawiającego. * Zamawiający wymaga przynajmniej dwóch podstawowych form kontaktu serwisowego tj. całodobowej infolinii oraz formularza online. * Oferowane wsparcie musi być świadczone w języku polskim bezpośrednio przez 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. * Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. * Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta.   Usługi serwisowe obejmują:   * Diagnozowanie problemów sprzętowych i programowych. * Aktualizacje firmware oraz dostęp do najnowszych wersji sterowników przez okres trwania wsparcia. * Naprawy na miejscu w siedzibie zamawiającego. * Czas reakcji serwisu do następnego dnia roboczego. * Naprawy muszą być przeprowadzone przez certyfikowany personel Producenta lub autoryzowanego partnera serwisowego posiadającego certyfikację ISO 9001, ISO 27001 – dokumenty załączyć do oferty. | (TAK / NIE)\* |
| 28. | Rozszerzone wsparcie serwisowe | System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:  • Wsparcie telefoniczne zespołu certyfikowanych inżynierów.  • Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.  • Doradztwo w zakresie konfiguracji.  • Zdalne wsparcie techniczne.  • Pomoc w zakładaniu zgłoszeń serwisowych u producenta.  • Przygotowanie do zdalnej konfiguracji.  • Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.  • Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.  • Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.  • Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.  **Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.**  Oferent winien przedłożyć dokumenty:   * Oświadczanie Producenta lub Autoryzowanego Dystrybutora producenta świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). * Certyfikat ISO 9001 oraz 27001 autoryzowanego podmiotu serwisującego. | (TAK / NIE)\* |
| 29. | Uwagi uzupełniające: | Jeżeli producent serwera nie dostarcza niezbędnego okablowania do interfejsów sieciowych (np. DAC/SFP/patchcordów), ich zapewnienie leży po stronie Wykonawcy. W szczególności dotyczy to:  • 4 szt. przewodów DAC do połączeń 10GbE SFP+ (długość 3 m),  • 4 szt. wkładek SFP28 25GbE oraz 4 szt. patchcordów światłowodowych SM, zakończonych złączami UPC–APC LC (dł. 3 m) | (TAK / NIE)\* |

**\* określić czy oferowany sprzęt/usługa spełnia/ją wymagania minimalne określone w tabeli stanowiącej opis przedmiotu zamówienia (wypełnić/zaznaczyć odpowiednio TAK/NIE).**

# **System NAC do izolacji sieci LAN w siedzibie zamawiającego – 80 IP**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
| **CZY SPEŁNIAJĄ WYMAGANIA?** |
| 1. | Opis funkcjonalności rozwiązania | Wymagane jest dostarczenie rozwiązania typu NAC (Network Access Control), służącego do monitorowania sieci lokalnych w celu uwidocznienia pracujących w nich urządzeń oraz wykrywania nowych urządzeń pojawiających się w sieci, w czasie rzeczywistym. Rozwiązanie musi raportować aktualny stan każdego urządzenia, z uwzględnieniem takich atrybutów, jak adres MAC, adres IP, nazwa hosta, system operacyjny, itp., pozyskując te informacje bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.).  Rozwiązanie ma za zadanie zapewnić, aby tylko urządzenia, których aktualny stan spełnia zdefiniowaną przez administratora politykę bezpieczeństwa, mogły bez ograniczeń ze strony NAC pracować w sieci lokalnej. Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenia, których aktualny stan nie spełnia danych warunków polityki bezpieczeństwa (np. nowe, po raz pierwszy pojawiające się urządzenie lub stacja robocza z wyłączonym oprogramowaniem antywirusowym). Mechanizm kwarantanny powinien umożliwiać całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym, jak również blokowanie częściowe, w zakresie definiowanym przez administratora (przez wskazanie adresów IP, z którymi urządzenie może się komunikować). Mechanizm kwarantanny musi działać bezagentowo, wykorzystując protokół ARP, bez konieczności dokonywania jakichkolwiek zmian w konfiguracji infrastruktury sieciowej.  Rozwiązanie musi posiadać funkcjonalność typu Captive Portal, służącą do rejestrowania i kontrolowania dostępu do sieci dla niezarządzanych urządzeń zewnętrznych, podłączanych przez pracowników (BYOD), gości i zewnętrznych konsultantów. | (TAK / NIE)\* |
| 2. | Wymagania ogólne rozwiązania NAC | 1. Ma zapewnić widoczność i monitorowanie wszystkich urządzeń pracujących w sieci lokalnej oraz powiadamiać o nowych urządzeniach pojawiających się w sieci. 2. Musi zapewniać automatyczne blokowanie komunikacji sieciowej między nowym, niezaufanym urządzeniem a zaufanymi, zarządzanymi urządzeniami pracującymi w sieci. 3. Musi umożliwiać sprawdzanie statusu aktualizacji oprogramowania antywirusowego i poprawek systemowych na zarządzanych stacjach roboczych Windows i w przypadku nie spełniania określonych wymagań, automatycznie ograniczać tym stacjom roboczym możliwość pracy w sieci. 4. Musi umożliwiać odbieranie komunikatów bezpieczeństwa z innych systemów bezpieczeństwa (np. firewalla) i automatyczne blokowanie na tej podstawie wskazanych urządzeń w sieci. 5. Musi mieć funkcję wykrywania faktu skanowania urządzeń i portów wykonywanego przez urządzenie w sieci lokalnej i automatycznie blokować takie urządzenie, aby zapobiegać potencjalnemu szerzeniu się malware. 6. Stosowany mechanizm blokowania musi wykorzystywać protokół ARP i działać całkowicie niezależnie od innych elementów infrastruktury sieciowej. 7. Rozwiązanie musi działać bezagentowo, bez konieczności instalowania jakichkolwiek agentów na urządzeniach w sieci oraz bez konieczności dokonywania zmian w infrastrukturze sieciowej. 8. Rozwiązanie musi umożliwiać wysyłanie alertów do administratora za pomocą e-maila oraz SMS 9. Rozwiązanie musi być zarządzane przez interfejs webowy, obsługiwany przeglądarką internetową 10. Wymaga się, aby rozwiązanie było dostarczone w postaci maszyny wirtualnej na platformę VMware oraz Hyper-V. System musi pozwalać na monitorowanie łącznie co najmniej 200 urządzeń. 11. Wymaga się, aby rozwiązanie było licencjonowane w modelu licencji wieczystej i dostarczone z licencją pozwalającą na monitorowanie 80 urządzeń wraz ze wsparciem technicznym minimum 12 m-cy. 12. Wsparcie techniczne musi obejmować dostarczanie aktualizacji oprogramowania/firmware oraz pomoc techniczną producenta w dni robocze w godzinach pracy. | (TAK / NIE)\* |
| 3. | Wymagania szczegółowe – monitorowanie podsieci | 1. Monitorowanie podsieci 2. Rozwiązanie musi wykrywać nowe nieznane urządzenie, dołączające się do sieci LAN lub WLAN, w czasie nie dłuższym, niż 5 sekund oraz wysyłać powiadomienie mailowe do administratora 3. Rozwiązanie musi wykrywać przypadki skanowania urządzeń i portów w monitorowanych podsieciach i blokować urządzenie inicjujące takie skanowanie 4. Rozwiązanie musi posiadać funkcję pułapki sieciowej (honeypot), symulującą w każdej monitorowanej podsieci standardowe usługi sieciowe, co najmniej: ssh, telnet, ftp i smb. Rozwiązanie musi rejestrować każdą próbę zalogowania się do takiej symulowanej usługi, zapisując użytą nazwę użytkownika, hasło użytkownika i źródłowy MAC/IP. 5. Rozwiązanie musi określać aktualny stan każdego urządzenia, pozyskując informacje bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.) oraz odświeżać te informacje cyklicznie. Musi być możliwość wykorzystania pozyskanych informacji do definiowania polityk bezpieczeństwa. 6. Rozwiązanie musi chronić przed podszywaniem się pod adres MAC (MAC spoofing), umożliwiając zdefiniowanie „odcisku palca” (fingerprint) dla każdego zaufanego urządzenia. Odcisk palca musi być kombinacją co najmniej: adresu MAC, adresu IP, nazwy hosta, nazwy systemu operacyjnego, otwartych portów TCP. Jeśli przeprowadzana cyklicznie weryfikacja odcisku palca wykaże jego zmianę, urządzenie powinno zostać zablokowane. 7. Rozwiązanie musi obsługiwać VLANy, tj. umożliwiać monitorowanie przez jeden fizyczny interfejs sieciowy wielu podsieci, zdefiniowanych jako VLANy | (TAK / NIE)\* |
| 4. | Wymagania szczegółowe – polityka bezpieczeństwa | 1. Rozwiązanie musi umożliwiać definiowanie polityki bezpieczeństwa, czyli określenie przez administratora, jakie warunki musi spełniać aktualny stan urządzenia, aby uzyskało ono określony dostęp do sieci. 2. W definiowaniu polityki bezpieczeństwa musi być możliwość wykorzystania informacji o aktualnym stanie urządzenia, pozyskanych bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.), poprzez integrację z tymi systemami. 3. Polityka bezpieczeństwa musi umożliwiać przypisanie do urządzenia jednego z trzech trybów dostępu do sieci:    1. pełny dostęp    2. blokowanie (całkowity brak dostępu)    3. ograniczony dostęp 4. Zakres ograniczonego dostępu powinien być definiowany przez administratora, np. w postaci list ACL, określających, do których adresów IP i portów urządzenie ma dostęp. Musi być możliwość zdefiniowania wielu różnych zakresów ograniczonego dostępu. 5. Rozwiązanie powinno automatycznie sprawdzać, które warunki polityki bezpieczeństwa spełnia urządzenie i na tej podstawie przypisywać do urządzenia właściwy zakres dostępu. 6. Zakres dostępu, wynikający ze spełnienia przez urządzenie danych warunków polityki bezpieczeństwa powinien być egzekwowany przez mechanizm kwarantanny. 7. Musi być możliwość łatwego, manualnego tworzenie białej listy adresów MAC, czyli listy urządzeń mogących bez żadnych ograniczeń ze strony NAC pracować w sieci. | (TAK / NIE)\* |
| 5. | Wymagania szczegółowe – mechanizm kwarantanny | 1. Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenie, aby wyegzekwować ograniczenia dostępu do sieci, wynikające z polityki bezpieczeństwa  2. Mechanizm kwarantanny powinien umożliwiać:  a. całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym,  b. częściowe blokowanie komunikacji urządzenia z otoczeniem sieciowym, w zakresie definiowanym przez administratora przez wskazanie adresów IP i portów, z którymi urządzenie może się komunikować  3. Mechanizm kwarantanny powinien blokować komunikację urządzenia w czasie nie dłuższym, niż 5 sekund od zaistnienia warunku, powodującego nałożenie kwarantanny  4. Dla urządzeń zaufanych, czyli w polityce bezpieczeństwa spełniających kryteria pełnego dostępu do sieci, rozwiązanie nie powinno w żaden sposób przekierowywać ani blokować komunikacji wychodzącej z tych urządzeń  5. Kwarantanna powinna być zdejmowana z urządzenia automatycznie, gdy spełni ono kryteria polityki bezpieczeństwa, pozwalające na pełny dostęp  6. Mechanizm kwarantanny musi działać bezagentowo, wykorzystując protokół ARP, bez konieczności dokonywania jakichkolwiek zmian w konfiguracji infrastruktury sieciowej, musi być niezależny od stosowanych w sieci przełączników, zarządzalnych bądź niezarządzalnych  7. Awaria rozwiązania nie może powodować blokady komunikacji w sieci, tj. w przypadku awarii rozwiązania wszystkie urządzenia mają mieć pełny dostęp do sieci  8. Rozwiązanie musi umożliwiać włączenie i wyłączenie mechanizmu kwarantanny (blokowania komunikacji) w każdej monitorowanej podsieci osobno | (TAK / NIE)\* |
| 6. | Wymagania szczegółowe – integracja z systemami zewnętrznymi | 1. Rozwiązanie musi umieć sprawdzić, czy urządzenia z systemem Windows są dołączone do domeny AD 2. Rozwiązanie powinno umożliwiać sprawdzanie statusu oprogramowania antywirusowego, poprawek systemowych i firewalla bezpośrednio na zarządzanych stacjach roboczych Windows w domenie AD, w sposób bezagentowy, przy użyciu WMI. 3. Rozwiązanie musi umożliwiać bezagentową integrację z serwerem zarządzającym poprawkami Windows i sprawdzanie statusu zainstalowanych poprawek na zarządzanych urządzeniach z systemem Windows. Wymagana jest możliwość integracji co najmniej z systemami: Microsoft WSUS. 4. Rozwiązanie musi umożliwiać bezagentową integrację z serwerem zarządzającym agentami antywirusowymi i sprawdzanie statusu agentów AV zainstalowanych na zarządzanych urządzeniach (co najmniej, czy agent jest zainstalowany, aktywny i ma aktualne sygnatury wirusów). Wymagana jest możliwość integracji co najmniej z systemami: Bitdefender, Carbon Black, CrowdStrike, Cybereason, Eset, FireEye, McAfee, SentinelOne, Sophos, Symantec, TrendMicro, Webroot. 5. Rozwiązanie musi umożliwiać wykorzystanie pozyskanych informacji, wymienionych w poprzedzających punktach 1-4, do definiowania polityki bezpieczeństwa. 6. Rozwiązanie musi umieć odbierać alerty przysyłane za pomocą e-mail lub syslog z innych urządzeń bezpieczeństwa (np. firewalla) i na podstawie zawartych w nich informacji blokować wskazane podejrzane urządzenie | (TAK / NIE)\* |
| 7. | Wymagania szczegółowe – rejestracja urządzeń zewnętrznych: pracowników, gości i konsultantów (Captive Portal) | 1. Rozwiązanie musi posiadać wbudowaną funkcję Captive Portal, służącą do rejestrowania i kontrolowania dostępu do sieci dla niezarządzanych urządzeń zewnętrznych, podłączanych przez pracowników (BYOD), gości i zewnętrznych konsultantów. NAC musi przekierowywać ruch HTTP/S od nieznanych urządzeń do tego portalu.  2. Captive Portal musi umożliwiać pracownikom rejestrowanie urządzeń prywatnych (BYOD) i wnioskowanie o dostęp do sieci w ograniczonym zakresie, zdefiniowanym przez administratora.  3. Przy rejestracji przez pracowników ich prywatnych urządzeń, Captive Portal powinien umożliwiać użycie ich kont Active Directory  4. Powinna istnieć możliwość ograniczenia ilości i rodzaju rejestrowanych przez pracownika prywatnych urządzeń  5. Powinna być możliwość przypisania ograniczonego dostępu dla zarejestrowanych urządzeń prywatnych  6. Captive Portal musi umożliwiać osobom nie będącym pracownikami (gościom lub konsultantom) wnioskowanie o ograniczony dostęp do sieci  7. W przypadku rejestracji urządzeń gości powinna być możliwość rejestracji samodzielnie przez gościa oraz przez uprawnionego pracownika firmy  8. Zarejestrowane urządzenia gości powinny automatycznie tracić przydzielony dostęp po upływie zdefiniowanego czasu  9. Powinna istnieć możliwość ograniczenia ilości urządzeń rejestrowanych przez gościa  10. Dla zarejestrowanych urządzeń gości powinna być możliwość ograniczenia, w jakich przedziałach czasu i z jakich podsieci będą one miały dostęp do sieci  11. Dla urządzeń gości powinna być możliwość przypisania dostępu ograniczonego tylko do dostępu do internetu  12. Dla urządzeń konsultantów powinna być możliwość przypisania dostępu ograniczonego do wybranych zasobów lokalnych  13. Rozwiązanie musi umożliwiać zatwierdzenie dostępu dla zarejestrowanego urządzenia gościa i konsultanta drogą mailową. Osoba zatwierdzająca powinna otrzymać z systemu e-mail z wnioskiem o dostęp i udzielić go, odpowiadając na maila lub klikając przygotowany link w treści maila.  14. Rozwiązanie musi przechowywać historyczne raporty dostępu do sieci użytkowników typu gość i konsultant  15. Wygląd Captive Portal musi być edytowalny w zakresie co najmniej zmiany firmowego logo i kolorów oraz informacji, jakie we wniosku rejestracyjnym musi podać gość lub konsultant | (TAK / NIE)\* |
| 8. | Pozostałe wymagania | 1. Rozwiązanie powinno oferować uwierzytelnianie administratora za pomocą dodatkowego faktora, oprócz hasła (2FA).  2. Rozwiązanie powinno oferować możliwość zainstalowania opcjonalnego agenta na zarządzanych stacjach roboczych (wymagane wsparcie dla Windows, Linux i MacOS), który przesyła do serwera zarządzającego NAC szczegółowe informacje na temat stacji roboczej, umożliwiając definiowanie na bazie tych informacji precyzyjnych polityk bezpieczeństwa.  3. Rozwiązanie nie powinno pogarszać wydajności pracy przełączników i routerów, nie może wymagać współpracy z przełącznikami przez port mirroring czy port spanning.  4. Rozwiązanie nie powinno pogarszać wydajność łącz WAN  5. Rozwiązanie nie powinno pogarszać wydajności pracy monitorowanych urządzeń w sieci | (TAK / NIE)\* |
| 9. | Usługi | Wymaga się, aby dostawca zaoferował usługę wdrożenia rozwiązania w infrastrukturze Zamawiającego, w wymienionym poniżej zakresie, przeprowadzoną przez wykwalikowanego inżyniera, certyfikowanego przez producenta rozwiązania w siedzibie Zamawiającego:  - instalacja i konfiguracja rozwiązania w maszynie wirtualnej na platformie Zamawiającego  - szkolenie dla administratora rozwiązania  - wsparcie w języku polskim w trybie 8x5 w dni robocze  - kwartalny przegląd konfiguracji rozwiązania    **Wymaga się, aby dostawca przedstawił:**  - oświadczenie Producenta lub Autoryzowanego Dystrybutora Producenta o posiadaniu przez dostawcę kwalifikacji technicznych, niezbędnych do wykonania wdrożenia oferowanego rozwiązania i szkolenia należy załączyć do oferty  - osobowy certyfikat inżynierski pracownika, który będzie wykonywał wdrożenie, należy załączyć do oferty | (TAK / NIE)\* |
| 10. | Testy penetracyjne infrastruktury wewnętrznej | * Głównym celem testów bezpieczeństwa jest identyfikacja luk po instalacji i konfiguracji oferowanego systemu NAC. * Prace zostaną przeprowadzone zdalnie z wykorzystaniem połączenia VPN do zasobów Zamawiającego. * Prace będą wykonywane z jednego stałego adresu IP Wykonawcy. * Testy bezpieczeństwa muszą objąć wymagania weryfikacyjne określone w następujących dokumentach: * OWASP Web Security Testing Guide v4.2, * OWASP Top 10 2021, * OWASP Application Security Verification Standard (ASVS) v4.0.3 (Level 2), * Przebieg procesu testowania bezpieczeństwa aplikacji * Próby zgromadzenia jak największej ilości dostępnych publicznie informacji na temat infrastruktury informatycznej * Identyfikacja udostępnionych usług poprzez skanowanie portów TCP/UDP wraz z próbą uzyskania informacji o zainstalowanych wersjach oprogramowania wykorzystując techniki fingerprinting oraz banner grabbing * Skanowanie podatności z wykorzystaniem automatycznych narzędzi * Manualna identyfikacja podatności * w oparciu o zgromadzone informacje * o wersjach zainstalowanego na badanych urządzeniach oprogramowania w publicznych bazach (np. Bugtraq, CERT, OSVDB), * Analiza mająca na celu weryfikację i eliminację potencjalnych fałszywych alarmów (false positives) oraz identyfikację krytycznych podatności, * Próba odnalezienia kodu oprogramowania wykorzystującego daną podatność – tzw. Exploit * Kontrolowane próby wykorzystania stwierdzonych podatności * Testy podatności są realizowane w oparciu o globalną metodykę, zgodną z opracowaniami OSSTMM (Open Source Security Testing Methodology Manual) LPT (License Penetration Testing) oraz najlepszymi praktykami w obszarze testów podatności. * Testy penetracyjne infrastruktury prowadzone będą z wykorzystaniem automatycznych narzędzi służących do weryfikacji poziomu bezpieczeństwa infrastruktury oraz przy wykorzystaniu technik manualnych, * Minimalne narzędzia jakie Wykonawca musi wykorzystać do przeprowadzenia testów zewnętrznych:   o Nmap  o Nessus Professional  o OpenVAS  o MetaSploit  o Foca  o Maltego  o Skrypty I narzędzia autorskie w Kali linux,  o Skrypty I narzędzia autorskie powershell do enumeracji infrastruktury Microsoft Windows,   * **Zamawiający wymaga, aby Wykonawca posiadał potencjał osobowy niezbędny do wykonania zamówienia.** **Zamawiający wymaga aby osoby testujące łącznie posiadały poniższe certyfikaty:**   o Offensive Security Certified Professional (OSCP);  o Certified Information Systems Security Professional (CISSP);  o Certified Security Analyst (ECSA);  o Wep Application Penatration Tester (eWPT);  o Certified Professional Penetration Tester (eCPPT);  **Certyfikaty należy załączyć do oferty** | (TAK / NIE)\* |

**\* określić czy oferowany sprzęt/usługa spełnia/ją wymagania minimalne określone w tabeli stanowiącej opis przedmiotu zamówienia (wypełnić/zaznaczyć odpowiednio TAK/NIE).**

# **System do kategoryzacji i archiwizacji logów**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
| **CZY SPEŁNIAJĄ WYMAGANIA?** |
| 1. | Dane producenta /model | Producent oferowanego rozwiązania /model i wersja modelu  ……………………………………………/……………………………………………… | (TAK / NIE)\* |
| 2. | Charakterystyka rozwiązania | 1. Rozwiązanie musi odbierać wiadomości Syslog  2. Rozwiązanie musi odbierać wiadomości Trap SNMP w wersji v1,v2, v3  3. Rozwiązanie musi nasłuchiwać Windows Event Log  4. Rozwiązanie musi posiadać graficzny interfejs użytkownika w przeglądarce internetowej  5. Rozwiązania musi mieć możliwość powiadamiania użytkowników drogą emailową na bazie otrzymanych zdarzeń  6. Rozwiązanie musi mieć możliwość uruchamiania zewnętrznych skryptów  7. Rozwiązanie musi mieć możliwość przesyłania dalej zebranych wiadomości do innych systemów w formatach Syslog oraz Trap SNMP w wersji v1, v2, v3  8. Rozwiązanie musi mieć możliwość eksportu zdarzeń do formatu .csv  9. Rozwiązanie powinno umożliwiać zarządzanie politykami retencji danych zdarzeń  10. Rozwiązanie musi wspierać standard IPv4 i IPv6  11. Rozwiązanie musi wspierać przesył danych na poziomie powyżej  2 000 000 zdarzeń na godzinę  12. Rozwiązanie musi być licencjonowanie w sposób nieograniczający ilości podłączonych urządzeń przesyłających informacje  13. Rozwiązanie powinno integrować się ze Splunk  14. Rozwiązanie powinno integrować się z rozwiązaniami typu SIEM  15. Rozwiązanie musi mieć możliwość instalacji na systemach Microsoft Windows Server 2016, 2019, 2022 oraz Microsoft Windows 10, 11. | (TAK / NIE)\* |
| 3. | Licencjonowanie | Licencja wieczysta na oprogramowanie, na okres minimum 12 m-cy. | (TAK / NIE)\* |
| 4. | Usługi | Wymaga się, aby dostawca zaoferował usługę wdrożenia rozwiązania w infrastrukturze Zamawiającego:  - instalacja i konfiguracja rozwiązania na platformie Zamawiającego  - szkolenie dla administratora rozwiązania  - wsparcie w języku polskim w trybie 8h x 5 (w dni robocze) | (TAK / NIE)\* |

**\* określić czy oferowany sprzęt/usługa spełnia/ją wymagania minimalne określone w tabeli stanowiącej opis przedmiotu zamówienia (wypełnić/zaznaczyć odpowiednio TAK/NIE).**

# **System do utrzymywania aktualności inwentaryzacji sprzętu i DLP**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
| **CZY SPEŁNIAJĄ WYMAGANIA?** |
| 1. | Architektura / budowa | 1. System musi umożliwić bezproblemową i stabilną obsługę co najmniej **30 Klientów jednocześnie.**   Architektura / budowa:   1. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej. 2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). 3. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach. 4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami. 5. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej.   Konfiguracja Architektury:   1. Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie. 2. System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem | (TAK / NIE)\* |
| 2. | Wymagania systemowe | 1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox, Chrome, Opera). 2. Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022/2025, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa. 3. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera wersja 63.0.3368.94, Chrome wersja 77.0.3865.90, FireFox wersja 69.0.2 4. Serwer musi działać na systemach 64 bitowych: Windows Server 2016/2019/2022/2025, Windows 7/8/8.1/10/11. 5. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2016/2019/2022/2025, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 9. 6. Baza danych musi działać na silniku Microsoft SQL bezpłatnej (np. Microsoft SQL Server Express Edition). 7. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare. | (TAK / NIE)\* |
| 3. | Interfejsy | 1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie. 2. System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL 3. System zapewnia integrację z modelem LLM. | (TAK / NIE)\* |
| 4. | Funkcjonalności systemu zarządzania infrastrukturą IT | 1. Funkcjonalność Klienta 2. System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkowniku. 3. Funkcjonalność konsoli administracyjnej. 4. Konsola administracyjna musi być wielojęzyczna (polski i angielski) i oferować intuicyjny interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie). Musi także zawierać co najmniej 140 różnorodnych dashboardów, w tym dashboardy użytkownika, prezentujące parametry infrastruktury, sieci oraz bezpieczeństwa. Użytkownicy powinni mieć możliwość samodzielnego konfigurowania dashboardów użytkownika, a dashboardy sieciowe i bezpieczeństwa muszą zawierać szczegółowe widżety z informacjami o stanie usług i bezpieczeństwie. 5. W konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem. 6. Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń. 7. Funkcjonalność panelu pracownika 8. Panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora. 9. Zarządzanie licencjami 10. System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania. 11. Wzorce aplikacji i pakietów 12. System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office. 13. Inwentaryzacja sprzętu komputerowego i urządzeń. 14. System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich podłączeń. 15. Inwentaryzacja urządzeń sieciowych. 16. System musi posiadać zdolności do identyfikacji i zarządzania środowiskami wirtualizacji Hyper-V i VMware oraz urządzeniami sieciowymi. Wymagane jest posiadanie skanera sieci i SNMP oraz dla środowisk wirtualizacji, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci. 17. Inwentaryzacja sprzętu. 18. System musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych. 19. Ochrona danych (DLP). System musi w pełni wspierać następujące polityki ochrony danych: 20. Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwolonymi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami. 21. Zdefiniowanie schematu, w którym można określić, które aplikacje są zabronione, zalecane, dodatkowe bądź nieokreślone. Schemat oprogramowania można przypisać do dowolnej grupy komputerów. Mechanizm musi umożliwić automatyczne odinstalowanie oprogramowania, które wg zdefiniowanego schematu jest zabronione 22. Wyświetlanie komunikatu na komputerach użytkowników podczas uruchamiania stacji roboczej. Komunikaty muszą być definiowalne z poziomu konsoli administracyjnej z wykorzystaniem edytora (możliwość utworzenia tabeli, dołączenia obrazu, wstawienia linku). 23. Blokowanie dostępu do wybranych typów urządzeń od strony sprzętowej. Wsparcie dla CD-ROM, portów USB, kart sieciowych, GPS, kart graficznych, modemów, klawiatur, czytników kart, drukarek, urządzeń Bluetooth i innych, monitorowanie podłączanych urządzeń. 24. Blokowanie dostępu do urządzeń USB, tworzenie czarnych list urządzeń, monitorowane podłączanych urządzań USB. 25. Zarządzanie dostępem do sieci społecznościowych, serwisów informacyjnych, blogów, bibliotek, forów dyskusyjnych oraz dowolnych stron www. 26. Blokowanie sieci ze względu na zdefiniowany typ i maskę sieci WIFI. Polityka musi zapewniać blokowanie dostępu do sieci zarówno otwartych jak i zabezpieczonych. 27. Umożliwienie powiadamianie o przekroczeniu dozwolonego czasu pracy komputera. 28. Podjęcie działania w momencie uruchomienia określonego procesu. 29. Podjęcie działań monitorowania i blokowania operacji w momencie próby kopiowania tekstu, zdjęcia czy ścieżki plików do schowka. 30. Monitorowanie wykonywanych zrzutów ekranu, blokowanie możliwości zapisania i wykorzystania zrzutów ekranu. 31. Przechwytywanie zrzutów ekranu z komputerów użytkowników wyzwalany akcją użytkownika lub na życzenie administratora zgodnie z wcześniej ustawionym interwałem czasowym. 32. Monitorowanie danych przesyłanych za pomocą poczty e-mail oraz blokowanie przesyłania plików określonych typów. 33. Monitorowanie danych przesyłanych do chmury oraz blokowanie synchronizacji plików określonych typów z wybraną chmurą. 34. Monitorowania i blokowania operacji (otwieranie/ usuwanie/ tworzenie/ zapis/ zmiana nazwy) na plikach. 35. Oznaczanie na dowolnym komputerze (znakowanie przez agenta) określonych plików wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami. 36. Znakowanie określonych plików przechowywanych w zasobach serwerów lub udostępnionych zasobach (np. samodzielna macierz dyskowa) wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami, z wykorzystaniem harmonogramu. 37. Szyfrowanie dysków wewnętrznych oraz zewnętrznych 38. System musi obsługiwać kompleksowe szyfrowanie dysków wewnętrznych i zewnętrznych USB, z wykorzystaniem BitLocker i różnych metod szyfrowania, takich jak XTS\_AES\_256 i AES\_128. Musi umożliwiać zdalne zarządzanie procesem szyfrowania/deszyfrowania, w tym masowe operacje na partycjach systemowych i niesystemowych, zarówno lokalnie, jak i zdalnie (poza NATem). Klucze szyfrujące są przechowywane i chronione w konsoli administracyjnej, dostępne tylko po uwierzytelnieniu administratora. Proces szyfrowania odbywa się w sposób niewidoczny dla użytkownika i nie może być przez niego przerwany, z wyjątkiem stanów hibernacji i wyłączenia systemu, po których jest automatycznie kontynuowany. 39. Zdalna administracja komputerami 40. System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia. 41. System musi umożliwiać zdalne w technologii WEBRTC. 42. System musi zapewniać zdalne zarządzanie komputerami przy użyciu technologii WEBRTC, umożliwiając jednoczesne połączenia z wieloma urządzeniami. Powinien oferować funkcje takie jak przejęcie kontroli nad pulpitami, zarządzanie plikami, uruchamianie i zarządzanie aplikacjami oraz instalowanie oprogramowania i aktualizacji. System powinien umożliwiać konfigurację połączeń WEBRTC, w tym instalację i konfigurację odpowiednich serwerów i portów. Dodatkowo, system powinien obsługiwać różne tryby przejęcia sesji, włączając opcje z lub bez zgody użytkownika, a także umożliwiać nagrywanie i zarządzanie sesjami połączeń, w tym wykonywanie zrzutów ekranu i nagrywanie sesji. System powinien również wspierać różnorodne konfiguracje wyświetlania i jakości sesji, a także umożliwiać uruchomienie do 12 sesji na jednym ekranie. 43. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia. 44. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu. 45. Zdalne Zarządzanie Zaporą (Firewall) 46. System musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe. 47. Automatyzacja 48. System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT. 49. Zarządzanie magazynem IT 50. System musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów. 51. Repozytorium 52. Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją. 53. Kody kreskowe 54. System musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych. 55. Wysyłanie wiadomości 56. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między użytkownikiem a administratorem systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji. System powinien także umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać szkolenie pracowników za pomocą wiadomości tekstowych z możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania. 57. System musi posiadać możliwość eksportu / importu treści. 58. Monitorowanie drukarek sieciowych i wydruków 59. System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych. 60. Monitorowanie stron www 61. System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści. 62. Monitorowanie serwerów WWW 63. System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie. 64. Monitorowanie dziennika zdarzeń 65. System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii. 66. System musi umożliwiać monitorowanie komunikatów Syslog. 67. Monitorowanie pracy komputerów 68. System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników. 69. Monitorowanie uprawnień ACL 70. System musi umożliwić skanowanie i monitorowanie uprawnień ACL, oferując szczegółowe raporty, automatyczną aktualizacją danych i filtrami do zarządzania informacjami. 71. Monitorowanie sensorów 72. System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów. 73. Wsparcie użytkowników – helpdesk. 74. System musi zapewniać kompleksowe wsparcie użytkowników poprzez helpdesk, oferując łatwy w użyciu interfejs do zgłaszania i zarządzania problemami, możliwość edycji i nadawania priorytetów zgłoszeniom oraz konfigurację powiadomień odpowiednich. 75. Repozytorium CMDB 76. System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych. 77. Worktime manager 78. System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostepnienia w panelu pracownika. 79. Raportowanie i eksport danych 80. System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu. 81. System musi zapewnić interfejs API. 82. System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki. 83. Powiadomienia 84. System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co najmniej 30 predefiniowanych powiadomień oraz możliwość ich personalizacji. 85. Bezpieczeństwo 86. System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługuje wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania danych. | (TAK / NIE)\* |
| 5. | Wsparcie i pomoc | Pomoc techniczna   * 1. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.   2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania.   3. Czas trwania usługi SLA wynosi 12 miesięcy od dnia zakupu. | (TAK / NIE)\* |

**\* określić czy oferowany sprzęt/usługa spełnia/ją wymagania minimalne określone w tabeli stanowiącej opis przedmiotu zamówienia (wypełnić/zaznaczyć odpowiednio TAK/NIE).**

# **Wdrożenia i szkolenie**

Zakres usług wdrożeniowych powinien obejmować:

– analizę przedwdrożeniową i przygotowanie konfiguracji zgodnie z wymaganiami Zamawiającego,

– konfigurację środowiska wirtualizacji (Proxmox lub równoważny) wraz z uruchomieniem minimum czterech maszyn wirtualnych,

– migrację podstawowych usług (w tym kontrolera domeny),

– uruchomienie i integrację z istniejącym środowiskiem (klaster CEPH, drugi węzeł),

– testy powdrożeniowe i przekazanie dokumentacji konfiguracyjnej.

## **Wdrożenie serwera**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
| **CZY SPEŁNIAJĄ WYMAGANIA?** |
| 1. | Analiza Przedwdrożeniowa | - Audyt Infrastruktury:  - Przeprowadzenie kompleksowego audytu aktualnej infrastruktury, w tym analizy sprzętu, oprogramowania, sieci oraz polityki bezpieczeństwa.  - Identyfikacja Wymagań :  - Konsultacje z kluczowymi interesariuszami w celu określenia wymagań technicznych i operacyjnych.  - Zdefiniowanie wymagań funkcjonalnych i niefunkcjonalnych dotyczących systemu serwerowego. | (TAK / NIE)\* |
| 2. | Cel | Wdrożenie w siedzibie Zamawiającego oferowanego rozwiązania, instalacja fizyczna w szafach teleinformatycznych, podłączenie do obecnej infrastruktury, konfiguracja urządzeń, zgodna z Zaleceniami Zamawiającego wraz z pełną konfiguracją przestrzeni dyskowej i systemu operacyjnego, a także przeprowadzenie szkolenia z zakresu obsługi serwerów.  W ramach realizacji projektu cyberbezpiecznego samorządu planowane jest wdrożenie środowiska serwerowego opartego na technologii wirtualizacji umożliwiającej uruchomienie maszyn wirtualnych (np. Proxmox VE, VMware ESXi, Microsoft Hyper-V lub równoważny). Przedmiot zamówienia obejmuje:  **Wdrożenie minimum czterech serwerów wirtualnych**, które będą obsługiwały kluczowe usługi podnoszące cyberbezpieczeństwo infrastruktury IT jednostki samorządu terytorialnego.   1. **Każdy serwer wirtualny** zostanie odpowiednio skonfigurowany pod kątem wydajności oraz dostępności, z zapewnieniem wysokiej staranności. 2. **Instalacja i konfiguracja oprogramowania podnoszącego poziom cyberbezpieczeństwa**, w tym:    * Systemy zapobiegania włamaniom (NAC),    * System do utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania    * Zintegrowane narzędzie do zarządzania logami i analizą zagrożeń    * Oprogramowanie tworzące mechanizmy tworzenia kopii zapasowych.    * Przeniesienie domeny i konfiguracja 3. **Ochrona przed zagrożeniami** zewnętrznymi poprzez konfigurację zapór ogniowych oraz zastosowanie zasad twardnienia systemów operacyjnych na serwerach. 4. **Szkolenie personelu technicznego** w zakresie obsługi i monitorowania infrastruktury wirtualnej oraz zastosowanych rozwiązań bezpieczeństwa.   Celem wdrożenia jest stworzenie elastycznej, skalowalnej i bezpiecznej infrastruktury IT, spełniającej wymogi zgodności z przepisami o ochronie danych oraz standardami cyberbezpieczeństwa dla administracji publicznej. W ramach wdrożenia przewidziane jest także dokończenie konfiguracji rozwiązania klastrowego opartego o redundantne zasoby dyskowe. Szkolenie przeprowadzone powinno być, przez inżyniera posiadającego fachową wiedzę zdobytą na autoryzowanych szkoleniach przeprowadzanych przez producenta oferowanego rozwiązania systemu serwerowego.  **Czas trwania szkolenia - nie mniej niż 10 godzin.** | (TAK / NIE)\* |
| 3. | Projekt Architektury Systemu | Opracowanie szczegółowego projektu architektury środowiska serwerowego, obejmującego platformę wirtualizacji (np. Proxmox VE 8.x lub równoważna), maszyn wirtualnych z systemem Windows Server 2025 Standard oraz pozostałych komponentów infrastruktury IT, takich jak: struktura sieciowa, mechanizmy zabezpieczeń, zasady dostępności usług oraz konfiguracja storage w oparciu o rozwiązania równoważne do CEPH. | (TAK / NIE)\* |
| 4. | Szkolenie | **Zakres Szkolenia: Środowisko Proxmox VE (lub równoważne) oraz system Windows Server**   1. **Wprowadzenie do Windows Server (2025 lub nowszy)**  Przegląd kluczowych funkcji Windows Server.  Wymagania systemowe i instalacyjne.  Przegląd dostępnych edycji i ich zastosowań. 2. **Instalacja i Konfiguracja systemu Windows Server w środowisku wirtualnym** Przygotowanie środowiska wirtualizacji (Proxmox VE lub równoważny). Proces instalacji Windows Server w maszynie wirtualnej. Podstawowa konfiguracja po instalacji (adresacja, rola, usługi). 3. **Zarządzanie tożsamościami i dostępem (AD DS)** Instalacja i konfiguracja Active Directory Domain Services. Zarządzanie użytkownikami, grupami i jednostkami organizacyjnymi. Tworzenie i stosowanie zasad grupowych (Group Policy). Konfiguracja jednej maszyny jako kontrolera domeny. 4. **Zarządzanie zasobami sieciowymi** Konfiguracja ról serwera: DNS, DHCP, File and Storage Services. Zarządzanie udostępnianiem plików i uprawnieniami. Obsługa woluminów, udziałów sieciowych i dysków wirtualnych. 5. **Zarządzanie środowiskiem wirtualnym (Proxmox VE lub równoważny)**  Przegląd interfejsu Proxmox VE.  Tworzenie i konfiguracja maszyn wirtualnych z Windows Server.  Zarządzanie zasobami, snapshotami, migracją maszyn (live migration).  Zarządzanie dostępem i aktualizacjami hypervisora. 6. **Bezpieczeństwo i ochrona danych** Zabezpieczenia systemu Windows Server: BitLocker, Defender, zapora ogniowa. Zarządzanie aktualizacjami i polityką aktualizacji. Wbudowane mechanizmy kopii zapasowych i odzyskiwania danych. **Monitorowanie i optymalizacja** Monitorowanie wydajności: Performance Monitor, Event Viewer. Zarządzanie zasobami i analiza obciążenia. Podstawy diagnostyki błędów i alarmów. 7. **Automatyzacja i zarządzanie konfiguracją** Wprowadzenie do PowerShell – zadania administracyjne. Tworzenie skryptów automatyzujących codzienne operacje. Przegląd Windows Admin Center i jego zastosowanie. 8. **Scenariusze rozszerzone** Podstawy integracji z chmurą (np. Azure AD, backup do chmury). Scenariusze zabezpieczeń wielowarstwowych (AD + GPO + firewall). Kopia i odzyskiwanie danych w środowisku Proxmox z maszyną Windows. | (TAK / NIE)\* |

**\* określić czy oferowany sprzęt/usługa spełnia/ją wymagania minimalne określone w tabeli stanowiącej opis przedmiotu zamówienia (wypełnić/zaznaczyć odpowiednio TAK/NIE).**

## **Wdrożenie serwera NAS z oprogramowaniem i dyskami**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
| **CZY SPEŁNIAJĄ WYMAGANIA?** |
| 1. | Wdrożenie | Wdrożenie w siedzibie Zamawiającego oferowanego rozwiązania, instalacja fizyczna w szafach teleinformatycznych, podłączenie do obecnej infrastruktury, konfiguracja urządzeń, zgodna z Zaleceniami Zamawiającego wraz z pełną konfiguracją przestrzeni dyskowej i systemu operacyjnego, a także przeprowadzenie szkolenia z zakresu obsługi serwerów NAS złożonego z 11 modułów. Szkolenie musi zostać **przeprowadzone przez certyfikowanego inżyniera** posiadającego fachową wiedzę zdobytą na autoryzowanych szkoleniach przeprowadzanych przez producenta oferowanego rozwiązania.  **Czas trwania szkolenia powinien potrwać nie mniej niż  30 godzin.** | (TAK / NIE)\* |
| 2. | Szkolenie | 1. **Zarządzanie przechowywaniem.** 2. Omówienie dostępnych typów RAID, ich specyfikacji, algorytmu działania, a także dobór najlepszego wariantu adekwatnie do przedstawionych wymagań. Szczegółowe omówienie tradycyjnych typów RAID takich jak RAID 1, 5, 6, 10 oraz niestandardowych SHR, SHR-2 i F1. 3. Omówienie dostępnych systemów plików, ich specyfikacji, funkcjonalności oraz architektury, a także dobór najlepszego wariantu do przedstawionych wymagań. 4. Omówienie specyfikacji dysków HDD i SSD kompatybilnych z posiadanym serwerem NAS pod kątem zastosowania w długoterminowym przechowywaniu danych. Objaśnienie różnic w mechanizmie zapisu na dyskach talerzowych oraz flash’owych. 5. Wpływ kluczowych parametrów SMART na działanie dysków w macierzy. 6. Procedura wymiany uszkodzonego dysku w grupie RAID. Rozbicie tematu na różne przypadki wraz z symulacją awarii. Wady i zalety stosowania dysków zapasowych. 7. Dostępne opcje rozbudowy istniejącej puli pamięci oraz ograniczenia z nimi związane z podziałem na zastosowane typy RAID. 8. Możliwości skalowalności urządzenia pod kątem zastosowania większej ilości dysków, a co za tym idzie zwiększenia pojemności istniejącej puli pamięci lub utworzenia nowej. 9. Wybór odpowiedniego priorytetu synchronizacji grupy RAID zależnie od zastosowanych dysków i przeznaczenia serwera NAS. Analiza obciążenia systemu i wykorzystania dysków przy jednoczesnym wykorzystywaniu zasobów serwera przez stacje klienckie. 10. Omówienie rodzajów testów SMART, ich cech charakterystycznych, przeznaczenia oraz przypadków zastosowania. Implementacja sensownego i bezpiecznego harmonogramu wykonywania testów, pełna automatyzacja poprzez dedykowane skrypty. 11. Dostępne mechanizmy wpływające na zwiększenie szybkości odczytu i zapisu danych, wymagania związane z implementacją takiego rozwiązania, wady i zalety zależenie od rodzaju środowiska serwerowego i wykorzystywanych aplikacji. Analiza żywotności wybranych nośników, symulacja czasu pracy oraz retencji w celu utrzymania najwyższego poziomu wydajności pamięci podręcznej w danej jednostce czasu z uwzględnieniem szacunkowych ilości zapisu i odczytu danych. 12. Algorytm szyfrowania danych – praktyczne zastosowanie, wpływ na obciążenie serwera i wydajność systemu, możliwości wykorzystania szyfrowania na różnego typu zasobach. Ograniczenia związana z włączeniem szyfrowania, zagrożenia wynikające z niezastosowania takiego algorytmu. 13. Kopiowanie przy zapisie (ang. copy on write) – zasada działania na przykładzie systemu plików btrfs. Zastosowanie praktyczne, wady i zalety, ograniczenia i wymagania. 14. **Użytkownicy i grupy.** 15. Zarządzanie użytkownikami i grupami lokalnymi, konfiguracja strategii bezpiecznego logowania, automatyzacja procesu tworzenia nowych użytkowników i wdrażania ich do korzystania z systemu. 16. Zarządzanie użytkownikami i grupami domenowymi, podłączanie serwera NAS jako klienta domeny, a także tworzenie niezależnego kontrolera domeny opartego o natywne rozwiązanie dostępne w systemie operacyjnym serwera NAS. Pełne wdrożenie testowe z uwzględnieniem zarządzania kontrolerem domeny w sposób rozszerzony poprzez dodatek RSAT, konfigurację profili mobilnych dla użytkowników domenowych z wykorzystaniem zasobów magazynowych serwera NAS. Konfiguracja polis związanych z automatyczną instalacją wskazanych programów na systemach klienckich. 17. Omówienie zasad nadawania uprawnień użytkownikom i grupom z wyszczególnieniem podziału na uprawnienia Unix i ACL. Implementacja obu wariantów w celu wyboru najbardziej odpowiedniego do postawionych wymagań. 18. **Foldery współdzielone.** 19. Zasada funkcjonowania folderów współdzielonych w systemie operacyjnym. Powiązanie z systemem plików działającym na podstawie wolumenów. 20. Omówienie działania systemu plików btrfs pod kątem utrzymania integralności danych z wykorzystaniem dodatkowych sum kontrolnych. 21. Wskazanie i wyjaśnienie algorytmu wykorzystywanego do kompresji danych. Wykorzystanie praktyczne wraz z testami oszczędności zajmowanej przez pliki przestrzeni po włączeniu kompresji. 22. Szczegółowe wytłumaczenie funkcjonalności WORM (ang. Write Once Read Many) działającej na poziomie folderów współdzielonych. Przykłady wykorzystania praktycznego oraz korzyści z tego płynące. 23. Foldery domowe – zasada funkcjonowania dla użytkowników lokalnych i domenowych. 24. Metody udostępniania plików osobom z zewnątrz z zachowaniem zasad bezpieczeństwa tj. szyfrowania transferu oraz zabezpieczenia dostępu przed osobami nieuprawnionymi. 25. **Ustawienia sieciowe.** 26. Zasada działania więcej niż dwóch interfejsów LAN w serwerze. Wyjaśnienie domyślnej adresacji LAN oraz przykładowa konfiguracja w sieci LAN bez serwera DHCP. 27. Agregacja łączy ze szczegółowym omówieniem specyfikacji każdego dostępnego trybu dedykowanego dla przełączników bez interfejsu zarządzania oraz dla tych z interfejsem zarządzania i wsparciem dla protokołu LACP (ang. Link Aggregation Control Protocol), standard 802.3ad. 28. Statyczny routing po stronie serwera NAS, ustawienia zasad filtrowania ruchu i sterowania ruchem z podziałem na konkretne usługi i porty. 29. Konfiguracja podstawowych parametrów połączeniowych serwera NAS z siecią Internet. Wyjaśnienie zasady działania takiego połączenia w momencie korzystania z kilku interfejsów LAN. Wady i zalety zamiennego stosowania nazwy serwera do połączeń CIFS/SMB zamiast adresu IP. 30. Zasada działania serwera proxy i przykład wykorzystania w realnym środowisku. 31. Konfiguracja niestandardowych portów zarządzania. Wyszczególnienie dostępnych metod lokalnego i zdalnego zarządzania serwerem poprzez interfejs Web UI oraz linię komend. 32. **Kopie zapasowe i ochrona danych.** 33. Zasady bezpiecznego przechowywania danych z przykładem implementacji w omawianym środowisku. 34. Metody wykonywania kopii zapasowej z uwzględnieniem różnego typu nośników tj. dysków USB, obudów RAID, bibliotek LTO, innych serwerów fizycznych oraz serwerów NAS. 35. Szczegółowe omówienie metod replikacji danych na inny serwer NAS tego samego producent oraz porównanie procesu do replikacji na inne rozwiązanie firmy trzeciej. Wskazanie najlepszej dostępnej metody do wykorzystania w sieci LAN oraz poprzez WAN. 36. Wyjaśnienie zasady działania mechanizmy migawek z wykorzystaniem kopiowania przy zapisie. Przedstawienie możliwości implementacji harmonogramu wykonywania migawek w systemie oraz związanych z tym najlepszych praktyk. Analiza potencjalnego wykorzystania przestrzeni przez migawki w długoterminowym procesie ich przechowywania oraz omówienie dostępnych strategii retencji wersji. 37. Metody odzyskiwania danych z migawek z opcją przywracania lokalnego oraz zdalnego. Wyjaśnienie różnic i cech szczególnych obu metod. 38. Utworzenie i przedstawienie w praktyce zasady działania replikacji migawek z uwzględnieniem przełączania awaryjnego między serwerami. Szczególnie w przypadku podłączenia do kontrolera domeny i odtwarzania danych wraz z uprawnieniami na serwerze docelowym. 39. Przedstawienie sposobów wykonywania kopii zapasowych do środowisk chmurowych. 40. **Klaster wysokiej dostępności.** 41. Omówienie wymagań dotyczących utworzenia klastra wysokiej dostępności z dwóch takich samych serwerów NAS. 42. Omówienie wymagań i ograniczeń dotyczących utworzenia klastra wysokiej dostępności z dwóch różnych serwerów NAS. 43. Zasada działania klastra SHA (ang. Synology High Availability). Wady I zalety oraz korzyści płynące z zastosowania rozwiązania klastrowego jako główne miejsce składowania danych i różnego typu usług. 44. Algorytm przełączania awaryjnego serwerów w klastrze. Jakie wymagania musi spełniać połączenie między serwerami, jakie ograniczenia występują, jakie problemy mogą wystąpić oraz jak w praktyce odczuwalna będzie praca na zasobach klastra SHA. 45. **Kopie zapasowe komputerów, serwerów i maszyn wirtualnych.** 46. Omówienie dostępnych metod wykonywania kopii zapasowych komputerów PC z zaprezentowaniem działania w praktyce z podziałem na kopie plikowe oraz bare-metal. 47. Opracowanie systemu wdrażania odpowiedniego rozwiązania do kopii zapasowej na dużą skalę. 48. Metody przywracania danych dostępne dla zwykłych użytkowników oraz administratorów. Praktyczne zastosowanie oraz instruktarz dotyczący każdej z dostępnych metod na przykładzie komputera z systemem Windows oraz Linux. 49. Możliwości masowego konfigurowania zasad tworzenia kopii zapasowych. 50. Wyjaśnienie i zaprezentowanie realnego wpływy szyfrowania i kompresji transferu danych na komputery lokalne. 51. Strategie przechowywania danych kopii zapasowych w planie długoterminowym z możliwością przywrócenia kopii zapasowej sprzed 6, 12, i 18 miesięcy. 52. Kontrola integralności danych kopii zapasowych i testowe odtwarzanie. 53. Możliwości automatyzacji procesu odtwarzania danych w przypadku awarii komputera. 54. Testowe przywracanie obrazu kopii w formie maszyny wirtualnej w natywnym wirtualizatorze dostępnym na serwerze NAS oraz na zewnętrznych wirtualizatorach. 55. Omówienie różnic w działaniu środowisk wirtualizacji opartych o KVM oraz QEMU. 56. Wyjaśnienie mechanizmów wpływających na redukcję zajmowanej przez kopie zapasowe przestrzeni takich jak deduplikacja i kompresja. Wykazanie algorytmu działania oraz wpływu na żywotność dysków. 57. Przedstawienie metody replikacji centralnego repozytorium kopii zapasowych na zapasowy serwer NAS z opcją przełączenia klientów na tę jednostkę i wznowienia harmonogramów kopii zapasowych. 58. Metody wykonywania kopii zapasowych systemów bazodanowych działających na serwerach fizycznych z systemami operacyjnymi z rodziny Windows oraz Linux oraz adekwatne metody przywracania. 59. Wykonywanie kopii zapasowych maszyn wirtualnych z różnych środowisk wirtualizacji obsługiwanych przez zintegrowane narzędzie dostępne w systemie serwera NAS. Wyjaśnienie zasady działania mechanizmu kopii, opcji przywracania natychmiastowego oraz pełnego. 60. **Serwer poczty.** 61. Omówienie dostępnych pakietów pozwalających na uruchomienie serwera pocztowego. Jakie są kluczowe różnice, plan licencjonowania, wady i zalety. 62. Wytypowanie odpowiedniego pakietu pozwalającego na utworzenie serwera pocztowego i na jego przykładzie zaprezentowanie praktycznego działania. 63. Wymagania dotyczące utworzenia serwera. 64. Wyjaśnienie zarządzania domeną oraz rekordami DNS. 65. Przekierowywanie portów wymaganych do działania usług na serwerze NAS. Niebezpieczeństwo płynące z tego typu praktyk. 66. Pełnoprawne uruchomienie serwera pocztowego po przeprowadzonej konfiguracji. Testy działania usług SMTP, IMAP i POP3. 67. Obsługa kont pocztowych za pomocą natywnego klienta oraz oprogramowania firm trzecich. 68. Monitorowanie stanu serwera pocztowego, potencjalnych zagrożeń, filtrowanie poczty oraz włączanie silników antyspamowych. 69. Praktyczne zaprezentowanie procedury migracji danych z istniejącego serwera pocztowego na nowe rozwiązanie zaimplementowane na serwerze NAS. 70. **System monitoringu.** 71. Omówienie wymagań związanych z wdrożeniem systemu monitoringu opartego o serwer NAS z centralnym zarządzaniem podległymi serwerami nagrywającymi. 72. Prezentacja funkcjonalności i zarządzania takim systemem w praktyce z wykorzystaniem co najmniej dwóch różnego typu kamer IP. Minimum jedna standardowa i jedna sterowana (ang. PTZ). 73. Konfiguracja przestrzeni przechowywania nagrań. Najlepsza dopuszczalna strategia retencji. 74. Analiza wydajności zapisu z wykorzystaniem systemów plików ext4 i btrfs. Wybór odpowiedniego rozwiązania pod kątem najlepszych osiągów. 75. Dodawanie różnego typu kamer do systemu monitoringu – kompatybilnych oraz z wykorzystaniem protokołu ogólnego ONVIF. 76. Przetestowanie działania wykrywania ruchu i innych podobnych funkcjonalności na poziomie zarządzania kamery oraz systemu monitoringu. 77. Automatyzacja dotycząca powiadamiania o zaistniałych zdarzeniach wykrytych przez system monitoringu. 78. Sposoby na redukcję przestrzeni zajmowanej przez nagrania, archiwizacja oraz tworzenie tzw. timelapse’ów. 79. **Zarządzanie systemem.** 80. Zarządzanie serwerem NAS i systemem operacyjnym pracującym na nim poprzez centralny system zarządzania, a także aplikacje mobilne. Wyszczególnienie ograniczeń i wymagań dotyczących każdej metody. 81. Zabezpieczenie serwera poprzez wdrożenie zasada automatycznego blokowania adresów IP, białej oraz czarnej listy, filtrowania ruchu przychodzącego. 82. Wdrożenie uwierzytelniania dwuskładnikowego dla użytkowników posiadających zdalny dostęp do zarządzania serwerem. 83. Konfiguracja systemu powiadomień wykorzystującego dedykowany serwer SMTP lub pośredniczące konto e-mail. 84. Przedstawienie dostępnych narzędzi monitorowania stanu różnego typu urządzeń, które udostępniają stan poszczególnych parametrów i ustawień poprzez protokół SNMP. 85. Omówienie zasad oraz metod wykonywania aktualizacji oprogramowania serwera NAS w przypadku pojedynczego serwera oraz klastra wysokiej dostępności. 86. Automatyzacja procesu wykonywania kopii zapasowej podstawowej konfiguracji systemu. Objaśnienie co dokładnie zawiera ta kopia, w jaki sposób można ją przywrócić i jakie są ograniczenia z tym związane. 87. **Sprzęt i konserwacja.** 88. Szczegółowe omówienie specyfikacji sprzętowej oferowanego serwera NAS oraz możliwości jego rozbudowy. 89. Przedstawienie instrukcji wymiany pamięci RAM oraz montowania dodatkowych kart rozszerzeń. 90. Omówienie procesu wymiany podzespołów podczas pracy takich jak dyski HDD. 91. Przedstawienie schematu działania w przypadku wystąpienia problemów z połączeniem do systemu zarządzania serwerem NAS lub w przypadku zatrzymania działania niektórych usług. 92. Symulacja różnych typów awarii, które mogą wystąpić podczas użytkowania serwera i sposobów szybkiego rozwiązywania powstałych problemów. 93. Instruktarz dotyczący bezpiecznego czyszczenia serwera NAS z wymontowaniem niektórych podzespołów.   Szkolenie powinno również obejmować krótkie przedstawienie możliwości wdrożenia prostych usług użytkowych, takich jak: komunikator lokalny (chat), współdzielone galerie zdjęć lub repozytorium multimediów, zgodnie z możliwościami platformy NAS i potrzebami Zamawiającego. | (TAK / NIE)\* |

**\* określić czy oferowany sprzęt/usługa spełnia/ją wymagania minimalne określone w tabeli stanowiącej opis przedmiotu zamówienia (wypełnić/zaznaczyć odpowiednio TAK/NIE).**

## **Wdrożenie systemu NAC do izolacji sieci LAN w siedzibie zamawiającego**

**\* określić czy oferowany sprzęt/usługa spełnia/ją wymagania minimalne określone w tabeli stanowiącej opis przedmiotu zamówienia (wypełnić/zaznaczyć odpowiednio TAK/NIE).**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
| **CZY SPEŁNIAJĄ WYMAGANIA?** |
| 1. | Wdrożenie i szkolenie | **Etap I. Przygotowanie wdrożenia**  1. Uzgodnienie wymagań technicznych i przygotowanie przez Klienta zasobów niezbędnych do realizacji prac wdrożeniowych  **Etap II: Wdrożenie rozwiązania**  1. Import maszyny wirtualnej na platformę wirtualizacyjną  2. Konfiguracja parametrów sieciowych i lokalnych interfejsów sieciowych  3. Konfiguracja powiadomień mailowych  4. Konfiguracja integracji z Active Directory  5. Konfiguracja integracji z Windows Management Instrumentation (WMI)  6. Krótki instruktaż dla administratora  7. Podsumowanie wdrożenia - ewentualne pytania  8. Odbiór prac wdrożeniowych  **Etap III. Szkolenie: konfiguracja i administrowanie rozwiązaniem NAC (4 godz.)**  Agenda:  1. NAC - sposób działania i wykorzystanie w infrastrukturze IT  2. Interfejs administratora  3. Konfiguracja sieciowa rozwiązania  4. Monitorowanie sieci i blokowanie dostępu (Device Manager, Network Map)  5. Ochrona przed spoofingiem (fingerprinting)  6. Powiadomienia mailowe  7. Automatyczna klasyfikacja urządzeń (Device Profiler, Auto Trust)  8. Zarządzanie dostępem (Roles & Access, ACLs)  9. Integracja z innymi systemami (AD, AV, WMI, Syslog & Email Orchestration)  10. Rejestrowanie urządzeń prywatnych i dostęp gości (Captive Portal)  11. Raporty (Device Manager Reports, Network Inventory)  12. Aktualizacja firmware  **Etap IV. Konsultacje powdrożeniowe (4 godz. zdalnie)**  1. Przegląd działania rozwiązania 1-3 miesiące od zakończenia wdrożenia  2. Odpowiedzi na pytania związane z eksploatacją rozwiązania NAC  **Wymaga się, aby dostawca przedstawił:**  - oświadczenie producenta o posiadaniu przez dostawcę kwalifikacji technicznych, niezbędnych do wykonania wdrożenia oferowanego rozwiązania i szkolenia, należy załączyć do oferty  - osobowy certyfikat inżynierski pracownika, która będzie wykonywał wdrożenie, należy załączyć do oferty. | (TAK / NIE)\* |

## **Wdrożenie systemu do utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
| **CZY SPEŁNIAJĄ WYMAGANIA?** |
| 1. | Wdrożenie i konfiguracja | Wdrożenie oprogramowania do zarządzania infrastrukturą IT, takiego jak system audytu i monitorowania, składa się z kilku kluczowych etapów. Każdy krok ma na celu zoptymalizowanie procesów IT oraz zapewnienie pełnej integracji systemu z istniejącą infrastrukturą firmy.   1. **Wstępna analiza i planowanie** Na tym etapie zespół wdrożeniowy przeprowadza szczegółową analizę infrastruktury klienta, identyfikuje kluczowe obszary działania oraz definiuje cele wdrożenia. Efektem jest szczegółowy plan działania z określonym harmonogramem oraz przypisaniem odpowiedzialności. 2. **Przygotowanie infrastruktury** Przed instalacją oprogramowania konieczne jest dostosowanie serwerów, infrastruktury sieciowej oraz zasobów do wymagań technicznych oprogramowania. Obejmuje to instalację serwera bazy danych, odpowiednich komponentów oraz konfigurację środowiska testowego. 3. **Instalacja oprogramowania** Instalacja systemu odbywa się na wskazanych serwerach, zgodnie z dokumentacją techniczną. Proces ten obejmuje również instalację modułów rozszerzeń oraz konfigurację podstawowych funkcji systemu. 4. **Integracja z istniejącymi systemami** Kluczowym etapem jest integracja oprogramowania z istniejącymi systemami IT, takimi jak serwery, systemy do zarządzania zasobami, kopie zapasowe, systemy monitorowania oraz narzędzia do bezpieczeństwa. Na tym etapie konfigurowane są połączenia oraz definiowane polityki dostępu do danych. 5. **Zarządzanie użytkownikami i politykami bezpieczeństwa** Tworzone są konta użytkowników i definiowane są role, aby każdy pracownik mógł korzystać z systemu zgodnie ze swoimi uprawnieniami. Implementowane są mechanizmy bezpieczeństwa takie jak szyfrowanie danych, monitorowanie dostępu oraz wykrywanie zagrożeń. 6. **Automatyzacja procesów** Wdrożenie oprogramowania zakłada automatyzację takich procesów jak inwentaryzacja sprzętu, monitorowanie stanu urządzeń, raportowanie oraz harmonogramowanie kopii zapasowych. Celem jest zmniejszenie ręcznego zarządzania i optymalizacja pracy działu IT. 7. **Testowanie i optymalizacja** Po instalacji systemu przeprowadzane są testy funkcjonalne oraz wydajnościowe, mające na celu sprawdzenie poprawności działania wszystkich elementów systemu. W razie potrzeby wprowadza się korekty w konfiguracji. 8. **Szkolenie personelu** Ważnym elementem wdrożenia jest przeszkolenie zespołu IT, który będzie odpowiedzialny za obsługę i administrację systemu. Uczestnicy uczą się korzystać z interfejsu, raportować problemy oraz monitorować działanie infrastruktury. 9. **Wsparcie powdrożeniowe** Po zakończeniu wdrożenia zapewniane jest wsparcie techniczne w pierwszych miesiącach działania systemu, w celu zapewnienia jego stabilności i optymalnego wykorzystania funkcji. Dodatkowo monitorowana jest wydajność systemu, aby wcześnie wychwycić ewentualne problemy.   **SZKOLENIE – Plan szkolenia:**  **Dzień 1:**   1. **Wprowadzenie do szkolenia (0.5 godziny)**    * Cel i struktura szkolenia    * Przegląd kluczowych funkcji systemu 2. **Instalacja i konfiguracja systemu (1 godzina)**    * Proces instalacji    * Konfiguracja podstawowych parametrów 3. **Zarządzanie użytkownikami (0.5 godziny)**    * Tworzenie kont użytkowników    * Zarządzanie uprawnieniami 4. **Inwentaryzacja zasobów IT (1 godzina)**    * Dodawanie sprzętu i oprogramowania    * Automatyczna inwentaryzacja 5. **Sesja pytań i odpowiedzi (0.5 godziny)**   **Dzień 2:**   1. **Monitorowanie infrastruktury (1 godzina)**    * Metody monitorowania urządzeń sieciowych    * Interpretacja wyników monitorowania 2. **Bezpieczeństwo IT (1 godzina)**    * Narzędzia do wykrywania zagrożeń    * Zabezpieczenia infrastruktury IT 3. **Zaawansowane funkcje monitorowania (1 godzina)**    * Monitorowanie wydajności w czasie rzeczywistym    * Alarmy i powiadomienia 4. **Sesja pytań i odpowiedzi (0.5 godziny)**   **Dzień 3:**   1. **Raportowanie i analiza danych (1 godzina)**    * Tworzenie raportów    * Analiza wyników monitoringu 2. **Zarządzanie licencjami i oprogramowaniem (1 godzina)**    * Kontrola wersji oprogramowania    * Audyt licencyjny 3. **Automatyzacja procesów IT (1 godzina)**    * Tworzenie skryptów automatyzujących zadania    * Harmonogramy zadań 4. **Sesja pytań i odpowiedzi oraz podsumowanie szkolenia (1 godzina)**    * Dyskusja na temat praktycznego zastosowania systemu    * Wskazówki do dalszego samodzielnego rozwoju   **Łączny czas trwania**: **12 godzin** | (TAK / NIE)\* |

**\* określić czy oferowany sprzęt/usługa spełnia/ją wymagania minimalne określone w tabeli stanowiącej opis przedmiotu zamówienia (wypełnić/zaznaczyć odpowiednio TAK/NIE).**