Projekt „Cyberbezpieczny Samorząd w Gminie Mochowo” jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy (FERC)

**Załącznik Nr 1 do SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Część I - Dostawa macierzy NAS i Serwera wraz z instalacją, konfiguracją i wdrożeniem**

**NAS – 1 szt.**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | Typu rack o wysokości maksymalnie 2U wraz z szynami przesuwnymi umożliwiającymi montaż w szafie rack w zestawie. |
| **Procesor** | Jeden procesor osiągający wynik minimum 4200 punktów w teście PassMark. |
| **Pamięć RAM** | Minimum 16GB DDR4 ECC. Możliwość rozbudowy pamięci RAM do minimum 32GB (2 x 16GB). |
| **Ilość obsługiwanych dysków** | Minimum 8 dysków o maksymalnej pojemności nie mniejszej niż 16TB każdy, po podłączeniu modułów rozszerzających minimum 12 dysków. |
| **Zainstalowane dyski** | 8 dysków HDD o pojemności min. 12TB każdy zgodne z listą kompatybilności oferowanego rozwiązania oraz charakteryzujące się następującymi parametrami:   * interfejs: SATA 6Gb/s, * prędkość obrotowa: minimum 7200 RPM, * pamięć cache: minimum 250 MB, * MTBF: minimum 1 milion, * możliwość aktualizacji oprogramowania dysków bezpośrednio z interfejsu systemu operacyjnego serwera NAS. |
| **Interfejsy sieciowe** | Minimum 4 porty 1GbE RJ-45 oraz 2 porty 10GbE RJ-45  Wsparcie dla agregacji łączy. |
| **Obsługa RAID** | Minimum RAID 0, 1, 5, 6, 10. Obsługa dysków zapasowych typu hot spare. |
| **Funkcje RAID** | Możliwość zwiększania pojemności poprzez wymianę dysków na większe. Migracja poziomu RAID w trybie online dla minimum RAID 1 i RAID 5. |
| **Szyfrowanie** | Możliwość szyfrowania wybranych udziałów sieciowych. |
| **Protokoły** | SMB, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP |
| **Usługi** | 1. Serwer VPN, Serwer pocztowy, Stacja monitoringu, Windows ACL, Integracja z Windows ADS, Firewall, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Usługa DDNS, 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 maszyn wirtualnych ze środowisk takich jak VMware vSphere, VMware free ESXi oraz Microsoft Hyper-V 2016, 2019, 2022 (wraz z klastrami przełączania awaryjnego) z wykorzystaniem centralnego panelu zarządzania oraz dodatkowo: 3. Wykonywanie kopii zapasowych typu bare-metal komputerów lokalnych z systemem Windows 7 lub nowszym według harmonogramu z możliwością zarządzania z poziomu centralnej konsoli dostępnej lokalnie oraz zdalnie, 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. Dane z kopii zapasowych muszą być redukowane poprzez globalną deduplikację po stronie miejsca przechowywania. Licencja musi umożliwiać podłączanie kolejnych komputerów do systemu kopii zapasowej bez limitu. 4. Instalacja i konfiguracja kopi zapasowych przez tunel VPN |
| **Język GUI** | Polski |
| **Pobór mocy** | Maksymalnie 63W w trybie pracy. |
| **System plików** | Dyski wewnętrzne: BTRFS. |
| **Szyfrowanie** | Mechanizm szyfrowania sprzętowego (AES-NI) |
| **Zasilacz** | Zasilacz redundantny o mocy minimum 340W. |
| **Gwarancja** | Gwarancja producenta co najmniej 36 miesięcy. |

**Serwer – 1 szt.**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | 1. Obudowa Rack o wysokości max 2U z możliwością instalacji min. 8 dysków 2.5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. 2. Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. 3. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |
| **Płyta główna** | 1. Płyta główna z możliwością zainstalowania do dwóch procesorów. 2. Obsługa procesorów 32 rdzeniowych. 3. Na płycie głównej powinny znajdować się minimum 16 sloty przeznaczone do instalacji pamięci. 4. Płyta główna powinna obsługiwać do 1TB pamięci RAM. |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| **Procesor** | Zainstalowane dwa procesory min. 8-rdzeniowe klasy x86, min. 2.6GHz, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 165 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |
| **RAM** | Minimum 256GB DDR5 RDIMM 4800MT/s, |
| **Funkcjonalność pamięci RAM** | * Demand Scrubbing, * Patrol Scrubbing, * Permanent Fault Detection (PFD) |
| **Gniazda PCI** | Min. trzy sloty PCIe |
| **Interfejsy sieciowe/FC/SAS** | * Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT * Dwuportowa karta sieciowa min. 25Gb Ethernet SFP28 |
| **Dyski twarde** | 1. Zainstalowane:    * 4x dyski SAS o pojemności min. 2,4TB, min. 10K RPM, Hot-Plug    * 2x dyski SSD o pojemności min. 480GB, Hot-Plug 2. Możliwość zainstalowania dwóch dysków M.2 NVME o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1. |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy, posiadający   * + Min. 8GB nieulotnej pamięci cache,   + Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.   + Wsparcie dla dysków samoszyfrujących |
| **Wbudowane porty** | 1. 4x USB, w tym min. 1 porty USB 3.0 2. 2x port VGA (jeden na panelu przednim) 3. Możliwość rozbudowy o Serial Port |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024 |
| **Wentylatory** | Redundantne, Hot-Plug |
| **Zasilacze** | Redundantne, Hot-Plug min. 1100W klasy Titanium |
| **System operacyjny/**  **dodatkowe oprogramowanie** | Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie sześciu instancji wirtualnych tego serwerowego systemu operacyjnego.  Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na zaoferowanym serwerze. Licencja powinna pozwalać na dostęp 30 użytkownikom.  Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.   1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: 10. pozwalają na zmianę rozmiaru w czasie pracy systemu, 11. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, 12. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, 13. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 14. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 15. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 16. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 17. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 18. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 19. Dostępne dwa rodzaje graficznego interfejsu użytkownika: 20. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, 21. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 22. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 23. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 24. Mechanizmy logowania w oparciu o: 25. Login i hasło, 26. Karty z certyfikatami (smartcard), 27. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 28. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.. 29. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 30. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 31. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 32. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 33. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 34. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: 35. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, 36. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: 37. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 38. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 39. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. 40. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.   c) Zdalna dystrybucja oprogramowania na stacje robocze.  d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej  e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:  I. Dystrybucję certyfikatów poprzez http  II. Konsolidację CA dla wielu lasów domeny,  III. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  IV. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.  f) Szyfrowanie plików i folderów.  g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).  h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.  i) Serwis udostępniania stron WWW.  j) Wsparcie dla protokołu IP w wersji 6 (IPv6),  k) Wsparcie dla algorytmów Suite B (RFC 4869),  l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,  m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:   1. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 2. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. 3. Obsługi 4-KB sektorów dysków 4. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra 5. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. 6. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)   26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.  27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).  28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.  29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.  30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |
| **Bezpieczeństwo** | 1. Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. 2. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. 3. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła 4. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. 5. Moduł TPM 2.0 6. Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera 7. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem 8. Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   * + zdalny dostęp do graficznego interfejsu Web karty zarządzającej;   + zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);   + szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;   + możliwość podmontowania zdalnych wirtualnych napędów;   + wirtualną konsolę z dostępem do myszy, klawiatury;   + wsparcie dla IPv6;   + wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;   + możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;   + możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;   + integracja z Active Directory;   + możliwość obsługi przez dwóch administratorów jednocześnie;   + wsparcie dla dynamic DNS;   + wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.   + możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera   + możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera   oraz z możliwością rozszerzenia funkcjonalności o:   * + Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej   + Przesyłanie danych telemetrycznych w czasie rzeczywistym   + Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze   + Automatyczna rejestracja certyfikatów (ACE) |
| **Oprogramowanie do zarządzania** | Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:   * + Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych   + integracja z Active Directory   + Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta   + Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish   + Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram   + Szczegółowy opis wykrytych systemów oraz ich komponentów   + Możliwość eksportu raportu do CSV, HTML, XLS, PDF   + Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.   + Grupowanie urządzeń w oparciu o kryteria użytkownika   + Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji   + Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach   + Szybki podgląd stanu środowiska   + Podsumowanie stanu dla każdego urządzenia   + Szczegółowy status urządzenia/elementu/komponentu   + Generowanie alertów przy zmianie stanu urządzenia.   + Filtry raportów umożliwiające podgląd najważniejszych zdarzeń   + Integracja z service desk producenta dostarczonej platformy sprzętowej   + Możliwość przejęcia zdalnego pulpitu   + Możliwość podmontowania wirtualnego napędu   + Kreator umożliwiający dostosowanie akcji dla wybranych alertów   + Możliwość importu plików MIB   + Przesyłanie alertów „as-is” do innych konsol firm trzecich   + Możliwość definiowania ról administratorów   + Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów   + Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)   + Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta   + Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów   + Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.   + Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.   + Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile   + Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.   + Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.   + Zdalne uruchamianie diagnostyki serwera.   + Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.   + Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |
| **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 * Serwer musi posiadać deklaracja CE. * Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami – załączyć do ofert dokumentację techniczną lub oświadczenie producenta serwera w celu potwierdzenia spełnienia normy * Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022. |
| **Dokumentacja użytkownika** | * Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. * Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| **Warunki gwarancji** | * 3-letnia gwarancja producenta świadczona na miejscu u klienta * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet. * Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie producenta (dla krytycznych zgłoszeń serwisowych) * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. * Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. * Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego * Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. * Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. |

**Instalacja, konfiguracja i wdrożenie zakupionego sprzętu – 1 pakiet**

Wykonawca zobowiązany jest do wykonania kompleksowej usługi instalacji, konfiguracji oraz wdrożenia zakupionego sprzętu, w tym:

1. **Serwera** – obejmuje:
   * montaż serwera w szafie rack,
   * podłączenie do infrastruktury sieciowej i zasilającej,
   * podstawowa konfiguracja sprzętowa (BIOS/UEFI, RAID, kontrolery, aktualizacja firmware),
   * instalacja i konfiguracja systemu operacyjnego (dołączonego do serwera),
   * konfiguracja dostępu zdalnego,
   * testy poprawności działania.
2. **Urządzenia NAS** – obejmuje:
   * fizyczna instalacja oraz podłączenie do sieci LAN i zasilania,
   * konfiguracja systemu plików, wolumenów, poziomu RAID oraz użytkowników i uprawnień,
   * konfiguracja dostępu sieciowego (SMB/NFS/FTP – zgodnie z wymaganiami Zamawiającego),
   * integracja z Active Directory,
   * testy odczytu i zapisu danych.
3. **Dodatkowo:**
   * dokumentacja powykonawcza konfiguracji sprzętu i ustawień systemowych,
   * krótka instrukcja administracyjna dla wyznaczonego pracownika Zamawiającego (szkolenie stanowiskowe, maks. 2h),
   * przekazanie haseł administracyjnych i loginów dostępu w sposób bezpieczny.

**Część II – Dostawa programowania antywirusowego i antyspamowego, oprogramowania do zarządzania tożsamością i dostępem oraz oprogramowania centralnego menadżera haseł.**

**Oprogramowanie antywirusowe i antyspamowe: 1 szt.**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Administracja zdalna w chmurze** | 1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. 9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej. |
| **Ochrona stacji roboczych** | 1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2. Rozwiązanie musi wspierać architekturę ARM64. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 10. Rozwiązanie musi integrować się z Intel Threat Detection Technology. 11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:  * tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, * tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, * tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, * tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, * tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.  1. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 2. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 3. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 4. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 5. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 6. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook. 7. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:  * tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, * tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, * tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, * tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.  1. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. 2. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. 3. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. 4. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. 5. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. 6. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 7. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. |
| **Ochrona serwera** | 1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux. 2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. 7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.   Dodatkowe wymagania dla ochrony serwerów Windows:   1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych*.* 8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.   Dodatkowe wymagania dla ochrony serwerów Linux:   1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. 4. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu. |
| **Szyfrowanie** | 1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11. 2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). 3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. 4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI. |
| **Ochrona urządzeń mobilnych opartych o system Android** | 1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. 5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:  * usunięcie zawartości urządzenia, * przywrócenie urządzenie do ustawień fabrycznych, * zablokowania urządzenia, * uruchomienie sygnału dźwiękowego, * lokalizację GPS.  1. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 2. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:  * nazwę aplikacji, * nazwę pakietu, * kategorię sklepu Google Play, * uprawnienia aplikacji, * pochodzenie aplikacji z nieznanego źródła. |
| **Ochrona serwera pocztowego MS Exchange** | 1. Rozwiązanie musi wspierać instalację na systemach Microsoft Windows Server 2012 i nowszych. 2. Rozwiązanie musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2010/2013/2016/2019. 3. Rozwiązanie musi zapewniać wsparcie dla ról Mailbox, Edge, Hub. 4. Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange. 5. Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI. 6. Rozwiązanie musi mieć możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum. 7. Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty. 8. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty. 9. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja. 10. Rozwiązanie ma posiadać mechanizm greylisting (szara lista). 11. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. |
| **Sandbox w chmurze** | 1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 2. Rozwiązanie musi wykorzystywać do działania chmurę producenta. 3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. 4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. 5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. 6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. 7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów. 8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy. 9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. 10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. 11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo. 12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:  * Czysty, * Podejrzany, * Bardzo podejrzany, * Szkodliwy.  1. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. 2. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki. 3. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia. |
| **Ochrona usługi Microsoft 365** | 1. Rozwiązanie musi obejmować ochroną usługi Microsoft, takie jak Exchange Online, Onedrive, Sharepoint oraz aplikację Teams. 2. Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Micosoft 365. 3. Administrator musi mieć możliwość wskazania, które konto użytkownika będzie objęte ochroną. 4. Rozwiązanie musi być zarządzane za pomocą dowolnej przeglądarki internetowej z dowolnego miejsca w sieci. 5. Rozwiązanie musi być dostępny w języku polskim. 6. Konsola rozwiązania musi posiadać możliwość raportowania co najmniej:  * użytkowników, otrzymujących najwięcej spamu, * użytkowników, otrzymujących najwięcej wiadomości typu „phishing”, * użytkowników, otrzymujących największą ilość szkodliwego oprogramowania, * kont użytkowników, które mogę być podejrzane.  1. Konsola rozwiązania musi posiadać funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online i Onedrive. 2. Dzienniki Exchange Online muszą posiadać funkcjonalność informowania co najmniej:  * jaka ilość wiadomości została przeskanowania, * wynik skanowania poszczególnej wiadomości, * czynność podjęta przez rozwiązanie.  1. Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o:  * zagrożeniach, które zostały wykryte, * na jakim koncie zostały wykryte, * jakie zagrożenie zostało wykryte, * podjętą czynność.  1. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online oraz Onedrive. 2. Musi istnieć możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem. 3. Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników. 4. Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o co najmniej:  * wykorzystania do analizy mechanizmów chmurowych, tego samego producenta, * wprowadzenia białych i czarnych list adresów ochrony Exchange’a Online, * dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing.  1. Rozwiązanie musi zapewniać funkcję ochrony przed zagrożeniami 0-day. 2. Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta. 3. Funkcja ochrony przed zagrożeniami 0-day musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. 4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. 5. Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail z funkcją wyboru preferowanego języka. |
| **Moduł XDR** | 1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. 2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. 3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. 4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. 5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”. 6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia. 7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. 8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta. 9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej. 10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku. 11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania. 12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny. 13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej. 14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych. 15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich. 16. Konsola administracyjna musi mieć możliwość tagowania obiektów. 17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell. |
| **Moduł zarządzania podatnościami i aktualizacjami** | 1. Rozwiązanie musi mieć możliwości wykrywania podatności w systemach operacyjnych (co najmniej Windows 10, Windows 11) oraz aplikacjach zainstalowanych na zarządzanych stacjach. 2. Baza wykrywanych podatności musi zawierać minimum 35000 CVE. 3. Rozwiązanie nie może wymagać instalacji dodatkowej konsoli, ani innych dodatkowych komponentów na stacjach końcowych. 4. Automatyczne wykrywanie podatności musi wykonywać się zgodnie z harmonogramem, nie częściej niż raz dziennie. 5. Moduł wykrywania podatności musi umożliwiać wyświetlanie szczegółów danej podatności zawierające minimum:  * nazwę aplikacji lub systemu operacyjnego * punktacje CVSS * opis wykrytej podatności * wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta  1. Moduł wykrywania podatności musi wykrywać podatności w minimum 700 aplikacjach. 2. Moduł zarządzania aktualizacjami musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 150 popularnych aplikacji. 3. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje będą aplikowane tylko i wyłącznie dla wskazanych aplikacji w białej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania. 4. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich - ponad 150 aplikacji, oprócz aplikacji wskazanych na czarnej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania. 5. Zarządzanie aktualizacjami aplikacji musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach. 6. Moduł zarządzania aktualizacjami oraz wykrywania podatności musi być zintegrowany bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze. 7. Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania aktualizacjami musi być w odpowiedni sposób oznaczona w konsoli centralnego zarządzania. 8. Administrator konsoli musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w konsoli centralnego zarządzania. 9. Moduł wykrywania podatności ma umożliwiać wyłączenie powiadomień dla wybranej podatności. |
| **Ochrona poprzez dwuskładnikowe uwierzytelnianie** | 1. Rozwiązanie musi wspierać systemy operacyjne Microsoft Windows Server: 2008 / 2008 R2 / 2012 / 2012 R2 / SBS 2008 / SBS 2011 / 2012 Essentials / 2012 R2 Essentials / Windows Server 2016 / Windows Server 2016 Essentials / Windows Server 2019 / Windows Server 2019 Essentials / Windows Server 2022. 2. Rozwiązanie musi wspierać system operacyjne Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows 11. 3. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows. 4. Oprogramowanie musi wspierać integrację z Microsoft Exchange 2007 / 2010 / 2013 / 2016 / 2019. 5. Oprogramowanie musi wspierać integrację z Microsoft Dynamics CRM 2011 / 2013 / 2015 / 2016. 6. Oprogramowanie musi wspierać integrację z Microsoft Sharepoint 2010 / 2013 / 2016 / 2019. 7. Oprogramowanie musi wspierać integrację z Microsoft Remote Desktop Web Access. 8. Oprogramowanie musi wspierać integrację z Microsoft Terminal Services Web Access. 9. Oprogramowanie musi wspierać integrację z Microsoft Remote Web Access. 10. Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS. 11. Aplikacja mobilna musi wspierać telefony działające pod kontrolą systemów mobilnych: Android (w wersji 4.4 lub wyższej), iOS (12 lub wyższej). 12. Aplikacja mobilna do generowania OTP (jednorazowego hasła) musi być dostarczona przez producenta rozwiązania w ramach zakupionej licencji. 13. Użytkownik musi mieć możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN. 14. Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP (jednorazowego hasła) musi odbywać się w trybie offline. 15. Dwuskładnikowe uwierzytelnienie musi być możliwe również przy użyciu jednorazowych haseł SMS. 16. Aplikacja zainstalowana na urządzeniach mobilnych musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego 17. Wsparcie techniczne do programu świadczone w języku polskim, przez polskiego dystrybutora autoryzowanego przez producenta programu. |
| **Licencja** | Ilość użytkowników: min. 40 szt.  Czas trwania subskrypcji baz danych zagrożeń do dnia 30.06.2026 r.  Wsparcie producenta do dnia 30.06.2026 r. |

**Oprogramowanie do zarządzania tożsamością i dostępem: 1 szt.**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Wymagania ogólne dla systemu zarządzania** | Oprogramowanie musi posiadać polski oraz angielski interfejs językowy.  Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji, Agenta/Konsoli zarządzającej.  Oprogramowanie musi umożliwiać obsługę dedykowanych kluczy szyfrujących podczas komunikacji pomiędzy agentami, serwer aplikacji i konsolą zarządzającą.  Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników.  Agent systemu nie może nasłuchiwać na żadnym porcie sieciowym po stronie stanowiska komputerowego użytkownika.  Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompilowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit.  Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe (lokalne lub sieciowe) wraz z hasłem, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania danych AES w obrębie przechowywania danych wrażliwych.  Oprogramowanie musi posiadać dodatkową autoryzację użytkownika konsoli zarządzającej za pomocą usługi Google Authenticator oraz Microsoft Authenticator.  Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control).  Oprogramowanie musi umożliwiać nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przelogowania użytkownika konsoli systemu).  Oprogramowanie musi umożliwiać blokadę wybranych uprawnień konkretnego użytkownika niezależnie od uprawnień wynikających z przypisanych ról.  Oprogramowanie musi współpracować z serwerem MSSQL Server 2008R2-2019  Oprogramowanie, w zakresie wszystkich warstw, nie może wymagać do prawidłowej pracy komponentów Java.  Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych .  Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do danych w zakresie wybranych jednostek organizacyjnych oraz typów zasobów poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko wynikowe obiekty.  Oprogramowanie musi być podpisane cyfrowo przez Producenta ważnym certyfikatem, z prawidłową ścieżką certyfikacji, w której główny urząd certyfikacji (Root CA) jest uczestnikiem programu certyfikatów głównych systemu Windows. Podpis cyfrowy dotyczy składników Producenta systemu w zakresie plików wykonywalnych (\*.exe), plików bibliotek współdzielonych (\*.dll), plików sterowników (\*.sys) oraz pakietów instalacyjnych oprogramowania (\*.msi).  Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Windows.  Oprogramowanie musi zapewniać dowolną konfigurację pracy wszystkich agentów, jednostek organizacyjnych, pojedynczego agenta, poprzez dziedziczenie definiowanych przez administratora parametrów. Zmiany konfiguracji agentów następują w trybie natychmiastowym (online).  Oprogramowanie musi posiadać raport przedstawiający różnice w konfiguracji poszczególnych agentów w stosunku do konfiguracji globalnej.  Oprogramowanie musi posiadać mechanizm logowania zmian w konfiguracji agentów przez użytkowników konsoli (data, czas, login, poprzednia i nowa wartość).  Oprogramowanie musi posiadać mechanizm analizy czasu pracy komputera, informujący użytkownika (alert oraz wymuszone działanie – restart) o przekroczeniu zadanego czasu pracy bez restartu systemu operacyjnego.  Oprogramowanie musi zapewniać automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieżdżeń z kontenera Active Directory/OpenLDAP), kont użytkowników i komputerów z zachowaniem ich oryginalnego położenia wg. OU.  Oprogramowanie musi zapewniać w obrębie synchronizacji z Active Directory/OpenLDAP tworzenie listy filtrów zawężających węzły danych wraz z możliwością wskazania docelowej gałęzi struktury organizacyjnej lub lokalizacyjnej Zamawiającego.  Oprogramowanie musi posiadać kreator powiązań (mapowanie atrybutów) dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych.  Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej.  Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej.  Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami.  Oprogramowanie musi umożliwiać tworzenie dynamicznych grup stanowisk w oparciu o kreator zawierający filtry (AND, OR) w zakresie min. wersja OS, nazwa oraz wersja wybranej aplikacji, RAM, CPU, HDD, jednostka organizacyjna, jednostka lokalizacyjna, architektura (x32, x64), zainstalowane oprogramowanie, wersja oprogramowania, lista usług systemowych, producent oraz model komputera, poziom uprawnień użytkownika, zainstalowana usługa systemowa, ostatnie uruchomienie systemu, obecność pliku EXE na dysku, predefiniowane atrybuty komputera (np. dostawca, numer faktury, data zakupu).  Oprogramowanie musi umożliwiać prezentację widoku zarządzanych stanowisk komputerowych w postaci listy stanowisk, drzewiastej struktury wg jednostek organizacyjnych, jednostek lokalizacyjnych, struktury Active Directory, struktury sieciowej (pule IP) oraz grup dynamicznych.  Oprogramowanie musi umożliwiać dynamiczne zawężanie wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów.  Oprogramowanie musi umożliwiać graficzną prezentację aktualnego stanu aktywności agenta (online/offline) z dokładnością do 1 minuty.  Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika. |
| **Inwentaryzacja konfiguracji komputerów** | Oprogramowanie musi umożliwiać wydruk kartoteki sprzętowej stanowiska komputerowego.  Oprogramowanie musi umożliwiać samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu.  Oprogramowanie musi umożliwiać zapisywanie edytowanych szablonów (min. kartoteka sprzętowa, protokoły przekazania/zwrotu zasobów) w kontekście zalogowanego operatora konsoli zarządzającej.  Oprogramowanie musi umożliwiać projektowanie, generowanie oraz wydruk etykiet inwentaryzacyjnych w zakresie: model, nr inwentaryzacyjny, data zakupu, jednostka, wraz z obsługą kodów kreskowych w standardzie EAN128 oraz PDF417  Oprogramowanie musi umożliwiać okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp.  Oprogramowanie Agenta musi umożliwiać audyt off-line, poprzez uruchomienie skanera (z GUI) bez konieczności instalacji, oraz zapis wyników do pliku w postaci zaszyfrowanej.  Oprogramowanie musi umożliwiać analizę sprzętową:   * płyty głównej w zakresie model, producent, nr. seryjny, * CPU w zakresie nazwy, modelu, producenta, częstotliwości, * HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci, * RAM w zakresie wielkości pamięci, * karty sieciowej w zakresie model, adres IP, adres MAC, * karty graficznej w zakresie model.   Oprogramowanie musi umożliwiać odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID.  Oprogramowanie musi umożliwiać odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej.  Oprogramowanie musi umożliwiać odczyt informacji sprzętowych z BIOS w zakresie nazwy BIOS, daty, producenta.  Oprogramowanie musi umożliwiać przegląd historii zmian parametrów sprzętowych komputerowych.  Oprogramowanie musi umożliwiać globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-systemowych.  Oprogramowanie musi zawierać raport stanowisk komputerowych posiadających co najmniej jedno konto z uprawnieniami administratora.  Oprogramowanie musi umożliwiać odczyt urządzeń podłączonych do stanowiska komputerowego przez interfejs USB, z możliwością odczytania nazwy urządzenia, producenta, modelu oraz numeru seryjnego (o ile urządzenie dostarcza ww. informacji)  Oprogramowanie musi umożliwiać globalną analizę urządzeń podłączonych do stanowisk komputerowych przez interfejs USB  Oprogramowanie musi umożliwiać integrację z zewnętrzną usługą Dell API w celu automatycznego odczytania informacji na temat okresu gwarancji stanowiska komputerowego na podstawie odczytanego przez agenta identyfikatora (ServiceTag)  Oprogramowanie musi umożliwiać okresowe próbkowanie obciążenia procesora oraz zajętości pamięci RAM z możliwością zapisu odczytanych wyników do bazy w celu późniejszej analizy (historia obciążenia komputera). |
| **Inwentaryzacja oprogramowania** | Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania.  Oprogramowanie musi umożliwiać globalny przegląd wszystkich programów zainstalowanych na komputerach.  Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.).  Oprogramowanie musi umożliwiać tworzenie wykazów z zainstalowanym, dowolnie wybranym programem.  Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach.  Oprogramowanie musi umożliwiać tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu.  Oprogramowanie musi posiadać wbudowany mechanizm umożliwiający, poprzez GUI konsoli, zdalną grupową dezinstalację oprogramowania np. pakietów MS Office.  Oprogramowanie musi umożliwiać oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem wraz z możliwością raportowania wg w/w klasyfikacji.  Oprogramowanie musi umożliwiać zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika.  Oprogramowanie musi posiadać globalne zestawienie pozwalające na zdalne usunięcie nielegalnych danych np. plików AVI, MP3, MP4 bez konieczności fizycznej obecności użytkownika przy stacji. |
| **Zarządzanie licencjami, audyt oprogramowania** | Oprogramowanie musi posiadać wbudowaną bazę sygnatur aplikacji (produktów) wraz z możliwością automatycznej aktualizacji wzorców ze strony Producenta oprogramowania  Oprogramowanie musi umożliwiać zdefiniowanie własnych sygnatur aplikacji (produktów) wykorzystywanych  w procesie automatycznego audytu licencji (rozliczenie ilościowe).  Oprogramowanie musi umożliwiać wykonanie audytu licencji tj. systemowego porównania zidentyfikowanego na stanowiskach komputerowych oprogramowania (produktów) z zakupionymi licencjami wprowadzonymi do systemu jako odpowiednie obiekty. Mechanizm audytu musi umożliwiać rozliczenie licencji z wykorzystaniem mechanizmów downgrade, upgrade.  Oprogramowanie musi umożliwiać zapis historii wykonywanych audytów licencji.  Oprogramowanie musi umożliwiać tworzenie bazy licencji systemowo/programowych i przypisywanie ich do stanowisk komputerowych oraz użytkowników. |
| **CMDB** | Oprogramowanie musi umożliwiać tworzenie własnych typów elementów konfiguracji (CI)  Oprogramowanie musi umożliwiać dodawanie dowolnych atrybutów dla typów CI w szczególności: wartości logiczne, data/czas, numeryczne, tekstowe, słownikowe  Oprogramowanie musi umożliwiać tworzenie podrzędnych i nadrzędnych typów CI  Oprogramowanie musi umożliwiać dziedziczenie atrybutów przez elementy konfiguracji posiadające typ nadrzędny  Oprogramowanie musi umożliwiać tworzenie dowolnych typów relacji do obsługi połączeń pomiędzy różnymi typami CI  Oprogramowanie musi umożliwiać tworzenie atrybutów dla relacji  Oprogramowanie musi umożliwiać prezentowanie powiązań pomiędzy elementami konfiguracji w formie struktury płaskiej oraz graficznej  Oprogramowanie musi umożliwiać zbiorczy podgląd relacji pomiędzy poszczególnymi elementami konfiguracji  Oprogramowanie musi umożliwiać modelowanie struktury relacji pomiędzy usługami, sprzętem, organizacją oraz pracownikami  Oprogramowanie musi umożliwiać nadzór nad wpływem zmian na poszczególne elementy konfiguracji  Oprogramowanie musi umożliwiać import elementów konfiguracji ze źródeł takich jak usługa katalogowa, skaner sieci, zewnętrzne pliki płaskie (CSV)  Oprogramowanie musi umożliwiać tworzenie oraz edycję własnych list elementów konfiguracji  Oprogramowanie musi umożliwiać wyszukiwanie i analizę elementów konfiguracji wg posiadanych atrybutów  Oprogramowanie musi umożliwiać tworzenie własnych typów relacji z określaniem nazwy relacji podstawowe i odwrotnej  Oprogramowanie musi umożliwiać tworzenie własnych formularzy dla wszystkich elementów konfiguracji |
| **Zarządzanie zasobami oraz użytkownikami** | Oprogramowanie musi umożliwiać tworzenie własnych szablonów widoków zasobów z określeniem analizowanych typów zasobów, widocznych atrybutów oraz informacji nt. powiązań pomiędzy zasobami.  Oprogramowanie musi umożliwiać tworzenie własnych atrybutów o typach co najmniej: tekst, liczba, bit, data, wartość słownikowa dla wybranego typu zasobu.  Oprogramowanie musi umożliwiać zapis oraz przegląd historii zmian dowolnego atrybutu zasobu w zakresie: operator, data, czas, poprzednia oraz nowa wartość.  Oprogramowanie musi umożliwiać zdefiniowanie dowolnych relacji pomiędzy zasobami (np. powiązania stanowiska z pracownikiem, licencją, innym zasobem) wraz z zapisem historii relacji zasobów.  Oprogramowanie musi umożliwiać przypisywanie do każdego z zarządzanych w systemie zasobów dokumentów typu: faktura zakupu, gwarancja, umowa serwisowa. Bazą dokumentów musi być centralne repozytorium umożliwiające powiazania dokumentów z zasobami w relacji 1:N wraz z podglądem przypisanych zasobów oraz wydrukiem.  Oprogramowanie musi umożliwiać zdefiniowanie dowolnego zasobu inwentaryzacyjnego (np. telefon, drukarka, nawigacja) w strukturze drzewiastej wraz z kreatorem widocznych/wymaganych atrybutów edycyjnych.  Oprogramowanie musi posiadać dedykowaną (zintegrowaną z systemem) aplikację na platformę Android umożliwiającą spis z natury zinwentaryzowanych zasobów.  Oprogramowanie musi umożliwiać import danych z zewnętrznego pliku CSV zawierającego informacje inwentaryzacyjne z nowo zakupionych urządzeń w zakresie: numer faktury, numer seryjny, model, nazwa, data zakupu.  Oprogramowanie musi umożliwiać zaprojektowanie własnego schematu importu danych z zewnętrznego pliku CSV.  Oprogramowanie musi umożliwiać automatyczne tworzenie relacji pracownik-komputer na podstawie atrybutów obiektu w usłudze katalogowej.  Oprogramowanie musi zawierać wbudowany kreator wydruków w zakresie protokołów przekazania, zwrotu, likwidacji wraz z możliwością utworzenia dowolnego typu dokumentu  Oprogramowanie musi umożliwiać export ww. protokołów w formacie PDF  Oprogramowanie musi umożliwiać obsługę kodów kreskowych oraz QR w obrębie ww. kreatora wydruków  Oprogramowanie musi umożliwiać użycie w kreatorze wydruków własnego logotypu organizacji  Oprogramowanie musi umożliwiać użycie w kreatorze wydruków dowolnego atrybutu zasobu  Oprogramowanie musi umożliwiać przypisanie dowolnej firmy serwisowej z bazy organizacji do zasobu  Oprogramowanie musi umożliwiać przypisanie załącznika do zasobu  Oprogramowanie musi umożliwiać pogląd wszystkich zgłoszeń serwisowych dotyczących danego zasobu  Oprogramowanie musi umożliwiać podgląd zasobów (przypisanych do danego pracownika) z poziomu jego portalu użytkownika końcowego  Oprogramowanie musi umożliwiać zarządzanie cyklem życia zasobu  Oprogramowanie musi umożliwiać tworzenie niestandardowych reguł biznesowych dla zarządzania zasobami  Oprogramowanie musi umożliwiać seryjne dodawanie zasobów  Oprogramowanie musi umożliwiać automatyczne nadawanie numerów inwentaryzacyjnych dla zasobów  Oprogramowanie musi udostępniać kreator raportów dla zasobów  Oprogramowanie musi udostępniać możliwość kopiowania widoku dla określonego typu(ów) zasobu z innego typ zasobu  Oprogramowanie musi udostępniać możliwość kopiowania formularz dla określonego typu(ów) zasobu z innego typ zasobu  Oprogramowanie musi umożliwiać ewidencję magazynów  Oprogramowanie musi umożliwiać ewidencję lokalizacji magazynowych  Oprogramowanie musi umożliwiać ewidencję produktów magazynowych  Oprogramowanie musi udostępniać informację o stanie magazynowym(ilościowo)  Oprogramowanie musi umożliwiać generowanie dokumentów PZ/PW/RW/MM  Oprogramowanie musi umożliwiać przyjęcie zasobów ewidencjonowanych i eksploatacyjnych na magazyn  Oprogramowanie musi umożliwiać wydawanie zasobów ewidencjonowanych i eksploatacyjnych z magazynu  Oprogramowanie musi umożliwiać zwrot zasobów na magazyn  Oprogramowanie musi umożliwiać zmianę szablonów dokumentów PZ/PW/RW/MM  Oprogramowanie musi umożliwiać wyszukiwanie dokumentów po dowolnym atrybucie  Oprogramowanie musi umożliwiać zarządzanie organizacjami/typami organizacji (np. klient, podwykonawca)  Oprogramowanie musi umożliwiać dowolne przypisanie osoby do organizacji  Oprogramowanie musi umożliwiać tworzenia dynamicznych grup użytkowników  Oprogramowanie musi umożliwiać zarządzanie kontaktami osób/organizacji  Oprogramowanie musi umożliwiać zarządzanie nieobecnościami użytkowników  Oprogramowanie musi umożliwiać zarzadzanie uprawnieniami i poziomami dostępu do danych w zakresie zarządzania zasobami  Oprogramowanie musi umożliwiać automatyczne pobieranie danych rejestrowych kontrahentów z bazy GUS |
| **Zdalny pulpit, zdalne zarządzanie komputerem** | Oprogramowanie musi umożliwiać interakcję administratora z użytkownikiem, polegającą na podłączeniu do stanowiska (przejęcie pulpitu) administratora bez konieczności uprzedniego wylogowania użytkownika. Funkcjonalność zdalnego pulpit nie może wymagać instalacji aplikacji firm trzecich, wymagane jest obsłużenie przejęcia zdalnego pulpitu przez mechanizm wbudowany w agencie (ten sam proces systemowy).  Oprogramowanie musi umożliwiać wybór monitora, którego ekran ma zostać przejęty podczas połączenia zdalnego. Podczas aktywnego połączenia zdalnego, użytkownik jest informowany o trwaniu sesji zdalnej poprzez wyświetlanie na aktywnym monitorze kontrastowego obramowania ekranu.  Oprogramowanie musi umożliwiać zdalne zarządzanie (bez użycia RDP/VNC itp.) lokalnymi kontami użytkowników w zakresie (tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta).  Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on LAN.  Oprogramowanie musi umożliwiać zdalną dwukierunkową linię poleceń.  Oprogramowanie musi umożliwiać przesyłanie plików/katalogów od zdalnego użytkownika do administratora i/lub od administratora do zdalnego użytkownika bez względu na lokalizację sieciową komputera (LAN, WAN, Internet).  Oprogramowanie musi umożliwiać konfigurację przez administratora parametrów połączenia z użytkownikiem w zakresie: ilość kolorów, ilość klatek/sekundę, skalowanie okna użytkownika, jeżeli jest ono większe niż rozdzielczość stacji administratora.  Oprogramowanie musi umożliwiać wybór aktywnych sesji terminalowych, do których chcemy się podłączyć.  Oprogramowanie musi umożliwiać zbiorczy podgląd zdalnych pulpitów stacji.  Oprogramowanie musi posiadać zarządzanie technologią iAMT, vPro w zakresie uwzględniającym min.: Serial Over Lan (SOL), IDE Redirection (IDER), Hardware KVM, Assets.  Oprogramowanie musi zapewniać zdalną konfigurację technologii iAMT w trybie Client Control Configuration Mode.  Oprogramowanie musi umożliwiać zarządzanie stacjami komputerowymi poza siecią LAN/WAN, wymagane jest tylko dowolne połączenie internetowe  Oprogramowanie musi umożliwiać zdalne wykonywanie zapytań WQL  Oprogramowanie musi umożliwiać zdalny odczyt oraz modyfikację rejestru Windows  Oprogramowanie musi umożliwiać pełne wykorzystanie funkcji zawartych w sekcji zdalne zarządzanie dla stacji posiadających dowolne połączenie do sieci INTERNET bez konieczności zestawiania połączenia VPN  Oprogramowanie musi umożliwiać przejęcie pulpitu zdalnego z poziomu konsoli zarządzającej znajdującej się poza siecią LAN organizacji poprzez połącznie konsoli ze wskazanym serwerem aplikacji.  Oprogramowanie musi umożliwiać prowadzenie w czasie rzeczywistym dwukierunkowej komunikacji tekstowej (chat) pomiędzy użytkownikiem a administratorem. |
| **Automatyzacja** | Oprogramowanie musi umożliwiać zdalną instalację pakietów \*.msi, plików \*.cmd, \*.bat, \*.reg, \*.ps1 poprzez utworzenie zadań dystrybucji aplikacji oraz wskazanie docelowych komputerów lub grup komputerów za pomocą dedykowanego GUI użytkownika. Zadanie dystrybucji musi umożliwiać określenie okresu aktywności, godziny rozpoczęcia oraz przedstawiać status instalacji na wybranych stanowiskach.  Oprogramowanie musi umożliwiać tworzenie zadań dystrybucji polegające na jednorazowym uruchomieniu wybranego szablonu akcji na wybranych stanowiskach komputerowych.  Oprogramowanie musi umożliwiać tworzenie polis uruchamianych cyklicznie na wybranych stanowiskach komputerowych wg aktualnej przynależności do struktury organizacyjnej, lokalizacyjnej lub wybranych grup dynamicznych.  Oprogramowanie musi umożliwiać tworzenie dystrybucji zadań oraz polis dla wybranych stanowisk komputerowych poprzez interaktywny kreator (krok po kroku). Wybór odbiorców musi uwzględniać listę stanowisk, strukturę organizacyjną, strukturę lokalizacyjną oraz dynamiczne grupy stanowisk.  Oprogramowanie musi umożliwiać globalną dystrybucję plików oraz folderów do wskazanych lokalizacji do wybranych stanowisk komputerowych wg przynależności do struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej wraz z automatycznym (polisa) odtworzeniem brakujących danych w przypadku wykrycia niespójności.  Oprogramowanie musi umożliwiać szyfrowanie plików źródłowych dla zadań instalacji.  Oprogramowanie musi umożliwiać globalny przegląd postępu wykonania wybranych zadań oraz polis wraz z odczytem standardowego wyjścia (stdout) oraz standardowego wyjścia błędów (stderr).  Oprogramowanie musi umożliwiać tworzenie własnych szablonów akcji zawierających zdefiniowaną listę akcji pozwalających na warunkowe uruchamianie akcji zależnych (oczekiwanie na zakończenie akcji, praca w tle).  Oprogramowanie musi umożliwiać konfigurację typów akcji co najmniej w zakresie: dystrybucja i uruchomienie plików wsadowego BAT, dystrybucja plików rejestru REG, dystrybucja i instalacja pakietu MSI, dystrybucja i instalacja poprawki MSP, dystrybucja i uruchomienie aplikacji EXE, dystrybucja i uruchomienie skryptu PowerShell, dystrybucja plików i folderów, uruchomienie/wyłączenie/restart usługi systemowej, zakończenie procesu systemowego, wywołanie polecenia CMD.  Oprogramowanie musi umożliwiać konfigurowanie dedykowanych parametrów dla każdej z ww. akcji.  Oprogramowanie musi umożliwiać uruchomienie na prawach administracyjnych pliku instalacyjnego EXE (z GUI) w sesji użytkownika z ograniczonymi uprawnieniami do instalacji aplikacji. Proces instalacji jest manualnie kontynuowany przez użytkownika.  Oprogramowanie musi umożliwiać ograniczenie zakresu działania zadania, polisy oraz zawężenie wszelkich raportów systemowych do stanowisk spełniających kryteria wybranej dynamicznej grupy stanowisk.  Oprogramowanie w zakresie automatyzacji musi realizować m.in. następujące przypadki użycia z wykorzystaniem mechanizmu grup dynamicznych dla zadań oraz polis:  1. Automatyczną instalacji aplikacji na komputerach spełniających warunki: stanowiska z Windows 10 z pamięcią RAM>4GB i zainstalowaną wybraną aplikacją w wersji mniejszej (np. 7.0)  2. Automatyczne odinstalowanie aplikacji na komputerach spełniających warunki: stanowiska z Windows 7 gdzie producentem komputera jest np. Dell i zainstalowaną wybraną aplikacją w wersji większej niż (np. 8.0)  3. Dystrybucję plików oraz folderów (ze wskazaną zawartością np. dokumenty, skróty do aplikacji) na pulpity stanowisk komputerowych spełniających warunki: stanowiska z Windows 10 z brakiem zainstalowanej wybranej aplikacji oraz nie posiadające konta użytkownika z prawami administracyjnymi  4. Uruchomienia wybranego skryptu PowerShell dla komputerów spełniających warunki: stanowiska z Windows 10 w architekturze 32 bitowej, zainstalowaną aplikacją X w wersji większej niż (np. 6.0) i brakiem zainstalowanej aplikacji Y.  5. Uruchomienia wybranych szablonów akcji w przypadku wykrycia zmiany jednostki organizacyjnej stanowiska komputerowego.  W przypadku wcześniej zdefiniowanych polis wymagane jest, aby zostały one automatycznie uruchomione dla nowych stanowisk komputerowych po spełnieniu warunków przynależności do określonych grup dynamicznych.  Oprogramowanie musi umożliwić instalację oprogramowania z plików exe, które nie posiadają instalacji w trybie cichym poprzez automatyzację procesu manualnej instalacji (nagrywanie makr w zakresie wyborów typu zaznaczenie checkbox, wybór pozycji z listy, kliknięcie przycisku, wpisanie parametru/ścieżki itp.)  Oprogramowanie musi posiadać repozytorium szablonów makr automatyzacji do późniejszego wykorzystania podczas procesów instalacji  Oprogramowanie musi zawierać funkcję testowania nagranych makr z poziomu interfejsu użytkownika  Oprogramowanie musi wznawiać instalację, w przypadku przerwania procesu instalacji (np. z powodu wyłączenia komputera)  Nagrywanie makr musi być realizowane przez wybranie/wskazanie elementu okna, na którym ma zostać wykonana akcja (np. kliknięcie, wprowadzenie tekstu, zaznaczenie)  Oprogramowanie musi umożliwiać wysyłanie komunikatów (Windows Notification) do wskazanych stanowisk komputerowych (wybór manualny, wg struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej)  Oprogramowanie musi umożliwiać wysyłanie komunikatów przed każdą zdefiniowaną akcją automatyzacji (np.: przed rozpoczęciem instalacji pakietu MSI, przed dystrybucją plików, przed uruchomieniem skryptu PowerShell)  Oprogramowanie musi umożliwiać automatyzację procesu konfiguracji dowolnej aplikacji Windows w celu odtworzenia zapamiętanych akcji (makr) dla wskazanych stanowisk komputerowych. |
| **Backup danych użytkownika** | Oprogramowanie musi umożliwiać tworzenie dowolnej ilości automatycznych zadań w zakresie archiwizacji danych – globalnie z poziomu głównej konsoli zarządzającej.  Oprogramowanie musi umożliwiać globalną zmianę parametrów zadań archiwizacji (ilość archiwów, kompresja, okres, zakres).  Oprogramowanie musi umożliwiać definiowanie rozszerzeń plików, które mają być pomijane podczas procesu archiwizacji oraz rozszerzeń plików np. \*.doc, które mają być archiwizowane.  Oprogramowanie Agenta musi umożliwiać kopię całościową danych oraz przesyłanie plików z archiwizacji na wskazany serwer FTP.  Mechanizm archiwizacji danych musi być realizowany przez Agenta systemu bez udziału zdalnych sesji (typu zdalny pulpit, wywoływanie skryptów)  Oprogramowanie musi umożliwiać definiowanie cyklu archiwizacji.  Oprogramowanie musi umożliwiać automatyczne usuwanie starszych plików kopii całościowej, definiowanie globalnego zadania archiwizacji. |
| **Zarządzanie urządzeniami USB Storage** | Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o kopiowaniu z/do urządzeń zewnętrznych typu: Pendrive USB, dysk zewnętrzny.  Oprogramowanie musi posiadać raport w zakresie rejestracji informacji na temat użytkownika, który kopiował i/lub uruchamiał napęd, kiedy miało miejsce zdarzenie i jakie dokumenty zostały skopiowane.  Oprogramowanie musi umożliwiać blokadę oraz autoryzację wybranych urządzeń USB w obrębie klasy USBStorage.  Oprogramowanie musi umożliwiać włączenie trybu ReadOnly dla klasy USBStorage  Oprogramowanie musi umożliwiać całkowitą blokadę klasy FDD/CD/DVD |
| **Monitoring stanowisk komputerowych** | Oprogramowanie musi umożliwiać zestawienie najpopularniejszych adresów (jakie stanowiska je wywoływały, kiedy) z możliwością zapisu całego adresu lub tylko głównej strony.  Oprogramowanie umożliwia zestawienie najaktywniejszych stanowisk (pod kątem WWW), jakie adresy odwiedzały, kiedy, wszystkie zestawienia do poziomu: jednostka organizacyjna, stanowisko, zalogowany użytkownik.  Oprogramowanie musi umożliwiać analizę uruchamianych aplikacji (aktywność stanowisk wg aplikacji oraz wykorzystanie zainstalowanych aplikacji wg stanowisk).  Oprogramowanie musi umożliwiać analizę efektywności pracy użytkowników na poszczególnych aplikacjach  Oprogramowanie musi umożliwiać blokadę stron www (biała i czarna lista adresów, blokada pełna lub selektywna) z możliwością automatycznego zamykania przeglądarki lub konkretnej karty przeglądarki (w przypadku wykrycia adresu zabronionego).  Oprogramowanie musi umożliwiać tworzenie statystyk aktywności stron WWW oraz aktywności stanowisk.  Oprogramowanie musi umożliwiać podział stron na dozwolone i zabronione.  Oprogramowanie musi umożliwiać wydruki tabelaryczne oraz graficzne (wykresy aktywności).  Oprogramowanie musi umożliwiać okresowe tworzenie zrzutu ekranu użytkownika z możliwością przesłania go na serwer.  Oprogramowanie musi umożliwiać rozróżnienie stanów monitorowanego komputera w szczególności stan aktywności (focus okna), hibernacji, uśpienia oraz wylogowania  Oprogramowanie musi umożliwiać odczyt aktywności użytkownika w czasie rzeczywistym w zakresie min. tytuł okna, adres www przeglądanej strony z dokładnością do 1 sekundy.  Oprogramowanie musi umożliwiać analizę aktywności myszy oraz klawiatury dla poszczególnych monitorowanych aplikacji oraz stron internetowych (ilość kliknięć).  Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach sieciowych udostępnionych przez centralny serwer wydruków i udostępnionych lokalnie przez port TCP/IP  Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach lokalnych udostępnionych przez port LPT, USB. Monitorowanie tych wydruków musi odbywać się poprzez agenta aplikacji zainstalowanego na stacji roboczej będącej serwerem wydruków dla drukarki lokalnej.  Oprogramowanie po zainstalowaniu musi przesyłać do serwera aplikacji następujące informacje: nazwa stacji roboczej, nazwa zainstalowanego sterownika drukarki, nazwa portu z jakiego dany sterownik korzysta, opis sterownika drukarki, format drukowanych stron oraz nazwę drukowanego dokumentu.  Oprogramowanie musi posiadać możliwość definicji kosztów wydruku dla poszczególnych urządzeń drukujących (podział kosztu na mono/kolor). |
| **ServiceDesk – Zarządzanie zgłoszeniami** | Oprogramowanie w części HelpDesk musi być oparte na zasadach ITIL w szczególności:   * Zarządzanie problemem * Zarządzanie incydentem * Obsługa procesów poprzez WorkFlow (wnioski o usługi, uprawnienia, zakupy) * Zarządzanie umowami serwisowymi * Definicje poziomów SLA (reakcja, naprawa, reklamacja)   Oprogramowanie musi umożliwiać zgłaszania przez użytkowników z poziomu przeglądarki WWW (dedykowany portal) awarii sprzętu, usług, oprogramowania i innych typów awarii zdefiniowanych przez administratora.  Portal ServiceDesk musi mieć możliwość obsługi przez wiodące przeglądarki WWW na urządzeniach mobilnych poprzez responsywny interfejs użytkownika.  Portal ServiceDesk musi umożliwiać wybór wersji językowej interfejsu (co najmniej polski i angielski).  Obsługa listy zgłoszeń serwisowych (incydentów i problemów) musi być realizowana przez portal ServiceDesk z zachowaniem nadanego poziomu uprawnień.  Oprogramowanie musi umożliwiać kontrolę obciążenia działu IT, optymalizację podziału pracy pomiędzy pracowników działu IT oraz przegląd awaryjności sprzętu.  Oprogramowanie musi umożliwiać uwierzytelnianie użytkowników wykorzystując bazę Active Directory poprzez protokół LDAP.  Oprogramowanie musi umożliwiać automatyczne autoryzowanie określonych stanowisk i użytkowników (z wykorzystaniem mechanizmy SSO), aby uniknąć każdorazowego uwierzytelniania przed korzystaniem z systemu zgłoszeń.  Oprogramowanie musi umożliwiać sortowanie listy zgłoszeń awarii, wg daty zgłoszenia, priorytetu, statusu.  Oprogramowanie musi umożliwiać filtrację zgłoszeń wg priorytetu oraz statusów zgłoszeń, stanowisk oraz inżynierów obsługujących zgłoszenia.  Oprogramowanie musi umożliwiać tworzenie dedykowanych list zgłoszeń z różnymi danymi, domyślnym filtrowaniem i sortowaniem.  Oprogramowanie musi umożliwiać określenie widoczności poszczególnych list zgłoszeń w zależności od zalogowanego użytkownika.  Oprogramowanie musi umożliwiać określenie widoczności zgłoszeń w zależności od kategorii i lokalizacji zgłoszeń przypisanych do zalogowanego użytkownika.  Oprogramowanie musi umożliwiać dostęp do zgłoszeń swoich podwładnych przez przełożonego.  Oprogramowanie musi umożliwiać dodawanie przez administratora nowych wpisów (komentarzy) w zgłoszeniu, jak i umożliwiać zmianę statusu sprawy. Użytkownik także ma możliwość dodawania nowych wpisów do zgłoszonego problemu wraz ze zmianą statusu.  Oprogramowanie musi umożliwiać tworzenie zadań w ramach konkretnego zgłoszenia z możliwością przekazania do realizacji przez innych użytkowników.  Oprogramowanie musi umożliwiać tworzenie globalnych zadań do realizacji przez zalogowanego użytkownika.  Oprogramowanie musi umożliwiać tworzenie szablonów zadań.  Oprogramowanie musi umożliwiać rejestrację czasu pracy poświęconego na realizację zgłoszenia przez opiekuna.  Oprogramowanie musi umożliwiać przesyłanie użytkownikom powiadomień pocztą elektroniczną o nowych wpisach i zmianach w zgłoszeniu.  Oprogramowanie musi umożliwiać edycję szablonów powiadomień email.  Oprogramowanie musi umożliwiać tworzenie wielopoziomowych list kategorii zawierających nazwę i opis kategorii.  Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii w zależności od zalogowanego użytkownika.  Oprogramowanie musi umożliwiać tworzenie pól dodatkowych na formularzu rejestracji zgłoszenia.  Oprogramowanie musi umożliwiać określenie widoczności poszczególnych pól dodatkowych w zależności od zalogowanego użytkownika.  Rozwiązania w bazie wiedzy muszą posiadać znacznik określający czy są dostępne dla użytkowników, czy są wewnętrznymi uwagami działu IT. Panel www użytkownika musi zawierać wyszukiwarkę tematów wg słów kluczowych oraz wewnętrznej treści.  Oprogramowanie musi umożliwiać edycję bazy wiedzy z poziomu przeglądarki WWW wraz z możliwością formatowania tekstu (wraz z grafiką) oraz wstawiania załączników.  Oprogramowanie musi umożliwiać administratorowi wprowadzenie do systemu zgłoszenia użytkownika, który nie ma dostępu do PC (np. telefoniczna informacja o awarii komputera).  Oprogramowanie musi umożliwiać delegowanie zgłoszenia innemu administratorowi (technikowi), jak również przejęcie innego zgłoszenia (np. w przypadku nieplanowanej nieobecności pracownika).  Oprogramowanie musi umożliwiać obsługę tzw. Linii wsparcia poprzez samodzielne tworzenie nowych linii wraz z przypisywaniem do nich dowolnej ilości kont operatorów HelpDesk. Zgłoszenie serwisowe musi mieć możliwość przekazania do dowolnej linii wsparcia lub dedykowanego operatora HelpDesk. Linia wsparcia musi mieć możliwość przypisania powiązanych z nią kategorii zgłoszeń.  Oprogramowanie musi umożliwiać informowanie pracowników o planowanych działaniach, awariach za pomocą komunikatów wprowadzanych na stronę główną panelu zgłaszania usterki, bądź do poszczególnych kategorii.  Oprogramowanie musi umożliwiać określenie widoczności komunikatów o planowanych działaniach, awariach w zależności od zalogowanego użytkownika.  Oprogramowanie musi umożliwiać tworzenia baz umów serwisowych powiązanych z bazami firm serwisowych (dostawców sprzętu, oprogramowania, lokalnych serwisów). lub z zakupionym sprzętem.  Oprogramowanie w oparciu o bazę firm/umów serwisowych musi umożliwiać zapis przekazania zgłoszenia do serwisu zewnętrznego.  Oprogramowanie musi umożliwiać przesyłanie powiadomień do firm serwisowych powiązanych ze zgłoszeniem.  Oprogramowanie musi posiadać możliwość rejestracji w historii zgłoszenia (w komentarzach) korespondencji  mailowej między opiekunami zgłoszenia a firmami serwisowymi powiązanymi ze zgłoszeniem.  Oprogramowanie musi posiadać dedykowane panele WWW w zależności od aktywnie zalogowanego użytkownika końcowego (panel dla użytkownika tj. zgłaszanie incydentów, panel dla operatora serwisowego – obsługa zgłoszeń, panel dla managera HelpDesk – analiza graficzna oraz tabelaryczna pracy operatorów HelpDesk).  Oprogramowanie musi umożliwiać wyświetlenie w panelu WWW użytkownika informacji nt. powiązanych z użytkownikiem zasobów (przypisane stanowiska PC, przydzielone licencje aplikacji, wydane urządzenia).  Oprogramowanie musi umożliwiać wybranie zasobu w określonej kategorii powiązanego z użytkownikiem podczas rejestracji zgłoszenia.  Oprogramowanie musi umożliwiać tworzenie zgłoszeń cyklicznych z możliwością definiowania częstości występowania oraz typu okresu (codziennie, co tydzień, co miesiąc)  Oprogramowanie musi umożliwiać tworzenie reguł w celu automatyzacji obsługi zgłoszeń. Reguły muszą uruchamiać się w odpowiedzi na określone zdarzenia w systemie i wykonywać akcje w zależności od spełnionych warunków. W zakresie reguł ServiceDesk musi realizować m.in. następujące przypadki użycia:   * Zmiana statusu po przejęciu zgłoszenia przez opiekuna. * Przejmowanie zadań po przejęciu zgłoszenia przez opiekuna. * Dodawanie zadań w zgłoszeniu w zależności od parametrów zgłoszenia. * Wznawianie zgłoszenia po odpowiedzi przez zgłaszającego użytkownika. * Zamykanie zgłoszenia po upływie czasu bez odpowiedzi użytkownika. * Zamykanie zgłoszenia po upływie czasu reklamacji. * Dodawanie wpisów (komentarzy) w zgłoszeniu na podstawie szablonów. * Zmiana parametrów zgłoszenia po znalezieniu wybranej frazy w treści komentarza. * Walidacja zamkniętych zadań w zamykanym zgłoszeniu. * Systemowe potwierdzanie realizacji zgłoszenia. * Wysyłanie dodatkowych powiadomień cyklicznych ze zgłoszeniami, np. zgłoszenia wymagające reakcji, zgłoszenia do realizacji lub zgłoszenia wstrzymane/wznowione.   Oprogramowanie musi umożliwiać tworzenie szablonów komentarzy wykorzystywanych przez opiekunów zgłoszeń.  Oprogramowanie musi posiadać możliwość rejestracji zgłoszeń i komentarzy drogą mailową, zarówno przez zarejestrowanych użytkowników systemu jak i niezarejestrowanych użytkowników.  Oprogramowanie musi umożliwiać obsługę dowolnej ilości kont pocztowych do wysyłania powiadomień i generowania zgłoszeń/komentarzy przez email.  Oprogramowanie musi posiadać wbudowane raporty prezentujące m.in. realizację obsługi zgłoszeń w zakładanym SLA (statystyka miesięczna, kwartalna, roczna).  Oprogramowanie musi umożliwiać definiowanie własnych widoków oraz zestawień dla każdego zalogowanego użytkownika  Oprogramowanie musi umożliwiać zdefiniowanie własne macierzy priorytetów na podstawie pilności oraz wpływu zgłoszenia  Oprogramowanie musi umożliwiać zamodelowanie trzy zmianowego trybu pracy inżynierów (opiekunów zgłoszeń)  Oprogramowanie musi umożliwiać informowanie użytkowników o nowych zdarzeniach systemowych za pomocą notyfikacji (dymku) podczas pracy z systemem  Oprogramowanie musi umożliwiać tworzenie obiegu procesu decyzyjnego dla wniosków o uprawnienia lub elementy konfiguracji w oparciu o bazę CMDB  Oprogramowanie musi umożliwiać zaprojektowanie dowolnego formularza do wprowadzania danych z wykorzystaniem własnych atrybutów (wraz ze zmianą układu/położenia atrybutów w projektowanym widoku)  Oprogramowanie musi umożliwiać definicję czasów SLA w oparciu o matrycę priorytetów, statusy, kategorie lub dowolne warunki i atrybuty zgłoszenia  Oprogramowanie musi umożliwiać dodanie Akceptacji do już istniejącego zgłoszenia  Oprogramowanie musi umożliwiać definiowanie własnych reguł zarządzania w oparciu o warunki i akcje dla Prawdy i Fałszu (zdarzenie -> warunek -> akcja)  Oprogramowanie musi umożliwiać tworzenie wielu zgłoszeń poprzez wybór kilku użytkowników w zgłoszeniu  Oprogramowanie musi umożliwiać tworzenie słowników wartości dla atrybutów w oparciu o strukturę płaską lub drzewiastą  Oprogramowanie musi umożliwiać tworzenie atrybutów zależnych poprzez określone warunki widoczności  Oprogramowanie musi umożliwiać definiowanie formularzy zamykających zgłoszenie oraz zatwierdzające zmiany w zgłoszeniu  Oprogramowanie musi umożliwiać definiowanie reguł biznesowych za pomocą graficznego/blokowego kreatora.  Oprogramowanie musi umożliwiać definiowanie obiegów za pomocą graficznego/blokowego kreatora.  Oprogramowanie musi umożliwiać tworzenie niestandardowych raportów za pomocą kreatora.  Oprogramowanie musi umożliwiać definiowanie poziomu dostępu do zgłoszeń dla dynamicznych grup użytkowników.  Oprogramowanie musi umożliwiać definiowanie formularzy dla zgłoszeń w danej kategorii za pomocą kreatora Drag&Drop z możliwością określenia układu kolumn.  Oprogramowanie musi umożliwiać tworzenie dowolnej liczby Dashboard-ów dla użytkownika za pomocą kreatora Drag&Drop.  Oprogramowanie musi umożliwiać zmianę układu szczegółów zgłoszenia za pomocą kreatora Drag&Drop.  Oprogramowanie musi umożliwiać udostępniania ogłoszeń w formie Widget-u oraz okienka modalnego z wymaganym potwierdzeniem dla użytkownika.  Oprogramowanie musi umożliwiać zaprojektowanie dowolnego szablonu protokołu zgłoszenia.  Oprogramowanie musi udostępniać matrycę(wpływ/pilność) dla obliczania priorytetu zgłoszeń.  Oprogramowanie musi umożliwiać zmianę koloru dla statusu/priorytetu/wpływu/pilności zgłoszenia prezentowanego na liście zgłoszeń.  Oprogramowanie musi umożliwiać definiowanie dowolnych kolejek zgłoszeń.  Oprogramowanie musi umożliwiać rejestrację nieobecności administratorów z możliwością wybrania zastępstwa. |
| **ServiceDesk – Zarządzanie wnioskami** | Oprogramowanie musi zapewnić obsługę Workflow w zgłoszeniach serwisowych poprzez zdefiniowanie logicznych ścieżek (zbiór węzłów logicznych).  Oprogramowanie musi umożliwiać wybór wielu zasobów na jednym formularzu wniosku. Przykładowo dla wniosku o nadanie uprawnień musi istnieć możliwość wskazania wielu systemów/zbiorów danych z podziałem na moduły lub poziomy uprawnień użytkownika.  Na poziomie każdego węzła logicznego w workflow musi być możliwość edycji/modyfikacji zawartości danych w szczególności statusu, uwag, załączników (o dowolnym typie pliku) wraz z utworzeniem wpisu w historii przetwarzanego obiegu. |
| **ServiceDesk – Zarządzanie uprawnieniami** | Oprogramowanie musi umożliwiać inwentaryzację Systemów Informatycznych oraz Zbiorów danych  Oprogramowanie musi umożliwiać określanie powiązań pomiędzy pracownikami z Systemami Informatycznymi oraz Zbiorami danych  Oprogramowanie musi umożliwiać budowanie powiązanych zestawów atrybutów dla Systemów Informatycznych oraz Zbiorów danych (np. termin ważności dostępu, poziom dostępu, przetwarzanie danych wrażliwych)  Oprogramowanie musi umożliwiać tworzenie ścieżek decyzyjnych dla dowolnych wniosków o uprawnienia do Systemów Informatycznych oraz Zbiorów danych  Oprogramowanie musi umożliwiać akceptację poszczególnych etapów przez dedykowane osoby decyzyjne zdefiniowane w konfiguracji ścieżek  Oprogramowanie musi umożliwiać akceptację etapów ścieżki przez automatyczny wybór powiązanych opiekunów merytorycznych oraz technicznych  Oprogramowanie musi umożliwiać definiowanie dowolnych akcji dla poszczególnych kroków (np. zmiana opiekuna, statusu)  Oprogramowanie musi umożliwiać automatyczne tworzenie powiązań pracownika z Systemem informatycznym lub Zbiorem danych po akceptacji wniosku  Oprogramowanie musi umożliwiać obsługę procesu (wniosku) o odebranie uprawnień (koniec terminu dostępu, zwolnienie pracownika)  Oprogramowanie musi umożliwiać raportowanie uprawnień wg Systemów Informatycznych oraz Zbiorów danych dla poszczególnych osób  Oprogramowanie musi umożliwiać raportowanie uprawnień w pracowników do Systemów Informatycznych oraz Zbiorów danych  Oprogramowanie musi umożliwiać generowanie edytowalnej Karty Uprawnień Pracownika |
| **ServiceDesk – Zarządzanie rezerwacjami** | Oprogramowanie musi umożliwiać rezerwację dowolnego aktywnego zasobu w systemie.  Oprogramowanie musi umożliwiać kategoryzowanie rejestrowanych rezerwacji.  Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii rezerwacji w zależności od zalogowanego użytkownika.  Oprogramowanie musi informować o możliwych konfliktach podczas tworzenia/edycji rezerwacji z zasobem.  Oprogramowanie musi prezentować informacje o rezerwacjach w formie graficznej – kalendarza.  Oprogramowanie musi umożliwiać akceptację, odrzucenie lub anulowanie rezerwacji przez upoważnionych użytkowników. |
| **Monitoring sieci LAN** | Oprogramowanie musi umożliwiać okresowe skanowanie sieci LAN (wg. zadanych kryteriów, na wybranych serwerach lokalnych) z wykorzystaniem protokołu SNMP, celem prezentacji aktywnych urządzeń IP w zakresie co najmniej komputery, drukarki, routery, smartphony  Oprogramowanie musi umożliwiać monitorowanie poprzez wykorzystanie protokołu SNMP stanu drukarek tj. poziomy tonerów, liczba wydrukowanych stron oraz informować błędach takich jak brak papieru, zacięcie papieru.  Oprogramowanie musi umożliwiać wizualizację ruchu sieciowego na poszczególnych portach urządzeń sieciowych wraz z wizualizacją w postaci mapy sieci dla wskazanego urządzenia typu switch, router.  Oprogramowanie musi umożliwiać z zdalną instalację agenta systemu z poziomu wykrytej struktury sieciowej z wykorzystaniem poświadczeń administracyjnych, w tym również stanowisk poza usługą katalogową.  Oprogramowanie musi umożliwiać monitorowanie stanu dowolnej usługi sieciowej TCP.  Oprogramowanie musi umożliwiać monitorowanie dowolnego licznika SNMP(v1/2/3) urządzenia.  Oprogramowanie musi umożliwiać monitorowanie stanu dowolnego urządzenia sieciowego poprzez odpytywanie typu PING.  Oprogramowanie musi umożliwiać tworzenie konfigurowalnych zdarzeń sieciowych powodujących wysyłanie komunikatów informacyjnych i/lub ostrzegawczych poprzez SMS i/lub Email. |
| **Zarządzanie dokumentami** | Oprogramowanie musi umożliwiać centralną ewidencję dokumentów  Oprogramowanie musi umożliwiać zawierać dedykowany formularz dodawania nowego dokumentu z możliwością edycji widocznych oraz wymaganych atrybutów dokumentu  Oprogramowanie musi umożliwiać dołączenie skanu dokumentu (m.in.: skany faktur, umów)  Oprogramowanie musi umożliwiać stworzenie dedykowanego zbioru ról i uprawnień w zakresie obsługi rejestru dokumentów  Oprogramowanie musi umożliwiać utworzenie pomocniczych rejestrów oraz słowników  Oprogramowanie musi umożliwiać przeszukiwanie bazy dokumentów oraz kontrahentów po dowolnie wskazanym atrybucie opisującym  Oprogramowanie musi umożliwiać utworzenie rejestru osób reprezentujących  Oprogramowanie musi umożliwiać analizę zmian wartości dowolnych atrybutów opisujących dokument w zakresie daty zmiany, aktualnej/poprzedniej wartości oraz osoby dokonującej zmiany |
| **System wewnętrznego komunikatora dla użytkowników** | Oprogramowanie musi zawierać wewnętrzny komunikator pracujący w sieci LAN, integrujący się z usługą katalogową w zakresie kont użytkowników (dane osobowe, avatar), jednostek organizacyjnych.  Oprogramowanie w zakresie modułu komunikatora dla użytkowników musi współpracować z serwerem MSSQL Server 2008R2-2019 lub PostrgeSQL  Oprogramowanie komunikatora musi umożliwiać automatyczne logowanie użytkowników pochodzących z usługi katalogowej.  Oprogramowanie komunikatora musi umożliwiać konwersację grupową oraz prywatną pomiędzy użytkownikami  Oprogramowanie komunikatora musi umożliwiać wysyłanie wiadomości powitalnych; komunikatów grupowych z raportowaniem doręczenia oraz odczytania.  Oprogramowanie komunikatora musi umożliwiać generowanie raportów doręczenia/odczytania wiadomości wymagających potwierdzenia.  Oprogramowanie komunikatora musi umożliwiać określenie maksymalnego rozmiaru transferowanego pliku (przez administratora).  Oprogramowanie komunikatora musi umożliwiać wysyłanie powiadomień e-mail o utworzeniu/modyfikacji użytkowników, którzy nie pochodzą z usługi katalogowej.  Oprogramowanie komunikatora musi umożliwiać automatyczną aktualizację wg. zadanej konfiguracji danych synchronizowanych (ze szczególnym uwzględnieniem danych o użytkownikach, jednostkach organizacyjnych z usługi katalogowej).  Oprogramowanie komunikatora musi umożliwiać archiwizację starych rozmów między użytkownikami.  Oprogramowanie komunikatora musi umożliwiać administratorowi wyłączenie globalnie możliwości zamknięcia/wylogowanie/zapisywanie poświadczeń dla klientów końcowych.  Oprogramowanie komunikatora musi umożliwiać administratorowi bezpieczeństwa wgląd do rozmów pracowników, wyłączenie wybranych funkcjonalności dla klienta końcowego (np. transferu plików, konferencji audio-video).  Oprogramowanie komunikatora musi umożliwiać wymianę plików pomiędzy zalogowanymi użytkownikami  Oprogramowanie komunikatora musi umożliwiać nawiązanie sesji audio oraz wideo pomiędzy zalogowanymi użytkownikami wraz z obsługą konferencji grupowych. |
| **Wymagania formalne** | Dostarczone licencje na oprogramowanie muszą być bezterminowe.  Dostarczone licencje na oprogramowanie muszą być dostarczone z 12 miesięcznym supportem producenta, liczonym od daty zakończenia wdrożenia.  Obsługa serwisowa w zakresie obsługi błędów realizowana ma być z czasem reakcji 16 godzin roboczych oraz czasem naprawy 80 godzin roboczych. W ramach supportu wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta.  Dostarczone licencje na oprogramowanie muszą objąć co najmniej 40 stanowisk komputerowych z systemem klasy Microsoft Windows. Licencje nie mogą mieć ograniczeń ilościowych dotyczących liczby obsługiwanych innych zasobów (np. drukarki, skanery, monitory itp). Ponadto musi posiadać co najmniej 1 licencję dostępową do konsoli zarządzającej  W przypadku wątpliwości zamawiający zastrzega sobie prawo (w przeciągu do 7 dni od terminu otwarcia ofert) do wezwania wykonawcy do prezentacji zaoferowanego rozwiązania celem weryfikacji zgodności z wymaganiami stawianymi przez zamawiającego w niniejszym postępowaniu.  Zamawiający wymaga od wykonawcy, aby w terminie 15 dni od podpisania umowy przeprowadził wdrożenie systemu zdalnie (wymagane co najmniej 3 sesje – 5 godzinne) |

**Oprogramowanie centralnego menadżera haseł: 1 szt.**

|  |  |
| --- | --- |
| **Parametr** | **Wymagane parametry techniczne** |
| **Oprogramowania** | **Minimalne wymagania funkcjonalne:**   1. Centralne zarządzanie kontami użytkowników oraz hasłami w ramach organizacji. 2. Możliwość nadawania ról i uprawnień użytkownikom. 3. Bezpieczne przechowywanie haseł z szyfrowaniem typu end-to-end. 4. Wsparcie dla logowania dwuetapowego (2FA). 5. Audyt bezpieczeństwa haseł i raportowanie dostępu. 6. Możliwość współdzielenia wpisów (np. loginów, danych uwierzytelniających) pomiędzy użytkownikami z zachowaniem zasad polityki bezpieczeństwa. 7. Interfejs użytkownika dostępny w języku polskim lub możliwość jego przełączenia. 8. Kompatybilność z systemami Windows, macOS, Android, iOS oraz przeglądarkami internetowymi. 9. Możliwość korzystania z aplikacji mobilnych i desktopowych.   **Wymagania licencyjne:**   1. Licencja dla 36 użytkowników. 2. Okres obowiązywania licencji: do dnia **30.06.2026**. 3. Wsparcie techniczne producenta oraz dostęp do wszystkich aktualizacji w okresie obowiązywania licencji. |

**Część III - Przeprowadzenie testów penetracyjnych infrastruktury IT**

**TESTY PENETRACYJNE**

**Zakres testów bezpieczeństwa infrastruktury**

1. Analiza konfiguracji i bezpieczeństwa serwerów na poziomie systemu operacyjnego i usługowego
2. sprawdzenie aktualności oprogramowania, obecności łatek systemowych,
3. dostępność domyślnych kont użytkowników, bezpieczeństwo kont administratorskich, zgodność z polityką haseł,
4. uruchomione usługi, ich celowość,
5. zarządzanie systemami plików, polityka kopii zapasowych,
6. zarządzanie ruchem sieciowym, zdalny dostęp, członkostwo w domenie,
7. obecność i aktualność oprogramowania antywirusowego,
8. logowane zdarzeń systemowych,
9. zgodność konfiguracji z zewnętrznymi oraz wewnętrznymi standardami
10. Analiza konfiguracji i bezpieczeństwa na poziomie aktywnych urządzeń sieciowych
11. aktualność oprogramowania, obecność łatek systemowych,
12. dostępność domyślnych kont użytkowników, bezpieczeństwo kont, administratorskich, zgodność z polityką haseł,
13. uruchomione usługi, ich celowość,
14. logowane zdarzeń systemowych, podłączenie do systemów korelacji zdarzeń
15. Analiza konfiguracji i bezpieczeństwa na poziomie kanałów komunikacji pomiędzy poszczególnymi komponentami :
16. weryfikacja ruchu sieciowego na poziomie aktywnych urządzeń sieciowych oraz usług udostępnionych na serwerach,
17. weryfikacja użytych protokołów i ich konfiguracji,
18. weryfikacja zabezpieczenia komunikacji pomiędzy poszczególnymi komponentami systemu informatycznego
19. Testy penetracyjne typu GreyBox obejmujące :
20. aktywne urządzenia sieciowe (routery, drukarki, dyski i inne),
21. potencjalne luki w systemach uwierzytelnienia,
22. poziom bezpieczeństwa haseł,
23. obecność kont typu “gość” oraz domyślnych haseł,
24. identyfikację urządzeń dostępnych z poziomu Internetu
25. analizę topologii sieci z wewnątrz i z poziomu Internetu,
26. analizę bezpieczeństwa systemów operacyjnych i oprogramowania używanego przez pracowników,
27. analizę bezpieczeństwa zapory sieciowej,
28. oszacowanie stopnia ryzyka wykrytych podatności
29. **Przygotowanie raportu końcowego z przeprowadzonych testów bezpieczeństwa ze szczegółowym opisem wykrytych zagrożeń oraz rekomendacjami co do implementacji mechanizmów obronnych.**

**Etapy wykonywania testów penetracyjnych sieci – pentestów**

1. **Konsultacja:**

Na początek omówienie zakresu i termin przeprowadzenia testów penetracyjnych zabezpieczeń sieci.

1. **Automatyczne testy penetracyjne sieci:**

W ramach testów penetracyjnych będzie symulowany atak hakerski, mający na celu uzyskać dostęp do sieci urzędu. Mają zostać wykorzystane profesjonalne skanery umożliwiającymi szybkie przetestowanie sieci pod kątem znanych metod ataków. Techniki testowania, podatność zasobów informatycznych na rozmaite działania cyberprzestępców – pod tym względem podczas testu penetracyjnego zabezpieczeń IT analizujemy m.in. otwarte porty, w celu uzyskania nieautoryzowanego dostępu do zasobów urzędu. Po testach urząd ma pewność bezpieczeństwa sieci i bezpieczeństwa systemów, wiedząc, czy są odporne na wszelkiego rodzaju techniki, technologie i narzędzia wykorzystywane do ataków hakerskich.

1. **Manualne testy penetracyjne sieci:**
2. W ramach testów manualnych weryfikujemy wykryte zagrożenia oraz wykonamy dodatkowe symulacje ataków, niedostępne z poziomu automatycznego skanowania.
3. **Analiza ryzyka:**
4. W ramach analizy ryzyka wykonane zostaną kompleksowe testy penetracyjne sieci, na ich podstawie oszacujemy poziom bezpieczeństwa systemu, stopień ryzyka wykrytych podatności oraz ustalimy priorytet naprawy poszczególnych błędów. Ta informacja, pozwoli na odpowiednią hierarchizację działań, tak aby najpoważniejsze nieprawidłowości usunąć na samym początku,   
   a najmniej istotne na końcu.
5. **Przekazanie raportu wraz z rekomendacjami:**
6. Po wykonaniu testów penetracyjnych sieci raport ze szczegółowym opisem wykorzystywanych technik ataku i wykrytych zagrożeń oraz rekomendacjami co do implementacji mechanizmów obronnych. Ta instrukcja, w której zawarte są gotowe do wdrożenia rozwiązania, a wszelkie nieprawidłowości zostają szczegółowo opisane. Przykładowy raport po testowaniu zabezpieczeń będzie zawierać dużą ilość dokładnych, ale czytelnie zaprezentowanych danych i rekomendacji.
7. **Restety:**

Po tym, jak prace zostały wykonane, zalecamy powtórzenie testów penetracyjnych sieci w celu upewnienia się, że wykryte podatności zostały usunięte. Dzięki temu można uzyskać stuprocentową gwarancję prawidłowości i skuteczności wdrożonych zabezpieczeń i bezpieczeństwa sieci i zasobów IT.