**Załącznik nr 10 do SWZ – OZP oraz Specyfikacja Techniczna**

**MINIMALNE WYMAGANIA TECHNICZNE JAKIE MUSZĄ SPEŁNIAĆ OFEROWANE SPRZĘTY/OPROGRAMOWANIE**

|  |  |
| --- | --- |
| **I. System centralnego backupu i zarządzania kopiami zapasowymi środowisk IT** | |
| **1. Opis ogólny przedmiotu zamówienia** |  |
| Przedmiotem zamówienia jest dostawa, instalacja i konfiguracja sprzętowego appliance do tworzenia i zarządzania kopiami zapasowymi środowisk fizycznych, wirtualnych oraz usług SaaS, wraz z pełnym wsparciem technicznym i licencjami wieczystymi. Rozwiązanie musi spełniać wszystkie niżej wymienione wymagania techniczne, funkcjonalne i organizacyjne.  **WYMAGANA ILOŚĆ: 1** |  |
| 1. **Oferowane rozwiązanie:** |  |
| 1. **Oferowana ilość:** |  |
| **2. Szczegółowa specyfikacja wymagań** |  |
| **2.1 Zarządzanie i magazyny** |  |
| 1. Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2024 r. |  |
| 2. System dostarczany w formie sprzętowego appliance z kompletem skonfigurowanych usług. |  |
| 3. Minimalne wymagania sprzętowe: |  |
| a. Obudowa rack – rozmiar Desktop. |  |
| b. Pamięć RAM 16 GB DDR4. |  |
| c. Pojemność na dane 8 TB. |  |
| d. Osobny dysk SSD M.2 NVMe dla oprogramowania i OS. |  |
| e. Zasilacz 350 W. |  |
| f. Interfejs 1 Gb Ethernet. |  |
| g. Gwarancja równoważna czasowi wsparcia technicznego. |  |
| 4. Produkt dostępny w polskiej wersji językowej. |  |
| 5. Konsola zarządzająca dostępna przez przeglądarkę. |  |
| 6. Kopie zapasowe na poziomie dysków. |  |
| 7. Kopie zapasowe na poziomie plików i folderów. |  |
| 8. Replikacja kopii do wielu lokalizacji docelowych. |  |
| 9. Backup i restore systemów UEFI/GPT. |  |
| 10. Współpraca z VSS firmy Microsoft. |  |
| 11. Definiowanie limitu przepustowości sieciowej dla backupu. |  |
| 12. System zarządzania bez relacyjnych baz danych. |  |
| 13. Architektura bez pojedynczego punktu awarii. |  |
| 14. Zoptymalizowana transmisja danych – wybór workerów i browserów. |  |
| 15. Klient wysyła dane bezpośrednio do magazynu; serwer backupu nie pośredniczy. |  |
| 16. Multi‑storage – tworzenie wielu repozytoriów równocześnie, także zdalnych. |  |
| 17. Retencja danych „bez limitu” lub wg czasu/cykli. |  |
| 18. Sprzęt oparty o standard x86, bez vendor lock‑in. |  |
| 19. Dowolny harmonogram replikacji między magazynami. |  |
| 20. Jednoczesny backup obrazów dysku, plików, katalogów i VM bez zatrzymania systemu, z zachowaniem spójności. |  |
| 21. Backup wielu strumieni na jedno urządzenie. |  |
| 22. Backup jednoprzebiegowy z granularnym odtwarzaniem. |  |
| 23. Automatyczne ponawianie zadań po błędzie. |  |
| 24. Klonowanie planów backupu, replikacji i testów restore. |  |
| 25. Obsługa skryptów PRE/POST i po migawce VSS. |  |
| 26. Definiowanie okien backupowych per zadanie. |  |
| 27. Automatyczne dodawanie nowych źródeł/VM do polityk backupu. |  |
| 28. Podgląd postępu każdego zadania (backup, restore, test, usuwanie, refresh storage). |  |
| 29. Powiadomienia e‑mail i Slack o wynikach zadań (OK, warning, error, cancel, not started). |  |
| 30. Powiadomienia na dowolne webhook (adresy definiowane przez użytkownika). |  |
| 31. Konfiguracja dobrana wg najlepszych praktyk producenta. |  |
| 32. Skalowanie z uwzględnieniem przyrostu danych i obiektów. |  |
| 33. Pełna funkcjonalność (deduplikacja, kompresja, workery, replikacja, test restore) dostępna od wdrożenia. |  |
| 34. Deduplikacja blokowa pomiędzy wszystkimi źródłami i kopiami. |  |
| 35. Deduplikacja możliwa na każdym typie magazynu. |  |
| 36. Deduplikacja bez dodatkowych komponentów pośredniczących. |  |
| 37. Deduplikacja bez pojedynczego punktu awarii. |  |
| 38. Deduplikacja z blokiem stałej wielkości. |  |
| 39. Szyfrowanie nie ogranicza deduplikacji w ramach tego samego klucza. |  |
| 40. Kompresja LZ4 lub Zstandard; poziomy: niski/średni/wysoki. |  |
| 41. Instalacja i zmiany polityk bez restartu systemu. |  |
| 42. Automatyczne aktualizacje oprogramowania. |  |
| 43. Kompresja i szyfrowanie danych w NAS. |  |
| 44. Backup kontenerów Docker uruchomionych na NAS. |  |
| 45. Niezmienność kopii (resilience). |  |
| 46. Szyfrowanie danych w kopii i ruchu wewnętrznego. |  |
| 47. Szyfrowane archiwum długoterminowe z restore z tego samego UI. |  |
| 48. Mechanizmy ochrony konta admina i definiowanie dodatkowych uprawnień. |  |
| 49. Gradacja ról (system operator, backup operator, restore operator, viewer) z możliwością blokady usunięcia danych. |  |
| 50. Możliwość nieodwracalnego usunięcia danych po spełnieniu warunków. |  |
| 51. Restore z archiwum przy użyciu innej instancji tego samego producenta. |  |
| 52. Konsola w chmurze producenta (lokalizacja PL) na czas awarii środowiska lokalnego. |  |
| 53. Dostęp do konsoli z wielu stacji roboczych. |  |
| 54. Mechanizm śledzenia zmienionych plików dla udziałów plikowych. |  |
| 55. Schematy backupu: G‑F‑S, Forever incremental. |  |
| 56. Kontrola dostępu RBAC. |  |
| 57. Składowanie kopii w chmurach AWS, Azure, Wasabi, Google Cloud, Backblaze B2, S3‑compatible. |  |
| 58. Składowanie kopii na SMB, NFS, iSCSI, katalog lokalny. |  |
| 59. Jedna konsola do zarządzania i restore, niezależnie od lokalizacji kopii. |  |
| 60. Retention time niezależny od czasu NTP (chroniony przed manipulacją). |  |
| 61. Harmonogramowane raporty dobowe. |  |
| 62. Zapis kopii do chmurowego magazynu producenta (DC w Polsce). |  |
| 63. Definicja maksymalnej liczby równoczesnych urządzeń w jednym planie. |  |
| 64. Podgląd szczegółów urządzenia (CPU, RAM, OS, IP). |  |
| 65. Powiadomienie e‑mail po przekroczeniu progu zajętości magazynu. |  |
| **2.2 Środowiska fizyczne i bazy danych** |  |
| 1. Tworzenie grup urządzeń dla automatyzacji zadań. |  |
| 2. Zadania dla grup oraz pojedynczych urządzeń. |  |
| 3. Automatyczne wyłączenie stacji roboczej po backupie. |  |
| 4. Backup zaszyfrowanych partycji (BitLocker, Veracrypt, TrueCrypt, ESET Endpoint Encryption). |  |
| 5. Niezależność od wersji Microsoft SQL – przywracanie do tej samej lub nowszej wersji. |  |
| 6. Obsługa Oracle RMAN z przyrostowym scalaniem. |  |
| 7. Granularne restore pojedynczych plików Windows/Linux. |  |
| 8. Bare Metal Restore na ten sam lub inny sprzęt z automatycznym dopasowaniem sterowników. |  |
| 9. Uruchomienie Bare Metal Restore z dowolnego bootowalnego nośnika. |  |
| 10. Scenariusze P2P, P2V, V2P, V2V. |  |
| 11. Restore obrazu dysku w formatach RAW, VHD, VHDX, VMDK. |  |
| 12. Restore z ACL lub bez, konfigurowalne przy przywracaniu. |  |
| 13. Restore plików między różnymi OS i systemami plików. |  |
| **2.3 Środowiska wirtualne** |  |
| 1. Backup application‑aware dla wszystkich wspieranych hypervisorów. |  |
| 2. Backup VM z HotAdd, SAN, LAN, w tym LAN‑Free. |  |
| 3. Change Block Tracking i Replica Change Tracking. |  |
| 4. Instant Recovery wielu VM bezpośrednio ze zdeduplikowanego backupu (VMware & Hyper‑V). |  |
| 5. Uruchomienie backupu z innych platform (VM, physical, public cloud) w vSphere/Hyper‑V. |  |
| 6. Prezentacja pojedynczego dysku z kopii do działającej VM vSphere. |  |
| 7. Harmonogramowana weryfikacja odtwarzalności VM w dowolnym środowisku. |  |
| **2.4 Aplikacje SaaS** |  |
| 1. Ochrona Microsoft 365 (skrzynki, OneDrive, kontakty, kalendarze) z jednej konsoli. |  |
| 2. Restore Microsoft 365 do lokalizacji, pliku PST lub innego tenant/organizacji. |  |
| 3. Granularne restore pojedynczych plików i wiadomości. |  |
| 4. Backup środowisk Git (GitHub, GitLab, Bitbucket). |  |
| 5. Backup środowisk Jira. |  |
| **2.5 Licencjonowanie i wsparcie techniczne** |  |
| 1. Wsparcie techniczne w języku polskim dla wszystkich linii. |  |
| 2. Support świadczony bezpośrednio przez producenta min. 12 miesięcy. |  |
| 3. Zgłoszenia supportowe z GUI (chat). |  |
| 4. Materiały samopomocowe PL (baza wiedzy, wideo, karty produktu). |  |
| 5. Zdalne połączenia, ticket system, telefon. |  |
| 6. Dedykowany opiekun produktu |  |
| 7. Dane kontaktowe CSM (tel., e‑mail) w dokumentacji posprzedażowej. |  |
| 8. Licencje wieczyste – nielimitowane VM, serwery, stacje robocze. |  |
| 9. Wsparcie techniczne nie wymagane do działania systemu. |  |
| 10. Replikacja kopii na dowolne zasoby własne. |  |
| **2.6 Anty‑ransomware i bezpieczeństwo** |  |
| 1. Odporny na ransomware, niezmienny system plików. |  |
| 2. Wbudowany menedżer haseł na tajne dane (secrets). |  |
| 3. Możliwość odzyskania hasła głównego administratora. |  |

|  |  |
| --- | --- |
| **II. System klasy Data Loss Prevention (DLP)** | |
| **1. Opis ogólny przedmiotu zamówienia** |  |
| Przedmiotem zamówienia jest dostawa, instalacja i konfiguracja systemu klasy Data Loss Prevention (DLP) w architekturze on‑premises, obejmującego serwer zarządzający oraz agentów końcowych, spełniającego wszystkie poniższe wymagania.  **WYMAGANA ILOŚĆ: 30** |  |
| **a. Oferowane rozwiązanie** |  |
| **b. Oferowana ilość** |  |
| **2. Szczegółowa specyfikacja wymagań** |  |
| 2.1 Wymagania systemowe i architektura |  |
| 1. Klient stacji roboczej musi obsługiwać systemy: |  |
| a. Windows 10 (64‑bit) z aktualizacjami zabezpieczeń, |  |
| b. Windows 11 (64‑bit) z aktualizacjami zabezpieczeń, |  |
| c. macOS 12 lub nowszy. |  |
| 2. Serwer administracyjny instalowany na: Windows Server 2016 (64‑bit) i nowszych. |  |
| 3. Obsługiwane bazy danych serwera: |  |
| a. MS SQL Server 2016 lub nowszy, |  |
| b. MS SQL Express, |  |
| c. Azure SQL S3 lub nowszy. |  |
| 4. Pomoc i dokumentacja – język angielski. |  |
| 5. Konsola administracyjna i komunikaty klienta – język polski. |  |
| **2.2 Instalacja i zarządzanie** |  |
| 6. Konsola musi umożliwiać pobranie pliku instalacyjnego agenta. |  |
| 7. Serwer musi obsługiwać zdalną instalację i dezinstalację agentów. |  |
| 8. Reguły DLP egzekwowane również offline. |  |
| 9. Brak połączenia klienta z serwerem – lokalne buforowanie logów do czasu ponownego połączenia. |  |
| 10. Zarządzanie z poziomu konsoli webowej. |  |
| 11. Automatyczna konserwacja bazy danych – usuwanie najstarszych danych po osiągnięciu limitu. |  |
| 12. Automatyczne pobieranie aktualizacji klasyfikacji stron, aplikacji i rozszerzeń plików z opcją wyłączenia. |  |
| 13. Tworzenie, usuwanie kont administratorów w konsoli. |  |
| 14. Przydzielanie/odbieranie uprawnień do modułów programu (ustawienia vs. logi). |  |
| 15. Synchronizacja użytkowników i stacji z Active Directory. |  |
| 16. Wymuszenie synchronizacji ustawień i logów w czasie rzeczywistym. |  |
| 17. Powiadomienia dla użytkownika końcowego przy naruszeniu reguł (konfigurowalna grafika, e‑mail, link do polityki). |  |
| **2.3 Audyt i kategoryzacja** |  |
| 18. Audyt czynności (aplikacje, urządzenia, strony WWW, druk, e‑mail, operacje na plikach). |  |
| 19. Możliwość tworzenia własnych kategorii stron, aplikacji i typów plików. |  |
| 20. Filtrowanie i sortowanie zebranych danych. |  |
| 21. Alerty wysyłane co najmniej e‑mailem. |  |
| 22. Dashboardy dla wskazanych stacji, użytkowników, grup i zakresu czasu. |  |
| 23. Wbudowany serwer SMTP producenta. |  |
| 24. Zadania kategoryzacji plików istniejących i nowych (stacje, zasoby sieciowe). |  |
| 25. Kategoryzacja plików według aplikacji, lokalizacji, URL, formatu i zawartości. |  |
| 26. Reguły blokowania/zezwalania dla plików skategoryzowanych (zapis, przeniesienie, druk, e‑mail, chmura, komunikatory). |  |
| 27. Wyszukiwanie/ochrona plików wrażliwych na podstawie numerów kart, PESEL, dowodu, paszportu, IBAN, regex, określone ciągi. |  |
| 28. Weryfikacja zawartości w czasie rzeczywistym. |  |
| 29. Eksport logów do systemów SIEM. |  |
| 30. Konfiguracja własnego serwera SMTP w konsoli. |  |
| 31. Konsola webowa – podgląd wersji agenta, aktualizacja lub dezaktywacja. |  |
| **2.4 Ochrona środowisk chmurowych** |  |
| 32. Ochrona poczty e‑mail Microsoft 365 – skanowanie każdej wysyłanej wiadomości. |  |
| 33. Ochrona plików w Microsoft 365 – kontrola aktywności w SharePoint, OneDrive for Business, Teams. |  |
| **2.5 Zaawansowane funkcje bezpieczeństwa** |  |
| 34. Mechanizm OCR do wykrywania treści poufnych w obrazach i skanach. |  |
| 35. Integracja z systemami analitycznymi (Power BI, Tableau itp.). |  |
| 36. Zarządzanie szyfrowaniem dysków twardych i urządzeń wymiennych. |  |

|  |  |
| --- | --- |
| **III. System wspierający zarządzanie usługami IT** | |
| **1. Opis ogólny przedmiotu zamówienia** |  |
| Dostawa obejmuje licencje bezterminowe, instalację, konfigurację oraz wdrożenie centralnego systemu do kompleksowego zarządzania zasobami IT, w tym sprzętem, oprogramowaniem, CMDB i magazynem. System umożliwia automatyzację oraz zdalne zarządzanie stacjami roboczymi, a także obsługę procesów ServiceDesk i Workflow zgodnych z ITIL, takich jak zarządzanie incydentami, problemami, zmianami i wnioskami. Dodatkowo zapewnia monitoring i raportowanie (np. sieci, drukarek, wykorzystania zasobów), kontrolę zgodności licencyjnej oraz wewnętrzną komunikację LAN, w tym czat, audio i wideo.  **WYMAGANA ILOŚĆ: 30** |  |
| **a. Oferowane rozwiązanie** |  |
| **b. Oferowana ilość** |  |
| **2. Zakres funkcjonalny (skondensowany)** |  |
| **2.1 Architektura i bezpieczeństwo** |  |
| Trójwarstwowa architektura (DB – AppServer – Agent/Console) na Linux, DB = MSSQL 2008 R2‑2019. |  |
| Komunikacja szyfrowana kluczami + TLS 1.2/1.3; certyfikowany podpis binariów. |  |
| RBAC + 2FA (Google/Microsoft Authenticator), integracja **AD/LDAP/Radius**, SSO, log zmian i audyt sesji. |  |
| **2.2 Integracja katalogowa & struktura org.** |  |
| Pełna synchronizacja AD/OpenLDAP (OU, grupy, atrybuty, filtry, mapowanie), obsługa wielu domen, dziedziczenie uprawnień, dynamiczne grupy użytkowników i stacji. |  |
| **2.3 Inwentaryzacja sprzętu, oprogramowania & licencji** |  |
| Agentowy i offline‑scanner audit HW (CPU, RAM, HDD, BIOS, gwarancja Dell API, historia zmian) oraz SW (installe/unistalle, forbidden/standard apps, licencje, downgrade/upgrade). |  |
| Drukowane kartoteki, etykiety EAN128/PDF417; raporty administratorów lokalnych; globalne zestawienia. |  |
| Wbudowana baza sygnatur + własne; audyt licencji z historią. |  |
| **2.4 CMDB & zarządzanie zasobami** |  |
| Definiowalne typy CI, atrybuty, relacje, formularze, model usług → sprzęt → organizacja → pracownik; wizualizacja graficzna, import CSV/scan/AD; dokumenty, cykl życia, magazyn (PZ/PW/RW/MM). |  |
| Aplikacja inwentaryzacyjna Android. |  |
| **2.5 Automatyzacja i zdalne zarządzanie** |  |
| Remote desktop (agent, bez RDP/VNC), file‑transfer, chat, Wake‑on‑LAN, PowerShell, RegEdit, iAMT/vPro KVM, Internet‑gateway (poza VPN). |  |
| Zadania, polisy, makra instalacji (EXE GUI recorder) z warunkami dynamicznych grup; szyfrowane pakiety; postęp & stdout/stderr. |  |
| **2.6 Backup użytkownika & kontrola USB** |  |
| Zadania archiwizacji plików (filtry, FTP, cykle, usuwanie starych), raporty. |  |
| Logowanie i blokowanie USBStorage (RW/RO/deny), raport kopiowania. |  |
| **2.7 Monitoring i raporty** |  |
| WWW/APP usage, wydruki, ekrany, CPU/RAM sampling, LAN scan SNMP, NetFlow port traffic map, licznik tonerów. |  |
| Kreator raportów, dashboardy drag‑and‑drop, eksport PDF/JPEG/CSV. |  |
| **2.8 ServiceDesk & Workflow** |  |
| Portal responsywny PL/EN, zgłoszenia (Incydent, Problem, Change, Request) + SLA matryca wpływ/pilność; wieloliniowe wsparcie; reguły automatyzacji; bazę wiedzy; zgłoszenia mail. |  |
| Uprawnienia/Access Management (workflows, akceptacje, karta uprawnień) |  |
| Rezerwacje zasobów (kalendarium, konflikty) |  |
| Reguły i obiegi graficzne, formularze drag‑and‑drop, dashboardy użytkownika, cykliczne zgłoszenia. |  |
| **2.9 Komunikator wewnętrzny** |  |
| Integracja AD, chat 1‑1 i grupowy, pliki, audio‑video, powiadomienia, archiwizacja rozmów, raport doręczeń. |  |
| **2.10 Formalne & licencyjne** |  |
| Licencje wieczyste, support producenta 12 mies. (reakcja ≤ 16 h rob., naprawa ≤ 80 h rob.) + aktualizacje. |  |
| Bez limitu innych zasobów, 1 konsola. |  |
| Zdalne wdrożenie (≥ 1 sesja 5 h) w ≤ 10 dni od umowy; prawo Zamawiającego do sesji demo w 7 dni. |  |
| **3. Etapy wdrożenia (skrót)** |  |
| 1. Analiza przedwdrożeniowa & projekt. |  |
| 2. Instalacja i konfiguracja wszystkich modułów. |  |
| 3. Integracja AD/LDAP, import zasobów, konfiguracja RBAC. |  |
| 4. Implementacja workflow, SLA, raportów, dashboardów. |  |
| 5. Instruktaż (5 h, on‑line). |  |
| 6. Testy akceptacyjne. |  |
| 7. Przekazanie do produkcji + dokumentacja. |  |

|  |  |
| --- | --- |
| **IV. System zarządzania podatnościami** | |
| **1. Opis ogólny przedmiotu zamówienia** |  |
| Przedmiotem zamówienia jest dostawa, wdrożenie i konfiguracja zintegrowanego rozwiązania do **zarządzania podatnościami (Vulnerability Management)** w dwóch wariantach instalacyjnych: |  |
| **1. Wersja lokalna (on‑premise)** – przeznaczona do kompleksowego skanowania sieci i aplikacji webowych w infrastrukturze Zamawiającego. |  |
| **2. Wersja chmurowa (SaaS)** – przeznaczona do prowadzenia kampanii phishingowych + edukacyjnych oraz do zarządzania podatnościami w modelu usługowym. |  |
| Obie wersje muszą być zarządzane z centralnej konsoli (Security Center) i udostępniać interfejs API, przy zachowaniu neutralności technologicznej i pełnej zgodności z poniższą specyfikacją.  **WYMAGANA ILOŚĆ:**   1. **Ilość komputerów: 25** 2. **Ilość systemów: 8** 3. **Ilość skrzynek pocztowych: 35** |  |
| a. Oferowane rozwiązanie |  |
| 1. Oferowana ilość   Ilość komputerów:  Ilość systemów:  Ilość skrzynek pocztowych: |  |
| **2. Szczegółowa specyfikacja wymagań** |  |
| **2.1 Wersja on‑premise – „System & Network Scanning”** |  |
| **2.1.1 Ogólne** |  |
| 1. System musi być udostępniony jako obraz OVA do wdrożenia w VMware. |  |
| 2. Sondy skanujące (Scanner Appliance) – gotowe OVA lub VHDX, rejestracja tokenem 6‑znakowym. |  |
| 3. Konsola Security Center wspiera logowanie 2FA (kod SMS). |  |
| 4. Integracje: Jira, TopDesk, ServiceNow. |  |
| 5. Powiadomienia: Slack, Microsoft Teams, Webhooks. |  |
| 6. Dodawanie dodatkowych administratorów i ról (uprawnienia przypisywalne). |  |
| 7. Zarządzanie przez REST API. |  |
| **2.1.2 Zarządzanie zasobami** |  |
| 8. Ręczne dodawanie urządzeń/aplikacji lub import CSV; IP pojedyncze, zakresy, podsieci. |  |
| 9. Aplikacje web: definiowanie autentykacji, list URL (white/black), rozszerzeń. |  |
| 10. Przypisanie wpływu biznesowego (Neutral, Low, Medium, High). |  |
| 11. Statyczne i dynamiczne tagi (kolor). |  |
| **2.1.3 Skanowanie sieci** |  |
| 12. Nieograniczona liczba skanów/ harmonogramów. |  |
| 13. Nieograniczona liczba sond – równoległe skanowanie segmentów. |  |
| 14. Obsługa IPv6, segmentowanych/geograficznych sieci. |  |
| 15. Profile skanowania: Full, Basic, Discovery; import profili producenta. |  |
| 16. Konfiguracja portów, TCP SYN/SYN‑ACK, ICMP; obejmowanie niszowych podatności. |  |
| 17. Opcje: testy potencjalnie niebezpieczne, skan drukarek, martwe hosty. |  |
| 18. Bruteforce haseł – opcjonalnie. |  |
| 19. Uwierzytelnione skany (Windows/Linux). |  |
| 20. Wybór intensywności, wybór testów podatności. |  |
| 21. Baza testów: ≥ 80 000 (on‑prem). |  |
| 22. Wybór sondy lokalnej/ grupy sond / sondy chmurowej. |  |
| 23. Raport CSV ze zleceń; automatyczne dodanie urządzeń i tagów; podatności przenoszone do VM managera. |  |
| **2.1.4 Zarządzanie aktywami** |  |
| 24. Lista zasobów z kolumnami: tagi, nazwa, liczba podatności, najcięższa podatność, biznes impact, OS, daty. |  |
| 25. Widoki szczegółowe + trendy (czas, severity, status). |  |
| 26. Edycja danych zasobu (nazwa, opis, impact, RODO flag, itp.). |  |
| 27. Skanowanie REST API, zakres indeksowania, nagłówki, cookies, uwierzytelnienie HTTP, whitelist/blacklist, itd. |  |
| **2.1.5 Menedżer podatności & zgłoszenia** |  |
| 28. Konfigurowalne dashboardy (wymienione widżety). |  |
| 29. Filtrowanie luk wg stanu, typu, statusu, severity, tagów, dat, kategorii. |  |
| 30. Masowe akcje ignore/disable (powód + expiry). |  |
| 31. Notatki, czat konwersacyjny, integracja z ticketami. |  |
| 32. Wbudowany ticketing (open/closed/resolved, owner, due date itd.). |  |
| 33. Widoki niestandardowe, proaktywne alerty zmian. |  |
| **2.1.6 Raportowanie on‑prem** |  |
| 34. Szablony raportów: Network Scan, WebApp, Patches, Remediation, Delta, Compliance. |  |
| 35. Compliance: SOX, HIPAA, OWASP Top 10 (2017), UODO, ISO 27001, GDPR, NIS, PCI‑DSS (+custom). |  |
| 36. Raporty wg czasu skanu / bieżących danych, trendów, filtry OS/asset/vuln, skrócone weekly/monthly (e‑mail). |  |
| **2.2 Wersja SaaS – „Phishing Campaigns + Cloud VM”** |  |
| **2.2.1 Ogólne** |  |
| 37. Usługowy model SaaS z DC zlokalizowanym w UE. |  |
| 38. Konsola Security Center – 2FA SMS. |  |
| 39. Integracje: Jira, TopDesk, ServiceNow. |  |
| 40. Powiadomienia: Slack, Microsoft Teams, Webhooks. |  |
| 41. Wielu administratorów, role, REST API. |  |
| **2.2.2 Kampanie phishingowe & edukacyjne** |  |
| 42. Tworzenie kampanii phishing/edukacja (email + strona). |  |
| 43. Własne profile lub import predefiniowanych (PL/EN). |  |
| 44. Profil: szablon mail / mail+strona. |  |
| 45. Kategorie domen wysyłkowych; min. 60 domen. |  |
| 46. Harmonogram startu; wysyłka jednorazowa, batched lub losowa w oknie czasowym. |  |
| 47. Min. 5 predefiniowanych szablonów phishing (lista). |  |
| 48. Łączenie kampanii phishing z kampanią edukacyjną. |  |
| 49. Własne profile edukacyjne lub import (PL/EN). |  |
| 50. Dynamiczna treść edukacyjna wg akcji (open, reply, click, form). |  |
| 51. Strona edukacyjna – tekst, grafika, wideo. |  |
| 52. Test wiedzy – pytania jednokrotne/wielokrotne. |  |
| 53. Anonimizacja danych uczestników. |  |
| 54. Import odbiorców z Azure AD. |  |
| **2.2.3 Raportowanie phishing/SaaS VM** |  |
| 55. Raporty: Phishing Score, Delta, Compliance (SOX, HIPAA, UODO, ISO 27001, GDPR, NIS, PCI‑DSS) + możliwość nowych profili. |  |
| 56. Raport trendów podatności (szczegóły, listy, filtry, 500‑char limit). |  |
| 57. Skrócone raporty weekly/monthly (e‑mail). |  |
| **3. Wymagania wspólne (on‑prem & SaaS)** |  |
| 1. Aktualizacja bazy testów podatności: ≥ 80 000 (on‑prem) i ≥ 110 000 (SaaS) – aktualizacje z serwera producenta. |  |
| 2. Integracja z AD/AAD (import użytkowników). |  |
| 3. Centralna konsola Security Center z jednolitą autoryzacją 2FA, zarządzaniem użytkownikami i rolami. |  |
| 4. Powiadomienia e‑mail (SMTP wbudowane) + Slack, Teams, Webhooks. |  |
| 5. REST API do automatyzacji. |  |
| 6. Możliwość eksportu logów do zewnętrznego SIEM. |  |
| 7. Wszystkie funkcje dostępne przez interfejs webowy PL/EN. |  |
| 8. System ticketowy lub integracja z zewnętrznymi systemami. |  |
| 9. Zgodność z politykami bezpieczeństwa Zamawiającego; neutralność technologiczna. |  |
| **4. Gwarancja i wsparcie** |  |
| Wsparcie producenta min. 12 mies. |  |
| Dostęp do aktualizacji bazy podatności i nowych szablonów kampanii. |  |
| Kanały: portal, e‑mail, telefon; czas reakcji w następnym dniu roboczym |  |
| Dokumentacja PL / EN. |  |

|  |  |
| --- | --- |
| **V. Serwer** | |
| **1. Opis ogólny przedmiotu zamówienia** |  |
| Przedmiotem zamówienia jest dostawa, instalacja i konfiguracja serwera klasy enterprise do pracy w środowisku szafy RACK 19" 2U wraz z oprogramowaniem do zarządzania oraz monitorowania infrastruktury serwerowej i pamięci masowych, spełniającego wysokie wymagania w zakresie bezpieczeństwa, niezawodności, certyfikacji oraz wsparcia serwisowego.  **WYMAGANA ILOŚĆ: 1** |  |
| **a. Oferowane rozwiązanie** |  |
| **b. Oferowana ilość** |  |
| **2. Opis przedmiotowy** |  |
| **Obudowa i chłodzenie:** |  |
| ·         serwerowa do montażu w szafie RACK 19" wielkości 2U |  |
| ·         Obudowa powinna posiadać panel LCD umieszczony na froncie obudowy i pozwalający jednoznacznie stwierdzić czy system działa poprawnie i pokazujący podstawowe stany działania serwera (umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze). |  |
| ·         Obudowa z możliwością wyposażenia w kartę do bezpośredniej komunikacji z urządzeniem mobilnym. |  |
| ·         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. |  |
| ·         W obudowie powinien być zainstalowany zestaw redundantnych wentylatorów. |  |
| **Płyta główna i chipset:** |  |
| ·         Płyta główna z możliwością zainstalowania jednego procesora |  |
| ·         Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |  |
| ·         musi być wyposażona w zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust), |  |
| ·         Musi umożliwiać utworzenie bezpiecznego profilu w oparciu o konfigurację sprzętową oraz o konfigurację wewnętrznego oprogramowania komponentów serwera. |  |
| ·         Zintegrowany z płytą główną moduł TPM w wersji co najmniej 2.0 |  |
| ·         Dedykowany przez producenta procesora do pracy w serwerach |  |
| **Zasilanie:** |  |
| ·         W obudowie powinien być zaistalowany zestaw redundantnych zasilaczy o mocy co najmniej 700W w standardzie Titanium każdy wymienialnych podczas pracy |  |
| **Procesor i RAM:** |  |
| [·         Procesor z uwagi na licencjonowanie posiadający dokładnie 16 rdzeni działając co najmniej z częstotliwością 3GHz i dający w teście Passmark dostępnym na stronie https://www.cpubenchmark.net/ wynik nie mniejszy niż 43 000 .](https://www.cpubenchmark.net/)  (nie ma obowiązku dołączenia do oferty wyniku testu). |  |
| ·         Na płycie głównej powinno znajdować się minimum 12 slotów przeznaczonych do instalacji pamięci taktowaną przynajmniej z częstotliwością 5600MT/s przy użyciu odpowiednich procesorów. |  |
| ·         128 GB pamięci RAM w modułach 64GB RDIMM przygotowanych na działanie z częstotliwością co najmniej 5600MT/s |  |
| **Dyski i kontrolery:** |  |
| ·         Serwer ma mieć przewidzianą przez producenta możliwość dodania modułu pozwalającego na startowanie systemu z kart SD lub dysków M.2 skonfigurowanych w RAID1 nie zajmujących slotów na dyski. |  |
| ·         Miejsce na co najmniej 12 dysków w rozmiarze 3.5"wymienialne bez wyłączania systemu |  |
| Zainstalowane co najmniej 2 dyski minimum 480GB SSD SATA Read Intensive 6Gbps Hot-plug Oraz 3 dyski SSD 1.92TB |  |
| ·         Serwer powinien posiadać kontroler RAID umożliwiający konfigurację RAID 0,1,5,10,50,6 |  |
| posiadający co najmniej 8GB pamięci cache zabezpieczonej przed awarią prądu. |  |
| **Sieć i grafika:** |  |
| ·         Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT ((porty nie mogą być osiągnięte poprzez karty w slotach PCIe)) |  |
| ·         Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |  |
| **Bezpieczeństwo:** |  |
| ·         Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. |  |
| ·         Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. |  |
| ·         Możliwość wyłączenia w BIOS funkcji przycisku zasilania. |  |
| ·         BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła |  |
| ·         Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. |  |
| ·         Moduł TPM 2.0 |  |
| ·         Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera |  |
| ·         Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem |  |
| ·         Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). |  |
| **Zarządzanie i kontroler eksploatacji:** |  |
| ·         Serwer powinien być standardowo wyposażony w kontroler eksploatacji |  |
| ·         Konfigurowanie ustawień BIOS i sprzętu. |  |
| ·         Uproszczoną instalację systemów operacyjnych z wbudowanymi sterownikami, z opcją instalacji bezobsługowej dla systemów Microsoft Windows i Red Hat Enterprise Linux 7. |  |
| ·         Aktualizację oprogramowania niezależnie od systemu operacyjnego, z możliwością przywrócenia poprzedniej wersji. |  |
| ·         Ciągłą dostępność diagnostyki bez zależności od dysku twardego, z automatyczną aktualizacją oprogramowania podczas wymiany komponentów. |  |
| ·         Usunięcie danych związanych z serwerem i pamięcią masową na wybranych komponentach. Możliwe jest usunięcie informacji z BIOS. |  |
| ·         Dostarczenie informacji o bieżącej i fabrycznej konfiguracji systemu. |  |
| ·         Udostępnianie logów sprzętowych w celu rozwiązywania problemów. |  |
| ·         Zdalne zarządzanie cyklem życia serwera co najmniej za pomocą interfejsu WS-Man |  |
| ·         Konfigurację ustawień sieci dla wbudowanej karty NIC, w tym ustawienia VLAN. |  |
| ·         Wykonywanie diagnostyki pamięci, urządzeń we/wy, procesora i dysków fizycznych. |  |
| ·         Aktualizację komponentów systemu za pomocą repozytoriów lub pojedynczych pakietów DUP. |  |
| ·         Powrót do poprzedniej wersji oprogramowania układowego. |  |
| ·         Umożliwia zabezpieczenie konfiguracji systemu - "System Configuration Lockdown mode" |  |
| ·         Automatyczną aktualizację oprogramowania i konfiguracji wymienionych części. |  |
| ·         Trwałe usunięcie danych przed ponownym wykorzystaniem lub wycofaniem systemu. |  |
| ·         Obsługę różnych metod aktualizacji, za pomocą różnych źródeł, takich jak FTP, udziały sieciowe (CIFS, NFS, HTTP, HTTPS) lub lokalne napędy USB/DVD |  |
| **Karta zarządzania:** |  |
| ·         Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: |  |
| o    - zdalny dostęp do graficznego interfejsu Web karty zarządzającej |  |
| o    - szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika |  |
| o    - możliwość podmontowania zdalnych wirtualnych napędów |  |
| o    - wirtualną konsolę z dostępem do myszy, klawiatury |  |
| o    - wsparcie dla IPv6 - wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH |  |
| o    - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. |  |
| o    - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer |  |
| o    - integracja z Active Directory |  |
| o    - możliwość obsługi przez ośmiu administratorów jednocześnie |  |
| o    - Wsparcie dla automatycznej rejestracji DNS - wsparcie dla LLDP |  |
| o    - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej |  |
| o    - możliwość podłączenia lokalnego poprzez złącze RS-232. |  |
| o    - możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. |  |
| o    - Monitorowanie zużycia dysków SSD |  |
| o    - możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, |  |
| o    - Automatyczne zgłaszanie alertów do centrum serwisowego producenta |  |
| o    - Automatyczne update firmware dla wszystkich komponentów serwera |  |
| o    - Możliwość przywrócenia poprzednich wersji firmware |  |
| o    - Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych |  |
| ·         Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram |  |
| **Oprogramowanie do zarządzania:** |  |
| Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania: |  |
|  |  |
| ·         Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych; |  |
| ·         Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta; |  |
| ·         Wsparcie dla protokołów – WMI, SNMP, IPMI, WSMan, Linux SSH; |  |
| ·         Możliwość oskryptowywania procesu wykrywania urządzeń; |  |
| ·         Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram; |  |
| ·         Szczegółowy opis wykrytych systemów oraz ich komponentów; |  |
| ·         Możliwość eksportu raportu do CSV, HTML, XLS; |  |
| ·         Grupowanie urządzeń w oparciu o kryteria użytkownika; |  |
| ·         Automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń; |  |
| ·         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 „asis” do innych konsol firm trzecich; |  |
| ·         Aktualizacja oparta o wybranie źródła bibliotek (lokalna, online producenta oferowanego rozwiązania); |  |
| ·         Możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta; |  |
| ·         Możliwość tworzenia ról administratorskich z różnym poziomem uprawnień np. oddzielna rola |  |
| pozwalająca na aktualizację oprogramowania układowego. |  |
| ·         Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów; |  |
| ·         Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCIe i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych. |  |
| **Oprogramowanie do monitorowania:** |  |
| Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: |  |
| ·         Monitoring: |  |
| o   ilość podłączonych oraz rozłączonych systemów |  |
| o   stan podłączonych urządzeń |  |
| o   informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów |  |
| o   Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia |  |
| o   informacje o statusie gwarancji dla poszczególnych urządzeń |  |
| o   informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń |  |
| o   informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. |  |
| o   Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych |  |
| o   Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. |  |
| o   Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. |  |
| o   Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. |  |
| o   Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. |  |
| o   Monitoring parametrów serwerów z informacją o minimum: |  |
| §  Obciążeniu procesora |  |
| §  Zużyciu pamięci RAM |  |
| §  Temperaturze procesorów |  |
| §  Temperaturze powietrza wlotowego |  |
| §  Zużyciu prądu |  |
| §  Zmianach w fizycznej konfiguracji serwera |  |
| §  Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. |  |
| o   Monitoring parametrów pamięci masowych z informacją o minimum: |  |
| §  Opóźnieniach |  |
| §  IOPS |  |
| §  Przepustowości |  |
| §  Utylizacji kontrolerów |  |
| §  Pojemność całkowita i dostępna |  |
| §  Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. |  |
| §  Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. |  |
| §  Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata |  |
| §  Informacje o poziomie redukcji danych |  |
| §  Informacje o statusie replikacji oraz snapshotów |  |
| o   Monitoring parametrów przełączników sieciowych z informacją o minimum: |  |
| §  Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny |  |
| §  Stanie komponentów: zasilacze, wentylatory |  |
| §  Podłączonych hostach |  |
| §  Ilości i statusu portów |  |
| §  Utylizacji procesora |  |
| §  Utylizacji poszczególnych portów |  |
| §  Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. |  |
| ·         Aktualizacja firmware |  |
| o   możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania |  |
| o   możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania |  |
| o   możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania |  |
| o   możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania |  |
| o   możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania |  |
| ·         Raporty |  |
| o   Możliwość generowania raportów dla serwerów zawierających informację o: |  |
| §  Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej |  |
| §  Średnim obciążeniu: procesorów, pamięci RAM, IO, |  |
| o   Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: |  |
| §  Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji |  |
| o   Generowanie raportów do plików CSV i PDF |  |
| ·         Cyberbezpieczeństwo |  |
| o   Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. |  |
| o   Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. |  |
| o   Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. |  |
| o   Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. |  |
| ·         Wspierane urządzenia |  |
| o   Urządzenie Producenta dostarczane w ramach postępowania |  |
| o   Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) |  |
| ·         Wirtualny asystent |  |
| o   Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; |  |
| ·         Możliwość rozszerzenia funkcjonalności |  |
| o   Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. |  |
| ·         Inne |  |
| Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android |  |
| **Wirtualny asystent i aplikacje mobilne:** |  |
| Algorytmy GenAI, dostęp do bazy wiedzy, obsługa alertów i konfiguracji |  |
| iOS/Android, zarządzanie serwerem, dostęp BLE/WiFi, szyfrowanie danych |  |
| **Moduł BLE/WiFi:** |  |
| Szyfrowana komunikacja TLS 1.2, ograniczony zasięg, aktywacja przez administratora |  |
| Wymiana danych możliwa tylko po lokalnym potwierdzeniu |  |
| **Certyfikaty:** |  |
| ISO9001:2015, ISO50001, ISO14001, CE, WEEE, Epeat Silver 2019+ lub równoważne |  |
| Certified for Windows Server 2019/2022 |  |
| **Gwarancja i serwis:** |  |
| 3 lata, 24/7/365, zgłoszenia online i telefoniczne |  |
| NBD (następny dzień roboczy), dysk uszkodzony pozostaje u Zamawiającego |  |
| Oświadczenie o serwisie przez Producenta lub Partnera |  |
| **Portal wsparcia produktu:** |  |
| Personalizowany panel w chmurze, planowanie IT, raportowanie stanu sprzętu |  |
| **Aplikacja do zarządzania wsparciem:** |  |
| Automatyczne zgłoszenia, aktualizacje firmware, integracja z systemem producenta |  |
| Pełna historia aktualizacji, możliwość eksportu raportów, działania z poziomu konsoli zarządzającej |  |

|  |  |
| --- | --- |
| **VI. System centralnego zarządzania bezpieczeństwem SIEM** | |
| **1. Opis ogólny przedmiotu zamówienia** |  |
| Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja oraz szkolenie użytkowników w zakresie nowoczesnego systemu **Security Information and Event Management (SIEM)**, spełniającego wszystkie wymagania funkcjonalne, techniczne i organizacyjne wymienione w niniejszym dokumencie. System ma zapewnić centralne gromadzenie, analizę i korelację zdarzeń bezpieczeństwa, budowę scenariuszy reakcji oraz pełny audyt aktywności, przy zachowaniu neutralności technologicznej.  **WYMAGANA ILOŚĆ: 1** |  |
| **a. Oferowane rozwiązanie** |  |
| **b. Oferowana ilość** |  |
| **2. Szczegółowa specyfikacja wymagań** |  |
| **2.1 Architektura i baza danych** |  |
| 1. System oparty o **nierelacyjną bazę danych typu NoSQL**. |  |
| 2. Środowisko oparte o **Linux**. |  |
| 3. Centralne zbieranie i zarządzanie logami w trybie near‑real‑time. |  |
| 4. Możliwość instalacji **niezależnych instancji** w oddziałach, z centralnym dostępem. |  |
| 5. Instancje działają autonomicznie w razie utraty łączności. |  |
| 6. Wydajność: **≥ 1 000 EPS lub ≥ 20 GB logów/dobę**. |  |
| 7. Retencja danych: **≥ 365 dni**. |  |
| 8. Licencja bez limitu zarejestrowanych lub jednoczesnych użytkowników. |  |
| 9. Rozbudowa bez wyłączeń/restartu (skalowanie horyzontalne). |  |
| 10. Podział ról na osobne komponenty: **Agregacja, Prezentacja, Retencja**; dynamiczne dołączanie nowych węzłów bez restartu. |  |
| 11. Wysoka dostępność dla warstw Agregacji i Retencji. |  |
| 12. Buforowanie danych min. **2 dni** przy awarii komponentu, z auto‑uzupełnieniem po odzyskaniu. |  |
| 13. Szyfrowanie TLS ≥ 1.2 między komponentami; TLS ≥ 1.3 do przeglądarki. |  |
| **2.2 Interfejs i bezpieczeństwo aplikacji** |  |
| 14. GUI dostępne w Firefox, Chrome, IE; język PL lub EN. |  |
| 15. Zgodność z **OWASP ASVS v4.0 L1** i OWASP TOP 10. |  |
| 16. Uwierzytelnienie: hasło lub certyfikat + integracja **AD, LDAP, Radius**, SSO. |  |
| 17. Hasła AD bind przechowywane w formie zaszyfrowanej. |  |
| 18. Zarządzanie timeoutem sesji. |  |
| 19. Widok zarządzania użytkownikami/rolami; obiekty (wyszukania, dashboardy) z uprawnieniami read‑only / full; niewidoczne bez prawa. |  |
| 20. Pełny audyt logowań, operacji, zapytań, zmian uprawnień; regulowana szczegółowość. |  |
| 21. Narzędzie producenta do monitoringu wydajności systemu (wliczone we wsparcie). |  |
| 22. Tryb **multitenant**. |  |
| **2.3 Parsowanie i wejście danych** |  |
| 23. Tworzenie parserów z GUI; predefiniowany zestaw parserów. |  |
| 24. Obsługa formatów: Syslog, WEF, Flat file, Event Log, WMI, SNMP trap, XML, JSON, JDBC/ODBC, CSV, Email + możliwość dodania nowych. |  |
| 25. Zbieranie logów z chmur **AWS, Azure**. |  |
| 26. Widok surowego logu (RAW). |  |
| 27. Metody agentowe i bezagentowe. |  |
| 28. Definiowanie parserów REGEX / JSON / XML; warunkowe parsowanie; anonimizacja; wzbogacanie pól; operacje matematyczne. |  |
| 29. Obsługa logów jedno‑ i wieloliniowych; normalizacja timestampów. |  |
| 30. Bad IP Reputation (bazy producenta) + geolokalizacja IP. |  |
| 31. Ryzyko czasowe: przyjęcie burstu +30 % bez dodat. zasobów/licencji. |  |
| **2.4 Korelacja i analityka** |  |
| 32. Min. **700 predefiniowanych reguł korelacyjnych**. |  |
| 33. Korelacja real‑time; tworzenie/edycja reguł i algorytmów z GUI i API. |  |
| 34. Typy reguł: match, blacklist/whitelist, change, frequency, trend, absence, novelties, sequence itd. |  |
| 35. Okna czasowe konfigurowalne; zapytania po pełnej historii. |  |
| 36. Integracja z NetFlow, skanerami podatności; korelacja trans‑źródłowa. |  |
| 37. Mechanizm **MITRE ATT&CK** + import IoC (MISP). |  |
| 38. Playbooki SOAR z symulacją, automatyczne podpowiedzi; akcje automatyczne na systemach. |  |
| 39. Wbudowany ticketing + integracja mail/SMS/chat; status/owner/priority. |  |
| 40. File Integrity Monitoring, CIS Benchmark compliance, rootkit scan, OpenSCAP tracking, built‑in vulnerability scan (Linux/Windows). |  |
| 41. Modele prognostyczne (ML) dla anomalii / predykcji. |  |
| **2.5 Wizualizacja i raportowanie** |  |
| 42. Dash‑, list‑, raw‑ i graph‑view; mapa połączeń IP; wizualizacja pól tekstowych/liczbowych. |  |
| 43. Eksport zdarzeń/incydentów do CSV & HTML. |  |
| 44. Raporty ad‑hoc i z harmonogramu; format **PDF, JPEG** z logo i komentarzami. |  |
| 45. Gotowe wizualizacje i polityki GDPR, PCI‑DSS, NIST. |  |
| 46. Generowanie raportów zgodności (SOX, HIPAA, UODO, ISO 27001, GDPR, NIS, PCI‑DSS) + custom. |  |
| **2.6 Szkolenia (1 voucher)** |  |
| 47. Zdalne szkolenie PL, certyfikowany instruktor producenta, materiały PL/EN. |  |
| **2.7 Wdrożenie** |  |
| 48. Analiza przedwdrożeniowa + projekt techniczny i harmonogram. |  |
| 49. Instalacja, konfiguracja, podłączenie wskazanych źródeł, implementacja parserów/dash/reguł (jeśli brak predef). |  |
| 50. Prezentacja listy reguł/dash do akceptacji. |  |
| 51. Scenariusze testowe wydajności i poprawności – akceptacja Zamawiającego. |  |
| **3. Gwarancja i wsparcie** |  |
| Licencje wieczyste + community support 1 rok. |  |
| Bez limitu urządzeń‑źródeł logów. |  |
| Wsparcie vendor: portal, e‑mail, telefon; obejmuje moduł wydajności. |  |

|  |  |  |
| --- | --- | --- |
| **VII. Zasilacz awaryjny klasy UPS** | | |
| **1. Opis ogólny przedmiotu zamówienia** |  |  |
| Przedmiotem zamówienia jest dostawa, instalacja i konfiguracja zasilacza awaryjnego klasy UPS (Uninterruptible Power Supply) typu **Rack/Tower 3 kVA / 3 kW** wraz z niezbędnym oprogramowaniem zarządzającym oraz akcesoriami montażowymi. UPS ma zapewniać nieprzerwane zasilanie krytycznych urządzeń IT Zamawiającego oraz możliwość rozbudowy o zewnętrzny moduł bateryjny.  **WYMAGANA ILOŚĆ: 1** | |  |
| **a. Oferowane rozwiązanie** | |  |
| **b. Oferowana ilość** | |  |
| **2. Szczegółowa specyfikacja techniczna** |  |  |
| *(wszystkie parametry są wymaganiami minimalnymi — oznaczenie „min.” dotyczy wartości granicznych)* | |  |
| **2.1 Parametry mocy** | |  |
| **Parametr** | Wymaganie |  |
| Moc wyjściowa (pozorna) | min. 3 000 VA |  |
| Moc wyjściowa (czynna) | min. 3 000 W |  |
| **2.2 Dane ogólne i środowiskowe** | |  |
| Parametr | Wymaganie |  |
| Topologia | VI (line‑interactive) |  |
| Typ obudowy | Rack / Tower |  |
| Chłodzenie | Wymuszone — wewnętrzne wentylatory |  |
| **2.3 Wejście AC** | |  |
| Parametr | Wymaganie |  |
| Napięcie znamionowe | 230 V AC |  |
| Zakres napięcia | 178 – 281 V AC ± 2 % |  |
| Częstotliwość znamionowa | 50 Hz |  |
| Zakres częstotliwości | 45 – 55 Hz ± 1 Hz |  |
| Progi przełączania (sieć → UPS) | 178 – 281 V AC ± 2 % |  |
| **2.4 Wyjście AC** | |  |
| Parametr | Wymaganie |  |
| Napięcie znamionowe | 230 V AC |  |
| Zakres napięcia — praca sieciowa | 195 – 253 V AC ± 2 % |  |
| Zakres napięcia — praca bateryjna | 230 V AC ± 5 % |  |
| AVR | ± 10 % |  |
| Kształt napięcia | Sinusoidalny (bateryjna) / jak na wejściu (sieć) |  |
| Częstotliwość wyjściowa | 50 Hz |  |
| Filtracja | Filtr RFI/EMI + warystor |  |
| Progi przełączania (UPS → sieć) | 183 – 276 V AC ± 2 % |  |
| Czas przełączenia na baterię | < 3 ms |  |
| Czas powrotu na sieć | 0 ms |  |
| Przeciążalność | > 105 % przez 15 s (auto‑wyłączenie) |  |
| **2.5 Akumulatory i czasy podtrzymania** | |  |
| Parametr | Wymaganie |  |
| Akumulatory wewnętrzne | min. 8 × 12 V / 7 Ah VRLA |  |
| Możliwość podłączenia zewn. modułu bateryjnego | min. 1 szt. |  |
| Czas podtrzymania (load = 2,5 kW, tylko UPS) | min. 5 min |  |
| Czas podtrzymania (UPS + 1 × moduł bat.) | min. 14 min |  |
| Czas ładowania do 90 % (80 % obc.) | ≤ 4 h |  |
| **2.6 Parametry mechaniczne** | |  |
| Parametr | Wymaganie |  |
| Wymiary (Rack) | ≤ 132 × 445 × 630 mm (W × S × G) |  |
| Masa | ≤ 45 kg |  |
| **2.7 Zabezpieczenia** | |  |
| Obszar | Wymaganie |  |
| Wejście AC | Bezpiecznik automatyczny 16 A / 250 V |  |
| Wyjście AC | Elektroniczne — przeciwzwarciowe i przeciążeniowe |  |
| Wejście DC (wewn. bat.) | Zabezpieczenie nadprądowe |  |
| DC (zewn. moduł) | Zabezpieczenie nadprądowe |  |
| **2.8 Wyposażenie i funkcje dodatkowe** | |  |
| Element | Wymaganie |  |
| Gniazda wyjściowe | ≥ 3 × IEC 320 C13 (10 A) — sterowalne |  |
| Sygnalizacja | Akustyczno‑optyczna + graficzny wyświetlacz LCD |  |
| Interfejsy komunikacyjne | USB HID, SNMP/HTTP |  |
| Slot rozszerzeń | ≥ 1 wolne gniazdo |  |
| Wsporniki do RACK | w zestawie |  |
| Oprogramowanie zarządzające | Narzędzie producenta UPS (monitoring, shutdown) |  |
| Aktualizacja firmware przez użytkownika | wymagana |  |
| Konfig. min. stopnia naładowania przed włączeniem | wymagana |  |
| **2.9 Standardy** | |  |
| Dokument | Wymaganie |  |
| Deklaracja | CE |  |
| Normy | PN‑EN 62040‑1:2009, PN‑EN 62040‑2:2008 lub równoważne |  |
| **2.10 Gwarancja i serwis** | |  |
| Element | Wymaganie |  |
| Gwarancja elektronika | min. 36 mies. |  |
| Gwarancja akumulatory | min. 24 mies. |  |
| Serwis | Autoryzowany serwis producenta |  |
| **4. Dokumenty i oświadczenia** | |  |
| 1. Deklaracja zgodności CE. | |  |

|  |  |
| --- | --- |
| **VIII. Urządzenie klasy firewall** | |
| **1. Opis ogólny przedmiotu zamówienia** |  |
| Przedmiotem zamówienia jest dostawa urządzenia klasy firewall z funkcjami zabezpieczeń sieciowych, obejmujących ochronę przed włamaniami (IPS), kontrolę ruchu, filtrowanie treści, VPN, uwierzytelnianie użytkowników oraz administrację ruchem i urządzeniem. Rozwiązanie ma zapewniać kompleksowe bezpieczeństwo infrastruktury IT oraz spełniać wymagania techniczne wyszczególnione poniżej.  **WYMAGANA ILOŚĆ: 1** |  |
| **a. Oferowane rozwiązanie** |  |
| **b. Oferowana ilość** |  |
| **2. Opis przedmiotowy** |  |
| Wszystkie poniższe wymagania muszą być spełnione. Wskazane funkcjonalności nie mogą być realizowane przy użyciu konkretnych produktów, lecz poprzez rozwiązania równoważne spełniające poniższe warunki techniczne: |  |
| **Obsługa sieci** |  |
| 1. Obsługa IPv4 i IPv6 w zakresie konfiguracji adresów, routingu, firewalla, IPS, DHCP. |  |
| **Zapora korporacyjna (Firewall)** |  |
| Firewall typu Stateful Inspection, translacje NAT/PAT, tryb router/bridge/hybrydowy, reguły oparte o interfejsy, adresy IP, reputację hostów, użytkowników LDAP, harmonogramy, geolokalizację; min. 10 zestawów reguł, analizator spójności reguł, uwierzytelnienie LDAP, RADIUS, Kerberos, routing dla pojedynczych reguł, harmonogramy bezpieczeństwa. |  |
| **IPS – system zapobiegania włamaniom** |  |
| IPS w jądrze systemu, analiza heurystyczna, sygnaturowa, ochrona przed min. 10 000 zagrożeń, możliwość tworzenia własnych sygnatur, inspekcja SSL, wybór trybu pracy (IPS, IDS, Firewall), ochrona przed SQLi, XSS, aktualizacje sygnatur, analiza protokołów przemysłowych. |  |
| **Traffic shaping** |  |
| Priorytetyzacja ruchu, kontrola pasma wg użytkownika, IP, DSCP, aplikacji; tworzenie kolejek monitorujących. |  |
| **Ochrona antywirusowa** |  |
| Możliwość rozbudowy o AV od zewnętrznego, europejskiego dostawcy; konfiguracja reakcji, maks. wielkość pliku, komunikaty dla POP3/SMTP/FTP. |  |
| **Ochrona antyspamowa** |  |
| Filtracja poczty oparta o białe/czarne listy, DNS RBL, heurystykę; modyfikowalna lista RBL, nagłówki zgodne ze Spamassassin. |  |
| **VPN** |  |
| Obsługa VPN client-to-site, site-to-site, typy PPTP/IPSec/SSL, tryb tunelu, captive portal, VPN failover, wsparcie XAuth, Hub ‘n’ Spoke, IPSec policy/route based. |  |
| **Filtr dostępu WWW** |  |
| Filtr URL (min. 50 kategorii), możliwość tworzenia własnych, przypisywanie akcji, komunikaty HTML, zmienne środowiskowe, obsługa HTTPS, filtrowanie MIME, whitelist HTTPS, SafeSearch. |  |
| **Uwierzytelnianie** |  |
| LDAP lokalny/zewnętrzny, AD, min. 5 baz LDAP, captive portal SSL, Radius, Kerberos, autoryzacja bez agenta, zgodność z VDI (Citrix, RDS), 2FA (TOTP), uwierzytelnianie dla SSL VPN, IPSec, GUI, SSH, ZTNA. |  |
| **Administracja łączami** |  |
| Load balancing, failover, SD-WAN, SLA (jitter, opóźnienia, utrata pakietów), monitorowanie ICMP/TCP. |  |
| **Routing** |  |
| Routing statyczny i dynamiczny (RIPv2, OSPF, BGP), Policy Based Routing, obiekty typu blackhole. |  |
| **Administracja urządzeniem** |  |
| Polski GUI, zarządzanie przez przeglądarkę i SSH, role administracyjne, centralne zarządzanie, syslog/IPFIX, eksport/backup konfiguracji, anonimizacja logów, aktualizacja offline, narzędzia diagnostyczne (ping, traceroute, nslookup), przechwytywanie pakietów, definicje polityk haseł, script recording. |  |
| **Raportowanie** |  |
| System raportowania bez licencji, predefiniowane raporty (WEB, IPS, AV, SPAM), min. 25 raportów, eksport CSV, edycja z poziomu raportu, SNMP v1/2/3, monitoring w GUI i SSH. |  |
| **Pozostałe funkcje** |  |
| DHCP (dynamiczne i statyczne), relay, DNS proxy, wsparcie VLAN (802.1Q), RSTP/MSTP, OpenAPI, redundantne partycje firmware, LACP. |  |
| **Gwarancja i serwis** |  |
| Gwarancja 12 miesięcy na sprzęt i licencje, wsparcie mailowe i przez portal. |  |
| **Parametry sprzętowe** |  |
| Brak dysku twardego, pamięć flash, port microSD, min. 8 portów 2.5Gbps, min. 1 port światłowodowy, obsługa modemów 3G/4G, przepustowość: Firewall 8Gbps, IPS 4Gbps, AV 1Gbps, VPN AES 2Gbps, min. 100 tuneli IPSec i SSL VPN, min. 400 000 sesji, klastry HA, brak limitu użytkowników, reguły filtrowania min. 8192, trasy routingu (statyczne 512, dynamiczne 10 000), redundantne zasilanie, moduł TPM. |  |