

Załącznik nr 1 do zapytania ofertowego nr I.271.10.2025

Dotyczy: Dostawa oprogramowania do monitorowania i zarządzania zasobami IT w ramach Konkursu Grantowego „Cyberbezpieczny Samorząd”

Szczegółowy opis przedmiotu zamówienia**1. Architektura / budowa**

1.1. System musi umożliwić bezproblemową i stabilną obsługę co najmniej 50 Klientów jednocześnie.

1.2. Architektura / budowa:

1.2.1. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przysyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.

1.2.2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej).

1.2.3. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach.

1.2.4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.

1.2.5. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej.

1.3. Konfiguracja Architektury:

1.3.1. Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie.

1.3.2. System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem.

2. Wymagania systemowe

2.1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet, FireFox, Chrome, Opera).

2.2. Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022/2025, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa.

2.2.1. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera wersja 63.0.3368.94, Chrome wersja 77.0.3865.90, FireFox wersja 69.0.2, Microsoft Edge.

2.3. Serwer musi działać na systemach 64 bitowych: Windows Server 2016/2019/2022/2025, Windows 7/8/8.1/10/11.

2.4. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2016/2019/2022/2025, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 8+.

2.5. Baza danych musi działać na silniku Microsoft SQL Server 2008/2014/2016/2017/2019/2022/2025 w wersji 64 bitowych, bezpłatnych (np. Microsoft SQL Server Express Edition).

2.6. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.

3. Interfejsy

- 3.1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.
- 3.2. System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL, Oracle
- 3.3. System zapewnia integrację z modelem LLM.

4. Funkcjonalności systemu zarządzania infrastrukturą IT

4.1. Funkcjonalność Klienta

- 4.1.1. System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkowniku.

4.2. Funkcjonalność konsoli administracyjnej.

- 4.2.1. Konsola administracyjna musi być wielojęzyczna (polski i angielski) i oferować intuicyjny interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie). Musi także zawierać co najmniej 140 różnorodnych dashboardów, w tym dashboardy użytkownika, prezentujące parametry infrastruktury, sieci oraz bezpieczeństwa. Użytkownicy powinni mieć możliwość samodzielnego konfigurowania dashboardów użytkownika, a dashboardy sieciowe i bezpieczeństwa muszą zawierać szczegółowe widżety z informacjami o stanie usług i bezpieczeństwie.

- 4.2.2. W konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem.

- 4.2.3. Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń.

4.3. Funkcjonalność panelu pracownika

- 4.3.1. Panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora.

4.4. Zarządzanie licencjami

- 4.4.1. System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania.

4.5. Wzorce aplikacji i pakietów

- 4.5.1. System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office.

4.6. Zarządzanie podatnościami

- 4.6.1. System musi posiadać zdolności do bieżąco i automatycznego identyfikowania podatności w zainstalowanym oprogramowaniu.
- 4.6.2. Wykrywanie podatności musi być oparte o analizę wzorców zainstalowanego oprogramowania i porównanie ich z globalnymi bazami podatności, takimi jak CVE (Common Vulnerabilities and Exposures).

- 4.6.3. System powinien posiadać co najmniej dwa wskaźniki umożliwiające ocenę poziomu ryzyka i priorytetyzację zagrożeń.
- 4.6.4. System musi mieć możliwość ustawiania powiadomień o wykrytych podatnościach.
- 4.6.5. System musi mieć możliwość automatycznego tworzenia incydentów w przypadku integracji systemu z systemem eHelpDesk.
- 4.6.6. Powinna istnieć funkcja raportowanie z możliwością filtrowania wg urządzenia, typu podatności lub poziomu krytyczności.
- 4.7. Inwentaryzacja sprzętu komputerowego i urządzeń.
- 4.7.1. System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich połączeń.
- 4.8. Inwentaryzacja urządzeń sieciowych.
- 4.8.1. System musi posiadać zdolności do identyfikacji i zarządzania środowiskami wirtualizacji Hyper-V i VMware oraz urządzeniami sieciowymi. Wymagane jest posiadanie skanera sieci i SNMP oraz dla środowisk wirtualizacji, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci.
- 4.9. Inwentaryzacja sprzętu.
- 4.9.1. System musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych.
- 4.10. Ochrona danych (DLP)
- 4.10.1. Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwołonymi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami.
- 4.10.2. System powinien posiadać możliwość **definiowania schematu**, w którym można określić, które aplikacje są zabronione, zalecane, dodatkowe bądź nieokreślone. Schemat oprogramowania można przypisać do dowolnej grupy komputerów. Mechanizm musi umożliwić automatyczne odinstalowanie oprogramowania, które wg zdefiniowanego schematu jest zabronione.
- 4.10.3. System musi mieć możliwość reakcji i powiadamiania o **przekroczeniu dozwolonego czasu** pracy komputera
- 4.10.4. System powinien umożliwić **wyświetlanie komunikatu na** komputerach użytkowników podczas uruchamiania stacji roboczej. Komunikaty muszą być definiowalne z poziomu konsoli administracyjnej z wykorzystaniem edytora (możliwość utworzenia tabeli, dołączenia obrazu, wstawienia linku).
- 4.10.5. **Szyfrowanie dysków wewnętrznych oraz zewnętrznych**
- 4.10.5.1. System musi obsługiwać kompleksowe szyfrowanie dysków wewnętrznych i zewnętrznych USB, z wykorzystaniem BitLocker i różnych metod szyfrowania, takich jak XTS_AES_256 i AES_128. Musi umożliwiać zdalne zarządzanie procesem szyfrowania/deszyfrowania, w tym masowe operacje na partycjach systemowych i niesystemowych, zarówno lokalnie, jak i zdalnie (poza NATem). Klucze szyfrujące są przechowywane i chronione w konsoli administracyjnej, dostępne tylko po uwierzytelnieniu administratora. Proces szyfrowania odbywa się w sposób niewidoczny dla użytkownika i nie może być przez niego przerwany, z wyjątkiem stanów hibernacji i wyłączenia systemu, po których jest automatycznie kontynuowany.
- 4.11. Zdalna administracja komputerami
- 4.11.1. System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać

technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia.

4.12. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.

4.13. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.

4.14. Zarządzanie Poprawkami i Aktualizacjami

4.14.1. System musi zapewniać ciągłe monitorowanie i identyfikację brakujących aktualizacji systemowych i komponentów infrastruktury IT, oferując funkcje rozpoznawania niezainstalowanych poprawek, ich pobierania, oraz klasyfikacji. Musi umożliwiać aktualizacje bez zakłócania pracy użytkowników, zarówno zbiorowo jak i indywidualnie, z opcją szybkiego przywrócenia poprzedniego stanu systemu poprzez odinstalowanie niechcianych poprawek. System powinien również umożliwiać pomijanie niechcianych poprawek i dostarczać szczegółowe raporty dotyczące stanu aktualizacji oraz urządzeń, które mogą wymagać restartu.

4.15. Zdalne Zarządzanie Zaporą (Firewall)

4.15.1. System musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe.

4.16. Automatyzacja

4.16.1. System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT.

4.17. Zarządzanie magazynem IT

4.17.1. System musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów.

4.18. Repozytorium

4.18.1. Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją.

4.19. Kody kreskowe

4.19.1. System musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych.

4.20. Wysyłanie wiadomości

4.20.1. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między użytkownikami a administratorem systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji. System powinien także umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać

- szkolenie pracowników za pomocą wiadomości tekstowych z możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania.
- 4.21. System musi posiadać możliwość eksportu / importu treści.
- 4.22. Monitorowanie drukarek sieciowych i wydruków
- 4.22.1. System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych.
- 4.23. Monitorowanie stron www
- 4.23.1. System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści.
- 4.24. Monitorowanie serwerów WWW
- 4.24.1. System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie.
- 4.25. Monitorowanie dziennika zdarzeń
- 4.25.1. System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii.
- 4.26. System musi umożliwiać monitorowanie komunikatów Syslog.
- 4.27. Monitorowanie pracy komputerów
- 4.27.1. System musi oferować monitorowanie pracy komputerów, w tym dat startu
- 4.27.2. i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników.
- 4.28. Monitorowanie uprawnień ACL
- 4.28.1. System musi umożliwić skanowanie i monitorowanie uprawnień ACL, oferując szczegółowe raporty, automatyczną aktualizacją danych i filtrami do zarządzania informacjami.
- 4.29. Monitorowanie sensorów
- 4.29.1. System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów.
- 4.30. Repozytorium CMDB
- 4.30.1. System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych.
- 4.31. Worktime manager
- 4.31.1. System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostępnienia w panelu pracownika.
- 4.32. Raportowanie i eksport danych
- 4.32.1. System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu.
- 4.33. System musi zapewnić interfejs API.



4.33.1. System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki.

4.34. Powiadomienia

4.34.1. System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co najmniej 30 predefiniowanych powiadomień oraz możliwość ich personalizacji.

4.35. Bezpieczeństwo

4.35.1. System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługując wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania danych.

5. Wsparcie i pomoc

5.1.1. Pomoc techniczna

5.1.1.1. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.

5.1.1.2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania.

5.1.1.3. Czas trwania usługi SLA od dnia zakupu do 30.06.2026 r.