Or.042.1.1.2024 Zał. nr 1 do SWZ

Opis przedmiotu zamówienia - aktualizacja

Zakup oprogramowania do zarządzania siecią w ramach projektu „Podniesienie poziomu cyberbezpieczeństwa w Starostwie Powiatowym w Lubaczowie"

Uwagi ogólne – Wdrożenie i wsparcie techniczne:

1. Program musi posiadać wieczystą licencję na 100 stanowisk ze wsparciem na okres przewidywany przez producenta, z zastrzeżeniem, że usługa bezpłatnego wsparcia dla oprogramowania musi obowiązywać przez minimalny okres 12 miesięcy.
2. Okres wsparcia technicznego liczony jest od dnia podpisania protokołu odbioru oprogramowania.
3. Zamówienie nie obejmuje kompleksowego wdrożenia oprogramowania. Wykonawca zobowiązany jest do dostarczenia oprogramowania oraz zapewnienia wsparcia w zakresie jego instalacji, konfiguracji i uruchomienia.
4. Wykonawca zobowiązany jest do przeprowadzenia szkolenia dla 1 osoby wskazanej przez Zamawiającego w zakresie podstawowej obsługi oprogramowania. Szkolenie może zostać przeprowadzone w formie zdalnej.
5. W ramach wsparcia Wykonawca zapewni:
   a) bezpłatny dostęp do wszelkich aktualizacji oprogramowania, wydań uzupełniających oraz poprawek programistycznych przez okres minimum 12 miesięcy;
   b) bezpłatny dostęp do telefonicznego i mailowego wsparcia technicznego dla oprogramowania przez okres 12 miesięcy w języku polskim;
   c) Wykonawca zapewni przyjmowanie zgłoszeń telefonicznych w godzinach od 8:00 do 16:00 w dni robocze;
   d) świadczenie usług Service Desk poprzez udzielanie odpowiedzi na zapytania kierowane pocztą elektroniczną lub telefonicznie przez przedstawicieli Zamawiającego pod wskazany przez Wykonawcę adres lub numer telefonu, w terminie nie dłuższym niż 1 dzień roboczy od dnia przekazania zapytania.

Specyfikacja techniczna oprogramowania

Zamawiający wymaga, aby oprogramowanie posiadało budowę modułową, składało się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Instalacje zdalnych konsoli zarządzania nie powinny podlegać limitom ani być objęte dodatkowym licencjonowaniem. Komunikacja pomiędzy Serwerem a Agentami i Konsolami musi odbywać się za pomocą szyfrowanego protokołu. Zamawiający wymaga, aby oprogramowanie umożliwiało zmianę portu komunikacyjnego wykorzystywanego przez konsolę zarządzającą.

Wymagane jest, aby moduły umożliwiały kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Oprogramowanie powinno wykorzystywać darmowy, bezpieczny, stabilny i wysoce wydajny silnik bazy danych z kodem źródłowym dostępnym na licencji open-source, a sama baza danych wymaga się aby była rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania. Oprogramowanie ma

zapewniać rozbudowany system raportowy z możliwością tworzenia własnych raportów oraz dostosowania wyglądu i przywrócenia bazowej konfiguracji raportów wbudowanych po ich edycji.

Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., muszą być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Wymagane jest grupowanie w osobnym, dedykowanym oknie, aby pozwoliło to na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.

Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, powinien być objęty kontrolą na poziomie wybranych Administratorów, a w programie winna być możliwość nadawania kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Zaleca się aby główny administrator miał możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. mógł wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów. Zamawiający wymaga, aby oprogramowanie posiadało dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta. Działania administratorów mogą być automatycznie eksportowane do zewnętrznego kolektora Syslog.

Lista kont użytkowników, w tym administratorów, musi być synchronizowana z Active Directory wraz z awatarami oraz dowolnymi atrybutami, również przez szyfrowane połączenie LDAPS. Zamawiający wymaga, aby oprogramowanie umożliwiało również tworzenie lokalnych kont użytkowników wraz z awatarami w środowiskach bez Active Directory. Wymaga się aby liczba kont użytkowników w konsoli nie była objęta limitem i nie podlegała licencjonowaniu.

Zamawiający wymaga, aby oprogramowanie umożliwiało konfigurację polityki haseł do lokalnych kont użytkowników konsoli. Polityka pozwala na określenie: minimalnej długości hasła, liter, cyfr, znaków specjalnych oraz automatycznie wymusza dostosowanie bieżących haseł do obowiązujących zasad.

MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO) POWINNO obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

- wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
- wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU)
- wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
- wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku
- wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze
- wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie
- wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny

- zablokowania mapy urządzeń przed przypadkową edycją
- serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów
- serwerów pocztowych:
  - ✓ program powinien monitorować czas logowania do serwisu odbierającego oraz czas wysyłania poczty
  - ✓ zaleca się, aby program miał możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem)
  - ✓ program powinien mieć możliwość wykonywania operacji testowych
  - ✓ program powinien mieć możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa
- monitorowania serwerów WWW i adresów URL
- cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS
- obsługi szyfrowania TLS w powiadomieniach e-mail
- obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID
- obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych
- monitoringu routerów i przełączników wg:
  - ✓ zmian stanu interfejsów sieciowych
  - ✓ ruchu sieciowego
  - ✓ podłączonych stacji roboczych – graficzna prezentacja panelu switcha
  - ✓ ruchu generowanego przez podłączone do portów stacje robocze
- serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie
- wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu
- monitorowania stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano
- zarządzania stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny
- wydajności systemów Windows:
- obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy

Zamawiający wymaga, aby oprogramowanie posiadało Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Kryteria automatycznego filtrowania dotyczyć mogą m.in. statusu Agenta, wygenerowanych alarmów, zainstalowanych aplikacji, przynależności do oddziału, serwisów sieciowych, danych z SNMP, danych z inwentaryzacji urządzenia itp. Zamawiający wymaga, aby oprogramowanie posiadało również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.

Wymagane jest również, aby oprogramowanie umożliwiało nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych

ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, wysłanie wiadomości SMS poprzez integrację z serwisem internetowym, wysłanie wiadomości przez Microsoft Teams (poprzez mechanizmy webhook i workflow) oraz Slack, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy budowane są przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. Wykonywanie akcji alarmów można skonfigurować automatycznie po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut. Dla akcji można nałożyć ograniczenie czasowe np. nie wykonuj między 8:00-16:00. Alarmy pozwalają na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. Oprogramowanie musi umożliwiać wykorzystanie w alarmowaniu skrzynek e- mail z wykorzystaniem autoryzacji OAuth 2.0

Program powinien posiadać możliwość integracji ze sprzętową bramką GSM HW-SMS-GW 3 w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP) oraz poprzez integrację z bramkami SMSEagle.

W ZAKRESIE INWENTARYZACJI wymagane jest aby program automatycznie gromadził informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:

1. Prezentował szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
2. Umożliwiał odczyt parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe.
3. Obejmował m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
4. Informuje o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.
5. Zbierał informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
6. Posiadał możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
7. Umożliwiał odczytanie numeru seryjnego (klucze licencyjne).
8. Umożliwiał automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
9. Umożliwiał przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
10. Umożliwiał utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).
11. Umożliwiał wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji powinny być logowane.

Moduł inwentaryzacji zasobów musi umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i oprogramowania, tj.:

- ✓ przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,

- ✓ przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów,
- ✓ tworzenia powiązań między zasobami a urządzeniami,
- ✓ tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
- ✓ tworzenia relacji pomiędzy zasobami,
- ✓ wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy,
- ✓ definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,
- ✓ określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
- ✓ określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,
- ✓ masową edycję atrybutów zasobów,
- ✓ definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
- ✓ importu danych z zewnętrznego źródła (.CSV),
- ✓ przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,
- ✓ kopiowanie oraz powielanie zasobów z możliwością wyboru atrybutów do powielenia,
- ✓ automatyczne nadawanie numeru inwentarzowego do powielanych zasobów,
- ✓ tworzenia powiązań między zasobami a dokumentami w relacji 1:N,
- ✓ oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,
- ✓ ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
- ✓ generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
- ✓ przygotowania wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
- ✓ konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca,
- ✓ konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,
- ✓ archiwizacji i porównywania audytów zasobów,
- ✓ tworzenia kodów kreskowych dla zasobów,
- ✓ drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,
- ✓ inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet,
- ✓ możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,

- ✓ inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),
- ✓ definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data" z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja")
- ✓ powiązania zgłoszeń w module pomocy użytkownikom z zasobami.

Wymaga się aby inwentaryzacja oprogramowania zawierała funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:

1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.
2. Informacje o aplikacjach używanych w organizacji.
3. Tworzenie własnych wzorców aplikacji.
4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.
5. Informacje o komputerach, na których aplikacja została wykryta.
6. Zarządzanie posiadanymi licencjami.
7. Wskazywanie osób odpowiedzialnych za licencję.
8. Wskazanie użytkowników licencji.
9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.
10. Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.
11. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.
12. Zarządzanie posiadanymi licencjami: raport zgodności licencji.
13. Możliwość przypisania do programów numerów seryjnych, wartości itp.

Okna audytowe mają posiadać możliwość filtrowania elementów per oddział.

W ZAKRESIE OBSŁUGI UŻYTKOWNIKÓW zamawiający wymaga, aby oprogramowanie umożliwiało monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:

- Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
- Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,
- Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,
- Informacji o edytowanych przez użytkownika dokumentach,
- Historii pracy (cykliczne zrzuty ekranowe),
- Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt),
- Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
- Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był

drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program posiadało możliwość monitorowania kosztów wydruków,

- Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.

Program ponadto powinien posiadać możliwość:

- wykrywania podejrzanej aktywności przez popularne „jigglery", mającej na celu symulowanie faktycznej pracy.
- zdefiniowania czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury.
- wyszczególnienia podejrzanej aktywności w raportach.
- wygenerowania alarmu i wykonania akcji po wykryciu podejrzanej aktywności.
- alarmowania o aktywności użytkownika poza zdefiniowanymi godzinami pracy.
- automatycznego włączenia zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności.
- blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane lub współdzielone pomiędzy grupami lub kontami.
- integracji list stron w formie plików .TXT z dowolnego adresu zewnętrznego np. CERT.
- skorzystania z wbudowanej listy stron sklasyfikowanych jako zagrożenia.
- automatycznego odświeżania list stron zintegrowanych z adresów zewnętrznych.
- blokowania ruchu na wskazanych portach TCP/IP,
- blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
- prowadzenia rejestru naruszeń blokad,
- wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady,
- przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),
- definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.

Oprócz tego wymagana jest możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.

Wymagany jest mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.

Zamawiający wymaga, aby oprogramowanie posiadało Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.

PROGRAM POWINIEN UMOŻLIWIAĆ REALIZACJĘ ZDALNEJ POMOCY UŻYTKOWNIKOM. W ramach kontroli stacji użytkownika preferowany jest podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Funkcja zdalnego dostępu oferuje również możliwość zasłonienia ekranu przed użytkownikiem w taki sposób, aby nie widział czynności wykonywanych przez administratora. Administrator w trakcie zdalnego dostępu posiada możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy oraz klawiatury dla użytkownika. Zdalne połączenie jest możliwe również do komputerów, które nie posiadają ekranów (maszyny wirtualne, komputery bez podłączonego monitora lub laptopy z zamkniętym skrzydłem matrycy). Funkcja zdalnego dostępu musi umożliwiać równoczesne podłączenie do tego samego komputera kilku administratorom. Zdalny dostęp jest automatycznie wznawiamy po utracie połączenia.

Funkcjonalność danego modułu powinna sprowadzać się do bazy zgłoszeń umożliwiającej użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal oraz przetwarzanie wiadomości e-mail, które są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Oprogramowanie powinno pozwalać na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0. Zaleca się aby moduł umożliwiał również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach") wraz z dedykowaną podstroną dla zgłoszeń sygnalistów oraz zawierał dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę. Preferowane jest umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. System powinien umożliwiać użycie pośredniego statusu „zgłoszenie rozwiązane" przed ostatecznym zamknięciem zgłoszenia.

Dany moduł ma zapewniać również komunikator (czat), który umożliwia prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i administratorami (wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów). Ponadto musi pozwalać na:

- zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej
- rozmowy również między „zwykłymi" użytkownikami
- osadzanie załączników w treści wiadomości,
- osadzanie obrazków w treści wiadomości,
- formatowanie tekstu,
- tworzenie pokojów tematycznych, rozmów grupowych
- oznaczanie kontaktów jako „ulubionych" na liście kontaktów
- uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku
- może być wyświetlany w trybie jasnym lub ciemnym

Funkcjonalność modułu musi zawierać również bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic). Zamawiający wymaga, aby oprogramowanie umożliwiało informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez

komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy. Użytkownik powinien posiadać możliwość przeglądnięcia historii odczytanych komunikatów bezpośrednio z poziomu ikony Agenta. Administrator powinien mieć możliwość tworzenia szkiców, archiwizowania, wstrzymywania i wznawiania komunikatów również wielu komunikatów równocześnie.

Preferuje się, aby dostęp do systemu zgłoszeń oraz bazy wiedzy realizowany był przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany w trybie jasnym lub ciemnym.

Funkcjonalność modułu musi umożliwiać uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika.

Wymaga się aby moduł pomocy zdalnej umożliwiał również:

- ✓ pobieranie listy użytkowników z Active Directory wraz z awatarami oraz dowolnymi atrybutami,
- ✓ wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym,
- ✓ zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,
- ✓ zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń,
- ✓ zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń,
- ✓ zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy,
- ✓ tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO,
- ✓ automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,
- ✓ definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji,
- ✓ przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii,
- ✓ powiązanie zgłoszeń z zasobami z modułu inwentaryzacji,
- ✓ wyświetlanie informacji o zasobach na liście zgłoszeń,
- ✓ wyświetlanie informacji o zasobach w metryczce zgłoszenia,
- ✓ wyświetlenie użytkownikowi dedykowanego widoku z zasobami, za które jest odpowiedzialny,
- ✓ wyświetlenie listy zgłoszeń powiązanych z zasobem,
- ✓ procesowanie zgłoszeń użytkowników z wiadomości e-mail,
- ✓ dostęp do plików źródłowych wiadomości e-mail przetworzonych na zgłoszenia,
- ✓ obsługę wielu adresów e-mail jednego użytkownika w celu przetwarzania jako zgłoszeń pochodzących od tej samej osoby,
- ✓ eksportowania listy zgłoszeń do plików CSV i XLSX,
- ✓ integrację ze wieloma skrzynkami e-mail w celu obsługi różnych kanałów zgłoszeń wraz z automatyzacjami,
- ✓ integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz

mechanizm OAuth 2.0,

- ✓ tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,
- ✓ uwzględnianie wyników zgłoszeń na podstawie wyszukiwania informacji z pól niestandardowych,
- ✓ współdzielenie pól dodatkowych pomiędzy wieloma kategoriami zgłoszeń,
- ✓ dedykowane pola dodatkowe dostępne tylko dla pracowników HelpDesk, administratorów i operatorów,
- ✓ informacje zawarte w polach dodatkowych widoczne w kolumnach widoku listy zgłoszeń,
- ✓ wykonywanie operacji na wielu zgłoszeniach równocześnie,
- ✓ dołączanie załączników do zgłoszeń,
- ✓ usuwanie zamkniętych zgłoszeń,
- ✓ rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,
- ✓ szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,
- ✓ wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,
- ✓ zrzuty ekranowe (podgląd pulpitu),
- ✓ zdalną modyfikację rejestrów,
- ✓ dystrybucję oprogramowania przez Agenty,
- ✓ definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku z Aplikacjami,
- ✓ przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników,
- ✓ dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),
- ✓ zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,
- ✓ możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,
- ✓ możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy,
- ✓ planowanie nieobecności pracowników helpdesk,
- ✓ obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem,
- ✓ generowanie raportów obsługi helpdesk,
- ✓ zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu),
- ✓ zdalne wykonywanie poleceń PowerShell, również równocześnie na wielu stacjach,
- ✓ zdalne wykonywanie skryptów PowerShell, również równocześnie na wielu stacjach,
- ✓ podpowiedzi składni poleceń PowerShell,
- ✓ zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),
- ✓ wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików.

Wymaga się, aby oprogramowanie zapewniało funkcjonalność ochrony danych przed wyciekiem (DLP), w szczególności poprzez możliwość blokowania urządzeń i nośników danych, oraz funkcjonalności:

1. Blokowanie urządzeń i nośników danych.

   Program powinien mieć możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.
2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.
3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
4. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.
5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
6. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.
7. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.
8. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker.
9. Tworzenie list (map) komputerów, które zostały już zaszyfrowane, lub jeszcze nie zostały zaszyfrowane.
10. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu.
11. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.
12. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender.
13. Funkcje wspierające bezpieczeństwo systemu: - monitorowanie stanu modułu TPM.

Zarządzanie prawami dostępu do urządzeń:

1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane.
3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.
4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.
5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.

Audyt operacji na plikach na urządzeniach przenośnych:

1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
2. Podłączenie/odłączenie urządzenia przenośnego.

Program powinien umożliwiać monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika oraz mieć możliwość definiowania reguł monitorowanych folderów w postaci list.

Wymaga się funkcjonalności monitorowania operacji na plikach na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.)

Program musi posiadać integrację z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych, a także przydzielanie uprawnień również do kont użytkowników lokalnych. Zaznacza się również, że program za zapewniać prowadzenie rejestru naruszeń blokad podłączanych nośników.

ZAMAWIAJĄCY WYMAGA, ABY PROGRAM WSPIERAŁ ZARZĄDZANIE CZASEM I ANALIZOWANIE AKTYWNOŚCI UŻYTKOWNIKÓW poprzez dostarczenie informacji o czasie poświęconym na pracę w poszczególnych aplikacjach i na stronach WWW z dowolnie wybranego okresu. Każdy pracownik organizacji może oznaczyć sesję aktywności jako czas prywatny gdy wykonuje czynności prywatne na sprzęcie firmowym. Może również uzyskać dostęp do własnych wskaźników aktywności w czasie pracy. Menedżerowie oraz przełożeni mogą uzyskać automatyczny dostęp do aktywności podwładnych w zespołach i indywidualnie oraz mogą przeanalizować aktywności w danym okresie i zyskać pełny obraz obszarów wymagających największego zaangażowania. Pracownik powinien móc przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje. Zastosowane reguły mają pozwalać zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania. Dostęp powinien być realizowany przez przeglądarkę internetową a strona wyświetlana w trybie jasnym lub ciemnym. Wymaga się aby były dostępne następujące dane:

1. Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu.
2. Statystyki aktywności grupy i jej członków widoczne dla menedżera grupy.
3. Statystyki aktywności podwładnych widoczne dla przełożonego.
4. Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem. Wspierane przeglądarki: Microsoft Edge, Mozilla Firefox, Google Chrome, Opera.
5. Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu.
6. Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników.
7. Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych.
8. Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne.
9. Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy.
10. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie).
11. Wskaźnik czasu poświęconego na aktywność produktywną.
12. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail.
13. Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka - predefiniowana lista kategorii z możliwością edycji.
14. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów.

Zamawiający wymaga, aby program posiadał portal informacyjny w formie platformy WWW

Oprogramowanie musi posiadać również obszar funkcjonalny w formie platformy WWW, który pozwala na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami, których nazwy można zmieniać wg potrzeb. Zawartość każdego z paneli informacyjnych powinna być automatycznie odświeżana oraz może być:

- ✓ Udostępniana w trybie „tylko do odczytu" z zabezpieczeniem tokenem.
- ✓ Wyświetlana w trybie jasnym lub ciemnym (nocnym).

Oprogramowanie ma umożliwiać zarządzanie uprawnieniami administratorów do funkcjonalności portalu informacyjnego.

Widgety powinny prezentować dane ze wszystkich modułów funkcjonalnych oprogramowania:

- ✓ Mapa sieci,
- ✓ Liczniki wydajności, Alarmy (wraz z filtrowaniem) oraz odpowiedzi serwisów TCP/IP, Ostatnie urządzenia w sieci,
- ✓ Zmiany w konfiguracji sprzętowej urządzeń z Agentami, Zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, Alarmy dla Zasobów,
- ✓ Statystyki z obszaru wydruków, Statystki użycia aplikacji, Użycie łącza, Aktywność WWW, naruszenia reguł blokad,
- ✓ Statystyki z obsługi zgłoszeń, Lista najnowszych nierozwiązanych zgłoszeń, Lista najstarszych nierozwiązanych zgłoszeń, Zgłoszenia z naruszonym SLA, Zgłoszenia, których SLA wkrótce wygaśnie,
- ✓ Ostatnio podłączone nośniki zewnętrzne, Ostatnie operacje na plikach (wraz z filtrowaniem), informacje o stanie Bitlocker, Windows Defender, Windows Firewall, naruszenia reguł dostępu do nośników danych,
- ✓ Produktywność dla grupy, Statystyki czasu nieproduktywnego.

Wymaga się aby program był zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej na której pracuje.