

Załącznik nr 1 do Zapytania ofertowego

Nr postępowania: **ZP.271.2.36.2024****OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)****I. PRZEDMIOT ZAMÓWIENIA:**

1. Nazwa: Zakup i dostawa oprogramowania do zarządzania zabezpieczeniami, monitorowania urządzeń sieciowych, zarządzania zasobami IT i użytkownikami oraz bezpieczeństwa i ochrony danych.

2. Szczegółowy opis przedmiotu zamówienia:

Oprogramowanie powinno posiadać budowę modułową, składać się z serwera zarządzającego, zdalnych konsol oraz Agentów. Moduły powinny umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych. Program musi wykorzystywać darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source (PostgreSQL w wersji 12), dzięki czemu nie powinien być objęty limitem ilości danych; baza danych powinna być rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania. Instalacja Serwera oraz Konsol zarządzających powinna wymagać 64-bitowego systemu operacyjnego Windows. 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. Powinny one być również grupowane w osobnym, dedykowanym oknie. Pozwoli 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 – w programie można nadawać kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator powinien mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną, np. wyłączenie możliwości zdalnej deinstalacji Agentów, ograniczenie dostępu do Opcji programu oraz logów działań innych administratorów. Działania administratorów powinny być logowane. Oznacza to, że program musi posiadać 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.

Typ licencji: licencja na czas nieokreślony/wieczysta

Licencje (ilość: 55 sztuk)

A. Monitorowanie infrastruktury sieciowej (bez użycia Agenta):

Monitorowanie powinno obejmować takie urządzenia jak: serwery (Windows, Linux, Unix, Mac), routery, przełączniki, urządzenia VoIP oraz firewall.

Program musi posiadać 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. Program powinien posiadać również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.

Program powinien umożliwiać również nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowania alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitu, wysłanie wiadomości e-mail, wysłanie SMS, wysłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl, wysłanie wiadomości przez Microsoft Teams oraz Slack, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy muszą być budowane 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 powinny pozwalać 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 mieć możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).

Monitorowanie infrastruktury sieciowej powinno odbywać się 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 umożliwiającą 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;
- serwerów pocztowych:
 - * program powinien monitorować czas logowania do serwisu odbierającego oraz czas wysyłania poczty,
 - * program musi mieć 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 znajdują się poza zakresem),
 - * program musi mieć możliwość wykonywania operacji testowych,
 - * program musi 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 SSL/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;
- wydajności systemów Windows: obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.

B. Automatyczne gromadzenie informacji o sprzęcie i oprogramowaniu na stacjach roboczych (inwentaryzacja) oraz:

- prezentacja szczegółów dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart, itp.;
 - prezentacja m.in.: zestawienia posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade;
 - informacja o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji;
 - zbieranie informacji w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP, itd.;
 - możliwość wysyłania powiadomienia, np. e-mailem w przypadku zainstalowania programu lub jakiegokolwiek zmiany konfiguracji sprzętowej komputera;
 - możliwość odczytania numeru seryjnego (klucze licencyjne);
 - możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych;
 - możliwość przeglądu informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań, itp.;
 - 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);
 - możliwość wymiany plików do i z stacji roboczej poprzez funkcję menedżera plików.
- Działania administratorów wykonywane w tej funkcji powinny być logowane.

Gromadzenie informacji o sprzęcie i oprogramowaniu w celu prowadzenia bazy ewidencji majątku IT – w zakresie:

- przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji;
- tworzenia powiązań między zasobami a urządzeniami;
- tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych;
- wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy;
- definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania powinna istnieć 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;
- 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.;
- tworzenia powiązań między zasobami a dokumentami w relacji 1:N;
- oznaczania statusów zasobów, np. w użyciu, w naprawie, zutilizowany, 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;
- przygotowanie 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”).

Inwentaryzacja oprogramowania powinna zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:

- skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów zip.;
- informacje o aplikacjach używanych w organizacji;
- tworzenie własnych wzorców aplikacji;
- tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe, itp.;
- informacje o komputerach, na których aplikacja została wykryta;
- zarządzanie posiadanymi licencjami;
- wskazywanie osób odpowiedzialnych za licencję;
- wskazanie użytkowników licencji;
- tworzenie powiązań między licencjami a dokumentami w relacji 1:N;

- 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;
- łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili powinna istnieć możliwość wykonania aktualnych raportów audytowych;
- zarządzanie posiadanymi licencjami: raport zgodności licencji;
- możliwość przypisania do programów numerów seryjnych, wartości, itp.

C. 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 z 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 (liczba odwiedzin stron z nagłówkami, liczbą i czasem 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 powinien mieć możliwość monitorowania kosztów wydruków;
- nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.

Dodatkowe możliwości:

Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie. Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji powinny być tworzone dla użytkownika lub grupy użytkowników i być kopiowane pomiędzy grupami lub kontami. Program powinien posiadać Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych, w szczególności:

- 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 powinny być tworzone dla użytkownika lub grupy użytkowników i być kopiowane pomiędzy grupami lub kontami;
- blokowania ruchu na wskazanych portach TCP/IP;
- blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem;
- wysyłania powiadomień, gdy użytkownik: odwiedzi stronę z określonej grupy domen; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia;
- 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.

D. Ochrona danych przed wyciekiem powinna być realizowana poprzez:

- 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;
- blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskiek;
- blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA;
- blokowanie urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz, itp.) mogą być podłączone;
- alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezauważalnych;
- funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender;
- funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker;
- funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu;
- funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.

Zarządzanie prawami dostępu do urządzeń:

- definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików;
- autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków, itp.;
- urządzenia prywatne powinny być blokowane;
- całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników;

- centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci;
- możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.

Audyt operacji na plikach na urządzeniach przenośnych:

Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.
Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych:

- zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych;
- podłączenie/odłączenie urządzenia przenośnego.

3. Termin realizacji (dostawy) przedmiotu zamówienia: 30 dni od dnia udzielenia zamówienia (od dnia wystawienia zlecenia).

- 4. Zamawiający nie dopuszcza składania ofert częściowych.
- 5. Zamawiający nie dopuszcza składania ofert wariantowych.
- 6. Przedmiot zamówienia jest realizowany w związku z:

Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC)

Priorytet II: Zaawansowane usługi cyfrowe

Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

**konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd”
o numerze FERC.02.02-CS.01-001/23.**

II. WYMAGANE DOKUMENTY, KTÓRE ZOBOWIĄZANY BĘDZIE ZŁOŻYĆ WYKONAWCA:

- 1) Formularz oferty (wg załączonego wzoru) – załącznik nr 2 do zapytania ofertowego;
- 2) Oświadczenie Wykonawcy – załącznik nr 4 do zapytania ofertowego;
- 3) Odpis lub informacja z Rejestru Przedsiębiorców Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej Rzeczypospolitej Polskiej, w zakresie art. 109 ust. 1 pkt 4 ustawy Pzp, sporządzonych nie wcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji.

III. WSPÓLNY SŁOWNIK ZAMÓWIEŃ (CPV):

CPV: 72268000-1 - Usługi dostawy oprogramowania.

IV. KRYTERIUM OCENY OFERT: Cena brutto oferty (waga-100 %).

Klembów, dnia 18.10.2024 r.

/-/Rafał Mathiak
Wójt Gminy Klembów

.....
(Data i podpis Kierownika Zamawiającego lub
osoby upoważnionej)