

Poprawa cyberbezpieczeństwa w Urzędzie Miasta i Gminy Solec nad Wisłą

(zmiany zaznaczono kolorem czerwonym)

1. Przedmiotem zamówienia jest dostawa oraz wdrożenie sprzętu i oprogramowania i usług do zarządzania infrastrukturą IT- 1 szt., Serwer – 1 szt., NAS – 1 szt., Urządzenie UTM – 1 szt., agregat zasilający – 1 szt. usługi doradcze w zakresie określenia poziomu cyberbezpieczeństwa, przygotowanie dokumentacji SZBI, Audyt końcowy, szkolenia z cyberbezpieczeństwa – 4 szt.
2. Zakres przedmiotu zamówienia podzielony został na 3 części:
Część I. Zakup i dostawa sprzętu.
Część II. Usługi doradztwa i szkoleń.
Część III. Zakup i dostawa agregatu zasilającego (prądotwórczego).

Signature Not Verified

Dokument podpisany przez
MAŁGORZATA FWELEINA
SZYMAŃSKA- MIASTO I
GMINA SOLEC NAD WISŁĄ
Data: 2025.05.09 12:55:09 CEST

UWAGA! Wykonawca może złożyć oferty częściowe na jedną lub więcej części zamówienia.

Część I. Dostawa sprzętu.

1. Przedmiotem zamówienia jest dostawa, instalacja, uruchomienie, konfiguracja z dostosowaniem do istniejącej infrastruktury informatycznej sprzętu wraz z oprogramowaniem i licencjami, zapewniające ochronę systemów informatycznych, zapewnienie funkcjonowania Urzędu Miasta i Gminy Solec nad Wisłą w zgodności z KRI oraz uoKSC oraz kształtowanie kultury cyberbezpieczeństwa wśród pracowników.

- Zakres prac obejmuje również:
 - **Konfigurację sieci wewnętrznej**, obejmującą modernizację lub dostosowanie istniejących urządzeń sieciowych (takich jak przełączniki, routery, punkty dostępowe) w celu zapewnienia bezpiecznego i wydajnego środowiska komunikacyjnego. W ramach prac przewiduje się również segmentację sieci (VLAN) dla wyodrębnienia stref dostępu zgodnych z obowiązującymi normami bezpieczeństwa.
 - **Podłączenie stacji roboczych do centralnej domeny Active Directory**, umożliwiające centralne zarządzanie kontami użytkowników, politykami bezpieczeństwa oraz dostępem do zasobów sieciowych. Proces ten obejmuje utworzenie struktury jednostek organizacyjnych (OU), wdrożenie zasad grupowych (GPO) oraz integrację z serwerami DNS i DHCP.
 - **Weryfikację poprawności działania oraz testy końcowe**, mające na celu zapewnienie, że wszystkie komputery poprawnie funkcjonują w nowym środowisku domenowym, a sieć wewnętrzna zapewnia wymaganą przepustowość, stabilność i bezpieczeństwo.

2. Dostarczony sprzęt winien być:

- 1) nowy tzn. nieużywany przed dniem dostarczenia, z wyłączeniem używania niezbędnego dla przeprowadzenia testów poprawnej pracy,
- 2) wyprodukowany po roku 2023,
- 3) wolny od wad technicznych,

- 4) wolny od wad prawnych,
 - 5) pochodzących z oficjalnych kanałów dystrybucyjnych producenta, zapewniających w szczególności realizację uprawnień gwarancyjnych,
 - 6) dostarczony w oryginalnych opakowaniach producenta sprzętu dla danego produktu, zaopatrzony w etykiety identyfikujące dany produkt,
 - 7) kompletny, w tym m.in. posiadać pełne okablowanie zapewniające funkcjonalność, oprogramowanie, licencję itp.
3. Uwaga: W kosztach składanej oferty wszelkie niezbędne licencje i wsparcie techniczne należy uwzględnić na okres kwalifikowalności wydatków projektu, który wynosi **maksymalnie do 30.06.2026 r.** Po upływie tego okresu Zamawiający przedłuży ze środków własnych licencje i niezbędne wsparcie na dodatkowy okres 24 miesięcy.
1. W skład urządzeń objętych przedmiotem zamówienia wchodzi:

1) Oprogramowanie do zarządzania infrastrukturą IT - (1 szt.)

Wymagane minimalne parametry i techniczne komponentu (wymagania jakościowe)
Pozyskiwanie informacji o sprzęcie, zarządzanie widokami, funkcje ogólne
Centralne zarządzanie wynikami skanowania sprzętu i oprogramowania
Zdalne wykrywanie urządzeń w sieci za pomocą protokołów PING, ARP oraz SNMP
Automatyczne wykrywanie adresów IP, MAC, DNS, Systemu Operacyjnego wraz z informacją o aktualizacji
Automatyczne wykrywanie, czy komputer jest członkiem domeny oraz do jakiej domeny lub grupy roboczej należy
Odwzorowanie struktury organizacji w oparciu o Active Directory
Jednostronna synchronizacja komputerów oraz drukarek z AD oraz AAD (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory)
Automatyczne skanowanie całości lub wybranych grup Active Directory (oraz AAD) oraz sieci
Mapowanie atrybutów obiektów AD (oraz AAD) do obiektów programu
Grupowanie wyposażenia z podziałem na jednostki organizacyjne w firmie (np. względem działów, lokalizacji, statusów)
Inwentaryzacja dowolnych elementów wyposażenia (biurka, szafy, telefony, etc.)
Utworzenie własnych typów elementów wyposażenia
Łączenie elementów wyposażenia w zestawy
Przypisywanie zasobu do wielu zestawów
Makrodefinicje w celu spersonalizowania nazw elementów w drzewku wyposażenia
Grupowanie, sortowanie i filtrowanie po dowolnie nadanych atrybutach
Podpięcie dowolnych załączników, np. skany faktur, gwarancji oraz wszelkich innych plików
Przypisywanie sprzętu do konkretnych osób, sprzętu do wybranej firmy

Automatyczne wyznaczanie 'Głównego użytkownika' komputera
Wiązanie wielu rekordów wyposażenia z użytkownikiem
Przypisywanie sprzętu do dowolnej lokalizacji
Definiowanie własnych, dowolnych atrybutów sprzętu
Aktywnym komputerom (bez określonego statusu) przydzielany jest status 'W użyciu'
Wydruk etykiet z kodami kreskowymi do inwentaryzacji wyposażenia
Dowolna treść kodu kreskowego
Określanie loga firmy oraz użycia go na wydrukach
Grupowa zmiana domeny/grupy roboczej zasobu
Informacje o sprzęcie
Automatyczne wykrywanie typu komputera (Desktop\Notebook\Serwer\Kontroler domeny) na podstawie wyników skanowania sprzętu
Wykrywanie komputerów typu All-In-One
Automatyczne wykrywanie typów stacji roboczej (Tower\Desktop\SFF\uSFF)
Automatyczne uzupełnianie informacji o procesorze, liczbie rdzeni, ilości pamięci RAM, rozmiarze dysku, nazwie karty graficznej i rozdzielczości monitora w obiekcie zasobu po wykonaniu skanowania sprzętu
Odczytywanie indeksów wydajności poszczególnych komponentów komputera: CPU, GPU, HDD, RAM
Automatyczna aktualizacja nazwy komputera w przypadku jej zmiany
Definiowanie statusów dla sprzętu (Nowy, Do kasacji, W serwisie, itd.)
Szczegółowa informacja na temat podzespołów sprzętu (procesor, bios, płyta główna, pamięć, dyski twarde, monitory, karty graficzne i muzyczne, etc.)
Odczyt informacji o module TPM, D3Dscore z WinSAT
Inwentaryzacja osprzętu komputerowego (monitory, drukarki, myszki, urządzenia sieciowe: Switch, Router, Access Point, Bridge, Modem, NAS, UPS, itd.)
Automatyczne wykrywanie lokalnych drukarek (USB) na podstawie wyników skanowania sprzętu, wykrywanie i tworzenie monitorów (producent, numer seryjny, rozdzielczość, odczyt firmy, działu, osoby odpowiedzialnej, głównego użytkownika), tworzenie zestawów: Komputer + Monitor, Komputer + drukarka lokalna, host + maszyny wirtualne, wykrywanie czy komputer jest maszyną wirtualną
Wykrywanie maszyn wirtualnych typu: Parallels Virtual Platform
Określanie informacji o wykorzystywanej wirtualizacji
Podgląd zestawów, do których należy zasób
Cykliczne wykonywanie skanowania sprzętu z różnymi ustawieniami
Przypisywanie stałego atrybutu COA, który będzie uwzględniany na raportach wyposażenia i audytu
Definiowanie szczegółowych informacji finansowych, bazy dostawców sprzętu i oprogramowania
Obsługa walut w danych finansowych
Automatyczne odczytywanie ServiceTag oraz modelu komputera (na podstawie wyników skanowania sprzętu) oraz automatyczna aktualizacja adresów IP komputerów bez zainstalowanego agenta
Agent odczytuje identyfikator SID komputera

Określanie adresu interfejsu webowego urządzenia sieciowego, typu gwarancji dla zasobu, wpływu biznesowego wybranego zasobu
Tworzenie własnych typów gwarancji
Określanie ikony dla typów zasobów
Integracja z Dell API
Wyszukiwanie i identyfikacja duplikatów zasobów
Geolokalizacja komputerów z agentem
Raporty zasobów
Raport dodanych załączników
Automatyczne tworzenie historii zmian sprzętu
Raport zbiorczy historii zmian w sprzęcie
Ewidencja zdarzeń serwisowych
Dodawanie notatek\komentarzy dla zdefiniowanych obiektów zasobów
Informacja na temat pojemności dysków twardych oraz wolnego miejsca
Wydruk\dodawanie jako załącznik protokołu przekazania\zwrotu\utyliczacji sprzętu, jako załącznik protokołu przekazania dla całego zestawu
Kreator szablonów wydruków WYSIWYG
Definiowanie dedykowanych profili protokołów
Zapisywanie protokołów podczas generowania jako załącznik do zasobu
Wydruk\dodawanie jako załącznik Karty informacyjnej do elementu wyposażenia
Wydruk lub zapis do pliku raportów ze szczegółami sprzętu
Porównywarka wyników skanowania sprzętu
Dzienniki zdarzeń systemu Windows
Automatyczny monitoring i raportowanie zmian w podzespołach sprzętu
Geolokalizacja komputerów z agentem
Zarządzanie zasilaniem
Zdalne włączanie i wyłączenie komputerów
Obsługa SecureOn przy WakeOnLan
Tworzenie harmonogramów wyłączania i włączania komputerów
Wybór 5 trybów zamknięcia systemu: Blokada komputera, Uśpienie, Hibernacja, Wyłączenie, Wymuszenie wyłączenia, Restart
Możliwość anulowania /wyświetlenia komunikatu jeśli jest zalogowany użytkownik
Możliwość przerwania / odłożenia zadania na żądanie użytkownika
Wymuszenie wylogowania użytkownika przed wyłączeniem komputera
Raport zadań jednorazowych oraz harmonogramów
Monitoring obciążenia CPU

Funkcje dodatkowe
Zdalne wykonywanie skryptów (batch/powershell) - Obsługa zadań jednorazowych i cyklicznych
Podpisywanie skryptów Powershell certyfikatem
Wykonywanie skryptów w kontekście sesji użytkownika lub usługi
Skrypty wykonywane po uruchomieniu komputera lub zalogowaniu użytkownika
Wykonywanie zadań dla wszystkich komputerów
Edytor skryptów z funkcją kolorowania składni
Wykorzystywanie predefiniowanych skryptów
Import informacji o wyposażeniu z pliku CSV
Wyszukiwanie sterowników, informacji o komputerze, informacji o gwarancji w bazie producenta (DELL)
Mechanizm automatycznego tworzenia rekordów producenta sprzętu (na podstawie wyników skanowania sprzętu)
Generowanie kodów paskowych, QR dla każdego elementu wyposażenia
Obsługa kodów QR
Archiwum zasobów
Przeniesienie utylizowanego wyposażenia do archiwum
Automatyczne usunięcie informacji sieciowych oraz licencji agenta dla zasobu archiwizowanego
Zarządzanie sprzętem przez aplikacje mobilną
Powiadomienia o kończącej się gwarancji\umowie serwisowej dla zasobu
Zachowanie ostatniego skanu sprzętu podczas konserwacji bazy danych
Powiadomienia o utworzeniu monitora, wykryciu maszyny wirtualnej
Grupowa zmiana atrybutów
Personalizacja statusów zasobów
Zarządzanie oprogramowaniem
Licencje
Inwentaryzacja licencji
Automatyczne tworzenie licencji na podstawie kluczy produktów
Odczytu OriginalProductKey (BIOS/UEFI) dla systemu operacyjnego
Import licencji z pliku tekstowego
Automatyczne generowanie historii zmian w licencji
Określanie statusu licencji
Tworzenie własnych atrybutów licencji, notatek oraz załączników w dowolnym formacie do licencji, licencji z poziomu rozliczenia audytu legalności, licencji z poziomu raportu kluczy licencji, zestawów licencji
Relacja licencji z użytkownikiem, firmą, działem, lokalizacją
Zmiana typu licencji dla wybranej grupy

Kompletna informacja na temat posiadanych licencji (typ, producent, program licencjonowania, czas ważności, informacje finansowe)
Przypisywanie licencji do komputera
Definiowanie wymaganych atrybutów legalności (faktura, nośnik, COA, etc.), ilości posiadanych licencji w rozbięciu na użytkowników oraz stanowiska, licencji przeznaczonych do przyszłego zakupu, kluczy seryjnych i przypisywanie do licencji
Automatyczne usunięcie wiązania pomiędzy zasobem archiwizowanym a licencją
Określenie wpływu biznesowego wybranej licencji
Skanowanie oprogramowania
Skanowanie oprogramowania na podstawie harmonogramu oraz definicji skanera
Automatyczna kontrola zmian w stanie zainstalowanego oprogramowania bez zlecenia skanów
Śledzenie zmian w stanie zainstalowanego oprogramowania
Zdalny skan komputerów (bieżący lub okresowy)
Zmiana priorytetu skanowania oprogramowania
Skan komputerów niepodłączonych do sieci
Wysyłanie wyników skanowania offline na serwer FTP (Audyt)
Przekazywanie konfiguracji wzorcowej dla skanera offline
Identyfikacja zainstalowanych aplikacji na podstawie wzorców oprogramowania
Prawidłowe rozpoznanie aplikacji nawet mimo zmiany jej nazwy
Określanie masek plików dla publikacji elektronicznych (e-book)
Skan plików skompresowanych
Skan oraz identyfikacja zawartości archiwów zapisanych w formatach: 7z, arj, bz2, bzip2, cab, gz, gzip, img, iso, jar, lha, lzh, lzma, msi, nrg, rar, tar, taz
Wbudowane profile skanowania (np. profil wzorcowy)
Definicja własnych ustawień skanowania
Porównywanie wyników skanowania oprogramowania
Wykrywanie plików multimedialnych
Wykrywanie i inwentaryzacja plików dowolnego typu (np. multimedia, czcionki, grafika)
Odczytywanie informacji o składnikach aplikacji, których programy instalacyjne nie są zgodne ze standardem MSI
Identyfikacja SID użytkownika, dla którego zainstalowano oprogramowanie
Bezpłatna, automatycznie aktualizowana baza wzorców aplikacji\pakietów\systemów operacyjnych
Nadpisanie bazy wzorców najnowszą, oficjalną bazą producenta
Definiowanie katalogów wykluczonych / uwzględnionych w skanowaniu z wykorzystaniem symboli wieloznacznych (*, %)
Audyt oprogramowania

Rozliczanie pakietów aplikacji, systemów operacyjnych, licencji typu „Downgrade”, „Upgrade” oraz instalacji innego oprogramowania w ramach licencji
Audyt oprogramowania rozliczany automatycznie - informacja o stanie posiadanych licencji i faktycznie zainstalowanych programach z uwzględnieniem wybranych zestawów licencji.
Historia audytów (Wyniki audytów są przechowywane w bazie danych - można do nich wracać w dowolnej chwili, porównywać je i generować stosowne raporty)
Wsparcie procesu Audytu przez zaimportowanie materiału zdjęciowego i jego obróbkę
Gotowe metryki audytowanego komputera - załącznik do protokołu przekazania stanowiska komputerowego (sprzęt + oprogramowanie)
Uwzględnianie w rozliczeniu oprogramowania liczby aktywacji zapisanej w szablonie licencji
Funkcje
Mechanizm informujący o nowej bazie wzorców oprogramowania
Definiowanie własnych wzorców oprogramowania
Automatyczne tworzenie wzorców oprogramowania dla systemów operacyjnych
Automatyczne dodawanie informacji o wydawcy oprogramowania dla nowych wzorców, tworzonych na podstawie wyników skanowania
Wykrywanie kluczy/identyfikatorów programów
W przypadku aktywacji systemu Windows z użyciem serwera KMS, klucza MAK (Multiple Activation Keys) lub VLK (Volume License Keys) odczytywane jest 5 ostatnich znaków klucza
Odczytywanie informacji o częściowych kluczach pakietów Microsoft Office
Drukowanie lub zapisywanie do pliku raportów ze szczegółami oprogramowania
Zbiórce raporty wyników skanowania oprogramowania - Pakiety, pliki, systemy operacyjne, kluczy zainstalowanych aplikacji
Raport z informacjami o pakietach oprogramowania uwzględniający parametry: przybliżona wielkość, adres strony internetowej, lokalizacja pliku instalacyjnego, architektura aplikacji, itd., oraz informacjami o systemach operacyjnych uwzględniający parametry: Data instalacji, Architektura systemu, Wersja kompilacji, itd.
"Wielkie raporty" (Możliwość utworzenia zbiorczych raportów obejmujących np. wszystkie przeskanowane pliki)
Zdalna instalacja dowolnego oprogramowania zgodnego ze standardem Windows Installer (*.msi), dezinstalacja oprogramowania
Utworzenie harmonogramu dezinstalacji oprogramowania
Generowanie skryptu deinstalacji aplikacji na podstawie otrzymanych wyników skanowania oprogramowania
Raport stanu oprogramowania antywirusowego, anty-szpiegowskiego oraz zapory sieciowej, zainstalowanych aktualizacji systemu Windows
Kontrola wykorzystania sprzętu i oprogramowania
Pozyskiwanie informacji o użytkownikach, zarządzanie widokami, funkcje ogólne
Dane gromadzone dla konkretnych użytkowników (na bazie kont Windows) - jeden użytkownik może mieć przypisanych wiele kont Windows i pracować na różnych komputerach
Odczyt informacji o kontach lokalnych komputera, wraz z odczytem grup do, których konto należy
Grupowanie użytkowników z podziałem na jednostki organizacyjne w firmie (np. względem działów)

Określanie firmy do której należy użytkownik, przełożonego dla użytkownika
Prezentacja 'stanu użytkownika' (obecny, nieobecny, nowy), 'statusu użytkownika' (Zatrudniony, zwolniony, itd.)
Zarządzanie stanowiskami użytkowników
Przeniesienie rekordu użytkownika do archiwum
Funkcjonalności automatycznego generowania zmian rekordu użytkownika – Historia użytkownika
Odczytywanie informacji o użytkownikach z Active Directory oraz AAD
Pełna synchronizacja rekordów użytkowników (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory oraz AAD)
Baza danych teleadresowych użytkowników z możliwością tworzenia raportów i zestawień
Podgląd zdjęcia przypisanego do użytkownika
Przypisywanie do użytkownika załączników (pliki), notatek do użytkownika
Ewidencja zdarzeń przypisanych do użytkowników
Automatyczne tworzenie działów na podstawie informacji odczytanych z Active Directory
Raporty
Analiza aktywności użytkowników
Grupowanie danych według komputerów jeśli użytkownik wykorzystywał więcej niż jedno stanowisko
Analiza zdarzeń sesji użytkownika (Logowanie, Wylogowanie, Zablokowanie, Odblokowanie, Nawiązanie połączenia RDP, Zakończenie połączenia RDP)
Analiza przerw w pracy, jakości pracy (liczba kliknięć myszą, liczba wpisanych znaków), aktywności mikrofonu oraz kamery, wykorzystania poszczególnych aplikacji w czasie, czasu działania aplikacji, na pierwszym planie oraz sumarycznie
Uwzględnienie lub wyłączenie z raportu aplikacji bez aktywności użytkownika
Kategoryzacja danych czasu pracy (czas pozytywny, neutralny oraz negatywny).
Statystyki najczęściej wykorzystywanych aplikacji, wykorzystania komputerów przez poszczególnych użytkowników, aktywności użytkownika i grup użytkowników
Generowanie raportów z monitoringu użytkowników dla wybranego zakresu godzin
Kontrola wydruków - historia zadań drukowania zainicjowanych przez poszczególnych użytkowników, Monitoring wydruków obejmuje szczegółowe parametry (np. format papieru, orientacje, skalowanie, itd.)
Informacje o drukowanych dokumentach (osoba, nazwa pliku, ilość stron, ilość kopii, cz-b/kolor, dpi)
Monitoring wydruków na drukarkach sieciowych, użytkowników stacji terminalowych
Informacja o operacjach na nośnikach zewnętrznych (CD/DVD, HDD, FDD, Pen Drive, etc.), o awariach, poczynaniach użytkowników: zakończonej aktualizacji, akcji podpięcia przenośnych dysków, włożenia płyt do napędów CD/DVD, śledzenie uruchomienia aplikacji przez użytkownika, monitoring informujący o małej ilości miejsca
Raport zbiorczy historii zmian w rekordach użytkowników
Funkcje
Blokada niepożądanych aplikacji. Programy mogą być blokowane dla całej firmy lub tylko dla wybranych użytkowników.

Autoryzacja nośników zewnętrznych na podstawie wykrytych urządzeń
Konfigurowanie praw dostępu do plików i katalogów zapisanych na nośnikach zewnętrznych
Automatycznie budowana baza informacji o napędach zewnętrznych
Blokada dostępu do napędów zewnętrznych (m.in. HDD, FDD, Pen Drive, etc.)
Odczyt i blokada urządzeń PTP/MTP
Określanie praw dostępu w zależności od typu urządzenia, np. Pendrive, CD/ROM
Komunikacja z użytkownikami (Skype, mail) bezpośrednio z zakładki Użytkownicy
Informacje o ostatnio zalogowanych osobach na stacjach klienckich
Automatyczne tworzenie licencji – Dodawanie do licencji użytkowników, którzy są głównymi użytkownikami komputera, na którym wykryto licencje
Komentowanie przerw pracy
Kategoryzacja przerwy w pracy na podstawie komentarza
Kontrola wykorzystania Internetu
Funkcje
Blokada stron internetowych dla poszczególnych użytkowników, możliwość zastosowania filtrów, blokada WWW po zawartości (ContentType)
Blokada stron internetowych dla protokołu http \ https w najpopularniejszych przeglądarkach WWW
Kategoryzacja stron internetowych
Import stron WWW z pliku lub ze schowka
Słowniki kategorii stron WWW
Blokada dostępu do witryn zgodnie z harmonogramem, trybu incognito w przeglądarce Google Chrome
Raporty
Raporty dotyczące aktywności użytkowników w Internecie
Analiza czasu przebywania na poszczególnych stronach lub domenach (z uwzględnieniem informacji o tytule strony i wersji przeglądarki)
Monitoring stron internetowych dla protokołu http \ https (Edge, Chrome, Opera, Vivaldi, Firefox)
Analiza liczby wejść na poszczególne strony lub domeny
Kategoryzacja odwiedzanych domen i stron
Raport informujący o plikach pobranych przez przeglądarki WWW, informujący o danych wysłanych przez przeglądarki (bez Firefox)
Monitoring plików pobieranych przez przeglądarki internetowe
Helpdesk
Obsługa
Rejestracja i obsługa zgłoszeń
Obsługa zgłoszeń w modelu Kanban

Określanie relacji pomiędzy zgłoszeniami (np.. Kopia, Incydent nadrzędny)
Edycja zgłoszeń powiązanych w oknie zgłoszenia bieżącego
Kategoria zgłoszeń może posiadać swojego opiekuna, który może zarządzać każdym zgłoszeniem danej kategorii
Komentarze zgłoszenia obsługujące HTML oraz osadzanie obrazów
Opis zgłoszenia w formacie HTML
Nawiązywanie połączeń zdalnych bezpośrednio z edytora incydent
Tworzenie notatek dla zgłoszeń
Zapisywanie wersji roboczej komentarza
Archiwizacja zgłoszeń
Monitoring czasu pracy nad incydem (time tracking)
Raport ewidencji czasu pracy nad zgłoszeniem
Informacja o czasie reakcji do podjęcia zgłoszenia
Dodanie prywatnego komentarza
Znaki @ oraz # pozwalają na wspomnianie użytkownika oraz wpisu bazy wiedzy w komentarzu zgłoszenia
Dodanie załączników do incydentów, również do komentarza
Określanie dodatkowych subskrybentów dla notyfikacji e-mail dotyczącej zmian w incydencie, uprawnień do incydentów (Publiczne, Prywatne, dla określonych działów)
Zarządzanie filtrami zdefiniowanymi dla listy zgłoszeń
Obsługa nazwy DNS oraz adresów IP (IPv4, IPv6) dla zgłoszeń
Wydruk historii zgłoszenia
Widok kalendarza (Planowanie rozwiązania incydentów)
Korelacja incydentu z elementem zasobów
Raport zbiorczy historii zmian
Tworzenie i planowanie zastępstw, osoba zastępująca otrzymuje na czas zastępstwa dostęp do obsługi zgłoszeń osoby zastępowanej
Wyszukiwanie komentarzy przy użyciu funkcji globalnego wyszukiwania
Czas reakcji oraz realizacji wyznaczany automatycznie na podstawie umów SLA
Automatyczne podpowiedzi rozwiązań dostępnych w bazie wiedzy na podstawie wpisywanego tematu
Określenie wpływu biznesowego wybranego zgłoszenia
Podgląd wiadomości źródłowej przy tworzeniu zgłoszenia lub komentarza na podstawie zgłoszeń email
Duplikacja i replikacja zgłoszeń
Powiadomienia o liczbie nieprzeczytanych zgłoszeń
Automatyzacja obsługi zgłoszeń z wykorzystaniem utworzonych reguł
Konfiguracja
Architektura drzewa dla kategorii zgłoszeń

Tworzenie szablonów odpowiedzi
Cykliczne raportowanie Listy incydentów
Tworzenie własnych dodatkowych atrybutów dla zgłoszeń
Personalizowane szablony wiadomości email z możliwością ustawienia stałego załącznika
Notyfikacje e-mail o utworzeniu\zmianie\usunięciu incydu, e-mail o zbliżających się terminach realizacji incydu (Deadline)
Automatyczny import wiadomości e-mail, jako zgłoszeń helpdesk (POP3 oraz IMAP)
Import zgłoszeń helpdesk ze skrzynek współdzielonych (shared mailbox)
Obsługa wielu kont pocztowych (Import + notyfikację email)
Tworzenie własnych trybów oraz priorytetów incydentów
Personalizacja widoku raportu listy incydentów
Profile zgłaszających w helpdesk
Personalizacja kolorów statusów zgłoszeń
Automatyczne przypisywanie zgłoszeń do użytkowników
Weryfikacja wiadomości źródłowych pobieranych z serwera pocztowego
Konfiguracja maksymalnej wielkości załącznika
Moduł połączeń zdalnych
Operacje na plikach i katalogach
Zarządzanie procesami i rejestrem
Monitoring pracy wykonywanej na komputerze
Zdalny podgląd pulpitu wielu stacji (Funkcja Company Online)
Wywoływanie Windows Remote Desktop na danej stacji z poziomu aplikacji
Wysyłanie wiadomości do użytkowników
Uruchamianie na stacjach programów z wiersza poleceń Command Line
Zdalne uruchamianie komputera za pomocą funkcji Wake-On-Lan
Wake-On-Lan pozwala na definicję portu oraz adresu komputera docelowego
Przejęcie kontroli nad stacją roboczą
Blokada klawiatury i myszki na stacji klienckiej w trakcie przejęcia kontroli pulpitu zdalnego
Przesyłanie kombinacji klawiszy Ctrl + Alt + Delete w zdalnym pulpicie
Przejęcie kontroli nad komputerem bez zalogowanego użytkownika
Wysyłanie pytania o zgodę na zdalny dostęp lub wysyłania komunikatu z informacją o rozpoczęciu podglądu pulpitu
Podgląd pulpitu zdalnego w osobnym oknie z opcją fullscreen
Obsługa wielu monitorów dla podglądu pulpitu
Wybór monitora, z którego ma być przekazywany obraz podglądu pulpitu

Nawiązywanie połączenia pulpitu zdalnego z wieloma komputerami jednocześnie
Połączenie pulpitem zdalnym w konfiguracji NAT-NAT
Zarządzanie usługami systemu Windows
Raport Sesje zdalnego pulpitu
Wybór adresu IP, na którym ma być zestawione połączenie DirectPC, portu, na którym klient nasłuchuje połączenia zdalnego
Wykorzystanie protokołu autorskiego lub MS RDP do połączeń zdalnych
Baza wiedzy
Wbudowana baza wiedzy
Artykuły bazy wiedzy mogą być przypisane do kategorii zgłoszeń helpdesk
Kopiowanie artykułów
Edytor HTML
Osadzanie załączników w treści artykułów
Osadzanie multimediów w treści artykułów
Baza wiedzy pozwala na tworzenia artykułów prywatnych oraz publicznych
Szybkie kopiowanie wpisów bazy wiedzy
Artykuły bazy wiedzy mogą zostać powiązane ze zgłoszeniami z systemu helpdesk oraz mogą zostać przypięte, dzięki czemu zawsze będą widoczne na liście artykułów
Informacja o liczbie odsłon artykułu bazy wiedzy
Bezpośrednie linkowanie artykułów bazy wiedzy
SLA
Definiowanie planów umów SLA, czasu obowiązywania umów SLA, czasu pracy działów wsparcia technicznego, dni wolnych na podstawie kalendarza świąt i dni wolnych, czasów reakcji oraz realizacji zgłoszenia
Notyfikacje mailowe o zbliżających się terminach reakcji oraz realizacji
Automatyczne przypisanie umowy SLA do zgłoszenia na podstawie informacji o rozwiązującym, temacie wiadomości, priorytecie, kategorii, opisie
Raportowanie o statusie i postępie w realizacji zgłoszeń z przypisaną umową SLA
Centralne repozytorium załączników
Funkcje
Załączniki przechowywane w centralnym repozytorium
Utworzenie relacji załącznika z innymi elementami systemu 1 - N (jeden do wielu)
Dodawanie i modyfikacja załączników z poziomu innych zasobów
Załączniki typu: link, udział oraz plik
Pełna informacja o załączniku: twórca, data utworzenia, rozmiar, nazwa pliku, miniatura
Historia zmian załącznika
Zarządzanie użytkownikami

Funkcje
Raportowanie aktywności pracy
Przeglądanie ostatnio zgłoszonych incydentów
Powiązanie użytkownika z licencją
Dostęp webowy do statystyk monitoringu, zgłoszeń helpdesk oraz powiązanych z użytkownikiem zasobów
Cykliczne, automatyczne generowanie raportów
Generowanie raportu obecności / nieobecności użytkownika wraz z korelacją jego aktywności na komputerze
Zgłoszenia dotyczące wniosków nieobecności użytkowników
Automatyczne typowanie użytkowników zastępujących dla zgłaszanych nieobecności
Zarządzanie wnioskami nieobecności użytkowników przez przełożonych, informowanie przełożonych N poziomów wyżej o urlopie użytkownika
Automatyczne utworzenie relacji przełożony - podwładny na podstawie skanów Active Directory
Możliwość drukowania karty informacyjnej użytkownika, zawierającej informacje kontaktowe, informacje o powiązanych zasobach, licencjach oraz dostępny nadane w module RODO
Generator struktury organizacji na podstawie powiązań użytkowników i ich przełożonych
Planowanie dni wolnych w widoku kalendarza, zastępstw podczas nieobecności
Raportowanie cykliczne
Użytkownicy
Raport historia sesji, Nośniki danych, Operacje na plikach, wydruków, użycia aplikacji, nagłówków okien, odwiedzonych stron WWW
Najczęściej odwiedzane strony internetowe
Raport Wysyłane pliki, czasu pracy przy komputerze
Zasoby
Raport historii zasobów, informujący o nowych zasobach, informujący o nadchodzących terminach w zasobach, Zasoby zarchiwizowane, Systemy Operacyjne
Podstawowe
Raport Informacje o autoryzowanych agentach
Oprogramowanie
Raport zainstalowanego oprogramowania, Szczegóły plików
Helpdesk
Raport incydentów (Helpdesk), czasu pracy nad zgłoszeniem, Cząsy SLA
Automatyzacja
Lista dostępnych reguł
Ogólne
Zakończenie asysty serwisowej AS lub AS Plus
Wygaśnięcie certyfikatu SSL

Kończące się licencje na agenta
Zapełniona baza danych
Zbyt duży rozmiar folderu cache
Zasoby
Brak połączenia od agenta, Brak wolnej przestrzeni na dysku, Ostrzeżenie od Windows Security Center, Zakończenie skanowania sprzętu, Dodanie zasobu, Zmiana zasobu, Usunięcie zasobu, Zakończenie okresu gwarancyjnego, Zakończenie umowy serwisowej, Powielenie zasobów
Oprogramowanie
Zmiana oprogramowania, Zakończenie skanowania oprogramowania, Zamknięcie audytu
Licencje
Dodanie/Zmiana/Usunięcie/Wygaśnięcie licencji, Planowana wymiana licencji
Użytkownicy
Dodanie/Zmiana/Usunięcie/Logowanie/Wylogowanie użytkownika
Helpdesk
Dodanie/Zmiana/Usunięcie zgłoszenia, Brak aktywności w zgłoszeniu
Lista dostępnych Akcji
Wykonywanie skryptu na podstawie zdefiniowanej reguły
Wysłanie powiadomienia w konsoli Master / Konsola Web na podstawie zdefiniowanej reguły, powiadomienia mailowego na podstawie zdefiniowanej reguły (inicjator zdarzenia, Administratorzy, konkretny użytkownik, rozwiązujący, zgłaszający, subskrybenci)
Modyfikacja zasoby / użytkownika / zgłoszenia - w zależności od reguły
Dodanie komentarza (dla reguł Helpdesk)
Wysyłka wiadomości SMS
RODO
Funkcje
Inwentaryzacja zbiorów danych, dostępów oraz powierzeń do zbiorów danych, dokumentów bezpieczeństwa, historii naruszeń bezpieczeństwa, szkoleń oraz wniosków o zapomnienie
Wydruk raportów tabelarycznych: czynności przetwarzania, dostępów, powierzeń, listy dokumentów, statystyki zgłoszeń RODO, listę szkoleń, historii naruszeń bezpieczeństwa, wniosków o zapomnienie
Wydruk wniosków o nadanie uprawnień, modyfikacji oraz anulowania upoważnienia
Wstępne wypełnienie wniosków o zmianę dostępu
Utworzenie zgłoszeń za pomocą przycisków szybkiej akcji
Delegowanie zadań w helpdesk dla osób odpowiedzialnych za zbiory danych
Archiwizacja zbiorów
Definiowanie czynności przetwarzania
Przypisywanie zbioru danych do czynności przetwarzania
Przydzielanie dostępów do czynności przetwarzania

Zapisywanie historii zmian wniosków o dostęp do zbiorów
Dodawanie historycznych dostępów oraz wniosków o dostęp
Filtrowanie użytkowników w raporcie Dostęp
Raporty
Raport zbiorczy Czynności przetwarzania, Zbiory danych, zinwentaryzowanych dostępów, zinwentaryzowanych powierzeń, zinwentaryzowanych dokumentów, historii naruszeń bezpieczeństwa, wniosków o dostęp, dostępy
Sygnalista
Funkcje
Tworzenie zgłoszeń w postaci anonimowej lub nieanonimowej
Usuwanie metadanych z załączników zgłoszeń, danych osobowych ze zgłoszeń
Podział interfejsu na publiczny oraz dla wewnętrzny
Dashboard podsumowujący wykorzystanie portalu sygnalisty
Przypisywanie rozwiązujących zgłoszenia sygnalistów w zależności od typu zgłoszenia lub jego źródła
Definiowanie własnych atrybutów, kategorii, trybów zgłoszeń oraz poziomów ryzyka, stron publicznych (dostępnych dla sygnalistów)
Obsługa wielu języków stron publicznych
Natywne wsparcie języka ukraińskiego
Definiowany limit załączników
Wyróżnienie zgłoszeń o przekroczonym czasie reakcji
Raporty
Raport zgłoszeń, Historia zmian, Statystyka zgłoszeń
Pozostały czas na przyjęcie zgłoszenia/ do zakończenia
Widżety: Kategorie zgłoszeń, Poziomy ryzyka, Tryby zgłoszeń, Statusy zgłoszeń, Ostatnio dodane
Portal Web
Funkcje
Wallboard - ekran zbiorczy prezentujący wybrane informacje z całego systemu
Dashboard każdego modułu z najważniejszymi informacjami w postaci widżetów
Widok "Mój dzień" zawierający oś czasu z aktywnością użytkownika
Rozbudowane filtry dla raportów tabelarycznych
Zarządzanie użytkownikami, agentami, zasobami, licencjami, działami, audytami
Konfiguracja portalu helpdesk, kont administracyjnych oraz organizacji
Raporty dla każdego modułu w formie tabelarycznej
Obsługa helpdesk oraz bazy wiedzy, modułu RODO, modułu automatyzacja, modułu Sygnalista
Automatyczne logowanie przy pomocy aplikacji
Logowanie za pomocą poświadczeń domenowych (SSO), konta AzureAD lub AAD

Wydruk raportów tabelarycznych
Kontrola statystyk użytkowników
Menu szybkiego dodawania nowych elementów (użytkownik, nieobecność, zasób, licencja, zgłoszenie, artykuł bazy wiedzy, zbiór danych, czynność przetwarzania)
Przełączanie wersji językowej bez ponownego logowania do systemu
Nawigacja Breadcrumb
Funkcjonalności ogólne
Określanie praw dostępu do grup zasobów lub użytkowników
Aplikacja desktopowa służąca do zarządzania systemem może być zainstalowana na dowolnej liczbie komputerów ("Licencja pływająca")
Dodatkowa aplikacja webowa umożliwiająca dostęp do systemu i zarządzanie systemem
Wersja angielska (en-US) interfejsu użytkownika
Praca w oparciu o silniki baz danych: MS SQL lub PostgreSQL
Swobodna migracja danych pomiędzy MS SQL i PostgreSQL
Zdalna instalacja i dezinstalacja agentów na stacjach roboczych
Odczytywanie struktury organizacji z Active Directory
Skaner sieci wykorzystywany do wykrywania nowych urządzeń
Mechanizm automatycznego tworzenia komputera na podstawie danych przesłanych przez agenta
Mechanizm automatycznego tworzenia użytkowników na podstawie danych przesłanych przez agenta
Automatycznie dodane komputery/użytkowników są powiązane z odpowiednią grupą zgodną z OU w Active Directory
Definiowanie nieograniczonej liczby użytkowników systemu
Określanie ról dla kont systemu: Administratorzy, Menadżerowie, Zarządcy, Pracownicy
Indywidualny login i hasło dla poszczególnych użytkowników
Automatyczne logowanie do systemu
Zarządzanie uprawnieniami użytkowników - określanie dostępu do poszczególnych obiektów systemu (konkretny użytkownik, konkretny zasób lub ich grupy) , możliwość ograniczenia operacji (wyświetlanie, tworzenie, edycja, usuwanie)
Dostęp do programu chroniony przy pomocy uwierzytelniania wieloskładnikowego
Określanie ról użytkowników - zarządzanie grupami
Zabezpieczenie Agentów przed nieautoryzowanym wyłączeniem lub usunięciem
Eksport danych do plików zewnętrznych (Excel, html, CSV, PDF, TXT, MHT, RTF, BMP)
Zgodny z pracą w sieciach WLAN
Podgląd aktualnych zadań serwera
Centrum informacji - przekrojowy raport na temat zdarzeń oraz statusu monitorowanych komputerów i użytkowników
Wielopoziomowe drzewo lokalizacji oraz relacje lokalizacji z firmami

Wyszukiwanie danych w tabelach raportów
Dowolne definiowania grup sprzętu i użytkowników
Tworzenie dowolnych raportów ad-hoc - sortowanie kolumn grupowanie, ukrywanie/odkrywanie kolumn, zaawansowane filtrowanie danych w oparciu o funkcje logiczne
Definiowanie i zapamiętywanie własnych widoków
Eksport danych bezpośrednio do MS Excel
Budowa zestawień metodą drag'n'drop
Budowa modułowa z możliwością przypisywania określonych wtyczek programu (funkcji) do poszczególnych Agentów
Obsługa protokołu SSL zapewniającego bezpieczną komunikację Master-Serwer oraz Agent-Server.
Połączenia pomiędzy komponentami realizowane za pomocą HTTP/HTTPS lub net.TCP
Mechanizm kompresji pakietów danych przesyłanych przez Agent
Automatyczne wykrywanie lokalizacji serwera aplikacji (WS-Discovery)
Przekazanie agentowi nowych parametrów połączenia z usługą serwera (serwer zapasowy)
Definiowanie konfiguracji serwera proxy dla połączenia Agent-Server
Mechanizm zdalnego pobierania bieżących aktualizacji do programu
Help kontekstowy wraz z podręcznikiem użytkownika w polskiej wersji językowej
Dostęp do bazy wiedzy systemu
Definiowanie ustawień pracy Agentów (optymalizacja dla dużej liczby komputerów)
Dedykowane narzędzie, dostarczane z systemem, do wykonywania kopii bazy danych, niezależnie od wersji silnika bazy danych (MSSQL, PostgreSQL). Uruchomienie narzędzia backupu bazy w trybie wsadowym
Manualna i automatyczna konserwacja bazy danych - usuwanie wyników skanowania oprogramowania
Personalizacja pakietu instalacyjnego agenta
Określanie polityki haseł dla systemu
Zmiana języka systemu podczas logowania
Określenie numeru BDO przy definiowaniu rekordu firmy
Opcja resetu hasła podczas logowania
Globalne wyszukiwanie obiektów w systemie
Utworzenie atrybutów jako lista/słownik
Podgląd aktualnie zalogowanych użytkowników. Umożliwienie wylogowania wybranych użytkowników
Definicja kalendarzy dni wolnych, uwzględnianych w module Helpdesk oraz Monitoring
Wyszukiwarka ustawień w opcjach systemowych
Instalacja konsoli zarządzającej w kontekście użytkownika (nie wymaga uprawnień administracyjnych)
Historia obiektu zawiera informacje o koncie serwisowym, które wprowadziło zmianę w obiekcie
Skanowanie lasu domen
Budowa personalizowanego pakietu instalacyjnego

Automatyczne zamknięcie konsoli Master po zakończeniu sesji
Logowanie do portalu Web za pomocą mechanizmu Single Sign On
Logowanie operacji kont serwisowych
Security Key - dodatkowa metoda uwierzytelniania klientów przed połączeniem do serwera
Logowanie nieudanych prób uwierzytelnienia
Eksport danych diagnostycznych oraz dzienników operacji
Integracja z SMS API
Dodatkowe informacje
Kreator instalacyjny ułatwiający wdrożenie systemu
Aplikacja Master\Server\ Agent w wersji x64
Rozproszona architektura systemu: Serwer, Master, Agent (Możliwa praca każdego z komponentów na różnych komputerach)
Praca w oparciu o MS SQL Server oraz MS SQL Express (2008/2012/2014/2016/2019/2022 32/64 bit)
Praca w oparciu o PostgreSQL 10 lub nowszy
Szyfrowane połączenie pomiędzy serwerem programu, a bazą danych
Obsługa systemów operacyjnych - Agent: Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 7, Windows 8, Windows 10, Windows 11
Obsługa systemów operacyjnych - Master : Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 7, Windows 8, Windows 10, Windows 11
Obsługa systemów operacyjnych - Serwer: Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 7, Windows 8, Windows 10, Windows 11
Wszystkie wykonywalne komponenty systemu są podpisane certyfikatem <i>DigiCert Code Signing Certificates for Microsoft Authenticode (Digicert)</i>
Sterowniki systemowe są podpisane certyfikatem <i>Extended Validation (EV) Code Signing Certificate (GlobalSign)</i> i mogą pracować w 64-bitowych systemach operacyjnych Microsoft Windows™.
Oprogramowanie z licencją bez ograniczeń czasowych dla 1 konsoli zarządzającej Master oraz 30 Agentów z Asystą Serwisową do 30.06.2026.
Asysta Serwisowa winna być świadczona wyłącznie przez producenta oprogramowania i powinna zawierać bezpłatny dostęp do wszelkich uaktualnień programu, nowych wersji oraz bazy wzorców aplikacji, wielokanałowy dostęp do pomocy technicznej – telefon, e-mail, on-line

2) Serwer - (1 kpl.)

Wymagane minimalne parametry techniczne komponentu

Obudowa typu RACK o wysokości max. 3U wyposażony w szyny ruchome oraz elementy do montażu w szafie serwerowej wraz systemem kopii zapasowych, pochodzący z oficjalnego kanału dystrybucji na rynek Unii Europejskiej

Zainstalowany min. 2 procesory 8 rdzeniowe w architekturze x64, cache 12MB przeznaczony do pracy ciągłej (serwerowy)

Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta serwera, trwale oznaczona (na laminacie płyty głównej) z nazwą producenta oferowanego serwera i dedykowana dla danego urządzenia. Płyta główna powinna umożliwiać zainstalowanie 2 procesorów oraz pamięci RAM

min. 64 GB DDR4 RDIMM o częstotliwości pracy 3200 MT/s

Zainstalowane min. 6 dysków, każdy o pojemności min. 2.4 TB, SAS 12 Gb/s, 2.5", Hot-Plug, Uszkodzone dyski pozostają u Zamawiającego bez ponoszenia dodatkowych kosztów.

Zainstalowany sprzętowy kontroler dyskowy RAID
SAS/SATA z min 8 GB Cache, RAID 0/1/5/6/10/50/60

Zintegrowany kontroler zdalnego dostępu umożliwiający administratorom monitorowanie, zarządzanie, aktualizowanie, rozwiązywanie problemów i naprawę z dowolnego miejsca i bez użycia agentów. Niezależnie od obecności lub stanu systemu operacyjnego lub hiperwizora.

Karta graficzna zintegrowana z płytą główną umożliwiającą wyświetlanie rozdzielczości min. 1280x1024.

Wbudowana w płytę główną dwu portowa karta sieciowa z min 2 portami 1Gbit/s.

Dodatkowo zainstalowana dwu portowa karta 10Gbit/s SFP+.

Interfejsy sieciowe muszą pochodzić od tego samego producenta.

na przednim panelu:

min. 1 port USB

min. 1 złącze video analogowe lub cyfrowe

na tylnym panelu:

min. 1 złącze video analogowe lub cyfrowe

min. 1 port USB 2.0

min. 1 port USB 3.0

min. 2 porty RJ-45

Ilość dostępnych złączy VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy

Min. 2 zasilacze o mocy co najmniej 1100W, redundancyjne, dedykowane do zaoferowanego sprzętu zwymiarowane do wewnętrznych podzespołów, wymienne bez wyłączania systemu

W komplecie do oferowanego sprzętu wszystkie niezbędne do uruchomienia kable zasilające, przewody sygnałowe.

System operacyjny – fabrycznie nowy, nieużywany, nie pochodzący z recyklingu, z licencją na czas nieoznaczony, nie naruszający praw osób trzecich. System operacyjny wraz ze wszystkimi wymaganymi sterownikami podzespołów ma być zainstalowany lub preinstalowany na oferowanym urządzeniu komputerowym. Zabrania się instalowania lub preinstalowania systemu operacyjnego w jakimkolwiek środowisku wirtualnym. Zamawiający nie dopuszcza zaoferowania systemu operacyjnego, programów i planów licencyjnych opartych o rozwiązania chmurowe oraz rozwiązań wymagających wnoszenia przez

Zamawiającego jakichkolwiek dodatkowych opłat związanych z użytkowaniem zakupionego systemu operacyjnego. Zamawiający wymaga, aby wszystkie elementy systemu operacyjnego oraz jego licencja pochodziły od tego samego producenta.

MS Windows Server 2025 Standard wersja polskojęzyczna z nieujawnianym wcześniej, nieaktywowanym wcześniej kluczem licencyjnym, pochodzący z oficjalnej sieci dystrybucji firmy Microsoft® wraz z licencjami dostępowymi CAL dla 20 użytkowników lub równoważne.

Warunki równoważności:

1. System operacyjny musi być przeznaczony do zastosowań serwerowych w Środowiskach fizycznych lub o minimalnej wirtualizacji.
2. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta.
3. Licencja na system operacyjny musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania.
4. Licencja na system operacyjny musi umożliwiać uruchomienie kontrolera domeny będącego w pełni zgodnym z domeną wdrożoną u Zamawiającego domeną Active Directory pracującą w oparciu o system Windows Server 2008 musi także być dostarczona możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server.
5. Licencja na system operacyjny musi być licencją stałą, bez ograniczeń czasowych.
6. Licencja na system operacyjny musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i min. 1 środowisku wirtualnym za pomocą wbudowanego mechanizmu wirtualizacji, bez konieczności zakupu dodatkowych licencji.
7. Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej.
8. System operacyjny musi posiadać graficzny interfejs użytkownika.
9. System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie:
 - a) zarządzania użytkownikami,
 - b) zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową,
 - c) możliwości przydzielania praw dostępu do zasobów sieciowych,
 - d) instalacji zdalnej oprogramowania z pakietów msi,
 - e) definiowania polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows: 8,8.1, 10, 11.
10. System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów.
11. System operacyjny musi wspierać zarządzanie przez dostępne narzędzia administracji serwera dla systemu Windows 10 (RSAT) oraz Windows Admin Centre.
12. System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP dla dostępu administracyjnego.
13. System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami.
14. Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta.
15. System operacyjny musi posiadać obsługę pamięci USB jako monitora kłastr.
16. System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego kłastr.
17. System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS.
18. System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień.
19. System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zapora musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ipv4 i v6;
20. System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;
21. System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
22. System operacyjny musi posiadać domyślną obsługę PowerShell 5.1;
23. System operacyjny musi posiadać obsługę certyfikatów w Active Directory.

24. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte muszą być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów). Wymagania dla równoważnych licencji dostępowych dla użytkownika: - Licencja dostępowa dla użytkownika umożliwiająca połączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera Microsoft Windows Server 2022 z wdrożoną rolą Active Directory. - Każda z licencji umożliwia użytkownikowi na dostęp z dowolnego urządzenia do zasobów serwera.
36 miesięczna gwarancja, świadczona na miejscu u klienta lub zdalnie z czasem reakcji serwisu w miejscu instalacji maksymalnie do 3 godzin roboczych w godzinach pracy Zamawiającego tj.: Poniedziałek: 07:30 – 15:30, Wtorek: 07:30 – 15:30, Środa: 07:30 – 17:00, Czwartek: 07:30 – 15:30, Piątek: 07:30 – 14:00
Serwisowe zgłoszenia za pomocą kodów QR. W ramach tej funkcji użytkownicy mają możliwość zgłaszać serwisowe problemy, skanując kod QR umieszczony na obudowie serwera. Po zeskanowaniu kodu zostaną przekierowani do formularza zlecenia serwisowego z wypełnionym automatycznie numerem seryjnym serwera, bez konieczności instalacji dodatkowych aplikacji. Formularz musi być zintegrowany systemem informatycznym Wykonawcy, w celu automatycznego stworzenia zlecenia serwisowego na podstawie wypełnionych danych w formularzu.
Zamawiający wymaga od Wykonawcy złożenia wraz z ofertą dokumentu potwierdzającego opracowanie, wdrożenie i scertyfikowanie systemu zarządzania jakością certyfikat ISO 9001 oraz ISO 27001 w zakresie wdrożeń systemów informatycznych i oprogramowania lub inny równoważny dokument, który poświadcza spełnienie wszystkich zasadniczych wymagań określonych w odpowiednich standardach ISO.
Zamawiający wymaga od Wykonawcy lub podwykonawcy zatrudnienia na podstawie umowy o pracę minimum 6 osób wykonujących wskazane czynności w trakcie realizacji zamówienia. W celu weryfikacji zatrudnienia, przez wykonawcę lub podwykonawcę, Zamawiający wymaga złożenia oświadczenia wykonawcy lub podwykonawcy wraz z ofertą.
W ramach postępowania wraz z dostawą wykonana zostanie instalacja, podłączenie oraz konfiguracja i uruchomienie sprzętu wraz z migracją danych z obecnego systemu posiadanego przez Zamawiającego. Wdrożenie: • Montaż fizycznych składników rozwiązania, podłączenie i konfiguracja interfejsów sieciowych, konfiguracja interfejsów zarządzających serwerami, aktualizacja oprogramowania sprzętowego. • Konfiguracja urządzeń sieciowych w odniesieniu do rozwiązania wirtualizacyjnego, • Instalacja systemów operacyjnych (np. serwer Windows), aktualizacja. • Konfiguracja usługi bazującej na oprogramowaniu definiowanym magazynem. • Konfiguracja usług klastra dotyczących wirtualizacji, definiowanie sieci wirtualnych, • Instalacja i konfiguracja maszyn wirtualnych (np. serwer Windows). • Tworzenie wzorcowego obrazu maszyny wirtualnej (np. serwer Windows). • Instalacja oprogramowania do zarządzania kopiami zapasowymi na dedykowanym serwerze, konfiguracja lokalnych zasobów serwera jako repozytorium kopii zapasowych, konfiguracja zadań tworzenia kopii zapasowych dla danego środowiska, weryfikacja ko • zapisowej - przywrócenie wybranej maszyny • Konfiguracja serwera VPN • Migracją danych z obecnego systemu posiadanego przez Zamawiającego wraz z obecnie wykorzystywanym oprogramowaniem. • Weryfikacja funkcjonowania środowiska. • Włączenie funkcji serwera usług katalogowych na wybranej maszynie wirtualnej. • Konfiguracja polityk usług katalogowych dotyczących urządzeń i użytkowników. • Konfiguracja profili użytkowników. • Konfiguracja dostępu do wybranych zasobów. • Instalacja usług serwera terminalowego na maszynie wirtualnej i konfiguracja usług zdalnego dostępu dla użytkowników. • Konfiguracja dostępu terminalowego na wszystkich hostach(komputerach klienckich) • Migracja obecnych profili użytkowników do serwera terminalowego • Konfiguracja połączeń VPN dla dostępu zdalnych na urządzeniach mobilnych

3) NAS – 1 kpl

Wymagane minimalne parametry techniczne komponentu (wymagania jakościowe)
Typ Online
Obudowa typu RACK o wysokości max. 2U wyposażony w szyny oraz elementy do montażu w szafie serwerowej, pochodzący z oficjalnego kanału dystrybucji na rynek Unii Europejskiej
Urządzenie montowane jest do szafy RACK 19"
Zainstalowany min. czterordzeniowy procesor ze sprzętowym mechanizmem szyfrowania AES 256bit i architekturze 64-bitów
Minimum 8 GB DDR4 pamięci RAM.
Obsługa min. 4 dysków oraz trybu RAID Single Disk, JBOD, RAID 0, 1, 5, 6, 10, zabezpieczającą przed utratą danych
Kompatybilność dysków: 2.5,3.5,M.2
System plików dla dysków zewnętrznych: EXT3, EXT4, NTFS, FAT32, HFS+
Zainstalowane min. 4 dysków, 16 TB, 6Gbp/s, 3,5", nominalny czas pracy 2.5 mln godzin, CMR. wymieniane podczas pracy
Wspierane systemy operacyjne min.: Apple Mac OS 10.10, Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12, IBM AIX 7, Solaris 10, Microsoft Windows 7, 8, 10, 11, Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022
Wpieran przeglądarki: Apple Safari, Google Chrome, Microsoft Edge, Mozilla Firefox
Min. 2 porty 2,5 Gigabit sieci Ethernet (2,5G/1G/100M)
Min. 2 porty USB 3.2 Gen 2 (10 Gb/s), 2 porty USB 2.0
Min. 1 Wyjście HDMI, Gniazdo PCIe Gen 3 x2
Ochrona systemu operacyjnego przed podwójnych rozruchem z wykorzystaniem pamięć flash min. 4 GB
Pobór mocy: Tryb pracy, typowy maksimum 37 W
Dźwiękowe ostrzeżenie systemowe,
36 miesięczna gwarancja, świadczona na miejscu u klienta lub zdalnie z czasem reakcji serwisu w miejscu instalacji maksymalnie do 8 godzin roboczych w godzinach pracy Zamawiającego tj.: Poniedziałek: 7.30 - 15:30, Wtorek 7:30 - 15:30, Środa 7:30 – 17:00, Czwartek 7:30 – 15:30, Piątek: 7:30 - 14:00
W komplecie do oferowanego sprzętu wszystkie niezbędne do uruchomienia kable zasilające, przewody sygnałowe.

4) UTM – 1 szt.

Wymagane minimalne parametry techniczne komponentu (wymagania jakościowe)

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.

2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

3. Monitoring stanu realizowanych połączeń VPN.

4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

- 5 portami Gigabit Ethernet RJ-45.
- 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
- 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
- 4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.

2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.

3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 990 Mbps.

4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4.4 Gbps.

5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.

6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps.

7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 310 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych.

Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.

12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.

13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

- Translację jeden do jeden oraz jeden do wielu.
- Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.

5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.

6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.

7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.

- Amazon Web Services (AWS).
- Microsoft Azure.
- Cisco ACI.
- Google Cloud Platform (GCP).
- OpenStack.
- VMware NSX.
- Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:

- Wsparcie dla IKE v1 oraz v2.
- Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
- Obsługę protokołu Diffie-Hellman grup 19, 20.
- Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
- Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.

- Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.

- Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.

- Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.

- Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling” dla połączeń Client-to-Site.

2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:

- Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.

- Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

- Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

2. Policy Based Routing (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łącz WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPsec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 10000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.



2. Baza Kontroli Aplikacji zawiera minimum 5000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
 - Hasła statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
 - Hasła statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - Hasła dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie



1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne

Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesiące. Gwarancja oraz wsparcie

System jest objęty serwisem gwarancyjnym producenta przez okres 24 miesiące, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. W ramach wdrożenia zostaną przeprowadzone szkolenia dla administratorów IT w celu podniesienia ich kompetencji w zakresie obsługi urządzeń UTM a co za tym idzie zwiększy płynność w administrowaniu elementami (firewall) struktury bezpieczeństwa oraz administrowania urządzeniem UTM. Zakres szkolenia winien obejmować:

- Architektura urządzenia
- Wstępna konfiguracja urządzenia
 - Tryby pracy NAT/Transparent
 - Konfiguracja sieci i routingu
 - System Dashboard i moduły systemu
- Konfiguracja routingu
- Polityki zapory sieciowej
 - Koncepcja firewall w urządzeniach
 - Tworzenie obiektów dla reguł firewall
 - Translacja adresów NAT i Virtual IP
- Konfiguracja funkcji ochronnych (profile bezpieczeństwa)
 - Ochrona antywirusowa
 - Filtrowanie antyspamowe
 - System IPS
 - Kontrola ruchu WWW / blokowanie URL
 - Kontrola aplikacji
 - Data Leak Prevention (DLP)
 - Wirtualne sieci prywatne – VPN IPSec
- Bieżąca obsługa systemu
 - Tworzenie kopii zapasowej konfiguracji i jej odtwarzanie
 - Aktualizacja firmware
- Logowanie i alerty
 - Filtry logów
 - Zewnętrzne mechanizmy logowania
 - Dobre praktyki w zarządzaniu

Termin realizacji do 14 dni od dnia podpisania umowy.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Część II. Usługi doradztwa i szkoleń.

a) Doradztwo w zakresie określenia poziomu cyberbezpieczeństwa

Przedmiotem zamówienia są usługi wspomagające realizację projektu „Cyberbezpieczny Samorząd”, na etapie wdrażania projektu oraz rozliczania, przez osobę o wiedzy technicznej, z zakresu cyberbezpieczeństwa oraz warunków realizacji projektu „Cyberbezpieczny Samorząd”.

Zakres usługi dotyczyć ma :

- wsparcia na etapie prowadzenia rozliczania projektu,
- opracowania procedury monitorowania utrzymania efektów w okresie trwałości projektu.

b) Przygotowanie dokumentacji SZBI.

Aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji dostosowanego do potrzeb i warunków pracy urzędu, zgodnego z aktualnie obowiązującymi normami w tym konsultacji w zakresie określenia poziomu cyberbezpieczeństwa, opracowanie dokumentacji zawierającej polityki i procedury SZBI, z uwzględnieniem technologii nowo zakupionych w ramach grantu wraz z wdrożeniem, zgodnie z wymaganiami Rozporządzenia w sprawie Krajowych Ram Interoperacyjności z dnia 21.05.2024r. dla podmiotów publicznych i wg wymagań normy ISO/IEC 27001.

Zakres prac:

Etap I – Inwentaryzacja zasobów

Etap II - Wywiad przedwdrożeniowy

Etap III – Szacowanie ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych w JST.

Etap IV – Opracowanie dokumentacji i procedur Systemu Zarządzania Bezpieczeństwem Informacji.

Etap V – Wdrożenie procedur SZBI.

Etap VI – Przegląd wdrożonego SZBI - monitorowanie, przeglądy, ocena, poprawki, aktualizacja, audyty powdrożeniowy.

Czas realizacji do 150 dni, wg planu, sposób realizacji:

Etap	Realizacja	Planowany czas realizacji (dni)
I	z wykorzystaniem zdalnej komunikacji.	30
II	z wykorzystaniem zdalnej komunikacji.	
III	w siedzibie Zamawiającego oraz z wykorzystaniem zdalnej komunikacji,	
IV	z wykorzystaniem zdalnej komunikacji.	30
V	w siedzibie Zamawiającego oraz z wykorzystaniem zdalnej komunikacji,	30
VI	z wykorzystaniem zdalnej komunikacji.	60

c) Audyt końcowy

Przedmiotem zamówienia jest przeprowadzenie audytu w zakresie bezpieczeństwa informacji, wymagany „Rozporządzeniem Rady Ministrów z dnia 21.05.2024r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych” wraz z przygotowaniem raportu z audytu ze wskazaniem istniejących zagrożeń i kierunków doskonalenia w ramach projektu „Cyberbezpieczny Samorząd” w Urzędzie Miasta i Gminy Solec nad Wisłą,

Zamawiający nie dopuszcza wykonanie usługi w formie zdalnej.

d) Szkolenia z cyberbezpieczeństwa

Przeszkolenie pracowników urzędu z zakresu cyberbezpieczeństwa. Szkolenia będą świadczyć osoby kompetentne, posiadające wymagane kwalifikacje.

Zakres szkolenia: praktyczne podejście do cyberbezpieczeństwa, zagadnienia związane z informatyzacją Urzędu zarządzaniem systemami teleinformatycznymi, zarządzaniem dokumentami elektronicznymi.

Warunki szkolenia:

- liczba uczestników: 25 osób, z podziałem na 2 grupy,
- liczba szkoleń: 4
- szkolenie dla 2 grup w ciągu jednego dnia, w kolejnych dniach roboczych
- czas szkolenia – 5 godzin szkoleniowych 45-minutowych
- tryb stacjonarny,
- szkolenie powinno odbyć się w dni robocze, w trakcie godzin pracy urzędu,
- zaświadczenie o udziale w szkoleniu,
- przekazany dla każdego uczestnika materiał informacyjny, w formie broszury lub publikacji - kompendium wiedzy z zakresu cyberbezpieczeństwa, budujący świadomość o zagrożeniach cybernetycznych oraz o cyberhigienie - zgodnie z wymogami Regulaminu Konkursu Grantowego.

Realizacja szkoleń:

Część I: do 60 dni od zawarcia umowy.

Warunki udziału w postępowaniu.

O udzielenie zamówienia Część II ubiegać się mogą Wykonawcy, którzy spełniają warunki łącznie:

1. dysponują co najmniej 1 audytorem o kwalifikacjach:

- audytor wiodący wg normy ISO/IEC 27001, z których co najmniej jeden otrzymał certyfikację nie później niż 1.07.2022r

2. dysponują co najmniej 1 audytorem o kwalifikacjach:

- audytor wiodący wg normy ISO/IEC 22301.

3. w okresie ostatnich 3 lat przed upływem terminu składania ofert o udzielenie zamówienia, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie – **wykonali należycie co najmniej 2 usługi** wdrożenia SZBI, obejmującą analizę ryzyka, opracowanie procedur i szkolenie w ramach dokumentacji SZBI na rzecz podmiotu publicznego o wartości minimum 30 000 zł brutto. **Liczba wykonanych wdrożeń SZBI stanowi kryterium oceny ofert.**

4. posiadają niezbędną wiedzę i doświadczenie, tzn.: w okresie ostatnich 3 lat przed upływem terminu składania ofert o udzielenie zamówienia, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie – wykonali należycie co najmniej 10 zamówień na rzecz podmiotów publicznych obejmujących swym zakresem audyt systemu bezpieczeństwa informacji zgodnie z wymaganiami określonymi w § 20 Rozporządzenia Rady Ministrów z dnia 12.04.2012 r. lub z 21.05.2024r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, zgodnym z normą ISO/IEC 27001.

5. dysponują szkoleniowcem o udokumentowanym doświadczeniu w prowadzeniu szkoleń obejmujących elementy

cyberbezpieczeństwa od co najmniej 3 lat oraz posiadającym certyfikat audytora wiodącego wg normy ISO/IEC 27001.

6. wymagane, aby Wykonawca był wpisany do Rejestru Instytucji Szkoleniowych od co najmniej 2 lat.

7. audytorzy wiodący wskazani przez Wykonawcę do realizacji niniejszego zlecenia nie mogą jednocześnie stanowić zespołu prowadzącego prace wdrożenia SZBI u Zamawiającego. Nie zastosowanie się do wymogu będzie podstawą do wykluczenia z postępowania.

Część III. Zakup i dostawa agregatu prądotwórczego – 1 szt.

AGREGAT ZASILAJACY (PRĄDOTWÓRCZY)

1. Podstawowe wymagania:

- Moc znamionowa w trybie gotowości ESP 133-137 kVA
- Moc znamionowa ciągła PRP 98-102 KW
- Napięcie 400 V (3 fazy), Częstotliwość 50 Hz
- Prąd znamionowy PRP 3 fazy minimum 180 A
- Klasa wydajności minimum G2 wg ISO 8528-5:1993, zdolność przyjmowania obciążenia w jednym kroku minimum 70% PRP wg EN ISO 8528-5
- Temperatura pracy: -25 – 40 °C
- Wymiary maksymalne: długość - 3000 mm, szerokość – 1100 mm, wysokość – 1.700 mm
- Waga agregatu z płynami eksploatacyjnymi bez paliwa maksymalnie 1600 kg
- Certyfikat CE
- Gwarancja minimum 12 miesięcy lub 2.000 godzin pracy co nastąpi szybciej
- Dostawa loco Klient + szkolenie obsługi po dostawie

2. Wymagane parametry obudowy:

- Typ: wyciszona do użytkowania na zewnątrz
- Ochrona antykorozyjna – blacha ocynkowana elektrolitycznie malowana proszkowo
- Moc akustyczna (LwA) maksymalnie 94 dBA zgodnie z 2000/14/WE
- Wewnątrz ochrona przed gorącymi elementami
- Stopień ochrony IP minimum 44
- Wyłącznik bezpieczeństwa tzw. grzybek
- Drzwi serwisowe zamknięte na klucz

3. Wymagane parametry silnika napędowego:

- Spalinowy / wysokoprężny spełniający normę minimum Stage I
- Liczba cylindrów 6
- Pojemność skokowa minimum 5,9 l
- Moc netto 119-123 kW
- Prędkość obrotowa 1.500 obr/min, elektroniczna lub elektryczna regulacja obrotów
- Pojemność układu chłodzenia 10 - 12 l
- Pojemność układu olejowego 14 - 15 l
- Zbiornik paliwa o pojemności minimum 260 l (minimum 10 h pracy przy 100% PRP),
- Korek wlewu paliwa wewnątrz obudowy
- Akumulator 24 V (2x 45 Ah, 2x 12 V)

4. Wymagane parametry prądnicy:

- Moc PRP min. 125 kVA przy 125 °C /40 °C
- Synchroniczna, samowzbudna, samoregulująca, bez szczotkowa, jednołożyskowa,

- Liczba biegunów 4
- Elektroniczny regulator AVR o stabilizacji napięcia +/- 1%
- Stopień ochrony IP minimum 23
- Klasa izolacji H
- Sprawność prądnicy przy 100% cos φ min. 90%
- Współczynnik mocy cos φ = 0,8

5. Wymagane parametry panelu sterującego (sterownika):

- Wyświetlacz LCD
- Tryb pracy: rozruch ręczny i automatyczny,
- Przegląd podstawowych parametrów pracy (prędkość obrotowa silnika, napięcie, częstotliwość, czas pracy, napięcie baterii)
- Wyświetlanie stanów alarmowych
- Ochrona i zabezpieczenie silnika i prądnicy
- Sterowanie układem SZR (wykrywanie zaniku zasilania z sieci i automatyczne przełączanie na zasilanie z generatora, przy powrocie zasilania z sieci automatyczne przełączenie z powrotem)

6. Wymagane wyposażenie:

- Listwa zaciskowa umożliwiająca wyprowadzenie maksymalnej mocy agregatu
- Gniazda odbioru mocy zabudowane w obrysie maszyny (400 V - 63A , 32 A , 16 A + 230 V – 1 szt)
- Rama bezwyciekowa mogąca pomieścić min. 100% łącznej objętości wszystkich płynów znajdujących się w generatorze (ON, chłodziwo, olej smarujący)
- Zewnętrzny punkt spustowy (wannę retencyjną, zbiornika paliwa, oleju, chłodziwa)
- Wyłącznik główny 4 biegunowy
- Układ SZR (samoczynne załączanie rezerwy) w oddzielnej otwieranej obudowie metalowej:
 - wymiary maksymalne: długość – 650 mm, szerokość – 350 mm, wysokość – 650 mm
 - ochrona IP min 54
 - układ sterowany przez sterownik generatora prądotwórczego
 - przełącznik 4 – polowy z napędem silnikowym
 - blokada mechaniczna i elektryczna przed równoczesnym załączeniem dwóch źródeł zasilania
 - prąd znamionowy 248 - 253 A
 - napięcie Vac 180 – 280 V
 - częstotliwość 50 Hz
- Ładowarka akumulatora
- Grzałka płynu chłodzącego minimum 1000 W
- Dokumentacja techniczno- ruchowa (instrukcja obsługi, katalog części)

Termin realizacji do 60 dni. Od dnia podpisania umowy.

Wszelkie ewentualnie użyte nazwy handlowe w opisie przedmiotu zamówienia należy traktować jako informację uściślającą, która została użyta wyłącznie w celu przybliżenia potrzeb Zamawiającego. Dopuszcza się użycie do realizacji prac produktów równoważnych, co do ich jakości, docelowego przeznaczenia i spełnianych funkcji i walorów użytkowych. Przez jakość należy rozumieć zapewnienie minimalnych parametrów produktu wskazanego w dokumentacji. Wykonawca, który do wyceny przyjmie rozwiązania równoważne jest zobowiązany udowodnić równoważność przyjętych urządzeń, sprzętu i materiałów Zamawiającemu.

Wymagania ogólne dla urządzeń i oprogramowania

1. Dostarczony sprzęt musi być fabrycznie nowy (rok produkcji co najmniej 2024), nieużywany, nieregenerowany, kompletny, dostarczony w opakowaniu oryginalnym (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta). Nie dopuszcza się

- zastosowania urządzeń tzw. „refurbished”, rozwiązań odnawianych oraz eksponowanych na wystawach czy prezentacjach.
2. Sprzęt musi być wolny od wad fizycznych i prawnych, musi być sprawny technicznie oraz musi pochodzić z autoryzowanego kanału dystrybucyjnego. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanych rozwiązań, potwierdzające pochodzenie urządzeń z oficjalnego kanału dystrybucyjnego producenta.
 3. Dostarczone oprogramowanie musi być nowe, nieużywane, nieaktywowane wcześniej na innym urządzeniu, dostarczone w najnowszej stabilnej wersji pochodzącej z oficjalnego kanału dystrybucyjnego producenta oprogramowania, nieobciążone prawami na rzecz osób trzecich. Dostarczone oprogramowanie i wszelkie jego nośniki (o ile występują) muszą być wolne od wad fizycznych i prawnych. Oprogramowanie musi być opatrzone we wszystkie atrybuty oryginalności i legalności wymagane przez producenta oprogramowania w zależności od dostarczanej wersji oprogramowania.
 4. Serwis w ramach udzielonej gwarancji będzie realizowany bezpośrednio przez producenta i/lub we współpracy z autoryzowanym partnerem serwisowym producenta.
 5. Wszystkie urządzenia powinny być zgodne z normami UE oraz powinny posiadać certyfikację oraz oznaczenie CE.
 6. W celu uniknięcia błędów kompatybilności Zamawiający wymaga, aby wszystkie elementy oferowanych zestawów oraz podzespoły montowane przez producenta były przez niego certyfikowane.
 7. W formularzu ofertowym należy podać nazwę producenta, model, symbol (nazwę handlową) oraz parametry oferowanego rozwiązania (jeśli są wymagane) umożliwiające jednoznaczną weryfikację oferowanej konfiguracji oraz w celu identyfikacji należy podać pełną nazwę handlową oferowanego oprogramowania.

Warunki dotyczące realizacji dostaw i odbiorów:

1. Wykonawca na swój koszt i ryzyko dostarczy przedmiot zamówienia, zgodny z wymaganiami przedstawionymi w niniejszym dokumencie.
2. Wykonawca w cenie oferty uwzględni wszystkie koszty niezbędne do realizacji dostawy, w tym rozładunek, wniesienie oraz utrzymanie porządku w czasie rozładunku prowadzonego na terenie urzędu.
3. Wykonawca, co najmniej na 3 dni przed dniem planowanej dostawy sprzętu, dokona jej awizacji, to znaczy skontaktuje się z Zamawiającym w celu ustalenia miejsca i potwierdzenia konkretnego terminu dostawy.
4. Dostawa sprzętu odbędzie się w dniu roboczym, od poniedziałku do piątku, w godzinach 8:00 - 14:00, transportem zapewnionym przez Wykonawcę, na jego koszt i ryzyko wraz z wniesieniem do miejsca wskazanego przez Zamawiającego.
5. Do czasu odbioru sprzętu przez Zamawiającego, ryzyko wszelkich niebezpieczeństw związanych z jego ewentualnym uszkodzeniem lub utratą ponosi Wykonawca.
6. Wraz ze sprzętem Wykonawca zobowiązany jest przekazać Zamawiającemu listę numerów seryjnych dostarczonych urządzeń wszelką dokumentację dostarczoną przez producenta sprzętu.
7. W ramach procedury odbioru, Zamawiający zastrzega sobie w przypadku wątpliwości prawo do przeprowadzenia weryfikacji oryginalności i legalności dostarczonego przez Wykonawcę oprogramowania bezpośrednio u producenta oprogramowania, przed podpisaniem protokołu odbioru w sposób, który uzna za bezsporny. W przypadku wykrycia, że dostarczony system operacyjny lub inne licencjonowane oprogramowanie jest nieoryginalne (nielegalne), nie jest nowe, było już używane lub było już wcześniej aktywowane, Zamawiający w takiej sytuacji

odmówi przyjęcia licencji oprogramowania i wezwie Wykonawcę do usunięcia nieprawidłowości w wyznaczonym terminie.