**Opis przedmiotu zamówienia (OPZ)**

Przedmiotem zamówienia jest dostawa, konfiguracja i wdrożenie zintegrowanego systemu zabezpieczania dostępu do sieci teleinformatycznej, monitorowania i logowania dostępu firm trzecich do infrastruktury informatycznej oraz zarządzanie stacjami roboczymi i urządzeniami mobilnymi Zarządu Transportu Miejskiego w Poznaniu.

Zakres przedmiotu obejmuje:

1. System do monitorowania i logowania dostępu firm trzecich do sieci oraz infrastruktury informatycznej Zarządu Transportu Miejskiego w Poznaniu.
2. Zintegrowane oprogramowanie do zarządzania stacjami roboczymi i urządzeniami mobilnymi
3. System typu Next Generation NAC (zwany dalej platforma NG-NAC), który dynamicznie identyfikuje i analizuje systemy podłączone do sieci oraz aplikacje natychmiast po podłączeniu ich do sieci Zarządu Transportu Miejskiego w Poznaniu.
4. Szkolenia w dwóch etapach:
	1. wdrożeniowe (8h)
	2. doszkalające (16h)
5. W ramach wdrożenia Zamawiający wymaga dostosowania dostarczonego oprogramowania do środowiska Zamawiającego.

Dostarczone licencje na oprogramowanie dla poniższych zadań są bezterminowe i zawierają minimum 12-miesięczne wsparcie producenta, w tym dostęp do najnowszych wersji oprogramowania. Zamawiający wymaga wsparcia producenta i/lub dostawcy w pełnym zakresie usług i w wersji polskojęzycznej.

Zamawiający zapewnia dostępność do infrastruktury teleinformatycznej w celu zapewnienia funkcjonowania dostarczonego oprogramowania.

Dla każdej części Zamówienia Zamawiający zapewni wymagany serwer wirtualny lub niezbędne zasoby dostępne w infrastrukturze teleinformatycznej Zamawiającego i spełanijące minimalne wymagania producenta oprogramowania.

Zamawiający nie zapewnia konfiguracji w oparciu o odpłatne warianty baz danych firm trzecich. Zapewni wersje darmowe MS Express, Postgres, MariaDB i inne.

**Zadanie 1**

**Wymagania funkcjonalne do systemu do monitorowania i logowania dostępu użytkowników oraz firm trzecich do infrastruktury informatycznej Zarządu Transportu Miejskiego (ZTM)**

**Opis funkcjonalny:**

* Oprogramowanie musi nagrywać sesje / połączenia w formie wideo do serwerów i stacji roboczych Windows, Mac, Linux, Citrix, VMware zarządzanych przez ZTM :

- Stacje robocze: 250

- Serwery Linux: 30

- Serwery Windows (max. 2 połączenia): 50

- Serwery Terminalowe Windows (wiele połączeń): 5

* Oprogramowanie musi mieć możliwość rozszerzenia liczby nagrywanych stacji roboczych, serwerów w przyszłości bez konieczności ponownej instalacji/rekonfiguracji oprogramowania.
* Oprogramowanie musi mieć możliwość nagrywania sesji przechodzących z poza infrastruktury ZTM np. VPN lub firm trzecich.
* Oprogramowanie musi mieć aktywny monitoring działań / sesji administratorów i użytkowników na podstawie zdefiniowanych scenariuszy z możliwością zerwania sesji w przypadku wykrycia działań niepożądanych.
* Wsparcie dla protokołów sesji zdalnej RDP, SSH, CITRIX, VMware.
* Wsparcie zewnętrznych zasobów dyskowych dla nagrywanych sesji.
* Możliwość podglądu wielu sesji na żywo przez wielu obserwujących.
* Oprogramowanie musi mieć możliwość przeszukiwania nagrywanych sesji na podstawie metadanych.
* Integracja rozwiązania z istniejącym u Zamawiającego Active Directory.
* Oprogramowanie musi mieć możliwość audytowania czynności administracyjnych użytkowników systemu monitorowania.
* Zarządzanie przez konsolę WEB dla najpopularniejszych przeglądarek internetowych bez konieczności użycia wtyczek firm trzecich (wtyczka Flash, Java).
* Możliwość wdrożenia rozwiązania w trybie wysokiej dostępności i szybkie przywrócenie działania w razie awarii.
* Oprogramowanie musi mieć możliwość zalogowania się do systemów z koniecznością podania dwóch różnych poświadczeń.
* Oprogramowanie musi mieć możliwość określenia kont użytkowników i grup domenowych, które mają być monitorowane lub wykluczone z monitorowania.
* Oprogramowanie musi mieć możliwość określenia adresów IP, które mają być monitorowane lub wykluczone z monitorowania.
* Możliwość eksportu nagrań wraz metadanymi do bezpiecznego, zaszyfrowanego formatu z możliwością weryfikacji autentyczności i integralności nagrania oraz z możliwością odtworzenia wyeksportowanego nagrania na każdym komputerze bez konieczności instalowania dodatkowego oprogramowania

|  |  |
| --- | --- |
| Funkcje dodatkowe ( opcjonalne) | Punktacja |
| 1. | Kryterium: Zarządzanie dostępem RDP i hasłami bez ujawniania poświadczeń | 1 |
| Zarządzanie sesjami i użytkownikami uprzywilejowanymi dla dostępu RDP, z wykorzystaniem bezpiecznego sejfu haseł. Poświadczenia do docelowych systemów pozostają niejawne dla użytkowników. |
| 2. | Kryterium: Tryb Multi-Tenant dla systemów Windows i Linux | 1 |
| Możliwość wydzielenia odrębnych środowisk w ramach pojedynczego systemu. Dane każdego środowiska, w tym dane monitorowania, poświadczenia użytkowników, nazwy monitorowanych punktów końcowych, konfiguracji systemu jest całkowicie niezależna i niedostępna dla innych środowisk. |
| 3. | Kryterium: Nagrywanie sesji X Windows, konsoli SSH oraz konsoli maszyn wirtualnych VMware na żywo | 1 |
| Możliwość nagrywania sesji graficznych Linux opartych o system okien X Windows, a także konsoli SSH oraz konsoli maszyn wirtualnych VMware. |
| 4. | Kryterium: Ręczne zatwierdzenie dostępu do serwerów Windows i Linux | 1 |
| W momencie logowania się użytkownika do serwera docelowego, administrator systemu monitorowania otrzyma powiadomienie z prośbą o akceptację/ odrzucenia połączenia. |
| 5. | Kryterium: Zatwierdzenie dostępu do serwerów Windows i Linux w oparciu o harmonogram | 1 |
| Możliwość zdefiniowania dostępu do serwerów w oparciu o kalendarz, z możliwość określenia przedziału godzinowego i dni tygodnia, w których dostęp ma być możliwy. Logowanie poza wyznaczonym przedziałem czasowym powinno być niemożliwe |
| 6. | Kryterium: Monitorowania udostępniania plików | 1 |
| Monitorowanie udostępniania plików poprzez okno dialogowe i metodę przeciągnij-i-upuść co najmniej w przeglądarkach Internet Explorer, Chrome, Opera, Firefox oraz w aplikacji desktopowej i webowej Skype. |
| 7. | Kryterium: Blokowanie urządzeń USB na stacjach roboczych Windows oparte o reguły na potrzeby nagrywania sesji | 1 |
| Zablokowanie możliwości korzystania z poszczególnych rodzajów urządzeń USB (np. pamięci masowe, drukarki, karty sieciowe) na stacjach roboczych Windows z określeniem wyjątków, które nie będą blokowane. |
| 8. | Kryterium: Ręczne zatwierdzenie dostępu do pamięci masowych USB na stacjach roboczych Windows na potrzeby nagrywania sesji | 1 |
| W momencie zablokowania urządzenia USB, użytkownik ma możliwość wysłania prośby do administratora systemu monitorowania o uzyskanie dostępu do urządzenia. |
| 9. | Kryterium: Wsparcie dla bazy danych PostgreSQL | 1 |
| Możliwość wdrożenia systemu monitorowania działającego w oparciu o darmową bazę danych PostgreSQL. |
| 10. | Kryterium: Integracja z Windows Event Log i Syslog | 1 |
| Możliwość udostępniania logów z monitorowanych maszyn do programu Windows Event Log i Syslog. |
| 11. | Kryterium: Nagrywanie audio | 1 |
| Nagrywanie dźwięków wejściowych i wyjściowych co najmniej w przeglądarkach Internet Explorer, Chrome, Opera, Firefox oraz w aplikacji desktopowej i webowej Skype. |
| 12. | Kryterium: 2FA dla stacji roboczych Windows | 1 |
| System monitorowania ma możliwość dwuskładnikowego uwierzytelniania przy logowaniu do stacji roboczych Windows (poświadczenia + token). |
| 13. | Kryterium: 2FA dla serwerów Windows | 1 |
| System monitorowania ma możliwość dwuskładnikowego uwierzytelniania przy logowaniu do serwerów Windows (poświadczenia + token). |
| 14. | Kryterium: 2FA dla systemów Linux | 1 |
| System monitorowania ma możliwość dwuskładnikowego uwierzytelniania przy logowaniu do systemów Linux (poświadczenia + token). |
| 15. | Kryterium: Licencjonowanie wspierające rejestrację sesji dla tymczasowych maszyn wirtualnych | 1 |
| System musi mieć możliwość automatycznego przypisania licencji z puli dla nowo utworzonych tymczasowych maszyn wirtualnych i automatycznego zwolnienia licencji w przypadku usunięcia maszyny. |
| 16. | Kryterium: Filtrowanie monitorowania sesji w oparciu o adres IP | 1 |
| Możliwość określenia adresów IP, które mają być monitorowane lub wykluczone z monitorowania. |
| 17. | Kryterium: Monitorowanie wyłącznie aktywnego okna | 1 |
| Możliwość monitorowania wyłącznie aktywnego okna, z pominięciem okien znajdujących się w tle. |
| 18. | Kryterium: Powiadomienie o niedostępności monitorowanego punktu końcowego | 1 |
| System monitorowania ma możliwość cyklicznego sprawdzania, czy monitorowany punkt końcowy jest dostępny, aby zapewnić stabilność i bezpieczeństwo działania systemu, a w razie jego niedostępności wysyła powiadomienia do administratorów. |
| 19. | Kryterium: Nagrywanie sesji dla niedostępnego punktu końcowego | 1 |
| Możliwość nagrywania sesji dla punktu końcowego, który utracił połączenie z systemem monitorowania. |
| 20. | Kryterium: Keylogger | 1  |
| Możliwość określenia nagłówków okien i nazw aplikacji, dla których mają być przechwytywane naciśnięcia klawiszy lub dla których naciśnięcia klawiszy mają nie być przechwytywane. |
| Suma punktów dodatkowych | 20 |

**Zadanie 2.**

**System do zarządzania stacjami roboczymi oraz urządzeniami mobilnymi ZTM**

**Funkcje podstawowe**

* Dostarczone licencje na oprogramowanie są bezterminowe z opcją możliwością zwiększenia ilości licencji w okresie 3 lat liczonej od momentu uruchomienia systemu w środowisku produkcyjnym.

- Stacje robocze: 250

- Urządzenia mobilne: 250

* Niezależnie od wykupionego supportu wymagany jest dostęp do nowych wersji systemu.
* Odczyt informacji dotyczących parametrów sprzętowych komputera odbywa się za pośrednictwem Agenta poprzez lokalny odczyt WMI oraz bezpośredni dostęp do komponentów np. bezpośredni odczyt parametrów z BIOS’u komputera.
* Oprogramowanie serwera aplikacji umożliwia wysyłanie powiadomień mailowych.
* Oprogramowanie zawiera system ról, dzięki któremu jest możliwe przypisywanie wybranych grup stanowisk do poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje grupowe obejmują wtedy tylko w/w przypisane grupy stanowisk.
* Oprogramowanie jest podpisane cyfrowo przez producenta ważnym certyfikatem, z prawidłową ścieżką certyfikacji, w której główny urząd certyfikacji (Root CA) jest uczestnikiem programu certyfikatów głównych systemu Windows. Podpis cyfrowy dotyczy każdego składnika systemu włączając w to pliki wykonywalne (\*.exe), pliki bibliotek współdzielonych (\*.dll), pliki sterowników (\*.sys) oraz pliki paczek oprogramowania (\*.msi).
* Oprogramowanie realizuje zarządzanie wszystkimi modułami systemu z poziomu tej samej konsoli zarządzającej.
* Oprogramowanie Agenta realizuje wszystkie wymagane funkcjonalności z poziomu jednej instancji usługi lub procesu, bez wykorzystywania aplikacji oraz usług firm trzecich za wyjątkiem aplikacji oraz usług wbudowanych w system operacyjny na którym zainstalowany został Agent.
* Oprogramowanie Agentów posiada obsługę sesji terminalowych Windows.
* Oprogramowanie zapewnia dowolną konfigurację pracy wszystkich Agentów, grupy Agentów, pojedynczego Agenta, poprzez dziedziczenie definiowanych przez administratora parametrów. Zmiany konfiguracji Agentów następują w trybie natychmiastowym (online).
* Oprogramowanie zapewnia import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieżdżeń z kontenera Active Directory/ LDAP ze wszystkimi atrybutami obiektów) z możliwością tworzenia listy filtrów zawężających węzły danych.
* Oprogramowanie współpracuje z systemami bazodanowymi Microsoft SQL Server (również w wersji Express), Oracle Server.
* Oprogramowanie współpracuje z dystrybuowanymi instalacjami (architektura 3-tier): serwer aplikacji, konsola zarządzająca, bazy danych różnorodnych systemów, itp.
* Oprogramowanie zawiera konsolę zarządzającą jako integralna część oprogramowania (nie tylko interfejs webowy).
* Oprogramowanie wspiera szyfrowanie wrażliwych danych przechowywanych w bazie danych.
* Oprogramowanie zawiera Agenta dla Mac OSX od min. 10.7 (Lion).
* Oprogramowanie zawiera Agenta dla systemów Android od min. 4.0.4. i Android Enterprise od min. 7.0.
* Oprogramowanie zawiera Agenta dla systemów z Samsung Knox.
* Oprogramowanie zawiera Agenta dla systemów iOS od min. 9.0.
* Oprogramowanie zawiera Agenta dla systemów Windows Mobile od min. 10.
* Oprogramowanie ma wsparcie dla więcej niż jednego serwera repozytorium (DIP-Server).
* Oprogramowanie ma wsparcie dla technologii PXE-Relay.
* Oprogramowanie ma wsparcie dla technologii WakeUp-Points.
* Oprogramowanie ma możliwość integracji z Active Directory.
* Oprogramowanie oferuje możliwość dowolnego definiowania portów dla komunikacji.
* Oprogramowanie zapewnia zabezpieczanie identyfikacji serwera za pomocą certyfikatów.
* Oprogramowanie obsługuje niewielką przepustowością łącza dla kontroli Agentów i przesyłania informacji o statusach.
* Oprogramowanie ma Agentów, które nie obciążają stacji roboczych.
* Oprogramowanie ma Agentów, które nie zakłócają pracy oprogramowania antywirusowego będącego w posiadaniu Zamawiającego (brak fałszywych monitów pracy Agenta).
* Oprogramowanie umożliwia indywidualną synchronizację pomiędzy pojedynczymi serwerami repozytorium (ograniczenie czasowe i przepustowości łącza).
* Oprogramowanie ma możliwość dostępu w trybie tylko do odczytu do AD, bez rozszerzeń schematu.
* Oprogramowanie wspiera zadania/Joby Push i Pull (łącznie z zadaniem typu shutdown).
* Oprogramowanie ma wsparcie dla komunikacji bez konieczności zestawiania połączenia VPN z urządzeniami, które są poza siecią poprzez bramkę Proxy instalowaną w strefie DMZ. Bramka Proxy musi stanowić integralną część Oprogramowania. Komunikacja pomiędzy bramką a agentem, jak i bramką a serwerem musi odbywać się poprzez protokół HTTPS.
* Oprogramowanie umożliwia logowanie do konsoli poprzez Windows Credentials (lub alternatywny Login).
* Oprogramowanie umożliwia podgląd w konsoli aktualnego statusu systemu Oprogramowania wraz ze wszystkimi istotnymi informacjami.
* Oprogramowanie ma możliwość zapisu ostatniego obrazu poprzez konsolę.
* Oprogramowanie umożliwia pracę wielu administratorów równocześnie na jednej konsoli.
* Oprogramowanie ma wsparcie dla LAN, zdalne i OFFLINE stanowiska pracy.
* Oprogramowania umożliwia wyświetlenie informacji i stanu/statusów dostępnych w czasie rzeczywistym.
* Oprogramowanie umożliwia na natychmiastowe generowanie komunikatów o błędach (wraz z informacją o docelowym systemie OS).
* Oprogramowanie ma poniższe funkcjonalności takie jak:
	+ Dowolnie definiowane dodatkowe pola (zmienne) przechowywane w tej samej bazie danych (np. Informacje o gnieździe sieciowym, danych dotyczących wynajmu, informacje supportowe, …).
	+ Rozbudowane funkcjonalności dotyczące zarządzania uprawnieniami.
	+ Wsparcie dla grup dynamicznych na potrzeby indywidualnych informacji/widoku.
* Oprogramowanie musi zawierać opcję ukrywania danych osobowych użytkowników (takich jak imię, nazwisko, login) dla wybranych administratorów.
* Oprogramowanie musi umożliwiać przyznawanie i blokowanie dostępu do wybranej części infrastruktury oraz wybranych części funkcjonalności oprogramowania wskazanym administratorom.
* Oprogramowanie pozwala na wysyłanie polecenia w trybie "Push".
* Oprogramowanie pozwala na wysyłanie polecenia w trybie "Pull".
* Oprogramowanie pozwala na wysyłanie polecenia w trybie "Shutdown".
* Oprogramowanie pozwala na indywidualną interakcję użytkownika w trakcie wykonywania zadania uruchomionego przez administratora w trybach: opóźnienie, odmowa, przypomnienie o instalacji.
* Oprogramowanie ma możliwość automatycznego generowania i wysyłania powtarzających się zadań.
* Oprogramowanie ma możliwość uruchomiania danego zadania z poziomu użytkownika końcowego poprzez Kiosk (dostępnego przez przeglądarkę internetową lub aplikację na urządzeniach mobilnych).
* Oprogramowanie ma możliwość inicjowania zadań z poziomu aplikacji selfservice będącej integralną część konsoli Webowej.
* Oprogramowanie ma funkcjonalność definiowania zawartości aplikacji Kiosku może być definiowana zarówno per Użytkownik lub Grupa Użytkowników jak i per stacja robocza lub jednostka organizacyjna (w AD).
* Oprogramowanie ma wbudowany kreator do tworzenia pakietów, w skład których wchodzi różnorodne oprogramowanie.
* Oprogramowanie ma wbudowaną detekcję oraz wsparcie kreatora dla wielu mechanizmów instalacji: MSI, InnoSetup, NullSoft, Wise-Installer i inne.
* Oprogramowanie ma możliwość uzupełniania instalacji oprogramowania na urządzeniu końcowym o dodatkowe kroki ze strony użytkownika końcowego (np.: deaktywacja okna powitalnego, itp).
* Oprogramowanie ma wbudowaną integrację dla procedury odinstalowania oprogramowania.
* Oprogramowanie ma dostarczone narzędzia do nagrywania kroków instalacji oprogramowania.
* Oprogramowanie ma także poniższe funkcjonalności takie jak:
	+ Natywna instalacja pakietów (a nie tylko wrap aplikacji w innym skrypcie instalacyjnym).
	+ Transparentna instalacja (w Logach znajduje się informacja dotycząca instalacji np.: msiexec.exe /i \\...\software-xyz.msi /qn /noreboot).
	+ Indywidualna konfiguracja zależności (np.: uprzednia instalacja framework .net w przypadku jeśli takowa nie miała jeszcze miejsca, następnie instalacja docelowego oprogramowania).
	+ Ustawianie zachowań w trakcie Reboot również dla oprogramowania.
	+ Możliwość użycia skryptów, w celu np: wdrożenia niestandardowych zakładek w przeglądarkach internetowych, zmian w rejestrze systemowym Windows, udziały dyskowe, Working Directories, itd.
	+ Użycie narzędzia do tworzenia własnych skryptów, w celu tworzenia własnych pakietów instalacyjnych (np.: "kopiuj pliki z .. , stwórz ikonę Start").
	+ Różnorodna weryfikacja instalacji (np.: jaka jest wartość zwrotna programu instalacyjnego, czy istnieje jakiś określony wpis do rejestru lub usługa).
	+ Przechowywanie wszystkich danych inwentaryzacyjnych w tej samej bazie danych.
	+ Provisioning formatów inwentaryzacyjnych (np.: inwentaryzacja Software i Hardware).
	+ Tworzenie indywidualnych szablonów inwentaryzacyjnych, takich jak WMI, plików itp.
	+ Definiowanie priorytetów skanowania (w celu nie obciążania urządzenia końcowego w trakcie pracy na nim przez użytkownika).
	+ Przetwarzanie wyników skanowania np. w grupach dynamicznych (np.: wszystkie komputery z kartą graficzną Nvidia, itp).
	+ Skanowanie cykliczne.
	+ Prezentacja wyników w konsoli zarządzania lub w dedykowanym narzędziu do raportowania.
	+ Zarządzanie aktywami.
* Oprogramowanie umożliwia zarządzanie urządzeniami mobilnymi z systemami operacyjnymi: iOS, Android, Windows 8.
* Oprogramowanie przechowuje dane dotyczące urządzeń mobilnych w tej samej bazie danych co do urządzeń typu PC (np.: dane inwentaryzacyjne, dane użytkownika takie jak e-mail etc.).
* Oprogramowanie zawiera własną bramkę gateway działającą w strefie DMZ dla zabezpieczenia serwera.
* Oprogramowanie ma wbudowany generator profili urządzeń mobilnych. Oprogramowanie posiada jedną stronę do konfiguracji dla stworzenia polityki zarządzania, niezależnie od tego jakie to urządzenie końcowe ma zainstalowany system operacyjny.
* Oprogramowanie ma wbudowany moduł inwentaryzacji oprogramowania i sprzętu (oraz jego elementów składowych) wraz ze wsparciem dla wielu równolegle przebiegających inwentaryzacji.
* Oprogramowanie ma wsparcie dla Samsung Knox/SAFE-Interfejs/Android Enterprise.
* Oprogramowanie wspiera systemy operacyjne iOS/WP8x SCEP (automatyczny roll out certyfikatów w takie sposób, że np. nie wymagane jest już podawanie hasła w trakcie logowanie się na serwerze Exchange).
* Oprogramowanie ma wsparcie dla Compliance (np.: automatyczne blokowanie urządzenia w przypadkach rootowania lub jailbreak).
* Oprogramowanie pozwala na blokowanie parametrów w ustawieniach urządzenia, takich jak: blokada kamery, wifi, bluetooth, dostępu do ustawień.
* Oprogramowanie umożliwia zarządzanie pełnym cyklem życia mobilnego urządzenia od wprowadzenia, aż po zdalne usunięcie z systemu.
* Oprogramowanie umożliwia zarządzanie urządzeniami również spoza firmowej sieci.
* Oprogramowanie posiada własny "KIOSK" umożliwiający przestrzeganie zasad zgodności z prawem i ochrony cennych danych przedsiębiorstwa.
* Oprogramowanie posiada własny "KIOSK", w którym użytkownik urządzenia ma dostępne tylko te aplikacje i dane, które są zgodne ze standardami w organizacji.
* Oprogramowanie umożliwia integracje prywatnych urządzeń pracowników (Bring Your Own Diveces).
* Oprogramowanie umożliwia zewidencjonowanie urządzenia poprzez sczytanie kodu QR lub za pomocą linku w e-mailu.
* Oprogramowanie ma możliwość dystrybucji poprawek dla systemu Windows bez udziału Microsoft WSUS.
* Oprogramowanie umożliwia wypychanie poprawek z poziomu WSUS.
* Oprogramowanie umożliwia obsługę systemów operacyjne Microsoft — Windows Vista i Server 2008, Windows 7, Windows 8, Windows 10, Windows Server 2008R2/2012/2016/2019 oraz późniejsze wersje wraz z natywną instalacją.
* Oprogramowanie umożliwia określenie ścisłych wymagań czasowych dla instalacji poprawek Microsoft i potrafi te wymagania kontrolować. Oprogramowanie nie wymaga ingerencji w reguły eksploatacji serwerów, a mimo to zapewnia ich odpowiednio szybkie zamknięcie w razie luk w zabezpieczeniach.
* Oprogramowanie musi pozwolić administratorowi na zarządzanie aktualizacjami systemów, w zakresie takim jak: możliwość sprawdzania tylko pod kątem brakujących poprawek i czy poprawki mają być od razu instalowane. Poprawki mogą być zatwierdzane automatycznie lub ręcznie. Oprogramowanie pozwala także ustalać reguły dla różnych grup w systemie IT.
* Oprogramowania pozwala by metodą „przeciągnij i upuść” w środowisku zgodnym z MMC określać, w jakich systemach mają być instalowane poprawki. W taki sam sposób definiowane są również automatyczne instalacje i sytuacje, w których administrator ma być wcześniej pytany o zgodę. Oprogramowanie automatycznie pobiera wszystkie poprawki Microsoft i na żądanie automatycznie je rozprowadza w infrastrukturze Klienta zgodnie z wytycznymi administratora.
* Oprogramowanie ma funkcjonalność wysyłania powiadomień o zdarzeniach z zdefiniowanymi triggerami/parametrami do zdefiniowanych grup użytkowników za pośrednictwem email.
* Oprogramowanie ma funkcjonalność wdrażania systemów z wcześniej przygotowanych obrazów systemów (typu master lub z backupów).

Zamawiający wymaga, aby producent oprogramowania zapewniał stały dostęp do bazy danych z poprawkami Microsoft - baza jest dostępna dla Klienta z poziomu konsoli oprogramowania w dniu jej opublikowania przez Microsoft.

|  |  |
| --- | --- |
| Funkcje dodatkowe ( opcjonalne) | Punktacja |
| 1. | Kryterium: Zarządzanie | 1 |
| Oprogramowanie pozwala zarządzać z jednej konsoli zarówno stacjami klienckimi, serwerami jak i urządzeniami mobilnymi z systemami operacyjnymi Android, iOS, Windows Phone oraz Windows Mobile. |
| 2. | Kryterium: Architektura 1 | 1 |
| Oprogramowanie, niezależnie od ilości funkcjonalności lub zarządzanych urządzeń końcowych działa w oparciu o 1 oprogramowanie typu Agent na urządzeniu końcowym. |
| 3. | Kryterium: Architektura 2 | 1 |
| Oprogramowanie posiada architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji oraz Agenta. |
| 4. | Kryterium: Uwierzytelnianie i autoryzacja | 1 |
| Oprogramowanie posiada procedurę uwierzytelnienia i autoryzacji Administratora w konsoli zarządzającej, która umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej może być zintegrowane z kontami Active Directory. |
| 5. | Kryterium: Dystrybucja oprogramowania | 1 |
| Oprogramowanie umożliwia dystrybucję dowolnego oprogramowania, nie tylko paczek MSI, ale również takich jak InnoSetup, InstallShield I inne. |
| 6. | Kryterium: Zdalna instalacja dowolnego oprogramowania | 1 |
| Oprogramowanie umożliwia zautomatyzowanie zdalnej instalacji dowolnego oprogramowania w taki sposób, by oprogramowanie można było zainstalować zdalnie w trybie cichym (Silent Mode) lub normalnym. |
| 7. | Kryterium: Wzbudzenie stacji klienckich | 1 |
| Oprogramowanie musi umożliwiać wzbudzanie stacji klienckich metodą Wake-On-LAN. |
| 8. | Kryterium: Zdalna dystrybucja oprogramowania | 1 |
| Oprogramowanie ma możliwość zdalnej dystrybucji oprogramowania z jednej konsoli zarówno na stacjach klienckich (jak PC I laptop/notebook) jak i urządzeniach mobilnych z systemem Android. |
| 9. | Kryterium: Automatyczna instalacja oprogramowania na stacjach klienckich | 1 |
| W przypadku automatycznej zdalnej instalacji oprogramowania na stacjach klienckich, oprogramowanie daje opcje tworzenia listy oprogramowania zależnego, tzn. w przypadku gdy do poprawnego działania aplikacja X wymaga instalacji aplikacji Y, Oprogramowanie daje opcję ustalenia listy takiego oprogramowania zależnego na poziomie konfiguracji aplikacji X z poziomu konsoli. W przypadku dystrybucji aplikacji X, gdy na stacji klienckiej nie będzie zainstalowana aplikacja Y, serwer automatycznie wypchnie na tą stację paczkę instalacyjną aplikacji Y. |
| 10. | Kryterium: Środowisko skryptowe | 1  |
| Oprogramowanie posiada własne środowisko skryptowe i umożliwia również tworzenie własnych skryptów, które następnie można automatycznie instalować na urządzeniach końcowych, typu stacja kliencka. |
| Suma punktów dodatkowych | 10 |

**Zadanie 3.**

**System typu Next Generation NAC (zwany dalej platforma NG-NAC), który dynamicznie identyfikuje i analizuje systemy podłączone do sieci oraz aplikacje natychmiast po podłączeniu ich do sieci ZTM.**

**Funkcje podstawowe**

* Dostarczone licencje na oprogramowanie są bezterminowe z opcją możliwością zwiększenia ilości licencji w okresie 3 lat liczonej od momentu uruchomienia systemu w środowisku produkcyjnym.

- Liczba urządzeń końcowych: 700 szt./IP

* **Monitorowanie stanu stacji końcowych w czasie rzeczywistym.** Platforma NG-NAC powinna posiadać aktualny katalog oraz monitorować stan wszystkich urządzeń, które zażądały i uzyskały dostęp do sieci korporacyjnej w ramach sieci kampusowej, WAN, VPN czy DC. Informacje powinny obejmować między innymi użytkownika, parametry urządzenia, systemu operacyjnego, listę aplikacji czy usług – wszystko, aby wspomóc zamawiającego w zarządzaniu ryzykiem przypisanym do każdego urządzenia w sieci.
* **Możliwość wymuszania precyzyjnych polityk dotyczących kontroli dostępu oraz zgodności z wymaganiami (ang. compliance).** PlatformaNG-NAC powinna wspierać gromadzenia wszystkich dostępnych danych ze stacji roboczych, aby umożliwić ich prezentację zespołom operacyjnym by z kolei pomóc im lepiej rozumieć ryzyko, podejmować lepsze decyzje oraz wymuszać akcje bazując na szerokim katalogu atrybutów, takich jak: typ urządzenia, użytkownik, lokalizacja, stan uwierzytelniania, stan zabezpieczeń, podatności czy inne w zależności od sytuacji. System dodatkowo powinien wspierać proces zarządzania gośćmi oraz automatycznie identyfikować i usuwać obce/szkodliwe urządzenia czy aplikacje.
* **Umożliwienie zespołom operacyjnym automatyczne reagowanie na incydenty.** Platforma NG-NAC powinna dawać możliwość automatycznego reagowania na naruszenia polityki bezpieczeństwa i zagrożenia poprzez realizację zautomatyzowanych akcji. Do najbardziej podstawowych akcji powinny należeć: alertowanie, notyfikacja zespołów IT czy powiadomienie dla użytkownika. Bardziej zdecydowane akcji powinny co najmniej zawierać reakcje na poziomie sieci w postaci ograniczania dostępu do zasobów sieciowych. Dodatkowo system powinien umożliwiać podjęcie prób naprawy systemu w postaci instalowania patcha, zmiany ustawień bezpieczeństwa czy wyłączenia/deinstalacji aplikacji lub usługi. Wszystkie te funkcjonalności mają na celu zmianę modelu zachowania użytkowników, redukcję czasu pomiędzy atakiem a jego wykryciem i reakcją oraz minimalizację wpływu ataków na działanie firmy.
* **Realizacja funkcji platformy integracyjnej rozwiązań bezpieczeństwa.** Platforma NG-NAC powinna posiadać możliwość integracji z innymi systemami poprzez otwarte standardy integracji. Celem integracji jest wymiana danych o systemach sieciowych aby zwiększyć możliwości analizy innych systemów jak SIEM, Threat Intelligence, MDM, firewalli czy skanerów podatności.
* Rozwiązanie powinno wspierać wielu producentów urządzeń sieciowych – w tym minimum Cisco, Brocade, Extreme, 3COM, HPE oraz Huawei. Dodawanie urządzeń do systemu powinno odbywać się ręcznie lub automatycznie poprzez użycie protokołów automatyzujących: CDP, FDP oraz LLDP.
* Rozwiązanie powinno wspierać wielu producentów urządzeń WLAN – w tym minimum: Aerohive, Cisco, Meru Networks, Aruba Networks oraz Xirrus.
* System powinien wspierać użycie protokołu 802.1x, jednakże, aby uzyskać pełną funkcjonalność użycie tego protokołu nie może być wymagane.
* Rozwiązanie powinno wspierać uwierzytelniania pre-admission oraz post-admission. Pre-admission oznacza, że urządzenie będzie uwierzytelniane i sprawdzane pod względem zgodności przed dostępem do sieci. Post-admission oznacza, że dostęp do sieci jest zapewniony od razu po podłączeniu jednak w tym samym czasie realizowane jest sprawdzanie pod względem zgodności z politykami.
* Rozwiązanie powinno wspierać centralne zarządzanie politykami bezpieczeństwa w ramach całej organizacji w ramach *systemu zarządzającego*.
* Rozwiązanie zapewnia widoczność wszystkich urządzeń widocznych w sieci, które posiadają co najmniej jeden z adresów: MAC, IP. Baza urządzeń jest aktualizowana w czasie rzeczywistym. Wśród monitorowanych urządzeń powinny być: stacje robocze, laptopy, smartfony, tablety, urządzenia IoT (projektory, kamery IP, systemy HVAC, systemy OT, itp.).
* System musi umożliwiać aktualizację oprogramowania za pomocą interfejsu graficznego.
* System musi umożliwić aktualizację definicji oraz aktualizacje modułów zależnych przez Internet bezpośrednio z serwerów producenta.
* System musi umożliwiać tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled).
* Kopie zapasowe powinny być możliwe do zapisania bezpośrednio na serwerach FTP, SFTP oraz SCP. Uwierzytelnianie do zasobu SCP powinno być możliwe poprzez użycie klucza publicznego.
* Powinna istnieć też możliwość zapisania kopii zapasowej na dysku lokalnym komputera administratora, jednak taka kopia powinna być zaszyfrowana z użyciem hasła.
* System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników.
* System powinien umożliwiać klasyfikację urządzeń bazując na definicjach dostarczonych przez producenta rozwiązania w ramach *silnika klasyfikacji*.
* System powinien dostarczyć minimum 80 kategorii klasyfikacji w tym podział na urządzenia IT oraz OT. Wśród dostępnych klasyfikacji powinny być dostępne co najmniej:
	+ Komputer
	+ Smartfon
	+ Smartwatch
	+ Tablet
	+ Drukarka
	+ Telefon IP
	+ Zestaw wideokonferencji
	+ Projektor
	+ Smart TV
	+ Urządzenia sprzedające (tzw vending machine)
	+ Kontrolery klimatyzacji
	+ Kamery IP
	+ Systemy kontroli dostępu
* Producent NG-NAC powinien stale aktualizować bazę klasyfikacji używaną przez *silnik klasyfikacji* oraz umożliwić pobieranie informacji zwrotnej od klientów, która to ma na celu udoskonalanie klasyfikacji w kolejnych aktualizacjach *silnika klasyfikacji*.
* W sytuacji, gdzie *silnik klasyfikacji* jest aktualizowany oraz niektóre systemy mają w konsekwencji zmienioną klasyfikację to system powinien wskazać, których systemów dotyczy zmiana i umożliwić akceptację przed podjęciem zmiany klasyfikacji.
* Klasyfikacja powinna dotyczyć systemów zarządzanych i niezarządzanych bazując na wielu technikach pasywnych i aktywnych. Do technik pasywnych powinny należeć co najmniej DHCP fingerprinting, HTTP User-Agent, TCP Fingerprinting. Do technik aktywnych powinno należeć co najmniej użycie skanów NMAP, RPC, SSH, SMB, WMI oraz SNMP.
* Silnik klasyfikacji obok wspomnianej wcześniej kategorii klasyfikacji powinien również umożliwić identyfikację systemu operacyjnego.
* System musi umożliwiać bezagentową inspekcję zarządzanych stacji, która jest w stanie określić wersję systemu operacyjnego, obecnie zalogowanego użytkownika, uruchomione procesy i usługi, zainstalowane aplikacje oraz weryfikację stanu oprogramowania zabezpieczającego.
* System musi wspierać następujące systemy klienckie w ramach bezagentowej inspekcji: Windows, MAC.
* Producent NG-NAC musi umożliwić w ramach licencji podstawowej instalację agenta, który może realizować funkcje inspekcji podobnej do inspekcji bezagentowej. Musi istnieć wersja agenta dla systemów Windows, MAC. Instalacja agenta powinna być realizowana przez rozwiązanie NG-NAC oraz powinna być możliwość instalacji przez system Microsoft SCCM.
* System powinien umożliwić wskazanie konta dostępowego, które ma być użycie w ramach inspekcji bezagentowej. Musi być możliwość podania konta domenowego w przypadku środowisk Microsoft ActiveDirectory.
* System musi wspierać następujące mechanizmy uwierzytelniania w stosunku do komputerów pracujących pod kontrolą systemu Microsoft Windows: NTLMv1, NTLMv2 oraz Kerberos.
* W przypadku inspekcji bezagentowej systemów Linux oraz Mac musi być możliwość uwierzytelniania zarówno z użyciem pary użytkownik i hasło oraz z użyciem klucza publicznego.
* System powinien wskazać otwarte porty TCP oraz UDP na wykrytych systemach w ramach inspekcji bezagentowej.
* System powinien umożliwiać obsługę procesu zarządzania gośćmi w ramach bazowej licencji. Jako gościa zamawiający rozumie osobę, która nie jest zatrudniona w firmie ale potrzebuje wykorzystać jej infrastrukturę za zgodą pracownika firmy (zwanego dalej sponsorem).
* Użytkownik po podłączeniu się do sieci powinien być przekierowany na stronę obsługi gości, gdzie może się zalogować lub utworzyć nowe konto. W ramach tworzenia nowego konta użytkownik powinien wskazać osobę w organizacji, która może zaakceptować jego żądanie dostępu do sieci – *sponsora*.
* System powinien umożliwić wskazanie, którzy użytkownicy mogą pełnić rolę sponsora i akceptować prośby dostępu do sieci.
* Email użytkownika powinien być weryfikowany w czasie rejestracji poprzez wysłanie linku aktywacyjnego.
* Sponsorzy powinni otrzymywać powiadomienie emailem każdorazowo, jeśli ktokolwiek zażąda dostępu do sieci wskazując ich jako sponsora.
* Hasło do konta użytkownika-gościa powinno spełniać możliwe do skonfigurowania wymagania dotyczące długości hasła, ilości małych i wielkich liter, obecności cyfr czy znaków specjalnych.
* W ramach zadanej polityki system powinien umożliwić wysyłanie informacji w następujący sposób:
	+ Wyświetlenie strony użytkownikowi bez użycia agenta
	+ Wyświetlenie strony użytkownikowi z użyciem agenta (Windows i Mac)
	+ Wysłanie email do użytkownika
	+ Wysłanie email do administratora systemu
	+ Wysłanie logu w formacie CEF oraz syslog do innego systemu. Log powinien być w pełni konfigurowalny.
* W ramach zadanej polityki system powinien umożliwić zrealizowanie następujących czynności na zarządzanych stacjach roboczych:
	+ zabicie wskazanego procesu
	+ uruchomienie wskazanego systemu antywirusowego
	+ wpisanie do rejestru konkretnej wartości
	+ dezaktywacja aplikacji typu peer-to-peer.
	+ dezaktywacja oprogramowania typu cloud storage
	+ wszczęcie procesu aktualizacji systemu (Windows, MAC)
	+ wyłącznie wskazanych urządzeń zewnętrznych jak dyski, drukarki czy modemy.
* W ramach zadanej polityki system powinien umożliwić realizację następujących reakcji na poziomie sieci przewodowej:
	+ przypisanie portu do zdefiniowanego VLANu
	+ przypisanie IP ACL do portu. System powinien sam konfigurować ACL na urządzeniu. Nie jest dopuszczone wymaganie ręcznej konfiguracji ACL przed jej użyciem w rozwiązaniu.
	+ wyłącznie portu
* W ramach zadanej polityki system powinien umożliwić realizację następujących reakcji na poziomie sieci bezprzewodowej WLAN:
	+ Blokowanie
	+ Przypisanie roli WLAN na poziomie kontrolera
* W ramach zadanej polityki system powinien umożliwić realizację następujących reakcji na poziomie private cloud.
	+ Zmianę portgrupy przypisanej do maszyny wirtualnej
	+ Wyłączenie maszyny wirtualnej
	+ Uśpienie maszyny wirtualnej
	+ Restart maszyny wirtualnej
	+ Włączenie maszyny wirtualnej
* W ramach licencji podstawowej powinna istnieć możliwość instalacji nieograniczonej ilości maszyn wirtualnych co najmniej na środowisku VMware oraz Hyper-V.
* Rozwiązanie powinno umożliwiać centralne zarządzanie z jednego punktu.
* Rozwiązanie NG-NAC powinno wspierać obsługę architektury centralnej i rozproszonej, gdzie niektóre urządzenia mogą być zainstalowane poza centralną lokalizacją firmy.
* Rozwiązanie powinno oferować funkcje wysokiej dostępności na poziomie systemu zarządzania. W przypadku awarii urządzenia podstawowego – urządzenie zapasowe powinno przełączyć się w tryb aktywny automatycznie.
* Rozwiązanie powinno być w pełni redundantne. Awaria jednego urządzenia nie powinna wpływać na funkcjonalność rozwiązania. W szczególności powinna być zapewniona redundancja:
	+ na poziomie 1:1 w ramach systemu zarządzania i podsystemu monitoringu.
	+ na poziomie N+1 w ramach podsystemu monitoringu.
* Redundancja rozwiązania powinna przywidywać scenariusz Disaster Recovery, gdzie jedno lub więcej urządzeń centralnych jest zainstalowanych w zdalnej lokalizacji.
* System powinien umożliwiać integrację z Microsoft Active Directory w celu odczytania właściwości użytkownika zalogowanego na analizowanej stacji.
* System powinien umożliwiać generowanie raportów w postaci PDF oraz plików XLS.
* W ramach raportów w postaci PDF powinno być możliwe wygenerowanie co najmniej następujących zestawień:
	1. Dane systemów gości
	2. Wyniki działania konkretnej polityki
	3. Wynik działania konkretnej polityki na przestrzeni czasu
	4. Zestawienie stanu występowania podatności dla wybranych hostów Windows
	5. Dane zgodności z wymaganiami firmy.
* Raporty powinny być generowane na żądane lub w określonym harmonogramie czasowym. Po wygenerowaniu raportu powinna istnieć możliwość automatycznej wysyłki na wskazany adres email.
* System powinien również umożliwiać przedstawianie wyników pracy w postaci interaktywnej strony WWW, gdzie możliwe jest drążenie danych.
* Rozwiązanie powinno być oparte o system operacyjny Linux.
* Rozwiązanie powinno być dostarczone jako appliance wirtualny. Nie jest dopuszczalne dostarczenie aplikacji, którą należy samodzielnie zainstalować na własnym systemie operacyjnym.

|  |  |
| --- | --- |
| Funkcje dodatkowe ( opcjonalne) | Punktacja |
| 1. | Kryterium: Inspekcja systemów zarządzalnych 1 | 2 |
| System musi wspierać następujące systemy klienckie w ramach bezagentowej inspekcji: Windows, MAC, Linux. |
| 2. | Kryterium: Inspekcja systemów zarządzalnych 2 | 2 |
| Producent NG-NAC musi umożliwić w ramach licencji podstawowej instalację agenta, który może realizować funkcje inspekcji podobnej do inspekcji bezagentowej. Musi istnieć wersja agenta dla systemów Windows, MAC oraz Linux. Instalacja agenta powinna być realizowana przez rozwiązanie NG-NAC oraz powinna być możliwość instalacji przez system Microsoft SCCM. |
| 3. | Kryterium: Remediacja i reakcja 1 | 2 |
| W ramach zadanej polityki system powinien umożliwić wykonanie predefiniowanego skryptu (Windows, Linux, MAC). Skrypt powinien być wgrywany na system w momencie wykonania. Nie dopuszczalne jest wymaganie, by wymagane było wgranie skryptu ręcznie przed jego wykonaniem. |
| 4. | Kryterium: Remediacja i reakcja 2 | 2 |
| W ramach zadanej polityki system powinien umożliwić wyłączenie interfejsów dual-home. |
| 5. | Kryterium: Remediacja i reakcja 3 | 2 |
| W ramach zadanej polityki system powinien umożliwić przypisanie MAC ACL do portu. System powinien sam konfigurować ACL na urządzeniu. Nie jest dopuszczone wymaganie ręcznej konfiguracji ACL przed jej użyciem w rozwiązaniu. |
| Suma punktów dodatkowych | 10 |

**Zadanie 4**

**Szkolenia w dwóch etapach**

**Opis funkcjonalny:**

a. wdrożeniowe (8h)

b. doszkalające (16h)