**Załącznik nr 2b do SWZ**

**Zestawienie wymagań technicznych systemu do zarządzania**

**i monitorowania zasobami IT, który ma być udostępniony Zamawiającemu w ramach oferowanych usług serwisowych opisanych w załączniku nr 2 do SIWZ**

|  |  |
| --- | --- |
| **L.p.** | **PARAMETRY TECHNICZNO-UŻYTKOWE**  **PARAMETRY WYMAGANE** |
| **1** | **2** |
| 1 | Rozwiązanie klasy RMM (Remote monitoring and management) musi posiadać wszystkie wymienione poniżej funkcjonalności w ramach jednego systemu i być zarządzane oraz widoczne w ramach Internetowego pulpit nawigacyjnego, który działa jak pojedyncza tafla szkła, zapewniając przegląd monitorowanych urządzeń, sieci i usług. |
| 2 | Pulpit nawigacyjny systemu powinien obsługiwać różne opcje zabezpieczeń w tym pozwolić na włączenie uwierzytelniania dwuskładnikowego. |
| 3 | Pulpit nawigacyjny systemu powinien mieć możliwość skonfigurowania wymagania weryfikacji logowania z nowych adresów IP oraz zarządzać dostępem tylko z określonych adresów IP. |
| 4 | System pozwala na zarządzanie użytkownikami Zamawiającego i Wykonawcy. |
| 5 | System posiada zdalny dostęp do zarządzanych komputerów Windows i Mac bezpośrednio z pulpitu nawigacyjnego. |
| 6 | System powinien posiadać możliwość definiowania i wdrażania dziedziczonych polityk bezpieczeństwa dla zdalnego dostępu takich jak:   * autoryzacja użytkownika końcowego na zdalną sesję, * metoda uwierzytelnienia zdalnej sesji na co najmniej 2 sposoby, * możliwość włączenia hasła do zasobnika systemowego (systray). |
| 7 | System musi wymuszać logowanie się do pulpitu nawigacyjnego przy użyciu aktywnego logowania dwuskładnikowego (2FA), zanim będą mogli zainicjować sesję zdalną. |
| 8 | System w kontekście obowiązujących przepisów musi tworzyć automatycznie rejestr historii logowań zdalnych. (Kto, Kiedy i do jakiego komputera). |
| 9 | Sesje zdalne powinny być zgodne z FIPS 140-2a, aby zwiększyć bezpieczeństwo całego ruchu od miejsca pochodzenia do miejsca docelowego. Ruch przejmujący kontrolę przez system zdalnego dostępu musi być zabezpieczony za pomocą modułów kryptograficznych OpenSSL zgodnych z FIPS 140-2. Dodatkowo w celu ochrony wymian kluczy publicznych / prywatnych, stanowiących element tworzenia instancji sesji powinna być zaimplementowana kryptografia z krzywą eliptyczną Diffie-Hellmana. |
| 10 | System pozwala na zarządzanie skryptami systemowymi, standardowymi i rozbudowanymi , które mogą być tworzone, przesyłane, a następnie wdrażane z pulpitu nawigacyjnego na dwa sposby:   * zadania rekurencyjne dla komputerów z systemem Windows , Linux i Mac * zadania automatyczne dla komputerów z systemem Windows i Mac. |
| 11 | System posiada wbudowany edytor skryptów, który umożliwia szybkie i łatwe tworzenie oraz testowanie własnych skryptów przed wdrożeniem na urządzeniach z systemem Windows. |
| 12 | System posiada funkcjonalność zarządzania poprawkami dla systemu Windows, w tym poprawkami bezpieczeństwa aplikacji Microsoft Windows i Office, a także aplikacji innych niż Microsoft, takich jak Adobe Reader, Adobe Flash Player, Mozilla Firefox, Mozilla Thunderbird, Java i inne. |
| 13 | System posiada funkcjonalność zarządzania poprawkami dla systemu Windows w ramach jednego skonsolidowanego procesu obsługi łatek dla wielu urządzeń.  System posiada funkcjonalność zarządzania politykami zatwierdzania, czyli zasady zatwierdzania jednej lub więcej reguł dla każdej poprawki, która określa działanie, które należy podjąć na serwerze lub stacji roboczej podczas identyfikowania i usuwania łatek. |
| 14 | System potrafi centralnie zarządzać (konfigurować treść i funkcje oraz instalować na komputerach Windows) aplikację zasobnika systemowego Windows, gdzie po włączeniu użytkownicy końcowi mogą jednym kliknięciem w Systray:   * zrobić zrzut ekranu z bieżącego ekranu (ekranów) i uruchomić klienta poczty z gotową wiadomością do wysłania wraz z załącznikiem i zdefiniowanym adresem Do:. * uruchomić klienta poczty z wstępnie predefiniowaną wiadomością do wysłania wraz i adresem Do:. * otworzyć wstępnie skonfigurowaną stronę internetową, na przykład w celu rejestrowania zgłoszeń. * inicjowania sesji zdalnego wsparcia. |
| 15 | System posiada zaawansowane zarządzanie w tle, która to funkcjonalność pozwala na:   * Działania w powłoce systemowej za pomocą CMD. * Działania w powłoce systemowej za pomocą PowerShell. * Transfer plików. * Informacje o systemie : Procesy, Usługi, Sieć, Aplikacje, Sterowniki, Uruchomione, Użytkownik interaktywny, Wydarzenia, Zdrowie systemu i Aktualizacje systemu Windows. * Dostęp zdalny do Rejestru systemu Windows. |
| 16 | System powinien mieć możliwość instalacji agentów na komputerach, którzy łączą się z centralną konsolą na dwa sposoby:   * do wdrażania agenta w sieci Active Directory za pomocą zasad grupy * do samodzielnego wdrożenia przez użytkownika. Rozpakuj plik i kliknij plik wykonywalny, aby zainstalować – z tym, że czas instalacji od momentu uruchomienia pliku \*.exe do skutecznego podłączenia agenta do konsoli centralnej, nie powinien przekraczać 5 minut. |