|  |
| --- |
| Przedmiot zamówienia - wymagania Zamawiającego System ochrony dla stacji roboczych wraz z systemem centralnego zarządzania.  W ramach postepowania wymaganym jest dostarczenie rozwiązania do ochrony stacji roboczych wraz z mechanizmami centralnego zarządzania.  Dostarczone rozwiązanie do ochrony stacji roboczych musi zapewniać wszystkie wymienione poniżej funkcje i mechanizmy. Dopuszcza się, aby poszczególne elementy wchodzące w skład rozwiązania były zrealizowane w postaci osobnych, komercyjnych platform lub komercyjnych aplikacji.  Parametry systemu ochrony dla stacji roboczych.   1. Elementy systemu ochrony dla stacji roboczych powinny zapewniać następujące funkcje i mechanizmy:    * Kontrola antywirusowa.    * Funkcja analizy plików w zewnętrznym systemie Sandbox.    * Opcja kwarantanny lokalnej plików przesłanych do Sandbox na czas analizy.    * URL filtering w oparciu o kategorie stron z opcją definiowania wyjątków.    * Kontrola aplikacji - w oparciu o wbudowany Firewall aplikacyjny.    * Mechanizmy analizy podatności na stacji roboczej - pozwalające wykryć zagrożenia w systemie operacyjnym oraz zainstalowanych aplikacjach.    * Mechanizmy szyfrowanych połączeń typu IPSec VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.    * Mechanizmy szyfrowanych połączeń typu SSL VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.    * Możliwość zastosowania certyfikatów cyfrowych w procesie uwierzytelnienia przy realizacji szyfrowanych połączeń.    * Mechanizmy uwierzytelniania dwuskładnikowego    * AntiExploit,    * blokowanie dysków przenośnych typu USB, 2. Poszczególne mechanizmy muszą być dostępne dla następujących systemów operacyjnych: Microsoft Windows 10 (32-bit, 64-bit), Windows 8.1 (32-bit, 64-bit), Windows 7 (32-bit, 64-bit),Windows Serwer 2019, Windows Server 2016, Windows Server 2012, 2012 R2, MacOS 11+, 10.15, 10.14, Ubuntu 16.04 i późniejsze, Red Hat 7.4 i późniejsze, CentOS 7.4 i późniejsze.   Parametry systemu centralnego zarządzania.   1. Dostarczony system centralnego zarządzania aplikacjami klienckimi musi zapewniać wszystkie wymienione poniżej funkcje. Wymaga się aby elementy wchodzące w skład systemu były zrealizowane w postaci komercyjnych platform wirtualnych lub aplikacji instalowanych na systemach operacyjnych: Microsoft Windows Server 2019, Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2. 2. System powinien umożliwiać automatyczną aktualizację oprogramowania zabezpieczającego na urządzeniach końcowych oraz musi zapewniać mechanizmy integracji z sieciowymi systemami bezpieczeństwa, w tym co najmniej: Firewall, Sandbox. 3. Ponadto wymagane jest aby system zapewniał:  * integrację z systemami zarządzania tożsamością użytkowników – co najmniej AD, * definiowanie różnych profilów (wersji konfiguracji) ochrony dla różnych grup użytkowników czerpanych z AD lub definiowanych lokalnie, * zautomatyzowany proces zarządzania aplikacja kliencką, * przygotowywanie paczek instalacyjnych przynajmniej dla systemu Windows 32/64 bit i MacOS w których administrator może określić komponenty dla ochrony stacji roboczych takich jak AV, WebFiler, Skaner Podatności. * możliwość edycji pliku konfiguracyjnego w zewnętrznym edytorze tekstowym, * panel, w którym wyświetlane są wyniki analizy podatności na stacjach roboczych, * panel w którym wyświetlane są informacje o podłączonych i zarządzanych stacjach roboczych, * możliwość wymuszenia patchowania wykrytych podatności na stacjach roboczych, * automatyczne wykrywanie stacji klienckich w grupach roboczych, * logowanie zdarzeń z aplikacji klienckich, możliwość ich przeglądania z funkcja filtrów oraz możliwością pobierania logów przez administratora, * generowanie alarmów: związanych z zarządzeniem aplikacją kliencką, w przypadku wykrycia ważnych podatności na stacjach oraz w sytuacji zaistnienia zdarzeń związanych z aktywnością złośliwego kodu, aktywności aplikacji botnet z wykorzystaniem komunikacji C&C, nieaktualnej bazy danych dla sygnatur antywirusa. * definiowanie grup administratorów lokalnie oraz w oparciu o AD z opcja przypisywania uprawnień do elementów panelu konfiguracyjnego, * automatyczne wykrywanie aplikacji zainstalowanych na stacjach klienckich z możliwością filtrowania przynajmniej po producencie i nazwie aplikacji, * możliwość przeniesienia użytkownika przez administratora do kwarantanny i personalizację komunikatu, który wyświetli się użytkownikowi, * możliwość wymuszenia przeskanowania stacji klienckiej za pomocą antywirusa i skanera podatności na żądanie jak i cyklicznie, * możliwość skonfigurowania weryfikacji zgodności (compliance) w celu sprawdzenia czy na stacji końcowej jest aktualna baza sygnatur dla AV, czy jest odpowiednia wersja systemu operacyjnego, czy jest uruchomiony odpowiedni proces.  1. Administrator musi mieć możliwość wykonywania backupu i odtwarzania bazy danych, w oparciu o którą działają elementy system. 2. Centralny system zarządzania musi zapewniać możliwość dystrybucji paczek instalacyjnych z lokalnych zasobów w oparciu o adres URL definiowany przez administratora lub w ramach postępowania koniecznym jest dostarczenie odpowiednio zabezpieczonego portalu, za pośrednictwem którego administrator będzie mógł dystrybuować paczki instalacyjne.   Licencje oraz serwisy.  W ramach postępowania wraz z konsolą centralnego zarządzania muszą zostać dostarczone niezbędne licencje upoważniające do:   1. Zainstalowania i centralnego zarządzania 700+25 licencji klienckimi na stacjach roboczych. 2. Dla wskazanej powyżej ilości stacji roboczych licencje powinny obejmować: 3. Kontrola Aplikacji, Antywirus, Web Filtering, Skaner podatności, Software inventory, Remote Access, Threat Outbreak Detection, Centralne zarządzanie na okres 12 miesięcy.   System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. |