

Opis oprogramowania równoważnego

Za rozwiązanie równoważne zamawiający uzna dostawę, instalację i skonfigurowanie oprogramowania, które będzie posiadało funkcjonalność na poziomie nie niższym niż oprogramowanie TRAPS oraz będzie spełniało wymagania funkcjonalne opisane poniżej

1. Oprogramowanie musi się składać z dwóch elementów. Jeden to system zarządzający instalowany na dedykowanym serwerze fizycznym lub wirtualnym. Drugi to agent instalowany na każdym komputerze.
2. Oprogramowanie musi umożliwiać ochronę co najmniej 500 stacji końcowych oraz 50 serwerów przez okres co najmniej 36 miesięcy.

A. Wymagania dotyczące systemu zarządzającego:

1. Serwer zarządzający musi mieć możliwość instalacji na co najmniej następujących systemach operacyjnych: Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2.
2. Serwer zarządzający musi korzystać z co najmniej następujących baz danych: Microsoft SQL Server 2008, Microsoft SQL Server 2012, Microsoft SQL Server 2014.
3. Pojedynczy serwer zarządzający musi mieć możliwość zarządzania co najmniej 50 000 agentami.
4. Serwer zarządzający musi mieć możliwość integracji z posiadanym przez zamawiającego Active Directory i tworzenia polityk na podstawie obiektów z Active Directory co najmniej takich jak nazwa użytkownika, nazwa grupy, OU.
5. W celu integracji z posiadanym systemem monitorowania SPLUNK serwer zarządzający musi mieć możliwość wysyłania informacji przy wykorzystaniu Sysloga w formacie CEF o zdarzeniach związanych z co najmniej: beczynną stacją końcową, zapobiegnięciu wykorzystaniu podatności, zapobiegnięciu złośliwemu oprogramowaniu.
6. System zarządzający z poziomu konsoli zarządzającej musi mieć możliwość zapisu konfiguracji polityk do pliku w formacie xml.
7. System zarządzający z poziomu konsoli zarządzającej musi mieć możliwość eksportu i importu konfiguracji.
8. Serwer zarządzający musi dystrybuować aktualizacje agentów.

B. Wymagania dotyczące agentów instalowanych na poszczególnych komputerach:

1. Oprogramowanie agenta musi zapobiegać wykorzystaniom podatności lub błędom w oprogramowaniu (exploitom), również tym korzystającym z nieznanych luk „zero-day”.
2. Oprogramowanie agenta musi uniemożliwiać uruchomienie złośliwych plików wykonywalnych, bez potrzeby posiadania wcześniejszej informacji na ich temat.
3. Oprogramowanie agenta musi dostarczać szczegółowe informacje dotyczące powstrzymanych ataków w celu dalszej analizy.
4. Oprogramowanie agenta musi mieć możliwość instalacji na co najmniej następujących systemach operacyjnych: dla stacji końcowych: Windows 7 32 oraz 64 bit, Windows 10 LTSC oraz LTSC 64bit. Dla serwerów: Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2, Microsoft Server 2008 R2.
5. Oprogramowanie agenta musi zawierać moduły chroniące przed wykorzystaniem podatności (anti-exploitation) oraz przed złośliwym oprogramowaniem typu malware (anti-malware):

- a. Moduł Anti-Exploit musi uniemożliwiać wykorzystanie narzędzi używanych do przejęcia zdalnej kontroli nad stacją końcową lub serwerem.
 - b. Moduł Anti-Malware musi umożliwiać analizę każdego nieznanego pliku wykonywalnego poprzez integrację z zewnętrznym systemem typu sandbox w chmurze. Analiza oraz informacja o potencjalnej szkodliwości danego pliku wykonywalnego powinna zostać przeprowadzona w przeciągu 15 minut od wysłania pliku do chmury. Oprogramowanie agenta musi mieć możliwość uniemożliwienia uruchomienia nieznanego pliku wykonywalnego do czasu otrzymania wyników analizy.
6. Oprogramowanie agenta musi mieć możliwość wysyłania tzw. hashów SHA-256 analizowanych plików wykonywalnych do chmury poprzez serwer zarządzający.
 7. Oprogramowanie agenta musi zapobiegać możliwości uruchomienia złośliwego oprogramowania, nie usuwając jednocześnie zainfekowanych plików. W momencie kiedy plik wykonywalny zostanie oznaczony jako malware, musi być możliwość zablokowania jego wykonania, a z poziomu serwera zarządzającego musi być widoczny odpowiedni alert oraz dodatkowe informacje o charakterystyce złośliwego oprogramowania. Oprogramowanie agenta musi mieć możliwość zablokowania uruchomienia danego pliku wykonywalnego na wszystkich stacjach końcowych objętych ochroną, do czasu kiedy werdykt odnośnie szkodliwości danego pliku zostanie przesłany z chmury do serwera zarządzającego.
 8. Komunikacja pomiędzy agentem a serwerem zarządzającym musi być szyfrowana za pomocą protokołu SSL.
 9. Oprogramowanie agenta musi mieć minimalny wpływ na obciążenie stacji końcowej lub serwera. Zużycie RAM powinno wynosić nie więcej niż 100 MB przy normalnym funkcjonowaniu, a obciążenie CPU może maksymalnie wzrosnąć o około 1%.
 10. Oprogramowanie agenta musi mieć możliwość działania w trybie "cichym", w którym nie będą pojawiały się komunikaty dla użytkownika końcowego.
 11. Oprogramowanie agenta musi mieć możliwość ukrycia ikony programu na pasku zadań systemu operacyjnego.
 12. Oprogramowanie agenta musi mieć możliwość przypisania polityki na podstawie: nazwy użytkownika, grupy Active Directory, OU, stacji końcowej bądź serwera.
 13. Oprogramowanie agenta musi mieć możliwość uruchomienia w trybie raportowania, w tym przypadku podejrzane pliki nie będą blokowane.

Oprogramowanie agenta musi posiadać mechanizmy chroniące je przed potencjalną ingerencją i manipulacją. Ochrona musi dotyczyć co najmniej ochrony plików systemowych, ochrony rejestru, ochrony sterowników oraz działających usług (serwisów).

Na wykonawcy ciąży obowiązek wykazania równoważności oferowanego oprogramowania równoważnego.