**BDG.zp.23.1.83.2018 ZAŁĄCZNIK NR 2a DO SIWZ**

**Wykonawca zobowiązany jest podać nazwę oraz producenta Systemu ochrony stacji roboczych i serwerów oraz wypełnić deklarację zgodności z opisem wymagań minimalnych określonych przez Zamawiającego w poniższej tabeli.**

**System ochrony stacji roboczych i serwerów:**

|  |  |
| --- | --- |
| **Producent Systemu:**  | ……………………….……………… |
| **Nazwa Systemu:** | ………………………….…………… |
| **Lp.** | **Opis wymagań minimalnych** | **Deklaracja zgodności z opisem wymagań minimalnych****(Tak / Nie)** |
|  | Możliwość zabezpieczenia co najmniej 1000 stacji roboczych i 100 serwerów. |  |
|  | Funkcjonowanie współbieżne z innymi rozwiązaniami zabezpieczeń stacji roboczych, wykorzystywanymi przez Zamawiającego w szczególności Symantec Endpoint Protection, w zakresie ochrony przed atakami aplikacyjnymi oraz złośliwymi kodami wykonywalnymi. |  |
|  | Zarządzanie poprzez graficzny interfejs użytkownika typu Web (Web GUI). |  |
|  | 3-warstwowa architektura składająca się z konsoli, serwera zarządzania oraz serwera bazy danych. Instalacja i uruchomienie wszystkich trzech komponentów jest możliwe na jednym serwerze sprzętowym lub w architekturze rozproszonej. |  |
|  | Instalacja wielu serwerów zarządzania w konfiguracji rozproszonej i zarządzanie nimi z poziomu pojedynczej konsoli. |  |
|  | Eksport logów w standardzie syslog do dowolnego zewnętrznego systemu zarządzania logów. |  |
|  | Rozwiązanie programowe działające na serwerowych systemach operacyjnych, w szczególności Windows Server 2012 R2. |  |
|  | Możliwość uruchomienia w środowisku zwirtualizowanym VMware. |  |
|  | Zapewnienie ochrony procesów i aplikacji z możliwością dodawania do listy chronionych procesów aplikacji własnych. |  |
|  | Funkcja monitorowania i uczenia się środowiska aplikacyjnego Zamawiającego (tj. rozpoznanie procesów i aplikacji działających na stacjach końcowych użytkowników) celem uruchomienia wdrożenia pilotażowego. |  |
|  | Ochrona w czasie rzeczywistym przed możliwością wykorzystania jakiegokolwiek błędu bezpieczeństwa aplikacji poprzez blokowanie technik wykonania ataku. |  |
|  | Zapewnienie, poprzez blokowanie technik ataków, skutecznej ochrony przed atakami wykonywanymi z użyciem exploit’ów dnia zerowego lub exploit’ów nieznanych, wykorzystujących dowolny błąd bezpieczeństwa aplikacji. |  |
|  | Możliwość monitorowania i zapobiegania atakom poprzez blokowanie szeregu technik ataków bez konieczności połączenia do serwera zarządzania i/lub usługi chmurowej i nie bazując na metodzie sygnaturowej. |  |
|  | W przypadku wykrycia techniki ataku ukierunkowanej na podatną aplikację, celem zablokowania ataku następuje zatrzymanie proces atakowanej aplikacji, zebranie pełnego zestawu danych dowodowych (takich jak nazwa atakowanego procesu, źródło pochodzenia pliku, znacznik czasowy, zrzut pamięci, wersja systemu operacyjnego, tożsamość użytkownika, wersja podatnej aplikacji, itp.) oraz zakończenie działania tylko tego konkretnego procesu. |  |
|  | Wykorzystywanie modułów zapobiegania i blokowania technik ataków. Działanie nie może być oparte o metodę sygnaturową, reputacyjną lub analizę heurystyczną pliku. Możliwość zastosowania modułów blokowania technik ataków zarówno dla powszechnie znanych i popularnych aplikacji jak i aplikacji własnych. |  |
|  | Wykorzystywane zasoby sprzętowe chronionego komputera:* użycie procesora nie więcej niż 2%,
* użycie pamięci RAM nie więcej niż 128MB.
 |  |
|  | Jednoczesna ochrona wszystkich aplikacji i procesów przed wszystkimi technikami ataków. |  |
|  | Tworzenie wyjątków konfiguracyjnych dla określonych stacji końcowych i działających na nich procesów bezpośrednio z poziomu i na bazie zebranych po stronie konsoli zarządzającej logów. |  |
|  | Ochrona przed uruchomieniem złośliwych plików wykonywalnych. |  |
|  | Funkcja monitorowania i uczenia się środowiska aplikacyjnego Zamawiającego (tj. rozpoznanie procesów i aplikacji działających na stacjach końcowych użytkowników). |  |
|  | Pełna kontrola i ustalanie restrykcji parametrów i sposobu uruchamiania plików wykonywalnych (np. dozwolone foldery źródłowe, ścieżki sieciowe, urządzenia zewnętrzne, możliwość uruchamianie plików nie posiadających podpisu cyfrowego wystawcy, możliwość tworzenia procesów potomnych, itp.). |  |
|  | Zapobieganie uruchamianiu złośliwego oprogramowania poprzez użycie modułów blokujących typowe zachowania złośliwych kodów wykonywalnych. |  |
|  | Konfiguracja globalnych list dozwolonych plików wykonywalnych w środowisku Zamawiającego. |  |
|  | Tworzenie wyjątków konfiguracyjnych dla określonych stacji końcowych celem wykluczenia ich z ogólnych reguł ochrony bezpośrednio z poziomu i na bazie zebranych po stronie konsoli zarządzającej logów. |  |
|  | Ochrona przeciwko złośliwemu oprogramowaniu oraz atakom aplikacyjnym nawet jeśli nie posiada połączenia do środowiska chmurowego. |  |
|  | Możliwość weryfikacji w chmurowym środowisku anty-APT (Advanced Persistent Threat) czy dany plik jest złośliwy, czy legalny na bazie skrótu cyfrowego pliku. |  |
|  | Możliwość wysłania poprzez serwer zarządzania potencjalnie złośliwego pliku do analizy w chmurowym środowisku anty-APT. |  |
|  | Możliwość wglądu w raport wynikowy analizy pliku w środowisku chmurowym anty-APT bezpośrednio z poziomu stacji zarządzania oprogramowaniem zabezpieczeń stacji końcowych. |  |
|  | Zapobieganie nieznanym złośliwym plikom wykonywalnym poprzez zastosowanie chmurowego środowiska anty-APT typu “sandbox”. Możliwość przedstawienia wyniku analizy pliku wraz z pełnym raportem z analizy. |  |
|  | Możliwość ręcznego dostrojenia lub nadpisania werdyktu będącego wynikiem analizy w środowisku chmurowym dla konkretnego skrótu cyfrowego pliku. |  |
|  | Możliwość zablokowania uruchomienia pliku wykonywalnego jeśli skrót cyfrowy pliku jest nieznany, tj. plik ten nie był uprzednio analizowany w środowisku chmurowym anty-APT producenta. |  |
|  | Możliwość uruchomienia analizy statycznej pliku opartej o algorytmy uczenia. |  |
|  | Wbudowane pulpity raportów (ang. Dashboard) do monitorowania poziomu i stanu bezpieczeństwa środowiska Zamawiającego (tj. Pulpit Stanu Komponentów Systemu, Pulpit Zdarzeń Bezpieczeństwa, Pulpit Szczegółowego Dziennika Zagrożeń, Pulpit Szczegółowego Dziennika Błędów Bezpieczeństwa). |  |
|  | Wbudowane pulpity raportów (ang. Dashboard) do monitorowania stanu poszczególnych stacji końcowych Zamawiającego (tj. Pulpit Szczegółowego Stanu/Statusu Stacji Końcowych, Pulpit Historii Reguł Bezpieczeństwa Stacji Końcowych, Pulpit Zmian Reguł Bezpieczeństwa Stacji Końcowych, Pulpit Historii Stanu Serwisu Stacji Końcowych). |  |
|  | Wyświetlanie informacji za pomocą przeglądarki www, na temat wykrytych zagrożeń i złośliwego oprogramowania oraz eksport dziennika zdarzeń zagrożeń i stanu stacji końcowych w formacie CSV. |  |
|  | Możliwość zbierania dokumentacji dowodowej i danych ze stacji końcowych w jednym centralnym punkcie. |  |
|  | Możliwość zbierania informacji w celu przeprowadzenia późniejszej analizy, w szczególności takich jak: Zrzut pamięci (Memory Dump), Otwarte pliki, Załadowane moduły, Otwarte URI, Procesy nadrzędne). |  |
|  | Możliwość przesyłania danych powiązanych z dokumentacją dowodową za pomocą niewykorzystanego pasma sieciowego przy pomocy usługi inteligentnego transferu w tle BITS (Background Intelligent Transfer Service) lub przy pomocy protokołu gwarantującego równoważną funkcjonalność. |  |
|  | Możliwość dostosowania polityk powiązanych z dokumentacją dowodową w ramach serwera zarządzającego, w celu zdefiniowania jaki typ danych powinien zostać zebrany w przypadku wystąpienia incydentu. |  |
|  | Wyświetlenie wysokopoziomowych informacji systemowych na temat stacji końcowej po wykryciu zagrożenia oraz możliwość zebrania danych odnoszących się do zastosowanego mechanizmu ochrony celem dalszej analizy i śledztwa. |  |
|  | Automatyczne tworzenie wyjątków odnośnie reguł oraz skrótów cyfrowych bezpośrednio z raportu dotyczącego wykrytego zagrożenia w celu umożliwienia uruchomienia danego procesu na poszczególnych stacjach końcowych. |  |

.............................., dn. ............ 2018 r. .....................................................................

*(podpis/y osoby/osób uprawnionej/ych)*