Załącznik nr 1 do Umowy nr …… z dnia ……..

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostarczenie i wdrożenie rozwiązania informatycznego obejmującego funkcjonalność wykrywania i reakcji na zagrożenia, zapewniającą ochronę stacji roboczych i serwerów przed atakami, zwanego dalej „Systemem" wraz ze Sprzętem niezbędnym do prawidłowego działania Systemu zwanym dalej „Sprzętem". System w formie platformy SaaS służyć ma do ochrony stacji końcowych i serwerów przed atakami, które wykorzystują różne technologie umożliwiające obejście tradycyjnych systemów zabezpieczeń.

Stosowane definicje:

System – całość oferowanego rozwiązania zawierająca wszystkie niezbędne komponenty w tym wszystkie licencje, cały Sprzęt, usługi uruchomione w modelu chmurowym (SaaS) dostarczane Zamawiającemu umożliwiające realizację funkcjonalności zgodnie z Przedmiotem Zamówienia.

Sprzęt – wszystkie niezbędne do prawidłowego działania Systemu urządzenia fizyczne w tym, kable sieciowe i inne fizyczne elementy na których zostanie uruchomione wdrażanie rozwiązanie w infrastrukturze Zamawiającego (w przypadku gdy oferowane rozwiązanie będzie zawiarało Sprzęt).

SaaS (Software as a Service) – oprogramowanie jako usługa w chmurze. Model świadczenia usługi zdalnego dostępu do oprogramowania w którym aplikacja jest przechowywana i wykonywana w śdodowisku dostawcy usługi i jest udostępniana Zamawiającemu przez Internet przy zachowaniu wysokiego poziomu bezpieczeństwa danych (tj. poufności, integralności i dostępności danych).

Agent – oprogramowanie instalowane na stacjach końcowych/serwerach.

Przedmiot zamówienia obejmuje:

1. Dostarczenie i wdrożenie systemu do ochrony stacji roboczych i serwerów zwanego dalej „Systemem" wraz ze Sprzętem i usługami SaaS niezbędnymi do prawidłowego działania Systemu oraz przeniesie na rzecz Zamawiającego własności Sprzętu, oraz udzielenie lub zapewnienie udzielenia licencji wymaganych do prawidłowego działania Systemu jako całości w szczególności:
   1.1. opracowanie projektu wdrożeniowego obejmującego instalację i konfigurację Systemu,
   1.2. dostawę całego niezbędnego do prawidłowego działania Systemu Sprzętu, udostępnienie i uruchomienie wszystkich wymaganych usług SaaS oraz wymaganych licencji do prawidłowego działania Systemu jako całości,
   1.3. dostawę licencji wraz wymaganymi plikami instalacyjnymi i konfiguracyjnymi dla wdrażanego rozwiązania umożliwiających obsługę w zakresie ochrony 40 tysięcy stacji roboczych i serwerów,
   1.4. wdrożenie Systemu w oparciu o założenia projektu wdrożeniowego,
   1.5. wykonanie dokumentacji powykonawczej,
   1.6. przeprowadzenie transferu wiedzy dla co najmniej 4 pracowników Zamawiającego z zakresu funkcjonowania dostarczonego Systemu i administrowania nim w wymiarze ninimum 40 godzin,
   1.7. udzielenie gwarancji dla wdrożonego Systemu wraz ze Sprzętem niezbędnym do prawidłowego działania Systemu przez okres 36 miesiecy od dnia podpisnia bez zastrzeżeń przez Zamawiającego Protokołu Odbioru Wdrożenia Systemu.
   1.8. Licencje muszą pozwalać na swobodne przenoszenie pomiędzy stacjami roboczymi i serwerami (np. w przypadku wymiany sprzętu) oraz możliwość przenoszenia dostarczonego w ramach umowy oprogramowania pomiędzy jednostkami organizacyjnymi resortu

sprawiedliwości. Licencjobiorcą jest Ministerstwo Sprawiedliwości a podmiotami uprawnionymi do korzystania z oprogramowania są jednostki podległe lub nadzorowane przez Ministra Sprawiedliwości oraz jednostki sądownictwa powszechnego.

2. Zapewnienie 500 roboczogodzin asysty technicznej do dowolnego wykorzystania w całym okresie obowiązywania umowy lub do czasu wykorzystania całej puli godzin przez Zamawiającego.

II Wymagania w zakresie realizującym funkcjonalność systemu kompleksowej ochrony stacji roboczych i serwerów w Ministerstwie Sprawiedliwości

II a. Wymagania dotyczące oferowanego rozwiązania

1. Oferowane rozwiązanie będzie pochodziło z oficjalnego kanału dystrybucyjnego producenta na terenie Unii Europejskiej.
2. Wszystkie oferowane urządzenia i oprogramowanie Systemu muszą stanowić jednolite środowisko tj. współpracować ze sobą bez konieczności stosowania dodatkowych modułów nie będących standardowym elementem oferowanego rozwiązania w szczególności pochodzić od innego producenta.
3. Oferowane rozwiązanie ma stanowić jednolity i kompleksowy system, który będzie skalowalny i elastyczny w kontekście potencjalnej rozbudowy tj. objęcia ochroną kolejnych stacji roboczych i serwerów. Wymaganiem Zamawiającego jest, aby możliwość zarządzania całością systemu odbywała się z wykorzystaniem jednej konsoli zarządzającej.
4. Oferowane rozwiązanie nie może być zabronione do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).
5. Oferowane rozwiązanie nie może być czasowo wstrzymane do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).
6. Zamawiający wymaga, aby wszystkie komponenty dostarczanego Systemu były w najnowszej wersji (tzn. najnowszej udostępnionej przez producenta rozwiązania) na dzień dostawy Systemu .
7. Żaden z komponentów oferowanego Systemu na dzień składania ofert nie może być przeznaczony przez producenta do wycofania z produkcji lub sprzedaży.
8. Czynności związane z wdrożeniem i konfiguracją Systemu w infrastrukturze Zamawiającego Systemu muszą być przeprowadzone przez personel Wykonawcy w obecności personelu IT Zamawiającego.
9. Wszystkie niezbędne komponenty sprzętowe i programowe wymagane do poprawnego działania Systemu muszą w pełni ze sobą współpracować, być dostarczone wraz z Systemem oraz być w pełni objęte gwarancją.

II b. Wymagania w zakresie gwarancji

1. W ramach udzielonej gwarancji Wykonawca udostępni oprogramowanie umożliwiające zdalne zgłaszanie i monitorowanie statusu zgłoszenia awarii,oprogramowanie to musi zapewnić Zamawiającemu brak ograniczeń, co do liczby dokonywanych zgłoszeń w zakresie awarii.
2. Wszelkie prace wykonywane przez Wykonawcę w Systemie nie mogą skutkować utratą praw gwarancyjnych do Systemu przez Zamawiającego.
3. W ramach udzielonej gwarancji Wykonawca będzie realizował zgłoszenia awarii Systemu w następujący sposób:
   - awaria krytyczna, tj. niedostępność systemu dla wszystkich użytkowników: czas reakcji do 4 godzin od chwili zgłoszenia awarii przez Zamawiającego, czas naprawy (przywrócenia funkcjonalności systemu) do 24 godzin od chwili zgłoszenia awarii przez Zamawiającego;
   - awaria niekrytyczna tj.niepowodująca niedostępności systemu: czas reakcji do 4 godzin od chwili zgłoszenia awarii przez Zamawiającego, czas naprawy (przywrócenia funkcjonalności systemu) do 72 godzin od chwili zgłoszenia usterki przez Zamawiającego.

- Wszelkie awarie będą zgłaszane przez Zamawiajacego za pomocą udostępnionego przez Wykonawcę oprogramowania o którym mowa w punkie 1 powyżej.

W przypadku potrzeby wydania poprawki do Systemu przez producenta, na wniosek Wykonawcy złożony w formie elektronicznej Zamawiający może zawiesić czas usunięcia awarii niekrytycznych, maksymalnie na 40 dni.

4. Obsługa zgłoszeń musi obejmować co najmniej:
   - wymianę przez Wykonawcę uszkodzonego Sprzętu,
   - aktualizację i konfigurację Systemu oraz Sprzętu przez Wykonawcę,,
   - rozwiązywanie przez Wykonawcę zgłaszanych problemów związanych z działaniem i obsługą Systemu,
5. Wykonawca w ramach udzielonej gwarancji na wezwanie i w uzgodnieniu z Zamawiającym wymieni uszkodzony Sprzęt (lub jego uszkodzone elementy) zainstaluje poprawki, usprawnienia i nowe wersje oprogramowania dla Systemu i Sprzętu, udostępniane przez producenta wdrożonego Systemu oraz Sprzętu.
6. W ramach w ramach udzielonej gwarancji Zamawiającemu przysługuje prawo do samodzielnej instalacji i używania wszystkich poprawek, usprawnień i nowych wersji Systemu udostępnianych przez producenta Systemu bez ponoszenia dodatkowych kosztów finansowych przez Zamawiającego. Powyższe nie może skutkować utrata uprawnień gwarancyjnych przysługujących Zamawiającemu.

II c. Wymagania w zakresie dokumentacji

1. Wykonawca opracuje i dostarczy następującą dokumentację dotyczącą projektu wdrożeniowego:
   a. projekt wdrożenia Systemu, który musi zawierać, w szczególności: opis funkcjonalny Systemu, wykaz wymaganych komponentów, sposób ich wdrożenia i konfiguracji, wykaz licencji i Sprzętu niezbędnego dla działania Systemu jako całości, szczegółowy opis architektury proponowanego rozwiązania wraz z opisem integracji z infrastrukturą techniczną Zamawiającego, harmonogram wdrożenia,
   b. dokumentację testów akceptacyjnych wdrożenia Systemu, która musi dokumentować działania, jakie należy wykonać, aby uzyskać potwierdzenie, że wdrożony System jest zgodny z opisem przedmiotu zamówienia,
2. Wykonawca opracuje i dostarczy dokumentację powykonawczą, która musi być jednym spójnym dokumentem, bez względu na jej objętość i musi zawierać procedury administracyjne i operacyjne oraz inne informacje, istotne w eksploatacji Systemu, w szczególności:
   a. procedury i instrukcje dotyczące instalacji, konfiguracji i aktualizacji Systemu,
   b. procedury dotyczące wykonywania i przechowywania kopii bezpieczeństwa,
   c. instrukcje dla użytkowników i administratorów w tym procedury zarządzania zdarzeniami dotyczącymi bezpieczeństwa,
   d. inne niezbędne dokumenty, jakie powstaną w trakcie realizacji wdrożenia Systemu, uzgodnione z przedstawicielem Zamawiającego.
3. Dokumentacja powinna być dostarczona w wersji elektronicznej w języku polskim lub angielskim.

II d. Wymagania w zakresie transferu wiedzy

1) W ramach wdrożenia Wykonawca umożliwi Zamawiającemu w siedzibie i w środowisku Zamawiającego transfer wiedzy dla co najmniej 4 pracowników Zamawiającego polegający na możliwości uczestniczenia ww. pracowników przy wdrażaniu, konfiguracji i administracji Systemem. W szczególności transfer wiedzy polegać będzie na:
   a) zapewnieniu możliwości udziału pracowników Zamawiającego przy przeprowadzanym przez inżyniera/inżynierów wdrożenia Systemu po stronie Wykonawcy,

b) udzielaniu odpowiedzi na pytania zadawane przez pracowników Zmawiającego w zakresie zagadnień związanych z czynnościami administracyjnymi, funkcjonowaniem wdrożonego Systemu w środowisku produkcyjnym Zamawiającego, w tym omówieniu wraz z przeprowadzeniem praktycznych scenariuszy możliwości Systemu w zakresie wykrywania, przeciwdziałania i usuwania złośliwego oprogramowania,
c) Zapewniueniu transferu wiedzy w zakresie konfiguracji Systemu i administracji Systemem, który musi być prowadzony na bieżąco w trakcie wdrożenia lecz przed zakończeniem wdrożenia. Transfer wiedzy przeprowadzony zostanie w języku polskim.

II e. Wymagania w zakresie wdrożenia

1. W ramach wdrożenia Systemu Wykonawca dostarczy, zainstaluje i skonfiguruje cały niezbędny Sprzęt, wymagane komponenty Systemu oraz licencje zgodnie z zaakceptowanym przez Zamawiającego projektem wdrożenia.
2. W ramach wdrożenia Systemu muszą zostać przygotowane tzw. paczki cichej instalacji dla systemów Windows 7, Windows 10, jak również systemów serwerowych Windows Server 2008, Windows serwer 2012, Windows serwer 2012 R2, Windows serwer 2016. Paczka instalacyjna musi zawierać mechanizm automatycznej konfiguracji rozwiązania tj. podłączenia agenta do modułu zarządzania Usługą oraz instrukcję ich przygotowania i instalacji. Wymagane są także paczki instalacyjne dla systemów MacOS 10 oraz Linux (co najmniej RedHat).
3. Miejsca realizacji przedmiotu Umowy: ul. Czerniakowska 100, 00-454 Warszawa, Na wniosek Wykonawcy Zamawiający może wyrazić zgodę w formie pisemnej na wykonanie prac zdalnie w całości lub części, pod warunkiem przestrzegania przez Wykonawcę zasad bezpieczeństwa określonych przez Zamawiającego.
4. Wykonawcy nie przysługuje dodatkowe wynagrodzenie ani zwrot poniesionych jakichkolwiek kosztów z tytułu realizacji prac w siedzibie Zamawiającego.
5. Potwierdzeniem prawidłowej realizacji przedmiotu Umowy w zakresie dokumentacji projektowej będzie podpisany bez zastrzeżeń przez Zamawiającego Protokół odbioru zawierający w szczególności: odbiór dokumentacji projektowej tj. projektu wdrożenia Systemu, dokumentacja testów akceptacyjnych, opis scenariusza wdrożenia mechanizmów ochrony dla wszystkich komponentów Systemu.
6. Potwierdzeniem prawidłowej realizacji przedmiotu Umowy w zakresie uruchomienia i skonfigurowania Systemu będzie podpisany bez zastrzeżeń przez Zamawiającego Protokół odbioru Systemu zawierający w szczególności:
    - odbiór Systemu realizującego funkcjonalność kompleksowej ochrony stacji roboczych i serwerów na podstawie przeprowadzonych testów akceptacyjnych,
    - odbiór dokumentacji powykonawczej,
    - odbiór realizacji transferu wiedzy,
    - odbiór licencji i Sprzętu.

II f. Wymagania w zakresie modułu instalowanego na stacjach roboczych i serwerach

1. Komponent zaawansowanej ochrony stacji roboczej i serwerów powinien bazować na architekturze typu SaaS, przy czym cała funkcjonalność realizowana przez ten komponent MUSI być realizowana na terenie Unii Europejskiej i przez podmiot posiadający centrum przetwarzania na terenie Unii Europejskiej. Przy czym Zamawiający wymaga zapewnienia bezpieczeństwa w zakresie zapewnienia integralności, poufności i dostępności usługi i przetwarzanych danych Zamawiającego.
2. Zamawiający wymaga, aby Agent na stacje był dostarczony w formie, która pozwoli na jego dystrybucje za pomocą narzędzi do centralnej dystrybucji i instalacji oprogramowania. Konfiguracja instalatora powinna być wykonana w postaci ukrytej, dać możliwość wskazania dedykowanej ścieżki instalacji.

3. Zamawiający wymaga, aby Agent wspierał co najmniej następujące wersje Systemów operacyjnych: Windows 7 i nowsze, Windows Server 2008 i nowsze, Mac OS X i nowsze oraz Systemy Linux RedHat).

4. Oprogramowanie agenta musi mieć zdolność aktywnej ochrony przed szkodliwym kodem za pomocą skanowania zgodnie z harmonogramem oraz na żądanie.
5. Oprogramowanie Agenta powinno posiadać mechanizm zabezpieczający, który zapobiegnie nieuprawnionej deinstalacji agenta.
6. Zamawiający wymaga, aby konfiguracja Systemu pozwalała na określenie wyjątków od działania agentów na stacjach. Co najmniej dla:
    a. funkcjonalności blokowania złośliwego kodu– wykluczanie spod ochrony (whitelisting) co najmniej wskazanych katalogów, procesów, aplikcji, sum kontrolnych,
    b. funkcjonalności silnika AV – całkowite wyłączenie silnika dla określonych grup komputerów.
7. Zamawiający wymaga, aby architektura i logika dostarczanego systemu zapewniała ciągły, aktywny i taki sam poziom ochrony przed szkodliwym oprogramowaniem dla stacjach roboczych podłączonych do sieci zarządzanych przez Zamawiającego (w obrębie sieci LAN Zamawiającego) oraz poza nią tj. dla użytkowników zdalnych, pracujących poza siecią Zamawiającego.
8. Oprogramowanie agenta i jego działanie nie może kolidować z oprogramowaniem bezpieczeństwa standardowo dostępnym w systemie operacyjnym stacji roboczej, serwera (tj. stanowiącego element systemu operacyjnego).
9. Zamawiający wymaga, aby agent umożliwiał aktywną detekcję i blokowanie prób wykorzystania makr i skryptów w plikach do zainicjowania ataku i uruchomienia złośliwego kodu (tzw. exploits) nie bazującą na sygnaturach lub regułach IoC. Monitorowane i chronione mają być co najmniej następujące aplikacje:
    a. MS Office: Microsoft Word/Excel/PowerPoint,
    b. Przeglądarki Web: Internet Explorer/Mozilla FireFox/Google Chrome,
    c. Adobe Reader i Flash,
    d. Oracle/Sun Java.
10. Zamawiający wymaga, aby System posiadał możliwość śledzenia i wykrywania nowych procesów na analizowanej stacji roboczej w celu wykrycia procesów powiązanych z działalnością złośliwego oprogramowania.
11. System powinien posiadać możliwość wykrywania prób eskalacji uprawnień w chronionych stacjach roboczych i serwerach.
12. Zamawiający wymaga, aby System zapewniał możliwość izolowania zainfekowanej stacji (blokowania komunikacji sieciowej na żądanie jak i automatycznie na podstawie zdefiniowanych reguł, alertów itp) np. poprzez zmianę reguł filtrowania ruchu sieciowego. Proces blokowania komunikacji sieciowej powinien zapewniać możliwość określenia wyjątków od blokowania komunikacji sieciowej co najmniej na podstawie adresów IP. Wyjątki powinny w szczególności umożliwiać komunikację z konsolą zarządzania, przeprowadzenie analizy zainfekowanej stacji itp.

13. Zamawiający wymaga, aby System posiadał narzędzia do przeprowadzania analizy powłamaniowej i wyszukiwania zidentyfikowanych cech ataku (tzw. wskaźników kompromitacji ang. IoC) w szczególności:
    a. zmiany umożliwiające instalację złośliwego oprogramowania w systemie,
    b. zmiany w rejestrze,
    c. operacje na poziomie procesów (tworzenie, zamykanie, etc.),
    d. operacje na poziomie plików (tworzenie, kasowanie, modyfikacja, etc.),
    e. operacje na poziomie pamięci masowej, zmiany w systemie plików,
    f. na poziomie zapytań DNS,
    g. operacje na poziomie komunikacji sieciowej,
    h. operacje zmiany konfiguracji, połączeń sieciowych,
    i. wskazane zdarzenia zbierane przez log systemowy.
14. Zamawiający wymaga, aby System zapewniał możliwość pozyskiwania (akwizycji) z systemu operacyjnego chronionego komputera co najmniej następujących danych:
    a. konfiguracji sieciowej,
    b. informacji o systemie operacyjnym,
    c. historii stron WWW przeglądanych przez użytkownika,
    d. aktywnych zadań systemowych,
    e. historii pobieranych plików,
    f. kont użytkowników i ich aktywności,
    g. pliki prefetch,
    h. klucze rejestru zwłaszcza odpowiedzialne za ukrycie malware w systemie na czas restartu komputera,
    i. procesy Systemowe i uruchomione z uprawnieniami użytkownika.
15. Zamawiający wymaga, aby System zapewniał możliwość przeszukania stacji roboczych, serwerów, tzn. istniała możliwość formułowania zapytań dla agentów, mających na celu potwierdzenie obecności potencjalnych zagrożeń lub wskaźników kompromitacji w oparciu o co najmniej poniższe parametry wyszukania:
    a. pliki – nazwa, ścieżka, sumy kontrolne,
    b. rejestr – ścieżka, nazwa, wartość,
    c. proces – nazwa, ścieżka, argument,
    d. usługa Systemowa – nazwa, stan, typ,
    e. zadania Systemowe – nazwa, stan, tryb,
    f. zdarzenia Systemowe – numer, typ, komunikat,
    g. znaczniki czasu – ostatnie uruchomienie/logowanie, dostęp/modyfikacja/utworzenie,
    h. komunikacja – adres IP, port (zdalny i lokalny), protokół, nazwa DNS,
    i. przeglądarki Web – wersja, nazwa, cookie, adres URL, odnośnik strony pobranego pliku (tzw. HTTP referrer), tytuł strony web, nagłówek http
16. Zamawiający wymaga, aby System umożliwiał tworzenie własnych wskaźników kompromitacji (ang. IoC) opartych co najmniej o takie parametry jak: ścieżka pliku, suma MD5 pliku, rozmiar pliku, zapytanie DNS, parametry połączenia sieciowego (docelowy adres IP, źródłowy adres IP, docelowy port, źródłowy port).
17. Reguły behawioralne muszą być dostarczane i tworzone przez producenta systemu.

18. System musi pozwalać na analizę w oparciu o reguły YARA lub IoC. Producent musi udostępniać i aktualizować listę reguł YARA oraz IOC. Ponadto musi istnieć możliwość ręcznego importu własnych plików z regułami.
19. System MUSI bazować na jednym agencie, to jest Zamawiający nie dopuszcza pracy kilku różnych agentów realizujących poszczególne funkcjonalności wskazane w OPZ.
20. System POWINIEN prezentować alerty w sposób czytelny i umożliwiający łatwą identyfikację przebiegu całego ataku, jak i jego poszczególnych faz.
21. System POWINIEN mieć możliwość automatycznego pobierania wskaźników IoC oraz informacji z Intelligence producenta bez dodatkowych licencji oraz modułów.
22. System MUSI pracować w sposób nieprzerwany także bez aktywnego dostępu do Internetu na stacji roboczej.

II g. Wymagania w zakresie modułu do analizy próbek Malware

1. Zamawiający wymaga, aby moduł posiadał wydajność umożliwiającą analizowanie co najmniej 1 tyś. próbek malware dziennie.
2. Zamawiający wymaga, aby analiza próbek była realizowna w izolowanym środowisku funkcjonującym jako:
    a. usłauga SaaS będaca standardowym elementem Systemu i pochodząca od tego samego producenta co System. Dodatkowo Wykonawca dostarczy całe oprogramowanie i licencje konieczne do uruchomienia tej usługi (np. oprogramowanie i licenicje na systemy operacyjne, licencje na hypervisory, etc). Wykonawca skonfiguruje i uruchomi wszystkie komponenty oprogramowania i usług SaaS.
    b. lub w postaci dedykowanego środowiska wirtualnego (tj. opogramowania uruchamianego w środowisku wirtualnym) przy czym oprogramowanie to musi być standardowym elementem Systemu i pochodzić od tego samego producenta co System gdzie cały proces analizy musi się odbywać w tym środowisku wirtualnym, nie jest dopuszczlane wysyłanie analizowanych plików/obiektów poza to środowisko (dopuszczlane jest jedynie wysyłanie cech charakterystycznych np. sum kontlolnych plików). Dodatkowo Wykonawca dostarczy całe oprogramowanie i licencje konieczne do uruchomienia tego środowiska wirtualnego (np. oprogramowanie i licenicje na systemy operacyjne, licencje na hypervisory, etc). Wykonawca skonfiguruje i uruchomi wszystkie komponenty oprogramowania na infrastrukturze zwirtualizowanej Zamawiającego.
3. Zamawiający wymaga, aby moduł analizy próbek malware był wyposażony w maszyny wirtualne wykonujące równolegle analizę dynamiczną próbek malware (w tym także adresów URL) w różnych wersjach systemu operacyjnego i aplikacji jednocześnie (co najmniej: Win 7 SP1, Win7 SP1, WIN10) różnych aplikacji i ich różnych wersji zainstalowanych w tych systemach (co najmniej FireFox, Chrome, IE, Adobe Reader, Java JDK JRE, MS Office, QuickTime Player, Win Media Player, Real Player, VLC Player, RunDLL). Wszystkie niezbędne licencje na systemy operacyjne i aplikacje MUSZĄ być dostarczone wraz z proponowanym rozwiązaniem.
4. Zamawiający wymaga, aby na potrzeby analizy próbek malware (tj. uruchamiania plików w izolowanym środowisku) System zapewniał co najmniej:
    a. środowisko, w jakim jest wykonywana analiza dynamiczna, posiadało mechanizmy utrudniające jego wykrycie przez analizowany malware,

b. maszyny wirtualne, w których wykonywana jest analiza zachowania ataku posiadały mechanizmy symulacji pracy realnego użytkownika,
c. możliwość nawiązania połączenia sieciowego badanej próbki umożliwiające pobranie dodatkowej zawarości z Internetu; kontkatu z serwerami C&C itp. (celem śledzenia działania badanej próbki w sieci),
d. możliwość parametryzacji środowisk wirtualnych w zakresie: nazwy domeny, folderów użytkowników, ostatnio otwartych plików, języka systemu operacyjnego, wpisania hasła w celu automatycznego odszyfrowania przekazywanej do analizy próbki malware,
e. możliwość ręcznego wysyłania próbek (plików/obiektów) jak również adresu URL do analizy dynamicznej z poziomu konsoli zarządzającej Systemu oraz możliwość prezentacji wyników tej analizy,

5. Zamawiający wymaga, aby moduł umożliwiał generowanie raportów zawierających co najmniej wyniki analiz i statystyki przeanalizowanych próbek. Raporty powinny mieć możliwość eksportu na przykład do formatu CSV lub PDF wraz z możliwością ustalenia okresu czasu dla generowanego raportu (na przykład: ostatnie 24 godziny, ostatni 7 dni, ostatnie 30 dni).
6. Zamawiający nie dopuszcza rozwiązań innych producentów niż producenta pozostałych komponentów Systemu w celu zapewnienia pełnego poziomu bezpieczeństwa i kompatybilności.

II h. Wymagania dotyczące Zarządzania rozwiązaniem

1) System musi pozwalać na zarządzanie wszystkimi komponentami dokonującymi analizy oraz wszystkimi ich parametrami (np.: konfiguracja trybów pracy, konfigurację zasad alarmowania, zasad eksportu danych do innych systemów bezpieczeństwa, zasad wykonywania kopii bezpieczeństwa, propagowanie poprawek i aktualizacje oprogramowania, zarzadzanie licencjami) przy pomocy komponentu realizującego funkcję centralnego systemu zarządzania.
2) Korzystanie z centralnego systemu zarządzania musi odbywać się przy pomocy interfejsu graficznego dostępnego zdalnie, przy wykorzystaniu standardowej przeglądarki internetowej.
3) Komunikacja służąca zapewnieniu zdalnego dostępu użytkowników i administratorów do Systemu jak również pomiędzy poszczególnymi jego komponentami musi być zabezpieczona kryptograficznie w zakresie zapewnienia poufności i integralności przesłanych danych.
4) Zarządzanie Systemem powinno być dostępne jako SaaS.
5) System zarządzania powinien zapewniać co najmniej:
   a) automatyczną wymianę wyników analiz między elemantami Systemu (zwłaszcza pochodzących z analizy próbek malware),
   b) przegląd wyników analiz z wszystkich elementów Systemu,
   c) dostęp do statystyk z działania poszczególnych komponentów,
   d) możliwość tworzenia kont użytkowników Systemu o różnych poziomach uprawnień,
   e) logowanie i przegląd działań w Systemie,
   f) możliwość tworzenia kopii zapasowych konfiguracji Systemu i jej odtwarzania.
6) System musi udostępniać możliwość integracji z systemem klasy SIEM poprzez API (preferowany otwarty standard RESTful Interface lub co najmniej syslog).
7) System MUSI udostępniać możliwość integracji z system analizy Malware w zakresie wysyłania próbek do analizy z poziomu konsoli Systemu.

III Wymagania w zakresie asysty technicznej eksperta

1. Świadczenie usługi asysty technicznej jest uprawnieniem Zamawiającego. Niewykorzystanie wszystkich przewidzianych w umowie roboczogodzin nie rodzi po stronie Wykonawcy żadnych roszczeń z tego tytułu w stosunku do Zamawiającego.
2. W roboczogodzinę asysty technicznej eksperta nie wlicza się czasu dojazdu oraz ilości osób zapewniających wsparcie tzn. nie ma znaczenia ile osób będzie świadczyło asystę techniczną eksperta w danej roboczogodzinie/roboczogodzinach u Zamawiającego. Rozliczenie roboczogodzin asysty technicznej eksperta odbywać się będzie za faktycznie wykorzystane roboczogodziny na podstawie Protokołów odbioru asysty technicznej eksperta. Do godzin asysty technicznej eksperta nie wlicza się roboczogodzin usług wykonywanych w ramach realizacji zgłoszeń awarii Systemu.
3. Asysta techniczna eksperta będzie dotyczyła oferowanego przez Wykonawcę Systemu i będzie polegała w szczególności na:
    a. bieżącym utrzymaniu i zażądaniu Systemem,

    b. konsultacji w zakresie szczegółowej analizy zdarzeń generowanych przez System z wyłączeniem awarii,
4. Osoby uprawnione w umowie przez Zamawiającego będą przekazywać Wykonawcy zlecenia asysty technicznej, w których każdorazowo określony zostanie przedmiot zlecenia, oczekiwany termin realizacji zlecenia oraz miejsce realizacji zlecenia.
5. Wykonawca w terminie wyznaczonym przez Zamawiającego, od otrzymania zlecenia, przekaże Zamawiającemu propozycję sposobu wykonania zlecenia zawierającą w szczególności wycenę prac zawartych w zleceniu, tj. proponowaną liczbę roboczogodzin niezbędnych do wykonania zlecenia.
6. Zamawiający może zaakceptować propozycję sposobu wykonania zlecenia albo odrzucić ją, co jest równoznaczne z nieudzieleniem zlecenia albo zażądać od Wykonawcy, dodatkowych wyjaśnień, informacji do przedstawionej propozycji sposobu wykonania zlecenia.
7. W przypadku akceptacji propozycji sposobu wykonania zlecenia, Zamawiający przedłoży Wykonawcy zaakceptowane zlecenie zawierające w szczególności: zakres prac, liczbę roboczogodzin niezbędną do wykonania prac, kwotę wynagrodzenia należnego za zrealizowanie zlecenia, termin wykonania prac.
8. Rozliczenie asysty technicznej odbywać się będzie na podstawie podpisanych bez zastrzeżeń, przez Zamawiającego, Protokołów odbioru asysty technicznej eksperta.
9. Zamawiający może wyrazić zgodę na wykonanie zlecenia zdalnie, w takim przypadku Wykonawca zobowiązany jest do przestrzegania wszystkich wymagań Zamawiającego. Zamawiający zastrzega sobie prawo do odmowy, przerwania świadczenia usługi zdalnego dostępu w dowolnym momencie bez wcześniejszego informowania Wykonawcy.

Zamawiający dopuszcza posiadanie przez Systemem funkcjonalności które nie są wymagane przez Zamawiającego lecz mogą stanowić dodatkową funkcjonalność Systemu ocenianą przez Zamawiającego dla każdej z poniższych funkcjonalności opcjonalnych niezależnie.

1. Jako funkcjonalność dodatkową: moduł do analizy próbek malware może być dostarczony jako rozwiązanie oparte na dedykowanym urządzeniu typu appliance dedykowanym do instalacji i pracy ciągłej w standardowej szafie przemysłowej typu rack 19” (standard EIA-310), czyli Sprzęt o przeznaczeniu przemysłowym (czyli nie jest adaptowanym sprzętem przeznaczonym do użytku osobistego lub biurowego). W takim przypadku Wykonawca skonfiguruje i uruchomi wszystkie komponenty oprogramowania na Sprzęcie. Zaoferowany moduł musi być też standardowym elementem Systemu i pochodzić od tego samego producenta co System. Przy czym cały proces analizy musi się odbywać na tym urządzeniu, nie jest dopuszczlane wysyłanie analizowanych plików/obiektów poza moduł (dopuszczlane jest jedynie wysyłanie cech charakterystycznych np. sum kontrolnych plików).
2. Jako funkcjonalność dodatkową: moduł do analizy próbek malware może posiadać spersonalizowany dedykowany interfejs użytkownika WWW (prosta storna WWW) w języku polskim umożliwiający ręczne wskazanie pliku z lokalnego zasobu dyskowego jak również adresu URL do analizy, wraz z możliwością prezentacji wyników tej analizy w zakresie informacji czy badany, plik lub URL jest lub nie jest niebezpieczny. Przy czym interfejs ten musi korzystać z zaoferowanego modułu do analizy próbek malware i być dostępmy dla wszystkich pracowników Zamawiającego
3. Jako funkcjonalność dodatkową: moduł do analizy próbek malware może posiadać funkcjopnalność odtworzenia przebiegu analizy tj. wizulanego śledzenia kolejnych któków analizy na osi czasu np. w postaci filmu, pokazu slajdów, zrzutów ekranu z pulpitu.
4. Jako funkcjonalność dodatkową: System może posiadać funkcjonalność zdalnego wyszukiwania i pobierania dowolnych plików z chronionej stacji roboczej lub serwara na całej zawartości dysków lokalnych
5. Jako funkcjonalność dodatkową System może posiadać funkcjonalność zdalnego uruchamienia zadań wykonywanych przez operatora Systemu poprzez agenta tj. skryptów i poleceń z poziomu konsoli CMD na chronionej stacji roboczej lub serwerze