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

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiotem zamówienia jest dostarczenie i wdrożenie systemu do ochrony stacji końcowych i serwerów Ministerstwa Sprawiedliwości, zwanego dalej „Systemem” zapobiegającego zaawansowanym włamaniom typu malware, ransomware wraz ze Sprzętem niezbędnym do prawidłowego działania Systemu zwanym dalej „Sprzętem” System w formie platformy SaaS służyć ma do ochrony stacji końcowych i serwerów Ministerstwa Sprawiedliwości 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,

**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).

**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. opracowanie projektu wdrożeniowego obejmującego instalację i konfigurację Systemu,
   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,
   3. dostawę licencji wraz wymaganymi plikami instalacyjnymi i konfiguracyjnymi dla wdrażanego rozwiązania umożliwiających obsługę w zakresie ochrony 1600 stacji roboczych i serwerów,
   4. wdrożenie Systemu w oparciu o założenia projektu wdrożeniowego,
   5. wykonanie dokumentacji powykonawczej,
   6. przeprowadzenie transferu wiedzy dla co najmniej 4 pracowników Zamawiającego z zakresu funkcjonowania dostarczonego Systemu i administrowania nim w wymiarze ninimum 40 godzin,
   7. udzielenie gwarancji dla wdrożonego Systemu wraz ze Sprzętem niezbędnym do prawidłowego działania Systemu przez okres 48 miesiecy od dnia podpisnia bez zastrzeżeń przez Zamawiającego Protokołu Odbioru Wdrożenia Systemu.
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.

1. 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,

1. 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.
2. 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:
2. 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,
3. dokumentację testów akceptacyjnych wdrożenia Systemu, która musi dokumentować działania, jakie należy wykonać, aby uzyskać potwierdzenie, że wdrożony System jest zgodny z opisem przedmiotu zamówienia,
4. 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:
5. procedury i instrukcje dotyczące instalacji, konfiguracji i aktualizacji Systemu,
6. procedury dotyczące wykonywania i przechowywania kopii bezpieczeństwa,
7. instrukcje dla użytkowników i administratorów w tym procedury zarządzania zdarzeniami dotyczącymi bezpieczeństwa,
8. inne niezbędne dokumenty, jakie powstaną w trakcie realizacji wdrożenia Systemu, uzgodnione z przedstawicielem Zamawiającego.
9. 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:
   1. zapewnieniu możliwości udziału pracowników Zamawiającego przy przeprowadzanym przez inżyniera/inżynierów wdrożenia Systemu po stronie Wykonawcy,
   2. 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,
   3. 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.
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 hostowana 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 System ochrony stacji roboczej posiadał narzędzia do przeprowadzania analizy powłamaniowej, w tym akwizycji danych i wyszukiwania zidentyfikowanych cech ataku (tzw. wskaźników kompromitacji ang. IoC).
3. Zamawiający wymaga, aby System wykrywał i blokował złośliwy kod exploit (w tym nieznanych wcześniej przypadków) na hostach w oparciu o analizę zachowania kodu a nie na bazie sygnatur i wzorców opisujących wcześniej rozpoznane przypadki exploitów).
4. Zamawiający wymaga, aby System wykrywał i blokował pliki zidentyfikowane jako malware.
5. 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.
6. Niezależnie od możliwości integracji, zamawiający wymaga, aby System posiadał swój własny interfejs zarządzania GUI (dostęp przez przeglądarkę i protokół HTTPS) oraz opcjonalnie dostęp zdalnie poprzez np. SSH.
7. Zamawiający wymaga, aby System analizował co najmniej następujące wskaźniki kompromitacji: zmiany w systemie plików, uruchamiane procesy, zmiany umożliwiające instalację złośliwego oprogramowania w systemie, zmiany procesów systemu operacyjnego, zapytania DNS, zmiany konfiguracji, połączenia sieciowe.
8. Zamawiający wymaga, aby Agent Systemu na stacji roboczej lub serwerze zapewniał możliwość zbierania informacji dotyczących stanu systemu operacyjnego i aktywności hosta w kontekście uruchamianych usług, aplikacji, połączeń, zmian systemowych. Zamawiający wymaga, aby System zapewniał możliwość przeglądu tych zdarzeń i stanu systemu w kontekście wykonywania analizy powłamaniowej i ustalenia wektora ataku.
9. Zamawiający wymaga, aby Log tworzony przez agenta zawierał co najmniej: zmiany w systemie plików, uruchamiane procesy, zmiany w rejestrze Windows służące zagnieżdżeniu się złośliwego oprogramowania w Systemie, zapytania DNS, połączenia sieciowe, historię odwiedzanych adresów web URL.
10. Zamawiający wymaga, aby System zapewniał możliwość izolowania zainfekowanej stacji (blokowania komunikacji sieciowej na żądanie).
11. Proces blokowania komunikacji sieciowej powinien wymagać co najmniej dwustopniowego potwierdzenia: żądanie wdrożenia izolacji stacji oraz zgoda na zablokowanie komunikacji, a takżezapewniać możliwość określenia wyjątków od blokowania komunikacji sieciowej co najmniej na podstawie adresów IP. Wyjątki powinny w szczególności umożliwiać operatorom Systemu przeprowadzenie analizy zainfekowanej stacji z ich komputerów.
12. Powiadomienie w postaci banera, który można personalizować w zakresie komunikatu wyświetlanego przynajmniej w języku angielskim, polskim, czy też możliwość użycia logów firmowego dla zapewnienia czytelności wyświetlanego komunikatu.
13. Zamawiający wymaga, aby System otrzymywał regularne uaktualnienia wskaźników kompromitacji (ang. IoC) opisujące ataki i rodzony ataków od producenta Systemu. Wskaźniki kompromitacji pochodzące od producenta Systemu powinny zapewniać co najmniej wykrywanie ataków typu APT, TPT i malware.
14. Dla agentów (lub ich określonej grupy) powinna istnieć możliwość aktywacji/dezaktywacji silnika antywirusowego/antymalware (AV) będącego integralnym elementem wdrażanego rozwiązania, wykrywającego zagrożenia na podstawie sygnatur dostarczanych regularnie przez producenta.
15. Korzystanie z modułu AV przez agenta opisanego w punkcie powyżej nie może generować dodatkowych opłat licencyjnych dla Zamawiającego.
16. Moduł ochrony AV w dostarczonym oprogramowaniu nie może kolidować z posiadanym przez Zamawiającego System ochrony Systemów końcowych, zwłaszcza z oprogramowaniem bezpieczeństwa standardowo dostępnym w systemie operacyjnym stacji roboczej.
17. Zamawiający wymaga, aby wbudowany moduł AV miał możliwość wykrywania, blokowania i przenoszenia do lokalnej kwarantanny obiektów które zostały wykryte dzięki otrzymywanym sygnaturom.
18. System agenta powinien posiadać mechanizm zabezpieczający, który zapobiegnie nieuprawnionej deinstalacji agenta. Proces lokalnej deinstalacji agenta powinien być poprzedzony wprowadzeniem hasła zabezpieczającego, który umożliwi jego przeprowadzenie.
19. Zamawiający wymaga, aby konfiguracja Systemu pozwalała na określenie wyjątków od działania agentów na stacjach. Co najmniej dla:
    1. funkcjonalności wykrywania i blokowania złośliwego kodu exploit – całkowite wyłączenie funkcji dla grup stacji, wyłączenie funkcji tylko dla określonych aplikacji i folderów, wyłączenie blokowania pozostawiając wykrywanie exploitów.
    2. funkcjonalności silnika AV – całkowite wyłączenie silnika dla określonych grup hostów, wykluczenie ze skanowania wskazanych folderów i plików na stacji.
20. Zamawiający wymaga, aby oferowany systemu zapewniał identyczny poziom ochrony dla stacji znajdujących się w obszarze sieci Zamawiającego jak również poza nią.
21. Zamawiający wymaga, aby System zapewniał operatorowi możliwość zdalnego pobrania dodatkowych danych, jeśli takowe są wymagane do szczegółowej analizy i zrozumienia zakresu ataku.
22. Zamawiający wymaga, aby zadanie akwizycji danych obejmowało aktywne (działające) stacje znajdujące się zarówno w sieci lokalnej Zamawiającego jak i poza nią.
23. Zamawiający wymaga, aby przekazywanie zebranych danych przez agenta do dalszego procesowania i analizy odbywało się w bezpieczny sposób (szyfrowanie danych lub szyfrowane połączenie).
24. Funkcja pobierania danych ze stacji ma pozwalać na akwizycje co najmniej:
    1. poszczególnych plików oraz spisu plików, które są znajdują się na stacji,
    2. standardowych i rozszerzonych informacji o zarejestrowanych przez agenta zmianach Systemowych tj. danych zawierających zestawienie parametryzacji systemu i usług
    3. pamięci (pamięci procesów Systemowych, pamięci sterowników, ale również całkowitej zawartości pamięci operacyjnej),
    4. całkowitej zawartości dysku,
    5. wykonanych komend na stacji z poziomu konsoli CMD.
25. Zamawiający wymaga, aby Agent wspierał co najmniej następujące wersje Systemów operacyjnych: Windows XP SP3, Windows 7/7 SP1, Windows 8/8.1, Windows 10, Windows Server 2008/2012 R2/2016, Mac OSX.
26. 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).
27. Zamawiający wymaga, aby System zapewniał możliwość analizy logów zebranych ze stacji użytkownika w momencie wystąpienia incydentu bezpieczeństwa lub na zebranych na żądanie administratora w zakresie co najmniej:
    1. filtrowania logów pod kątem wybierania danych interesujących dla analityka zajmującego się incydentem,
    2. oznaczania poszczególnych zdarzeń w logu etykietami pozwalającymi na kategoryzację zdarzeń,
    3. wyświetlania zdarzeń z logu tylko z danego okresu czasu,
    4. ukrywania zdarzeń z logu z danego okresu czasu,
28. Zamawiający wymaga, aby System zapewniał możliwość pozyskiwania z systemu operacyjnego chronionego komputera co najmniej następujących danych:
    1. konfiguracji sieciowej (adres IP komputera, adres MAC, adres IP domyślnej bramy, adres IP serwera DHCP, tablice ARP, rekordy DNS, tablice routingu),
    2. informacji o systemie operacyjnym (wersja),
    3. historii stron WWW przeglądanych przez użytkownika,
    4. aktywnych zadań systemowych,
    5. historii pobieranych plików,
    6. kont użytkowników i ich aktywności,
    7. pliki prefetch,
    8. zmodyfikowane klucze rejestru odpowiedzialne za ukrycie malware w systemie na czas restartu komputera,
    9. procesy Systemowe i uruchomione z uprawnieniami użytkownika.
29. Zamawiający wymaga, aby System zapewniał możliwość przeszukania systemu agenta, tzn. istniała możliwość formułowania zapytań dla agentów, mających na celu potwierdzenie obecności potencjalnych zagrożeń lub wskaźników kompromitacji na komputerach użytkowników.
30. Zamawiający wymaga, aby Wyszukiwanie odbywało się zarówno w zakresie logów gromadzonych przez agenta na stacji oraz poza tym co najmniej: sprawdzenie całej powierzchni dysku pod kątem występowania pliku o danej wartości sumy kontrolnej (MD5, SHA256), wyszukanie konkretnego rodzaju zdarzenia zarejestrowanego w Systemowych eventlog.
31. Zamawiający wymaga, aby mechanizm przeszukiwania i odpytywania agentów Systemu wspierał budowanie zapytań w oparciu o co najmniej poniższe parametry wyszukania na stacjach roboczych:
    1. pliki – nazwa, ścieżka, certyfikat, atrybut, podpis, sumy kontrolne MD5/SHA1/SHA256,
    2. rejestr – ścieżka, nazwa, wartość,
    3. proces – nazwa, ścieżka, argument, nazwa procesu nadrzędnego,
    4. usługa Systemowa – nazwa, stan, typ,
    5. zadania Systemowe – nazwa, stan, tryb,
    6. zdarzenia Systemowe – numer (event ID), typ, komunikat,
    7. znaczniki czasu – ostatnie uruchomienie/logowanie, dostęp/modyfikacja/utworzenie,
    8. komunikacja – adres IP, port (zdalny i lokalny), protokół, nazwa DNS,
    9. przeglądarki Web – wersja, nazwa, cookie, adres URL, odnośnik strony pobranego pliku (tzw. HTTP referrer), tytuł strony web, nagłówek http.
32. Zamawiający wymaga, aby Agent był wyposażony w dodatkowy, nie bazujący na sygnaturach lub regułach IoC, mechanizm aktywnej detekcji i blokowania prób wykorzystania podatności (także nieznanych wcześniej) i uruchomienia złośliwego kodu (tzw. exploits). Monitorowane i chronione mają być co najmniej następujące aplikacje:
    1. MS Office: Microsoft Word/Excel/PowerPoint,
    2. Przeglądarki Web: Internet Explorer/Mozilla FireFox/Google Chrome,
    3. Adobe Reader i Flash,
    4. Oracle/Sun Java.
33. Zamawiający wymaga, aby Agent wykrywał i blokował próby wykorzystania makr w plikach do zainicjowania ataku.
34. Zamawiający wymaga, aby System posiadałć możliwość śledzenia i wykrywania nowych procesów na analizowanej stacji roboczej w celu wykrycia procesów powiązanych z działalnością złośliwego oprogramowania.
35. System powinien posiadać możliwość wykrywania prób logowania na inne konta na stacji roboczej (prób eskalacji uprawnień)
36. Dostarczany system ma mieć możliwość monitorowania stanu jego pracy z wykorzystaniem SNMP oraz SYSLOG.
37. Zamawiający wymaga, aby System umożliwiał zarządzanie i komunikację z agentami zainstalowanymi na komputerach użytkowników pracujących w obrębie sieci lokalnej (LAN) Zamawiającego jak i z komputerami użytkowników zdalnych (poza siecią lokalną).
38. Zamawiający wymaga, aby Architektura i logika dostarczanego systemu zapewniała ciągły i identyczny poziom ochrony dla stacji roboczych podłączonych wewnątrz (w obrębie sieci LAN Zamawiającego) oraz poza siecią LAN (w obrębie sieci Internet). Oferowany system ma gwarantować identyczny poziom ochrony dla stacji znajdujących się w obszarze sieci LAN, jak również poza nią – w sieci Internet, np. dla użytkowników zdalnych, pracujących poza siecią Zamawiającego.
39. Zamawiający wymaga, aby w Systemie była zapewniona możliwość integracji z systemami gromadzenia i obróbki zdarzeń (SIEM) na potrzeby wdrożenia automatycznej reakcji na incydent przez operatora SIEM na podstawie danych przesyłanych w co najmniej w formatach: CEF, JSON oraz poprzez email.
40. Zamawiający wymaga, aby System udostępniał interfejs API (w formie otwartego standardu REST Interface) umożliwiający co najmniej: zdalne pobranie wskazanych danych z chronionych hostów, listę alertów wykrytych w ostatnim czasie, przeszukiwanie hostów pod kątem występowania wskaźników kompromitacji (ang. IoC), wdrożenie blokowania komunikacji sieciowej stacji.
41. Zamawiający wymaga, aby Wykonawca w ramch realizacji przedmiotu zamówienia zapewnił kilka poziomów uprawnień dostępu – co najmniej: administrator (pełny dostęp), monitor (dostęp read-only tylko konfiguracji), audytor (dostęp do plików z zapisem zmian konfiguracji w wyniku działań innych użytkowników), analityk/starszy analityk/badacz (zróżnicowany dostęp do wyników analizy i podejmowania akcji odpowiedzi na atak), API (dostęp do interfejsu programistycznego).

**II g. Wymagania w zakresie modułu do analizy próbek Malware**

1. Zamawiający wymaga, aby moduł posiadał wydajność umożliwiającą analizowanie co najmniej 2 tyś. próbek malware dziennie.
2. Zamawiający wymaga, aby wykrywanie ataków (analiza próbek) odbywała się przez dedykowane urządzenie typu appliance dedykowane do instalacji i pracy ciągłej w standardowej szafie przemysłowej typu rack 19” (standard EIA-310), czyli Sprzęt o przeznaczeniu przemysłowym. Zamawiający nie dopuszcza dostarczenia Sprzętu koniecznego do poprawnego funkcjonowania rozwiązania na adaptowanym sprzęcie przeznaczonym do użytku osobistego lub biurowego.
3. Zamawiający wymaga, aby urządzenie było wyposażone w maszyny wirtualne wykonujące równolegle analizę dynamiczną próbek malware (w tym także adresów URL) w różnych wersjach systemu operacyjnego i aplikacji jednocześnie.
4. Wykonawca skonfiguruje i uruchomi wszystkie komponenty oprogramowania na Sprzęcie.
5. Zamawiający wymaga, aby dedykowane urządzenie typu appliance na potrzeby analizy wykorzystywało dedykowane środowisko wirtualne (hypervisor), przy czym:
   1. środowisko, w jakim jest wykonywana analiza dynamiczna, MUSI posiadać mechanizmy utrudniające jego wykrycie przez analizowany malware,
   2. maszyny wirtualne, w których wykonywana jest analiza zachowania ataku MUSZĄ posiadać mechanizmy symulacji realnego użytkownika (w tym co najmniej: ruchy myszą, historię odwiedzanych stron web, pliki cookies).
   3. analiza zachowania i cech ataku MUSI się odbywać z poziomu hypervisora – nie może być wymagane instalowanie dodatkowych procesów/agentów monitorujących wewnątrz maszyn wirtualnych
6. Zamawiający wymaga, aby analiza danych przez urządzenia do ochrony przed atakami w module odbywała się w całkowicie izolowanym na appliance’ach środowisku.
7. Zamawiający wymaga, aby analiza ataku w module odbywała się za pomocą dynamicznej analizy zachowania kodu umożliwiających równoczesną analizę zagrożenia w różnych wersjach systemu operacyjnego i aplikacjach.
8. Zamawiający wymaga, aby funkcjonalność wykrywania malware w plikach, obiektach i adresach URL wskazanych przez użytkownika realizowała statyczną analizę (analizę cech) i dynamiczną analizę (analizę zachowania po uruchomieniu środowisku wirtualnym) podejrzanych obiektów.
9. Zamawiający wymaga, aby analiza dynamiczna (uruchomienie badanej próbki w izolowanym środowisku) wykonywana była z wykorzystaniem różnych wersji systemów operacyjnych Windows (co najmniej: Win XP SP3, Win 7 SP1, Win7 SP1 x64), 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) oraz w systemie MAC OS X i centOS. Wszystkie niezbędne licencje na systemy operacyjne i aplikacje MUSZĄ być dostarczone wraz z proponowanym rozwiązaniem.
10. Zamawiający wymaga, aby urządzenie posiadało wbudowaną możliwość analizy ruchu zarówno dla systemów operacyjnych klasy Windows jak i Mac OS bez konieczności instalacji i posiadania dodatkowych licencji czy komponentów.
11. Zamawiający wymaga, aby moduł miał możliwość wpisania hasła w celu automatycznego odszyfrowania przekazywanej do analizy próbki malware.
12. Zamawiający wymaga, aby moduł miał możliwość podglądu lub nagrania / odtworzenia filmu z przebiegu analizy w środowisku wirtualnym.
13. Zamawiający wymaga, aby moduł posiadał możliwość parametryzacji środowisk wirtualnych na przykład w zakresie: nazwy domeny, folderów użytkowników, ostatnio otwartych plików w celu utrudnienia wykrycia przez analizowany malware.
14. Moduł opcjonalnie powinien posiadać możliwość wskazania zasobu plikowego w celu oddzielenia analizowanych plików w zależności od wyników analizy (brak malware, wykryty malware, ścieżka wejściowa).
15. Zamawiający wymaga, aby moduł umożliwiał analizę malware w jednym z wybranych trybów:
    1. tryb otwarty - detonacja obiektu i możliwość połączenia badanej próbki z dedykowanym łączem internetowym,
    2. sandbox - detonacja obiektu w zamkniętym środowisku
16. Zamawiający wymaga, aby Moduł miał możliwość konfiguracji próbki przesyłanej do analizy w zakresie:
    1. wymuszenia trybu analizy (tryb otwarty lub sandbox),
    2. określenia czasu wykonywanej analizy,
    3. wskazania systemu operacyjnego w którym będzie wykonana analiza (co najmniej Windows XP, 7, 10, MacOS X, linux),
    4. podglądu trwającej analizy,
17. Zamawiający wymaga, aby moduł umożliwiał generowanie raportów zawierających co najmniej statystyki przeanalizowanych próbek.
18. Raporty muszą mieć możliwość eksportu do formatu CSV lub PDF wraz z możliwością ustalenia okresu czasu dla generowanego raportu (co najmniej ostatnie 24 godziny, ostatni 7 dni, ostatnie 30 dni).
19. Zamawiający wymaga, aby moduł miał możliwość integracji przez restAPI celem umożliwienia przesyłania próbek malware przez portal WWW.
20. Zamawiający wymaga, aby moduł miał możliwość zapisu przesłanych malware do wybranych folderów sieciowych.
21. Zamawiający wymaga, aby moduł miał stworzony zgodnie z wymaganiami Zamawiającego dedykowany interfejs użytkownika WWW w języku polskim umożliwiający ręczne wskazanie pliku jak również adresu URL do analizy, wraz z możliwością prezentacji wyników tej analizy co najmniej w zakresie informacji czy badany, plik lub URL jest / nie jest niebezpieczny.
22. Zamawiający wymaga, aby moduł był automatycznie zintegrowany z Systemem ochrony stacji roboczych, to jest posiadać automatyczną możliwość wysyłania próbek (plików/obiektów) do analizy dynamicznej z poziomu konsoli Systemu.

**II h. Wymagania dotyczące Zarządzania rozwiązaniem**

1. Zamawiający wymaga, aby zaoferowany System umożliwiał centralną korelację ataków pomiędzy różnymi wektorami ataków (pomiędzy Modułem analizy próbek, a Systemem ochrony stacji roboczej).
2. Zarządzanie Systemem powinno być oparte na dedykowanej maszynie wirtualnej lub być dostępne jako SaaS.
3. Zamawiający wymaga, aby centralne zarządzanie rozwiązaniem było dostępne dla administratorów niezależnie od ich lokalizacji.
4. Zamawiający wymaga, aby centralny system zarządzania rozwiązaniem umożliwiał automatyczną wymianę wyników analizy ataków między zarządzanymi komponentami, w tym utworzonych automatycznie reguł blokowania wykrytych ataków.
5. System zarządzania powinien zapewniać co najmniej:
   1. zebranie wyników analiz z każdego z podłączonych komponentów rozwiązania i dostępu do nich za pomocą jednego interfejsu GUI,
   2. dostęp do statystyk z działania poszczególnych komponentów,
   3. możliwość tworzenia kopii zapasowych poszczególnych modułów.
6. System zarządzania powinien udostępniać interfejs API (preferowany otwarty standard RESTful Interface lub co najmniej syslog) umożliwiający przekazywanie danych do systemów klasy SIEM,
7. Zarządzanie powinno się odbywać przez interfejs graficzny GUI z przeglądarki Web poprzez HTTPS.

**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:
   1. bieżącym utrzymaniu i zażądaniu Systemem,
   2. 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.