LOTNICZE POGOTOWIE RATUNKOWE

CENTRALA

ul. Księżycowa 5, 01-934 Warszawa, tel. (22) 22-99-931/932, fax. (22) 22-99-933

OPIS PRZEDMIOTU ZAMÓWIENIA

Zakup oprogramowanie agenta ochrony antymalware dla komputerów, serwerów oraz urządzeń mobilnych

Spis treści

1. Słownik i skróty

Dla potrzeb niniejszego opracowania przyjmuję się następujące definicje skrótów i pojęć:

Skrót/pojęcie	Definicja
Dni Robocze	Oznacza każdy dzień tygodnia od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy, w godz. od 8:00 do 15:35.
Oprogramowanie Standardowe	Oznacza oprogramowanie powszechnie dostępne i eksploatowane na dzień złożenia oferty, będące w użytkowaniu Zamawiającego.
Oprogramowanie	Oprogramowanie antywirusowe będące przedmiotem niniejszego postępowania.
Umowa	Umowa zawarta pomiędzy Wykonawcą a Zamawiającym na potrzeby realizacji niniejszego przedmiotu zamówienia.
Usługa Serwisu	Usługa świadczona w ramach gwarancji udzielonej przez Wykonawcę, polegająca na zapewnieniu przez Wykonawcę poprawności i ciągłości prawidłowego działania Oprogramowania oraz jego poszczególnych komponentów.
Użytkownik	Zamawiający oraz jego pracownicy.
Wykonawca/Dostawca	Podmiot realizujący zamówienie.
Zamawiający/LPR	Lotnicze Pogotowie Ratunkowe.

2. Przedmiot zamówienia

Przedmiotem zamówienia jest zakup systemu ochrony infrastruktury LPR:

Oprogramowanie agenta ochrony antymalware dla komputerów, serwerów oraz urządzeń mobilnych:

subskrypcja na okres 3 lat dla 350 agentów. Konsola znajdująca się w chmurze publicznej dla zarządzania systemem ochrony antymalware dla komputerów, serwerów oraz urządzeń mobilnych wraz z niezbędnymi usługami subskrypcyjnymi na okres 3 lat. System sandbox dostępny w chmurze publicznej pozwalający na analizę dynamiczną 200 plików dziennie z usługami subskrypcyjnymi na okres 3 lat.
Dostęp do interfejsu graficznego konsoli zarządzania systemem sandbox dla min. 1 administratora.

1.1. Wymagania dotyczące oprogramowania agenta ochrony stacji końcowej/serwera (350 agentów)

Kod wymagania	Opis wymagań
WOA.01	Agent ochrony stacji roboczej musi obsługiwać następujące systemy operacyjne z pełnym wsparciem producenta: 1) Windows 7; 2) Windows 8 i 8.1; 3) Windows 10; 4) Windows Server 2012; 5) Windows Server 2019; 6) MacOS/OSX 10.11 i późniejsze; 7) Linux Red Hat Enterprise 7.2 i nowsze; 8) Linux CentOS 7.2 i nowsze.
WOA.02	Agent ochrony dla urządzeń mobilnych musi obsługiwać system Android 2.1 i nowsze oraz iOS 11 i nowsze.
WOA.03	Agent ochrony stacji końcowej musi dostarczać następujące narzędzia i funkcje wspierające proces wykrywania oraz eliminacji zdarzeń naruszenia polityki bezpieczeństwa poprzez złośliwe lub niechciane oprogramowanie: 1) „wskaźniki przełamania zabezpieczeń” – poszczególne zdarzenia dotyczące plików oraz pojedyncze zachowania elementów systemu operacyjnego/procesów/aplikacji są korelowane

Kod wymagania	Opis wymagań
	w incydenty i mają nadawane odpowiednie priorytety w celu zwrócenia uwagi administratora systemu na te najważniejsze; 2) „reputacja plików” - zaawansowane metody analizy zbieranych informacji przez agenta o plikach powinny wystarczyć do określenia ich dyspozycji – czy są złośliwe, neutralne czy czyste; 3) „wizualizacja zachowania systemu operacyjnego” – ciągła analiza zachowania monitorowanego systemu operacyjnego pod kątem aktywności na plikach oraz procesów w połączeniach sieciowych dająca możliwość ich wizualizacji w celu szybszego wykrycia przyczyny infekcji złośliwym oprogramowaniem; 4) „elastyczne wyszukiwanie” – proste i nieograniczone wyszukiwanie szczegółowych informacji o wykrytych zdarzeniach pozwalające w szybki sposób: a) zrozumieć formę wykrytego ataku, b) wskazać powiązane ze sobą zdarzenia, c) pomóc w szybki sposób usunąć zagrożenia z monitorowanego środowiska dzięki korelacji wyszukiwania na wielu warstwach zbieranych informacji; 5) „rozpowszechnianie” – funkcja pozwalająca na wyświetlenie wszystkich plików, które zostały uruchomione na wszystkich monitorowanych systemach w danej organizacji i posortowanie ich według ilości wykryć; 6) wsparcie dla sygnatur „OpenIOC” – w celu wykrycia targetowanych ataków administrator bezpieczeństwa ma możliwość wykorzystania mechanizmu OpenIOC. W szczególności mechanizm taki umożliwia wczytanie przygotowanych wcześniej szablonów opisujących nieprawidłowości występujące w skompromitowanych hostach i daje możliwość uruchomienia skanowania na żądanie – tzn. przeszukanie wszystkich monitorowanych stacji roboczych pod kątem tych nieprawidłowości. Funkcja ta pozwala na import ogólnie dostępnych szablonów OpenIOC, jak również posiada narzędzie edytora ułatwiającego pisanie własnych szablonów; 7) „spis podatności”, który pokazuje listę podatnego oprogramowania wykrytego na monitorowanych stacjach końcowych i serwerach oraz sortuje wyświetlane informacje według poziomu zagrożenia, jakie te podatności ze sobą niosą. Narzędzie wspiera administratora w eliminowaniu – możliwie najszybciej - z monitorowanych systemów operacyjnych znanych podatności typowo wykorzystywanych przez malware; 8) „kontrola rozpowszechniania infekcji” – funkcja pozwalająca uzyskać kontrolę nad podejrzanymi plikami i zatrzymać ich rozpowszechnianie się bez zwłoki związanej z zebraniem większej ilości dokładniejszych informacji. Funkcja ta umożliwia: a) zablokowanie konkretnego pliku/aplikacji rezydującej na wskazanych lub wszystkich monitorowanych systemach operacyjnych, b) opisanie zaawansowaną sygnaturą pliku, którego część zmienia się wraz z mutującym polimorficznym kodem i jego blokowanie bez względu na jego aktualną formę, c) blokowanie niechcianych aplikacji – w szczególności lista niechcianych aplikacji umożliwia wymuszenie polityki bezpieczeństwa blokującej zainfekowane aplikacje, będące „bramą” dla malware i zatrzymuje proces nawracającej się infekcji, d) zdefiniowanie listy niezbędnych aplikacji – w szczególności pozwala na określenie listy dopuszczonych aplikacji i zezwala na ich funkcjonowanie bez względu na poziom zagrożenia jaki ze sobą wnoszą, jeśli istnieje taka potrzeba lub wymaga tego biznes, e) blokowanie komunikacji zwrotnej złośliwego oprogramowanie C&C, w szczególności w przypadku komputerów znajdujących się poza siecią korporacyjną poprzez wykorzystanie reputacji adresów IP, przy czym baza reputacyjna utrzymywana będzie przez dostawcę rozwiązania.

Kod wymagania	Opis wymagań
WOA.04	Agent musi mieć możliwość uruchomienia jako proces, bez własnego interfejsu graficznego widocznego dla użytkownika.
WOA.05	Agent musi mieć możliwość uruchomienia silnika antywirusowego skanującego dysk twardy i pamięć za pomocą tradycyjnych sygnatur antywirusowych. Silnik ten jest uruchamiany opcjonalnie i może być uruchomiony tylko dla wskazanej grupy stacji końcowych.
WOA.06	Agent musi mieć możliwość pracy równocześnie z innymi systemami antywirusowymi poprzez zdefiniowanie wyjątków od skanowania. Definicja tych wyjątków jest możliwa na dwa sposoby: 1) Wybór wyjątków z gotowej listy przygotowanej przez producenta rozwiązania dla wykorzystywanego równocześnie systemu antywirusowego; 2) Możliwość zdefiniowania własnych wyjątków zawierających: a) Ścieżkę do konkretnego katalogu/folderu, b) Wskazanie konkretnego pliku wykonywalnego poprzez podanie ścieżki lub zdefiniowanie jego sumy kontrolnej SHA, c) Zdefiniowanie rozszerzeń plików.
WOA.07	Agent musi być wyposażony w mechanizm zabezpieczający przed atakami typu „exploit”. Ochrona polega na przydzieleniu nowego obszaru pamięci dla aplikacji poprzez inny mechanizm niż standardowy algorytm przydziału pamięci przez systemy operacyjne. Operacja ta jest niewidoczna dla użytkownika.
WOA.08	Agent musi być wyposażony w zaawansowany mechanizm zabezpieczenia krytycznych procesów systemów Windows przed wstrzyknięciem złośliwego kodu przez inne procesy.
WOA.09	Agent musi być wyposażony w mechanizm zaawansowanego wykrywania ataków typu Ransomware, polegający na monitorowaniu zachowania się uruchomionych programów i operacji w przestrzeni dyskowej a także blokowaniu w przypadku nieprawidłowego ich zachowania.
WOA.10	Agent musi być wyposażony w mechanizm izolacji stacji końcowej, polegający na zablokowaniu całego ruchu z tej stacji i do niej za wyjątkiem ruchu kontrolnego systemu antymalware – tzw. izolacja hosta.

1.2. Wymagania dotyczące konsoli zarządzającej systemem ochrony antymalware znajdującej się w chmurze publicznej – podstawowe funkcjonalności

Kod wymagania	Opis wymagań
WKZ.01	Konsola powinna procesować informacje o plikach, które przychodzą od podłączonych innych elementów ochrony antymalware, w tym agenci ochrony stacji roboczych.
WKZ.02	Konsola musi wspierać następujące systemy operacyjne stacji roboczych oraz serwerów: 1) Windows; 2) Linux; 3) MacOS; 4) Android; 5) iOS.
WKZ.03	Konsola musi zapewniać narzędzia szybkiej reakcji na zdarzenia - co najmniej w postaci możliwości zweryfikowania reputacji danego pliku, jeśli był on już wcześniej widziany w sieci, i określenie jego statusu w trzech stanach (czysty, neutralny, złośliwy). Konsola zapewnia współdzielenie informacji o plikach z globalnym centrum (Threat Intelligence) w sposób zanonimizowany np. poprzez sumy kontrolne (SHA-256) lub inne rozwiązanie oferowane przez producenta.
WKZ.04	Konsola musi umożliwiać zdefiniowanie własnego zbioru typu Whitelist oraz Blacklist dla plików przez następujące mechanizmy: 1) Zdefiniowanie pojedynczej sygnatury pliku; 2) Import pliku tekstowego z wieloma sygnaturami plików; 3) Automatyczne wygenerowanie sygnatury pliku poprzez upload pliku do konsoli.
WKZ.05	Konsola musi wykorzystywać mechanizmy uczenia maszynowego celem oceny pliku wykonywalnego i próby ustalenia jego dyspozycji (malware lub czysty) na podstawie analizy jego metadanych takich jak nagłówek, odnośniki do bibliotek DLL, atrybuty COFF.
WKZ.06	Konsola musi wykorzystywać mechanizmy porównywania i grupowania sygnatur plików, pozwalający na blokowanie całej rodziny malware'u i pomagający wykrywać warianty malware'u polimorficznego.
WKZ.07	Konsola musi umożliwiać zdefiniowanie zbiorów adresów IP typu Blacklist w celu uniemożliwienia komputerom komunikacji z tymi adresami.
WKZ.08	Konsola musi zapewniać możliwość automatycznej propagacji do systemów ochrony antymalware informacji o widzianych plikach oraz ich statusie celem ich blokowania.
WKZ.09	Konsola musi zapewniać automatyczne i niezwłoczne przesyłanie do systemów ochrony informacji o plikach, które podczas początkowej analizy otrzymały status „czysty" lub „neutralny", a których status został obniżony do statusu „złośliwy" – tzw. blokowanie wsteczne.
WKZ.10	Konsola musi zapewniać własny interfejs graficzny do analizy zdarzeń i dokonywania zmian konfiguracji polityk bezpieczeństwa.
WKZ.11	Wymagana jest możliwość podłączenia do konsoli co najmniej 350 konektorów (agentów) na stacjach roboczych.
WKZ.12	Dostęp do zaawansowanych ustawień konsoli ma mieć możliwość zabezpieczenia poprzez mechanizm uwierzytelnienia dwuskładnikowego (ang. Multi-Factor Authentication - MFA).
WKZ.13	Konsola musi umożliwiać podział zarządzanych stacji roboczych na grupy, którym przypisuje się ich własną politykę. Do każdej takiej grupy istnieje możliwość przypisania innych administratorów. Administratorzy mogą zarządzać polityką komputerów i mają wgląd w zdarzenia tylko w ramach swojej grupy.
WKZ.14	Konsola musi być wyposażona w moduł obrazujący poprzez różne kolory ilość infekcji w różnych grupach hostów.
WKZ.15	Konsola musi zawierać zestaw danych demonstracyjnych, którymi są przykładowe ataki (WannaCry, przechwytywanie wiersza poleceń) wraz z instrukcjami, dzięki którym administrator może zobaczyć w jaki sposób skutecznie odczytywać zdarzenia.
WKZ.16	Konsola musi pozwalać na zdefiniowanie polityki dla agentów w taki sposób, aby mogły działać na stacji roboczej razem z innym oprogramowaniem antywirusowym lub antymalware'owym omijając skanowanie ich katalogów. System zawiera wbudowane zestawy wykluczeń oraz zezwala na konfigurację tych wykluczeń przez administratora.
WKZ.17	System musi zezwalać na pełną konfigurację polityki w trybie monitorowania, tak by wszystkie mechanizmy działały i były generowane zdarzenia w konsoli zarządzania oraz monity informacyjne

Kod wymagania	Opis wymagań
	na stacji użytkownika, natomiast działania niepożądane nie są blokowane. Włączenie trybu blokowania odbywa się przez zmianę jednego parametru w polityce agenta.
WKZ.18	Konsola musi posiadać narzędzie do szybkiej identyfikacji aplikacji, które najczęściej są wykorzystywane przez złośliwe oprogramowanie w danej sieci do osadzenia się na komputerach lub do uzyskania do komputerów dostępu. Dane przedstawiane są administratorowi w następujący sposób: 1) w formie wykresu z procentowym podziałem wykorzystania aplikacji; 2) na osi czasu pokazującej ilość zagrożeń wprowadzonych przez daną aplikację w danym czasie.
WKZ.19	Konsola współpracuje z systemem sandbox w następującym zakresie: 1) zezwolenia na ręcznie przesyłanie plików do analizy przez system sandbox i odczytanie wyników analizy bez potrzeby logowania się do systemu sandbox; 2) umożliwienia odczytu wyników analizy próbki przez system sandbox bez konieczności logowania się do systemu sandbox w następującym zakresie: a) Nazwy pliku oraz jego sumy kontrolne (SHA-256, SHA-1 oraz MD5), b) Typu pliku wykryty na podstawie tzw. „file magic numer”, c) Znaczników czasu rozpoczęcia procesu detonacji i jego zakończenia, d) Odczytu wskaźników detekcji behawioralnej ze szczegółami, e) Odczytu żądań i odpowiedzi HTTP, zapytań DNS oraz nawiązywanych sesji TCP/IP, f) Odczytu uruchamianych procesów, artefaktów, zmian w rejestrach, g) Odczytu operacji na plikach (tworzenie, odczyt, modyfikacja, usunięcie pliku), h) Możliwości pobrania całego badanego pliku, i) Możliwości pobrania badanego pliku w postaci PCAP, j) Możliwości pobrania wszystkich plików wygenerowanych przez badaną próbkę; 3) otrzymywania następujących szczegółowych informacji z analizy behawioralnej: a) nazwy wskaźnika, b) opisu, c) kategorii, d) znaczników (tagów), e) poziomu zagrożenia związanego z tym wskaźnikiem, f) pewności detekcji, g) listę URL znalezionych w dokumentach, h) informacji na temat artefaktów, ścieżek do plików, domen, z którymi program się komunikuje; 4) umożliwienia pobrania nagrania ekranu wideo z procesu detonacji plików w celu sprawdzenia aktywności pulpitu.

1.3. Wymagania dotyczące systemu sandbox dostępnego w chmurze publicznej

Kod wymagania	Opis wymagań
WSC 01	System musi zapewniać przetwarzanie 200 próbek na dobę z możliwością rozszerzenia za pomocą licencji
WSC 02	Środowisko sandbox w proponowanym rozwiązaniu nie może opierać się na mechanizmach emulacji systemów operacyjnych oraz aplikacji, ale na niestandardowym silniku wirtualizacji w celu utrudnienia możliwości jego wykrycia przez złośliwe oprogramowanie.
WSC 03	Maszyny wirtualne z obrazami systemu operacyjnego nie mogą mieć żadnych mechanizmów analitycznych wewnątrz maszyn wirtualnych, aby wykrywanie prób analiz przez złośliwe oprogramowanie było trudniejsze. Wszystkie analizy są przeprowadzane poza maszynami wirtualnymi.
WSC 04	Rozwiązanie musi wspierać następujące systemy operacyjne: Windows 7 - 64-bitowy, Windows 10 - 64 bitowy.
WSC 05	Obraz systemu operacyjnego maszyny wirtualnej nie może być najbardziej aktualny zawierający wszystkie patche. Instalowana jest jedna z najbardziej podatnych na zagrożenia wersji.
WSC 06	Dostępna jest lista zainstalowanych pakietów oprogramowania na każdej z dostępnych maszyn wirtualnych. Lista zawiera co najmniej całkowitą liczbę programów, ich nazwy i konkretne wersje. Zainstalowane zestawy programów są uniwersalne a ich dobór jest przeprowadzany przez producenta rozwiązania na podstawie analiz aktualnych standardów oprogramowania widzianych w środowiskach produkcyjnych.
WSC 07	Analiza dynamiczna konkretnego pliku w systemie sandbox musi polegać na uruchomieniu dedykowanej maszyny wirtualnej dla tego pliku. Wszelkie szczegółowe wyniki analizy dotyczą tylko tego badanego pliku oraz wszystkich jego pochodnych (innych plików wygenerowanych przez badany plik).
WSC 08	System musi obsługiwać min. następujące typy plików: 1) .DLL – biblioteki (PE32 i PE32+); 2) .EXE – plik wykonywalny PE32; 3) .JS – JavaScript; 4) .JSE - encoded JavaScripts; 5) Pliki MSOffice – (w tym .DOC, .DOCX, .MSG, .RTF, .XLS, .XLSX, .PPT, .PPTX); 6) .PDF - Portable Document Format (razem z skryptami Java); 7) .PS1 - Powershell; 8) .VBS - Visual Basic Script ; 9) .ZIP – skompresowane archiwa oraz pliki tzw. kwarantanny; 10) .BAT – Batch; 11) .BZ2 – skompresowany bzip2; 12) .CHM – skompilowany plik pomocy - Microsoft Compiled HTML Help; 13) .EML - Wiadomości email zapisane w postaci pliku; 14) .GZ – skompresowany gzip; 15) .HTA – aplikacja HTML; 16) .ISO - obraz ISO; 17) .JAR – archiwum Java; 18) .LNK - Windows shortcut; 19) .MSI - Microsoft Installer; 20) .MHTML - Mime HTML; 21) .SEP - Tagged Image File Format; 22) .SLK - Microsoft Symbolic Link (SYLK); 23) .SWF - Flash Files; 24) .TAR – tar; 25) Podawanie URL i do obiektów znajdujących się na Internecie; 26) .VBE - Encoded Visual; 27) .VBN - Virus Bin; 28) .WSF - Windows Script File; 29) .XML - XML Based Office Document Types (.DOCX, .XLSX, .PPTX) oraz Extensible Markup Language (.XML); 30) .XPS – XML Paper Specification; 31) .XZ – skompresowane archiwum.

Kod wymagania	Opis wymagań
WSC 09	Rozwiązanie sandboxingu musi być w stanie zidentyfikować pliki i powiązać wyniki analizy przeszukując bazę danych zawierającą wyniki poprzednich analiz innych próbek oraz globalne informacje o zagrożeniach dostarczone przez producenta rozwiązania. Poszukiwanymi elementami są: 1) adresy IP wykorzystywane w komunikacji podczas detonacji; 2) domeny wykorzystywane w komunikacji podczas detonacji; 3) adresy URL wykorzystywane w komunikacji podczas detonacji; 4) wskazania behawioralne; 5) ścieżka; 6) nazwa pliku; 7) suma kontrolna: SHA256, SHA1, MD5; 8) unikalny identyfikator przypisany podczas przesyłania plików do urządzenia sandboxingu; 9) tagi; 10) mutex; 11) artefakty pobrane podczas analizy; 12) rejestrowanie zdarzeń związanych z analizą plików.
WSC 10	System sandbox analizując całą aktywność pliku musi porównywać każde pojedyncze jego zachowanie do swoich wbudowanych wskaźników zainfekowania systemu operacyjnego (Indication of Compromise). Każdy z tych wskaźników opisany jest poziomem zagrożenia zawierającym się w liczbie od 1 do 100. Poziom zagrożenia wyrażony jest dodatkowo czterema flagami: niski, średni, wysoki, krytyczny.
WSC 11	Ogólny wynik całej analizy musi zawierać się w jednej liczbie w zakresie od 1 do 100 reprezentującej ogólny poziom zagrożenia związanego z określonym plikiem, który liczony jest na podstawie algorytmu, który bazuje na takich zmiennych jak liczba i rodzaj wskaźników zainfekowania systemu operacyjnego oraz ich indywidualnych wartości poziomu zagrożenia i pewności detekcji.
WSC 12	Liczba wskaźników zainfekowania systemu operacyjnego bazujących na elementach kodu jak i analizie zachowań musi wynosić ponad 1600.

1.4. Wymagania dotyczące systemu sandbox dostępnego w chmurze publicznej – dostęp do interfejsu graficznego

Kod wymagania	Opis wymagań
WSG.01	System musi zapewniać możliwość ręcznego przesyłania pliku do analizy przez zalogowanego użytkownika systemu. Podczas tego procesu powinny istnieć następujące możliwości wyboru systemu operacyjnego maszyny wirtualnej: 1) użytkownik wybiera żądany system operacyjny; 2) system sandbox sam decyduje, który system operacyjny będzie najbardziej adekwatny na podstawie analizy właściwości pliku.
WSG.02	Podczas ręcznego przesyłania pliku do analizy użytkownik musi mieć możliwość wskazania następujących automatycznych akcji, które system operacyjny na VM będzie podejmował podczas badania pliku: 1) Zamykanie uruchomionych plików lub programów; 2) Wywołanie trzech programów i symulowanie przełączania się między oknami tych programów w celu wyzwolenia działania malware'u, który do aktywacji potrzebuje zmian aktywności okien aplikacji; 3) Identyfikacja obiektów osadzonych w dokumentach MS Word i zasymulowanie ich podwójnego kliknięcia przez użytkownika, łącznie z akceptacją okien dialogowych, które mogą się pojawić po otwarciu osadzonego obiektu (zabezpieczenie przed próbą ominięcia przez malware systemów automatycznej analizy plików poprzez zastosowanie osadzonych obiektów); 4) Wyszukiwanie na ekranie obrazów wymagających interakcji użytkownika (okna dialogowe, przyciski, itp.) i klikanie w nie w celu uruchomienia aktywności oraz klikanie lewym i prawym klawiszem myszy w trakcie losowego ruchu kursora po pulpicie; 5) Uruchomienie przeglądarki Internet Explorer i wywołanie rzeczywistej strony www dostępnej przez sieć Internet.
WSG.03	System musi umożliwiać użytkownikowi ręczne przesłanie pliku do analizy tak, by plik ten i wynik jego analizy były widoczne tylko dla tego użytkownika i były niewidoczne dla pozostałych użytkowników systemu sandbox z tej samej organizacji.
WSG.04	Rozwiązanie podczas analizy wyników złośliwego oprogramowania musi dawać możliwość przeszukiwania pobranych artefaktów. Dostępne opcje wyszukiwania to: 1) rodzaj pliku rozpoznany po tzw. „file magic number" a nie tylko rozszerzeniu; 2) ścieżka do pliku; 3) źródło pochodzenia pliku; 4) sygnatura AV; 5) rozmiar pliku.
WSG.05	Raport z analizy pliku musi zawierać następujące dane: 1) nazwa pliku; 2) jego sumy kontrolne (SHA-256, SHA-1 oraz MD5); 3) typ pliku wykryty przy wykorzystaniu tzw. „file magic number"; 4) znaczniki czasu procesu detonacji i jej zakończenia; 5) szczegółowy raport z aktywowanych wskaźników szkodliwego zachowania; 6) szczegółowy raport z zachowania ruchu sieciowego podczas detonacji – odpowiedzi http; 7) zapytania DNS oraz nawiązywanych sesji TCP/IP; 8) zestawienie aktywowanych procesów systemu operacyjnego oraz możliwość wizualizacji wszystkich procesów i odzwierciedlania ich wzajemnych relacji, a także zaznaczania ich działalności; 9) lista użytych dodatkowych artefaktów (plików), których nie było w oryginalnej maszynie wirtualnej a powstały podczas detonacji; 10) aktywności w rejestrach systemowych; 11) aktywności systemu plików.
WSG.06	System musi pozwalać na interakcję za pomocą klawiatury i myszy w system operacyjny VM analizujący plik.
WSG.07	System umożliwia wybór czasu detonacji próbek w zakresie od 5 do 30 minut

Kod wymagania	Opis wymagań
WSG.08	Każdy raport zawiera link do pobrania: oryginalnej próbki pliku, plików powstałych w procesie detonacji, raportu w formacie html, szczegółowej analizy w formacie json, przechwytywanych pakietów ruchu sieciowego w formacie pcap oraz harmonogram aktywności procesów.
WSG.09	System umożliwia ponowne przesłanie pliku, który jest już obecny w systemie w celu próby ujawnienia nowych informacje o złośliwym kodzie i jego zachowaniu.
WSG.10	Wszystkie informacje dotyczące analizy zagrożeń są dostępne i przeszukiwalne we wszystkich raportach z dostępnych analiz. System musi umożliwiać przeszukiwanie danych o zagrożeniach za pomocą następujących elementów: 1) artefakty; 2) domeny; 3) adresy IP; 4) ścieżki; 5) klucze rejestru; 6) adresy URL; 7) wskaźniki zagrożeń (Indication of Compromise).
WSG.11	Wszystkie wskaźniki zainfekowania systemu operacyjnego są opisane w taki sposób, aby obejmowały następujące informacje: 1) nazwa wskaźnika; 2) opis; 3) kategoria; 4) znaczniki (tagi); 5) poziom zagrożenia związany z tym wskaźnikiem; 6) pewność detekcji; 7) listę URL znalezionych w dokumentach; 8) informacje na temat artefaktów, ścieżek do plików, domen, z którymi program się komunikuje.
WSG.12	Każdy mechanizm opisujący szkodliwe zachowanie lub typową dla szkodliwego kodu charakterystykę struktur w danym pliku opisany w kilku zdaniach tak, aby w łatwy i przyjazny sposób można było zrozumieć na czym polega dane zagrożenie. Dodatkowo każde wykrycie powinno zawierać fragmenty pliku lub kodu, które by potwierdzały wykorzystanie danego mechanizmu w analizowanej próbce.
WSG.13	System musi umożliwiać pobranie nagrania ekranu wideo z procesu detonacji plików w celu sprawdzenia aktywności pulpitu.
WSG.14	Oferowane rozwiązanie musi pozwalać na różne opcje integracji z rozwiązaniami firm trzecich (bram sieciowych, serwerów proxy, systemy SIEM, itp.) na wielu poziomach dostępu do informacji poprzez moduły API: 1) możliwość przesyłania plików; 2) udostępnianie informacji o zagrożeniach przychodzących w formie subskrypcji (feeds); 3) dostarczanie raportów z analizy pliku.

3. Wymagania dodatkowe.

Wykonawca musi zapewnić Zamawiającemu możliwość odnowienia subskrypcji oraz wsparcia technicznego na opisane produkty, po wygaśnięciu zawartej umowy, bez konieczności uiszczania dodatkowych opłat wznowieniowych, z wyjątkiem sytuacji, kiedy producent w okresie trwania usługi zakończy świadczenie usług wsparcia technicznego dla licencji, będących przedmiotem zamówienia.

4. Świadczenie serwisu gwarancyjnego i gwarancji.

Kod wymagania	Opis funkcjonalności
WUS.01	Na dostarczone oprogramowanie wykonawca zapewni serwis gwarancyjny liczony od daty podpisania protokołu odbioru produktu na okres 36 miesięcy opartego na świadczeniach serwisowych producenta.
WUS.02	Usługa wsparcia technicznego dla zakupionego produktu musi być realizowana w trybie 24 godzin na dobę, 7 dni w tygodniu, 365 dni w roku.
WUS.03	Wykonawca w ramach realizacji Umowy zapewni Zamawiającemu przez okres minimum 36 miesięcy od podpisania protokołu odbioru produktu: 1) prawo do pobierania nowych wersji i aktualizacji; 2) możliwość aktualizacji oprogramowania poprzez dostęp do zasobów producenta rozwiązania; 3) dostęp do pomocy technicznej producenta; 4) nieograniczona ilość zgłoszeń serwisowych; 5) dostęp do materiałów producenta takich jak: techniczna dokumentacja, internetowa baza wiedzy, forum internetowe producenta oprogramowania/urządzeń; 6) dostęp do poprawek i uaktualnień oprogramowania objętego usługą wsparcia oraz nowych wersji; 7) dostęp do portalu www producenta oprogramowania umożliwiającego zarządzanie posiadanymi licencjami, podniesienie lub obniżenie (jeśli producent oficjalnie wspiera poprzednie wersje) wersji oprogramowania; 8) dostęp do rejestru licencji (dostępnego przez portal www producenta oprogramowania/urządzeń).
WUS.04	Do kontaktów/zgłoszeń Wykonawca udostępnia: 1) numer telefonu – _____ (infolinia bezpłatna), _____ (dla telefonów komórkowych i z zagranicy); 2) e-mail - _____. Do kontaktów/zgłoszeń Zamawiający udostępnia: 1) numer telefonu – _____; 2) e-mail - _____.
WUS.05	Przyjęcie do realizacji zgłoszenia powinno zostać niezwłocznie potwierdzone przez Wykonawcę, zwrotnie na adres e-mail zgłaszającego.
WUS.06	Za moment zgłoszenia przyjmuje się datę i godzinę zarejestrowania przez system elektroniczny Wykonawcy, w szczególności odebrania przesyłki e-mail przez system pocztowy lub zarejestrowanie zdarzenia przez Zamawiającego w udostępnionym przez Wykonawcę systemie zgłoszeniowym. W przypadku zgłoszenia telefonicznego moment zgłoszenia zostanie ustalony z Zamawiającym w trakcie tego zgłoszenia i potwierdzony w e-mailu, o którym mowa w wymaganiu WUS.04.
WUS.07	W przypadku zdiagnozowania błędów w używanej przez Zamawiającego wersji oprogramowania, Wykonawca zapewni Zamawiającemu dostęp do najnowszych wersji oprogramowania urządzeń posiadających wsparcie producenta, pozwalających na usuniecie tych błędów. W przypadku wykrycia błędu, dla którego brak jest w danym momencie odpowiedniej aktualizacji, Wykonawca dokona eskalacji zgłoszenia do producenta. Wykonawca zapewnia i zobowiązuje się, że zgodnie z niniejszą specyfikacją korzystanie przez Zamawiającego z oprogramowania w ramach wsparcia technicznego nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich.
WUS.08	Z tytułu świadczenia przez Wykonawcę usługi serwisu gwarancyjnego Zamawiający nie ponosi dodatkowych kosztów.

WUS.09	Dla oprogramowania obowiązują prawa gwarancyjne producenta.
WUS.10	Stosowanie praw wynikających z udzielonej gwarancji nie wyłącza stosowania uprawnień Zamawiającego wynikających z rękojmi za wady.

5. Zasady odbioru przedmiotu zamówienia

I.Zasady Ogólne

1. Przedmiot Umowy należy dostarczyć zgodnie z zasadami i terminami wskazanymi w Umowie.
2. Odbiór zostanie przeprowadzony w biurze Zamawiającego przy ul. Księżycowej 5, w Warszawie, w obecności przedstawicieli Wykonawcy i Zamawiającego w godz. 8:00 – 15:35 lub w formie elektronicznej na wskazany przez Zamawiającego w Umowie adres e-mail.
3. Przedmiot Umowy podlegać będzie odbiorowi ilościowo - jakościowemu.
4. Odbiór zostanie potwierdzony podpisaniem przez przedstawicieli Zamawiającego i Wykonawcy protokołu ilościowo-jakościowego, którego wzór stanowi załącznik nr 3 do Umowy.

II.Odbiór ilościowo – jakościowy

1. Celem czynności kontrolnych prowadzonych w ramach odbioru ilościowo – jakościowego jest sprawdzenie kompletności dostarczonego przedmiotu Umowy i potwierdzenie zgodności z ilością określoną w Umowie oraz sprawdzenie wszystkich wymagań funkcjonalnych i potwierdzenie zgodności ze szczegółowym opisem przedmiotu Umowy.
2. Wykonawca będzie odpowiedzialny za dostarczenie i zaprezentowanie dostarczonego przedmiotu Umowy.
3. Podstawą dokonania odbioru ilościowo – jakościowego jest przeprowadzenie z pozytywnym skutkiem sprawdzeń kompletności oraz poprawności działania Oprogramowania dostarczonego w ramach Umowy wraz z wymaganymi licencjami.
4. Pozytywny wynik odbioru ilościowo – jakościowego zostanie potwierdzony podpisaniem protokołu odbioru ilościowo – jakościowego.