Załącznik nr 1 do Umowy _____/DI/_____2610

Specyfikacja Analizatora plików

WYMAGANIA DOTYCZĄCE ANALIZATORA PLIKÓW

Wymagania:

1) Analizator plikowy musi umożliwiać analizę repozytoriów plikowych w celu znalezienia złośliwego oprogramowania (typu malware, exploit, itp).
2) Wykrywanie ataków musi odbywać się przez dedykowane fizyczne urządzenie przeznaczone do instalacji w szafie RACK 19".
3) Analizator plikowy musi posiadać co najmniej 4 interfejsy miedziane 1Gb/s.
4) Analizator musi posiadać minimum dwa redundantne zasilacze i co najmniej dwa dyski redundantne pracujące w RAID.
5) Analizator musi posiadać wydajność umożliwiającą skanowanie co najmniej 60 000 analiz unikalnych obiektów dziennie wykazanych w specyfikacji Producenta.
6) Analizator plikowy musi umożliwiać wykonanie analizy dynamicznej (sandbox) w równoległym środowisku (uruchamianym jednocześnie) maszyn wirtualnych.
7) Analizator musi działać w oparciu o dedykowane platformy sprzętowe (urządzenia fizyczne) dostarczane przez Producenta rozwiązania z systemem operacyjnym utwardzonym (hardening) przez Producenta.
8) Analizator musi umożliwiać skanowanie udziałów plikowych: ciągłe, zaplanowane i na żądanie oraz poddawać kwarantannie złośliwe oprogramowanie odnalezione na zasobach plikowych
9) Analizator plikowy musi umożliwiać tworzenie niezależnych skanowań (zadań skanowania) dla podłączonych repozytoriów plikowych (zasobów plikowych).
10) Analizator musi umożliwiać skanowanię i filtrowanie tylko wskazanych typów plików do skanowania.
11) Analizator musi umożliwiać zatrzymanie i wznawianie skanowania.
12) Analizator musi umożliwiać przenoszenie niezłośliwych plików do wskazanego zasobu, a złośliwych plików do oddzielnego zasobu kwarantanny.
13) Analizator musi umożliwiać przywrócenie pliku do jego pierwotnej lokalizacji po zwolnieniu go z kwarantanny.
14) Analizator musi umożliwiać dostarczenie raportu analitycznego z informacjami o zachowaniu pliku - zaangażowanych procesach, dostępie do plików / zapisie na dysku, zmianach w rejestrze.
15) Analizator musi umożliwiać filtrowanie zadania skanowania na podstawie typu pliku oraz daty modyfikacji.
16) Analizator musi posiadać oprócz silnika analizy dynamicznej, silnik analizy statycznej.
17) Analizator musi umożliwiać analizę plików do 1024 MB. Maksymalny rozmiar plików, które będą skanowane, musi być konfigurowalny.
18) Analizator musi umożliwiać analizowanie plików .eml (wiadomości email zapisane do pliku)
19) Analizator musi obsługiwać natywną integrację z Microsoft SharePoint w trybie online **lub z wykorzystaniem API (uwierzytelnianie i autoryzacja),** aby zapewnić bezpieczne udostępnianie plików.
20) Analizator musi umożliwiać skanowanie i ochronę dla następujących typów repozytoriów plikowych: CIFS, NFS, WebDAV, Secure WebDAV.
21) Analizator musi umożliwiać analizę malware w formatach co najmniej:, JAVA, PDF, MS Office documents, common multimedia contents such as JPEG, QuickTime, MP3 and ZIP/RAR/7ZIP/TNEF archives, 3gp, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm.
22) Funkcjonalność analizy obiektów musi realizować statyczną analizę (analizę cech) i dynamiczną analizę (analizę zachowania po uruchomieniu środowisku wirtualnym) podejrzanych obiektów zebranych z analizowanego ruchu.
23) Analizator musi na potrzeby analizy dynamicznej wykorzystywać środowisko wirtualne (hypervisor), przy czym:
    a) środowisko, w jakim jest wykonywana analiza dynamiczna, musi posiadać mechanizmy utrudniające jego wykrycie przez analizowany malware,
    b) 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).
24) Analizator musi umożliwiać konfigurację środowisk wirtualnych co najmniej w zakresie: nazwy domeny, nazwy użytkownika, folderów użytkowników, ostatnio otwartych plików, historii przeglądania stron www w przeglądarce internetowej oraz kont FTP, Outlook i Skype w celu utrudnienia wykrycia przez analizowany malware.
25) Analiza zachowania i cech ataku musi się odbywać z poziomu hypervisora – nie może być wymagane instalowanie dodatkowych procesów/agentów monitorujących wewnątrz maszyn wirtualnych.

26) Maszyny wirtualne z różnymi systemami operacyjnymi i aplikacjami muszą być dostarczone wraz z urządzeniami i okresowo aktualizowane przez producenta i nie mogą wymagać dodatkowych licencji wymaganych do konfiguracji po stronie Zamawiającego.
27) Sposób działania maszyn wirtualnych musi umożliwiać wykonanie analizy zachowania obiektów PDF, Java, MS Office z użyciem kilku wersji tych aplikacji bez uruchamiania dodatkowych maszyn wirtualnych.
28) Analiza ataku musi umożliwiać wykrywanie zagrożeń typu kernel rootkit, code injection, DLL injection.
29) W wyniku analizy Analizator musi umożliwiać dostęp do szczegółowych danych analitycznych (forensic data) z przeprowadzonej analizy. Wśród tych danych muszą się znaleźć co najmniej: adresy URL jeśli są związane z analizowanym malware, funkcje skrótu (hash) MD5 oraz wykryty plik malware.
30) Analizator musi być zoptymalizowany pod kątem minimalizacji ilości przypadków false-positive (błędne wykrycie zagrożenia w poprawnym ruchu).
31) Analizator musi umożliwiać wykrywanie wszystkich faz zaawansowanych ataków: exploit, dropper/malware, callback oraz lateral movement.
32) Analizator wykonując analizę zagrożeń musi umożliwiać generyczne (bez wcześniejszej znajomości złośliwego kodu) wykrywanie ataków typu exploit, w tym nowych exploit, nie znanych wcześniej.
33) Wykrywanie exploit musi się odbywać po analizie co najmniej takich formatów plików jak Java Script, zakodowany (obfuscated) Java Script, obiekty Flash, PDF, pliki graficzne, pliki multimedialne mp3/mp4, pliki MS Office, Java.
34) Informacja o wykryciu fazy exploita musi być wskazana w zapisie sekwencyjnym z analizy dynamicznej ataku.
35) Analizator musi umożliwiać tworzenie dedykowanych pulpitów w GUI rozwiązania z możliwością dostosowania wyświetlanych informacji.
36) Analizator musi umożliwiać wykorzystanie reguł, stworzonych samodzielnie przez Zamawiającego, opisujących cechy podejrzanych obiektów w formacie YARA.
37) Analizator musi posiadać dodatkowy mechanizm wykrywania zdarzeń typu prawdopodobny malware (takich jak zaszyfrowane dokumenty MS Office, zdegradowane pliki wykonywalne Windows PE, formularze web przekazujące hasła, pliki niewykonywalne umożliwiające komunikację do niestandardowego portu). Zdarzenia te powinny być konfigurowalne jako alert lub automatyczna kwarantanna.
38) Analizator musi generować wynik analizy dynamicznej przynajmniej do pliku PDF.
39) Analizator musi umożliwiać tworzenie raportów ze szczegółami wykrytych alertów do formatów co najmniej JSON, CSV.
40) Analizator musi umożliwiać tworzenie raportów z przeprowadzonych skanowań do formatu PDF zawierających co najmniej statystyki wykrytych zagrożeń.
41) Analizator musi umożliwiać przegląd nowych funkcjonalności po aktualizacji oprogramowania.
42) Analizator musi umożliwiać tworzenie raportów uruchamianych cyklicznie (godzinowo/dzienne/tygodniowo/miesięcznie) zawierających co najmniej wykryte zagrożenia. Raporty te muszą być dostarczane przez email.
43) Analizator musi umożliwiać wysyłanie alertów o zdarzeniach poprzez protokoły **SYSLOG**, SMTP, SNMP, HTTP.
44) Analizator musi integrować się bezpośrednio z posiadanym przez zamawiającego rozwiązaniem Trellix Detection as a Service, co najmniej w oparciu o wymianę artefaktów ataku wykrytych w skanowanych repozytoriach plików oraz musi umożliwiać przegląd generowanych alertów. **W przypadku zaoferowania rozwiązania posiadającego funkcjonalność w pełni zgodną z Trellix Detection as a Service wbudowaną w proponowane rozwiązanie w celu zapewnienia analitykom wysokiego stopnia automatyzacji w aspekcie wdrażania schematów działań Zamawiający dopuszcza wykorzystanie innego narzędzia wyłącznie przez interface API.**
45) Analizator musi umożliwiać korelację alertów z MITRE Technics.
46) Analizator musi umożliwiać natywną integrację umożliwiającą skanowanie plików z Office 365 SharePoint Online storage lub z wykorzystaniem API (uwierzytelnianie i autoryzacja).
47) Analizator musi umożliwiać natywną integrację umożliwiającą skanowanie plików z Microsoft OneDrive **lub z wykorzystaniem API (uwierzytelnianie i autoryzacja).**
48) Analizator musi umożliwiać podłączenie repozytoriów CIFS po SMBv3.
49) **Architektura rozwiązania Analizatora plików musi pracować w trybie wysokiej dostępności (High availability).**