Załącznik nr 3 do SWZ

Szczegółowy Opis Przedmiotu Zamówienia

Zadanie nr 2 - Usługa monitorowania, wykrywania i reagowania na cyberzagrożenia wraz z dostawą narzędzi do kompleksowego wykrywania, monitorowania, blokowania i usuwania zaawansowanych zagrożeń i ataków cybernetycznych wraz z możliwością wykonania automatycznie oraz manualnie działań naprawczych.

Spis

1. Wstęp

Przedmiotem zamówienia jest dostarczenie usługi monitorowania, wykrywania i reagowania na cyberzagrożenia w zakresie realizacji I, II i III linii SOC wraz z dostawą narzędzi do kompleksowego wykrywania, monitorowania, blokowania i usuwania zaawansowanych zagrożeń i ataków cybernetycznych wraz z możliwością wykonania automatycznie oraz manualnie działań naprawczych (ang. remediation), minimalne wymagania dotyczące świadczenia usługi opisane są w punkcie 3. Usługa zostanie zakontraktowana na okres 36 miesięcy z możliwością przedłużenia na okres późniejszy. Usługą objętych ma być 145 punktów końcowych.

W ramach usługi ma być dostarczony Komercyjny System (lub systemy) których minimalne wymagania, są opisane w punkcie 4.

2. Wymagania ogólne dla oprogramowania.

- całość oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów;
- oprogramowanie powinno być objęte min 36-miesięczną licencją czasową zawierającą wsparcie i utrzymanie obejmującą swoim zakresem poprawność działania w zakresie wdrożonych funkcjonalności wg stanu na dzień podpisania stosownego protokołu odbiory (chyba że zapisy szczegółowe stanowią inaczej).

3. Wymagania dotyczące zakresu usługi monitorowani, wykrywania i reagowania na cyberzagrożenia

W ramach usługi zamawiający oczekuje zapewnienia usługi monitorowani, wykrywania oraz reagowania na cyber incydenty oraz niezbędnych narzędzi spełniających co najmniej wymagania minimalne opisane w punkcie 4. Akceptowalne jest dostarczenie systemu (lub systemów) w modelu onpremis (wariant instalacji lokalnej) oraz saas w cloud. W ramach świadczonej usługi Dostawca zapewni licencje niezbędne do realizacji usługi.

3.1 Zakres usługi

3.1.1 24h/7 dni w tygodniu przez 365 dni w roku
3.1.2 monitorowanie i analiza zdarzeń (logi systemowe, ruch sieciowy, zdarzenia z systemów bezpieczeństwa, informacje od administratorów)
3.1.3 wykrywanie incydentów, klasyfikacja incydentów
3.1.4 reagowanie na incydenty - zdalnie
3.1.5 współpraca z zamawiającym w zakresie implementacji środków zaradczych
3.1.6 we współpracy z zamawiającym przywrócenie normalnego działania po ataku

3.2 Raportowanie:

3.2.1 Rodzaj zagrożeń

3.2.2 Incydenty oraz sposoby mitygacji wynikających z nich zagrożeń

3.2.3 Wykryte podatności i rekomendacje w zakresie ich usunięcia lub wprowadzone środki zaradcze, jeżeli podatności nie można wyeliminować

3.2.4 Wykryte zagrożenia w infrastrukturze zamawiającego

3.2.5 Znane podatności i zagrożenia pochodzące od producentów systemów, systemów bezpieczeństwa i jednostek CSIRT

3.2.6 Alerty spływające ze wszystkich opisanych systemów muszą być prezentowane w jednym centralnym dashboardzie.

3.2.7 Raportowanie w cyklach miesięcznych

3.3 Szkolenia

3.3.1 Dla osób biorących udział w procesie wdrożenia i utrzymania współpracy z Dostawcą oraz dla kadry kierowniczej

3.3.2 Szkolenia z zakresu bezpieczeństwa teleinformatycznego dla pracowników (np. e-learning, szkolenia na miejscu u Zamawiającego, inne)

3.4 Zarządzanie podatnościami:

3.4.1 Raportowanie podatności

3.4.2 Wprowadzanie rozwiązań w zakresie monitorowania pozwalających na wyłapanie prób wykorzystania znanych podatności

3.4.3 Podział podatności na bezwzględnie konieczne do usunięcia przez wymianę oprogramowania/infrastruktury i te, które można monitorować (w porozumieniu z zamawiającym)

3.5 Współpraca z Zamawiającym w zakresie określania zakresu usługi:

3.5.1 wypracowanie wspólnie z zamawiającym procedur współpracy i reagowania na incydenty (wykonawca jako moderator i ostateczny autor procedur), procedury muszą uwzględniać harmonogram pracy zamawiającego, dostępne obu stronom narzędzia

3.5.2 korygowanie procedur, w uzgodnieniu z Zamawiającym, w odpowiedzi na zdarzenia, incydenty, podatności, wyniki audytów, itp.

3.5.3 wypracowanie zakresu odpowiedzialności i wyłączeń z odpowiedzialności

3.5.4 ciągła korekta procedur - PDCA (plan, do, check, act)

3.5.5 współpraca w zakresie wykorzystania i konfiguracji narzędzi Zamawiającego do wsparcia systemów bezpieczeństwa

3.6 Narzędzia:

3.6.1 Wykorzystanie narzędzi posiadanych przez zamawiającego (UTM, WAF, AD, systemy monitorowania zamawiającego) do zwiększenia bezpieczeństwa realizowanej usługi

3.6.2 Dostarczenie pozostałych, niezbędnych narzędzi do zapewnienia bezpieczeństwa wraz z zarządzaniem całym cyklem życia tych narzędzi (wymagania w punkcie 5)

3.6.3 W obu przypadkach środowiska Sanbox (on-premise, cloud) koszty wszystkich wymaganych licencji winny być wliczone w cenę rozwiązania i nie powinny powodować konieczności ponoszenia dodatkowych opłat.

3.6.4 System wykorzystywany winien być licencjonowany jako subskrypcja na liczbę chronionych urządzeń/systemów końcowych bez rozróżnienia na typ chronionego hosta (serwer, stacja końcowa) oraz system operacyjny (Windows, Linux, MacOS), koszty subskrypcji pokrywa Wykonawca.

3.6.5 Dostarczona w ramach usługi subskrypcja zawiera wszystkie opisane elementy funkcjonalne, nieograniczona liczbę instancji serwerów centralnych, wsparcie producenta wraz z usługa SOC producenta 24/7.

3.7 Zakres objęty usługą:

3.7.1 Sieć wewnętrzna Zamawiającego .

3.7.2 Wszystkie urządzenia pracujące w sieci, które są wyposażone w agenta systemów zakupionych w ramach niniejszej usługi (stacje robocze, serwery fizyczne i wirtualne).

3.7.3 Dla aplikacji kupionych w modelu SaaS - zapewnienie bezpieczeństwa ruchu między aplikacją a infrastrukturą Zamawiającego w oparciu o agentów systemów zakupionych w ramach niniejszej usługi oraz urządzenia brzegowe Zamawiającego.

3.7.4 Analiza zachowań użytkowników (wykrywanie niepożądanych zachowań użytkowników, podatność na socjotechniki).

3.8 Odpowiedzialność Wykonawcy

3.8.1 Mitygacja zagrożeń i usunięcie skutków wywołanych przez incydent

3.8.2 Uszkodzenie/usunięcie danych

3.8.3 Kradzież danych

3.8.4 Zaszyfrowanie danych

3.8.5 Modyfikacja przelewów bankowych prowadząca do przywłaszczenia określonej kwoty

3.8.6 Modyfikacja zobowiązań wpływająca na zmniejszenie wpływów lub zwiększenie należności

3.8.7 Naruszenia polityk bezpieczeństwa, kradzież danych i inne incydenty wywołane przez własnych pracowników Wykonawcy

3.9 Etap uruchomienia usługi:

3.9.1 Analiza środowiska Zamawiającego,

3.9.2 Audyt przedwdrożeniowy – przekazanie rekomendacji w zakresie zabezpieczenia infrastruktury,

3.9.3 Ustalenie scenariuszy działania i eskalacji dla poszczególnych incydentów,

3.9.4 Instalacja i uruchomienie niezbędnych systemów,

3.9.5 Pilotażowe uruchomienie i tuning,

3.9.6 Uruchomienie produkcyjne.

4. Wymagania techniczne dla rozwiązania do wykrywania, monitorowania, usuwania oraz zapobiegania zagrożeniom i zaawansowanym atakom cybernetycznym w wewnętrznej sieci informatycznej, które bedzie wykorzystywane przez wykonawce do świadczenia usługi opisanej w punkcie 3

4.1 W zakresie prewencji i detekcji zagrożeń:

4.1.1 Monitoruje i wizualizuje zagrożenia cybernetyczne w czasie rzeczywistym zarówno na fizycznych jak i wirtualnych komputerach użytkowników końcowych oraz serwerach.

4.1.2 Zapewnia także ochronę przed znanym złośliwym oprogramowaniem na podstawie sygnatur.

4.1.3 Identyfikuje złośliwe oprogramowanie w oparciu o analizę zachowania aplikacji w czasie rzeczywistym.

4.1.4 Zapewnia ochronę przy wykorzystaniu statycznych mechanizmów uczenia maszynowego.

4.1.5 Wykorzystuje metadane (IOC) dostarczone przez producenta rozwiązania do analizy i wykrywania zagrożeń

4.1.6 Wykorzystuje metadane (IOC) dostarczone przez dział SOC do analizy i wykrywania zagrożeń.

4.1.7 Zapewnia możliwość prewencyjnego blokowania ataków oraz zagrożeń typu Memory Injection i Ransomware.

4.1.8 Umożliwia wykrywanie zdarzeń dotyczących bezpieczeństwa, pochodzących przynajmniej z niżej wymienionych obszarów w infrastrukturze informatycznej:

4.1.9 ruchu sieciowego,

4.1.10 urządzeń końcowych (stacje robocze oraz serwery),

4.1.11 zachowanie plików na urządzeniach końcowych,

4.1.12 Zachowanie użytkowników na urządzeniach końcowych. Zapewnia wykrywanie zagrożeń m.in. typu:

4.1.12.1 Malware

4.1.12.2 Trojan

4.1.12.3 Rootkit

4.1.12.4 MITM (Man in the Middle)

4.1.12.5 DLL Injection

4.1.12.6 Ransomware

4.1.12.7 Port Scanner Detection

4.1.12.8 Reflective DLL injection
4.1.12.9 Authentication spoofing (Pass the Hash/SMB Relay)
4.1.12.10 Mimikatz
4.1.12.11 Powershell Empire
4.1.12.12 Meterpreter
4.1.12.13 DNS Tunneling
4.1.12.14 ICMP Tunneling
4.1.12.15 Brute Force
4.1.12.16 Powersploit
4.1.12.17 ARP Poisoning
4.1.12.18 Raw Disk Writing

4.1.13 Ogranicza generowanie fałszywych alarmów z wykorzystaniem co najmniej poniższych metod:

4.1.13.1.1 Automatycznej weryfikacji wskaźników wykrytych zagrożeń w odniesieniu do wbudowanej bazy znanych zagrożeń, która jest na bieżąco uaktualniana za pośrednictwem dostępnego w chmurze producenta zestawu narzędzi, zawierających

4.1.13.1.2 Meta-skanowanie antywirusowe, wykorzystujące wszystkie silniki dostępne w bazie VirusTotal.

4.1.13.2 Wzorce schematów działania malware oraz bazy przykładowych kodów źródłowych (ang. Post Ex Sources)

4.1.13.3 Manualne oznaczanie poziomu ważności wykrytego zagrożenia na podstawie analizy przez zespół SOC.

4.1.14 Wykrywa nietypowe zachowania urządzeń, użytkowników oraz plików w sieci.

4.1.15 Zbiera wskaźniki kompromitacji (IOC) i zachowania z obszaru stacji końcowych, zachowania użytkowników, połączeń sieciowych oraz aktywności w systemie plików.

4.1.16 Posiada funkcjonalność samodzielnego „uczenia się” zachowań typowych w organizacji poprzez zbieranie i ustalenie wskaźników dotyczących zachowania monitorowanych elementów w lokalnej oraz rozległej sieci komputerowej.

4.1.17 Profilowanie typowych zachowań i odstępstw od nich

4.1.18 Umożliwia stworzenie tzw. „białej listy” (ang. White list) znanych i zaufanych plików na każdym monitorowanym urządzeniu w celu obniżenia poziomu fałszywych alarmów i poprawy wydajności działania całego rozwiązania.

4.1.19 Rozwiązanie powinno posiadać funkcjonalność szczegółowego skanowania zachowania konkretnego wykonywalnego pliku (*.exe) na chronionej stacji. (bez udziału sandbox)

4.2 W zakresie mylenia atakującego:

4.2.1 Posiada wbudowany mechanizm pułapek (ang. Decoys) wspomagający wczesne wykrywanie nieznanych ataków oraz źródeł zagrożeń a także aktywności szpiegowskiej w infrastrukturze informatycznej w oparciu o obiekty:

4.2.1.1 Hostów (fałszywe usługi sieciowe)

4.2.1.2 Użytkowników

4.2.1.3 Plików

4.3 W zakresie reakcji oraz remediacji:

4.3.1 Posiada możliwość wykonania manualnych i automatycznej działań naprawczych (ang. Remediation), niwelujących skutki ataków oraz zapobiegających podobnym zdarzeniom w przyszłości.

4.3.2 Wykrywanie w czasie rzeczywistym i automatyczne blokowanie na chronionych stacjach końcowych i serwerach poprzez analizę behawioralną m.in. zagrożeń typu:

4.3.2.1 Ransomware

4.3.2.2 Memory Injection

4.3.3 Rozwiązanie ma możliwość automatycznego zabicia (ang. kill) procesu, jeśli wykryje metodę ataku typu Memory Injection

4.3.4 Powiadamia o wykryciu zagrożenia w panelu zarządzania co najmniej drogą mailową oraz SMS i ma możliwość wysyłania logów do zewnętrznego systemu SIEM.

4.3.5 Posiada możliwość wykonania predefiniowanych akcji naprawczych (ang. Remediation) bezpośrednio na chronionych komputerach i serwerach, polegających na możliwości utworzenia reguł, które umożliwią usuwanie w sposób automatyczny każdego kolejnego zagrożenia o podobnym charakterze, z możliwością indywidualnego dostosowania sposobu reakcji systemu.

4.3.6 System umożliwia podjęcie automatycznej lub ręcznej akcji na minimum poniższych obiektach:

4.3.7 Plik (usuń plik, poddaj plik kwarantannie, zabij powiązany proces)

4.3.8 Host (zrestartuj hosta, wyłącz hosta, wyłącz wszystkie karty sieciowe, izoluj – zablokuj komunikację sieciową poza komunikacją związaną z działaniem Systemu, uruchom komendę)

4.3.9 Użytkownik (zablokuj użytkownika)

4.3.10 Sieci (blokuj ruch, przekieruj adres domenowy,

4.3.11 Rozwiązanie winno posiadać możliwość konfiguracji automatycznego wysyłania nieznanych plików wykonywalnych do analizy w środowisku Sandbox.

4.4 W zakresie badań poincydentowych oraz wyszukiwania zagrożeń:

4.4.1 Posiada możliwość przeprowadzania szczegółowych analiz po włamaniowych. Wspiera działania takie jak przeszukiwanie drzew procesów biorących udział w incydencie. Wspiera wyszukiwanie w organizacji plików biorących udział w incydencie np. poprzez wynik funkcji skrótu MD5.

4.4.2 Posiada możliwość wysłania podejrzanych plików do wykonania w sandbox producenta lub w infrastrukturze lokalnej.

4.4.3 Posiada możliwość wysłania podejrzanych plików do SOC producenta w trybie 24/7 celem analizy, oceny ryzyka oraz zalecanych działań naprawczych.

4.4.4 Umożliwia badanie zdarzeń dotyczących bezpieczeństwa, pochodzących przynajmniej z niżej wymienionych obszarów w infrastruktury informatycznej:

4.4.4.1 ruchu sieciowego,

4.4.4.2 urządzeń końcowych (stacje robocze oraz serwery),

4.4.4.3 zachowanie plików na urządzeniach końcowych,

4.4.4.4 zachowanie użytkowników.

4.4.5 Zbiera wskaźniki kompromitacji (IOC) i zachowania z obszaru stacji końcowych, zachowania użytkowników, połączeń sieciowych oraz aktywności w systemie plików.

4.4.6 W zakresie wsparcia analiz po włamaniowych i prowadzenia dochodzeń (and. Forensics) system powinien umożliwiać przeszukiwanie IOC w powiązaniu z minimum poniższymi obiektami:

4.4.6.1 Pliki,

4.4.6.2 Hosty,

4.4.6.3 Użytkownicy,

4.4.6.4 Połączenia sieciowe (zarówno w oparciu o adresy domenowe jak i adresy IP),

4.4.7 Rozwiązanie w obszarze wsparcia zaawansowanych analiz i przeszukiwania danych powinno umożliwiać przeszukiwanie zdarzeń dotyczących obiektów plikowych poprzez minimum:

4.4.7.1 nazwa pliku:

4.4.7.1.1 Rozpoczyna się od

4.4.7.1.2 Kończy się na

4.4.7.1.3 Zawiera

4.4.7.1.4 Nie Zawiera

4.4.7.1.5 Jest równy

4.4.7.1.6 Nie równa się

4.4.7.2 Poziom przypisanego ryzyka w postaci liczbowej:

4.4.7.2.1 większy niż

4.4.7.2.2 mniejszy niż

4.4.7.2.3 równy

4.4.7.3 wystąpienia pliku

4.4.7.3.1 mniej niż

4.4.7.3.2 więcej niż

4.4.7.3.3 równe

4.4.7.4 pierwsze zarejestrowanie pliku

4.4.7.4.1 Od data

4.4.7.4.2 Do data

4.4.7.4.3 Dnia (określony dzień)

4.4.7.4.4 W ciągu ostatnich (minut)

4.4.7.5 ostatnie zarejestrowanie pliku

4.4.7.5.1 Od data

4.4.7.5.2 Do data

4.4.7.5.3 Dnia (określony dzień)

4.4.7.5.4 W ciągu ostatnich (minut)

4.4.7.6 Binarny atrybut (tak/nie) czy plik jest uruchamiany automatycznie (autostart)

4.4.7.7 Binarny atrybut (tak/nie) czy plik ukrywa swoje okno

4.4.7.8 Binarny atrybut (tak/nie) czy plik występuje w folderze typu „program files”

4.4.7.9 Binarny atrybut (tak/nie) czy plik otwiera połączenia sieciowe

4.4.7.10 Binarny atrybut (tak/nie) czy plik uruchamia się także w nocy

4.4.7.11 Binarny atrybut (tak/nie) czy plik występuje w folderze System32

4.4.7.12 Binarny atrybut (tak/nie) czy plik występuje w folderach tymczasowych

4.4.7.13 Adres IP z którym się komunikuje (poprzez podanie adresu IP)

4.4.7.14 Rozmiar pliku

4.4.7.15 Funkcję skrótu MD5

4.4.7.16 Funkcję skrótu SHA256

4.4.8 Informacje o zebranych plikach powinny zawierać minimum korelację dotyczące powiązanych obiektów:

4.4.8.1 Procesy potomne,

4.4.8.2 Typ procesu (np. usługa, proces, załadowany moduł),

4.4.8.3 Użytkownicy, w których kontekście był uruchamiany plik,

4.4.8.4 Powiązany ruch sieciowy (zarówno w kontekście adresów IP oraz portów jak i nazw domenowych),

4.4.8.5 Załadowanych bibliotek dll,

4.4.8.6 Powiązanych operacjach w systemie plików, przynajmniej utworzenie pliku, uruchomienie pliku, usunięcie lub zmiana nazwy,

4.4.9 Rozwiązanie powinno umożliwiać przeszukiwanie oraz wyświetlanie szczegółowych danych dotyczących hostów, które obejmują minimum:

4.4.9.1 Nazwa hosta z filtrowaniem:

4.4.9.1.1 Rozpoczyna się od

4.4.9.1.2 Kończy się na

4.4.9.1.3 Zawiera

4.4.9.1.4 Nie Zawiera
4.4.9.1.5 Jest równy
4.4.9.1.6 Nie równa się

4.4.9.2 Poziom przypisanego ryzyka w postaci liczbowej:

4.4.9.2.1 większy niż
4.4.9.2.2 mniejszy niż
4.4.9.2.3 równy

4.4.9.3 Data ostatniego skanowania hosta,
4.4.9.4 Adres IP hosta,
4.4.9.5 Wersja systemu operacyjnego,
4.4.9.6 Liczba procesów wykrytych na hoście,
4.4.9.7 Liczba i dane użytkowników, którzy logowali się na hoście,
4.4.9.8 Liczba i szczegóły połączeń sieciowych wykrytych na hoście,
4.4.9.9 Informacje o bieżącym obciążeniu hosta minimum w zakresie:

4.4.9.9.1 CPU,
4.4.9.9.2 Pamięć (całkowita, wolna),
4.4.9.9.3 Dysk systemowy (rozmiar całkowity, wolna przestrzeń),

4.4.9.10 Informacje o wykorzystywanych portach,
4.4.9.11 Zainstalowane certyfikaty,
4.4.9.12 Zainstalowane aktualizacje systemu (preferowane wskazanie KBxxxxxxxx),
4.4.9.13 Zainstalowane oprogramowanie wraz z wersją,

4.4.9.14 Udziały sieciowe.

4.4.10 System powinien wspierać przeszukiwanie użytkowników wykrytych na hostach, poprzez minimum poniższe atrybuty:

4.4.10.1 Nazwa użytkownika
4.4.10.2 Poziom ryzyka związany z danym użytkownikiem
4.4.10.3 Status blokady konta (zablokowane/nie zablokowane)
4.4.10.4 Status konta (włączone/wyłączone)
4.4.10.5 Ilość otwartych plików przez użytkownika
4.4.10.6 Wiek hasła użytkownika
4.4.10.7 Data ostatniego logowania
4.4.10.8 Data pierwszego logowania (zarejestrowanego przez system)
4.4.10.9 Ilość komputerów, do których logował się użytkownik w ostatnim czasie (dzień wcześniej, w ostatnim tygodniu, w ostatnim miesiącu, w ostatnich 3 miesiącach, całkowita ilość).
4.4.10.10 Ilość prawidłowych logowań
4.4.10.11 Ilość błędnych logowań
4.4.10.12 Nazwa hosta na którego jest zalogowany

4.4.11 Narzędzie powinno umożliwić zapisanie filtrów wyszukiwania do późniejszych analiz.

4.4.12 System powinien zawierać informacje o otwartych portach i połączeniach sieciowych realizowanych na monitorowanych hostach oraz umożliwiać przeszukiwanie ich minimum poprzez:

4.4.12.1 Adres IP hosta
4.4.12.2 Port Lokalny
4.4.12.3 Adres IP zdalny
4.4.12.4 Port Zdalny
4.4.12.5 Data i czas pierwszego wystąpienia

4.4.12.6 Data i czas ostatniego wystąpienia

4.4.13 Rozwiązanie winno posiadać możliwość ręcznego wysyłania nieznanych plików wykonywalnych do analizy w środowisku Sandbox.

4.4.14 System winien posiadać możliwość wyszukania dowolnej frazy w pamięci operacyjnej chronionych systemów.

4.5 W zakresie zapewnienia wysokiej dostępności, skalowalności oraz wsparcia infrastruktury rozproszonej oraz architektury:

4.5.1 Umożliwia instalowanie hierarchicznych instancji serwerów zarzadzania systemem w układzie Master-Slave, które zapewniają również separację wielu domen administracyjnych (tzw. multitenant).

4.5.2 System nie ogranicza licencyjnie liczby instancji serwerów zarządzania zarówno głównych (Master) jak i zależnych (Slave), które mogą być wdrażane w infrastrukturze zarówno lokalnej jak i rozproszonej.

4.5.3 Rozwiązanie winno posiadać możliwość konfiguracji lokalnego środowiska Sandbox oraz wykorzystania środowiska.

4.6 W zakresie wspieranych platform:

4.6.1 Oprogramowanie systemu umożliwia instalację na serwerach fizycznych oraz wirtualnych w środowisku Windows Server 2012 R2 (wersja angielska) lub nowszych oraz mechanizmów wirtualizacji Hyper-V.

4.6.2 System umożliwia monitorowanie i ochronę m.in. następujących systemów operacyjnych:

4.6.2.1 Windows – od wersji XP SP3

4.6.2.2 Windows Server – od wersji Windows 2003 R2

4.6.2.3 Linux – co najmniej Fedora, CentOS, RedHat, Suse, Debian, Ubuntu, OracleLinux

4.6.2.4 MacOSX – co najmniej El Capitan

4.7 W zakresie ochrony nadmiernego wykorzystania zasobów na ochranianych hostach:

4.7.1 Rozwiązaniu powinno umożliwiać wybranie predefiniowanego maksymalnego poziomu obciążania CPU na monitorowanej i chronionej stacji, co najmniej w zakresie zajętości pamięci operacyjnej. Ustawienie maksymalnej zajętości pamięci operacyjnej powinno być definiowane procentach.

4.8 W zakresie instalacji i wdrażania Systemu:

4.8.1 System umożliwia zdefiniowanie hostów do automatycznej instalacji agenta minimum poprzez:

4.8.1.1 Adres IP,

4.8.1.2 Zakres adresów IP,

4.8.1.3 OU hosta z Active Directory.

4.8.2 Instalacja agenta powinna wymagać jedynie uprawnień na poziomie lokalnego administratora stacji końcowej.

4.8.3 Monitorowanie stacji powinno działać minimum w 3ch trybach:

4.8.3.1 Interwałowym – połączenie w celu przeskanowania monitorowanego hosta jest inicjowane przez serwer centralny w określonych interwałach czasowych i nie wymaga instalacji na stałe żadnego oprogramowania na systemie końcowym. Po przeskanowaniu proces jest usuwany z pamięci operacyjnej.

4.8.3.2 Agenta ulotnego – po każdorazowym uruchomieniu hosta serwer centralny implementuje oprogramowanie agenta monitorującego w pamięci operacyjnej. Agent działa do momentu restartu chronionego systemu.

4.8.3.3 Normalnego Agenta – oprogramowanie monitorujące jest instalowane jako usługa uruchomiona w postaci rezydentnego procesu w pamięci operacyjnej urządzenia końcowego.

4.8.4 Agent na hoście powinien działać z uprawnieniami „LocalSystem” w celu minimalizacji ew. konfliktów z innymi systemami zainstalowanymi na tym samym systemie operacyjnym w obszarach takich jak sterowniki, itp.

4.8.5 System winien umożliwiać dystrybucję agentów służących do ochrony stacji końcowych przynajmniej za pomocą następujących mechanizmów:

4.8.5.1 Wbudowane mechanizmy Microsoft – TCP 445

4.8.5.2 SSH – port 22

4.8.5.3 Scheduled Tasks dla systemów Windows

4.8.5.4 RPC

4.8.5.5 Poprzez pliki .msi

4.9 W zakresie współpracy z innymi platformami:

4.9.1 Zapewnia możliwość przyjęcia kopii ruchu sieciowego przy wykorzystania SPAN portu lub TAP-a.

4.9.2 Umożliwia wysyłanie syslogiem informacji do narzędzi klasy SIEM.

4.9.3 Umożliwia integrację z zewnętrznymi systemami i narzędziami za pośrednictwem pełnego REST API.

4.9.4 System umożliwia zdalną w pełni automatyczną instalację agenta monitorującego stacje końcowe.

4.9.5 System umożliwia korelowanie i parsowanie danych z zewnętrznych systemów (np. firewall, proxy, inne komponenty sieci IP) w celu wzbogacenia zebranych danych.

4.10 W zakresie raportowania:

4.10.1 Koreluje minimum następujące elementy aktywności na hoście w celu oceny poziomu zagrożenia w postaci liczbowej odrębnie dla każdego hosta, pliku, użytkownika oraz zewnętrznych adresów IP:

4.10.1.1 wskaźniki kompromitacji (IOC)

4.10.1.2 zachowania w zakresie połączeń sieciowych
4.10.1.3 aktywności procesów
4.10.1.4 aktywności użytkownika
4.10.1.5 aktywności w ramach systemu plików

4.10.2 Umożliwia generowanie raportów na podstawie zebranych danych, takich jak np.:

4.10.2.1 Alerty otwarte i zamknięte
4.10.2.2 Szczegółowe raporty związane z wykrytym ryzykiem
4.10.2.3 Trendy alertów, pokazujące podatne elementy w sieci w funkcji czasu
4.10.2.4 Najczęstsze typy alertów

4.10.3 Możliwe do wygenerowania z Systemu raporty powinny zawierać informacje o poziomie ryzyka związanego z danym obiektem.

4.10.4 Rozwiązanie powinno umożliwiać generowanie raportów w postaci plików (csv lub excel) oraz widoków dla obiektów plikowych, zawierających minimum:

4.10.4.1 Nazwę pliku
4.10.4.2 Powiązaną ocenę ryzyka w postaci liczbowej
4.10.4.3 Nazwę twórcy (publisher)
4.10.4.4 Ilość stacji roboczych na których dany plik występuje
4.10.4.5 Nazwa produktu
4.10.4.6 Binarny atrybut (tak/nie) czy plik jest uruchamiany automatycznie (autostart)
4.10.4.7 Binarny atrybut (tak/nie) czy plik ukrywa swoje okno
4.10.4.8 Binarny atrybut (tak/nie) czy plik występuje w folderze typu „program files”
4.10.4.9 Binarny atrybut (tak/nie) czy plik otwiera połączenia sieciowe
4.10.4.10 Binarny atrybut (tak/nie) czy plik uruchamia się także w nocy

4.10.4.11 Binarny atrybut (tak/nie) czy plik występuje w folderze System32
4.10.4.12 Binarny atrybut (tak/nie) czy plik występuje w folderach tymczasowych
4.10.4.13 Adres IP z którym się komunikuje
4.10.4.14 Rozmiar pliku
4.10.4.15 Funkcję skrótu MD5
4.10.4.16 Funkcję skrótu SHA256

4.11 W zakresie interfejsu użytkownika/administratora:

4.11.1 Zapewnia dostęp do panelu operatorskiego przez zwykłą przeglądarkę (GUI webowe).

4.11.2 Wyświetla dodatkowe informacje związane z alertami, m.in.: opis zdarzenia, zalecenia dotyczące usunięcia przyczyn alertu oraz wszystkie powiązane ze zdarzeniem obiekty (hosty, użytkowników, pliki i adresy IP).

4.11.3 Posiada panel informacyjny, w którym są wyświetlane informacje o statusie podatności monitorowanych urządzeń końcowego, alertach, skanowaniach i przeprowadzonych analizach.

4.11.4 Na konsoli operatorskiej wyświetlane są wygenerowane przez system aktywne alerty oraz status skompromitowania poszczególnych urządzeń końcowych.

4.11.5 Wyświetla informacje potrzebne podczas analizy dokonywanej po incydentach w zakresie informacji o plikach, użytkownikach, stacjach i ruchu sieciowym.

4.11.6 Wyświetla informacje o wykonanych akcjach naprawczych.

4.11.7 Wskazuje listę chronionych hostów z informacją o aktualnym stanie ich ochrony. Przypisuje poziom ryzyka hostom wyrażony w postaci liczbowej na podstawie powiązanych z danym hostem zdarzeniami/anomaliami.

4.11.8 Zapewnia ogólny widok z poziomu panelu konsoli do zarządzania (ang. dashboard), pokazujący aktualny pogląd sytuacyjny, zawierający przynajmniej liczbę otwartych alertów w podziale na monitorowane obszary takie jak: pliki, użytkownicy, stacje i komunikacja sieciowa.

4.11.9 Wykryte alerty powinny być dodatkowo opisywane kolorem wskazującym na ich ważność za pomocą zróżnicowania kolorystycznego, przy czym alerty krytyczne powinny być wyświetlane zgodnie z branżowymi standardami na czerwono, a alerty o średnim poziomie krytyczności w kolorze pomarańczowo/żółtym. Zdarzenia o niższym poziomie mają być wyświetlane w odcieniach zieleni lub niebieskiego.

4.11.10 Umożliwia umieszczenie i prezentację systemów wg ich lokalizacji geograficznej i odpowiadających im alertów na mapie.

4.11.11 Umożliwia dynamiczne wyświetlanie poziomu alertów dla każdej z lokalizacji wyświetlonych na mapie. Alerty są wyświetlane dynamicznie w zależności od poziomu zagrożenia/kompromitacji. Dostęp do szczegółów alertów powinien być możliwy bezpośrednio po kliknięciu na alert umieszczony na wyświetlanej mapie.

4.11.12 Posiada widok prezentujący ilość alertów na wykresie czasowym, zawierającym liczbę alertów wygenerowanych w poszczególnych dniach w podziale na monitorowane obszary w tym minimum na: hosty, pliki, użytkowników oraz ruch sieciowy.

4.11.13 Dostępne w systemie widoki powinny pozwalać zarządzać alertami i posiadać listy alertów w podziale minimum na: otwarte, zamknięte, oznaczone do ignorowania przez operatora systemu.

4.11.14 Użytkownik administrator może tworzyć nowe reguły oceny ryzyka w oparciu o metadane na hostach.

4.11.15 W ramach działań forensic system powinien prezentować powiązane obiekty do aktualnie wybranego w postaci przynajmniej uproszczonej (zminimalizowanej) linii czasowej z listą informacji dystynktywnych dla danego typu obiektu.

4.11.16 System zapewnia graficzną wizualizację informacji o użytkowniku, ułożoną na linii czasowej, która zawiera informacje o wykrytych zdarzeniach związane z zachowaniem danego użytkownika.

4.11.17 System zawiera graficzną reprezentację powiązań użytkownika z innymi obiektami w środowisku. Powiązania hosta z innymi obiektami obejmują m.in. wykaz plików na danym hoście, połączenia z zewnętrznymi adresami IP, innymi hostami w sieci wewnętrznej oraz użytkowników logujący się do danego hosta.

4.11.18 System zapewnia informacje o domenach, do których były zapytania z monitorowanych hostów.

4.11.19 System powinien generować automatycznie listę domen z którymi występowała komunikacja, która zawiera przynajmniej poniższe informacje:

4.11.19.1 Nazwa Internetowa domeny

4.11.19.2 Poziom ryzyka związany z domeną

4.11.19.3 Klasyfikacja domeny (biała lista, brak klasyfikacji)

4.11.19.4 Data i czas, kiedy po raz pierwszy wystąpiła komunikacja z domeną

4.11.19.5 Data i czas, kiedy po raz ostatni wystąpiła komunikacja z domeną

4.11.19.6 Liczba hostów komunikujących się z daną domeną

4.11.19.7 Liczba adresów IP rozwiązywanych pod daną domeną

4.11.19.8 Liczba lokalnych adresów IP łączących się z daną domeną

4.11.19.9 Liczba użytkowników łączących się z daną domeną

4.11.20 Dla listy inwentaryzacyjnej połączeń monitorowane są m.in. pola:

4.11.20.1 Nazwy hostów związanych z ruchem sieciowym

4.11.20.2 Poziom ryzyka związany z danym połączeniem

4.11.20.3 Lokalny adres IP związany z ruchem sieciowym

4.11.20.4 Lokalny port źródłowy

4.11.20.5 Docelowe IP związane z ruchem sieciowym

4.11.20.6 Port docelowy związany z ruchem sieciowym

4.11.20.7 Data i czas, kiedy po raz pierwszy dany ruch sieciowy był widoczny
4.11.20.8 Data o czas, kiedy po raz ostatni dany ruch sieciowy był widoczny

4.11.21 Rozwiązanie z interfejsu administratora winno umożliwiać automatyczne tworzenie na urządzeniach końcowych fałszywych obiektów, tzw. pułapek (ang. Decoy), których zadaniem jest wprowadzanie atakujących w błąd. Zestaw pułapek winien być automatycznie generowany z poziomu serwera centralnego i nie wymaga manualnego przygotowania na hostach. Włączanie i wyłączanie funkcjonalności Decoy winno być dostępne z poziomu konsoli administratora systemu.

4.11.22 System winien posiadać możliwość gradacji poziomu dostępu do konsoli administracyjnej w sposób granularny wraz z możliwością tworzenia własnych poziomów dostępu.

4.11.23 Rozwiązanie winno posiadać możliwość włączenia i wyłączenia określonych reguł korelacyjnych (alertów) minimum dla poniższych typów zdarzeń:

4.11.23.1 Skanowanie portów
4.11.23.2 Zatruwanie tablic ARP
4.11.23.3 Atak typu Pass the Hash
4.11.23.4 Wykrycie Mimikatz
4.11.23.5 Wykrycie Powershell Empire
4.11.23.6 Zdarzenia administracyjne związane z VSS
4.11.23.7 Tunelowanie DNS
4.11.23.8 Tunelowanie ICMP
4.11.23.9 Atak Brute Force
4.11.23.10 Wykrycie narzędzi Hackerskich
4.11.23.11 Wykrycie narzędzi do zdalnego dostępu
4.11.23.12 Wykrycie Trojana
4.11.23.13 Wykrycie tunelowania Http
4.11.23.14 Alerty związane wykorzystaniem NetBIOS (np. atak LLMNR)

4.11.24 System winien umożliwiać wyświetlanie w konsoli operatorskiej także tych alertów, które zostały przejrzane i zostały zamknięte przez operatora systemu.

4.11.25 Lista alertów winna być możliwa do wyeksportowania m.in. w formacie Excel (*.xlsx).

4.11.26 System winien umożliwiać integrację z Active Directory w celu autoryzacji użytkowników konsoli administracyjnej/operatorskiej.

4.11.27 System winien posiadać widoki dostarczające informacje z zakresu Vulnerability Management tj. Minimum:

4.11.27.1 Listę zainstalowanych poprawek Windows

4.11.27.2 Lista nie autoryzowanych Aplikacji

4.11.27.3 Walidacja wersji wybranych Applikacji

4.11.27.4 Walidacja wersji Agenta Systemu

4.11.28 System powinien posiadać możliwość anonimizacji minimalnie nazwy Hosta i nazwy użytkownika dla danych wysyłanych do SOC

4.11.29 W obu przypadkach środowiska Sanbox (on-premise, cloud) koszty wszystkich wymaganych licencji winny być wliczone w cenę rozwiązania i nie powinny powodować konieczności ponoszenia dodatkowych opłat.

4.11.30 System winien być licencjonowany jako subskrypcja na liczbę chronionych urządzeń/systemów końcowych bez rozróżnienia na typ chronionego hosta (serwer, stacja końcowa) oraz system operacyjny (Windows, Linux, MacOS)

4.11.31 Subskrypcja zawiera wszystkie opisane elementy funkcjonalne, nieograniczona liczbę instancji serwerów centralnych, wsparcie producenta wraz z usługa SOC 24/7.