Załącznik do Umowy

Minimalne wymagania dla oprogramowania – specjalistyczna ochrona EDR dla urządzeń końcowych.

1. System ochrony i reagowania na zaawansowane zagrożenia dla urządzeń końcowych musi zapewniać kompleksową ochronę przed malware, zaawansowanymi atakami wykorzystującymi techniki opisane w modelu MITRE™ ATT&CK, ataki typu „fileless" – bez użycia plików, ataki z wykorzystaniem oprogramowania dostępnego w ramach systemu operacyjnego lub w znanych aplikacjach tzw. „LOLBAS". System musi potrafić zarówno wykrywać zagrożenia na poszczególnych etapach infekcji jak i mieć możliwość granularnego reagowania na wykryte incydenty zależnie od poziomu klasyfikacji danego zagrożenia.
2. Wsparcie dla systemów operacyjnych.
   System musi wspierać ochronę następujących systemów operacyjnych (agentów działających na poniższych systemach operacyjnych):
   a) Systemy Windows 8.x/10/11/Server 2016/Server 2019/Server 2022.
   b) Systemów „legacy" (Windows 7, Windows XP, Windows Server 2003).
   c) Systemy Apple MacOs.
   d) Systemy Linux – minimum Redhat, Ubuntu, Oracle, SUSE.
3. Zarządzanie instalacją i aktualizacją agentów.
   3.1. System musi umożliwiać instalację agenta poprzez SCCM, JAMF i RHEL Satellite.
   3.2. System musi umożliwiać aktualizację wersji agenta z poziomu konsoli zarządzania bez udziału użytkownika końcowego.
   3.3. System musi dostarczać możliwość kreowania instalatorów zawierających parametry umożliwiające podłączenie agenta do określonej grupy hostów oraz danej instancji systemu zarządzającego.
   3.4. Podłączanie się do systemu zarządzającego musi wymagać podania hasła w postaci parametru – bez podania poprawnego hasła nie może być możliwości podłączenia się do systemu zarządzania.
4. Wpływ agentów na zasoby urządzenia końcowego.
   4.1. Poziom zużycia pamięci RAM dla procesów agenta musi wynosić poniżej 350 MB.
   4.2. Poziom średni zużycia procesora (CPU) dla procesów agenta musi wynosić mniej niż 2%.
   4.3. Instalator oprogramowania nie może zajmować więcej niż 100 MB.

5. Wykrywanie zagrożeń.
   5.1. System musi umożliwiać wykrywanie podejrzanych aktywności dla działających, uruchamianych i zatrzymywanych procesów oraz w ramach interakcji pomiędzy procesami.
   5.2. System musi umożliwiać analizę i odzwierciedlanie informacji o parametrach, z jakimi został wykonany dany proces (np. parametry z linii poleceń).
   5.3. System musi umożliwiać wykrywanie złośliwych zmian w rejestrach, co najmniej w kontekście śledzonego wykonania danego procesu.
   5.4. System musi umożliwiać wykrywanie żądań DNS wysyłanych z chronionej stacji.
   5.5. System musi umożliwiać wykrywanie podejrzanej aktywności związanej z używaniem dynamicznie ładowanych bibliotek DLL.
   5.6. System musi potrafić identyfikować podejrzane zachowanie użytkownika jak i samej stacji końcowej.
   5.7. System musi posiadać zintegrowane informacje na temat zagrożeń bezpieczeństwa (tzw. Threat Intelligence), pozwalające na dokładniejszą analizę zagrożenia.
   5.8. System musi umożliwiać agentowi działającemu na końcówce wykrywanie i reagowanie na zagrożenia w przypadku odłączenia od sieci (offline).
   5.9. System musi wykrywać zagrożenia korzystając z silnika NGAV.
   5.10. System musi umożliwiać dodawanie wykluczeń ze skanowania przez silnik NGAV.
6. Prewencja.
   6.1. System musi umożliwiać wykrywanie i kategoryzowanie urządzeń niezarządzanych w bezpośrednim sąsiedztwie sieciowym danego agenta.
   6.2. System musi umożliwiać blokowanie uruchamiania złośliwych plików wykonywalnych i bibliotek DLL.
   6.3. System musi umożliwiać zablokowanie połączeń sieciowych zewnętrznych jak i wewnętrznych wykonywanych przez złośliwe oprogramowanie.
   6.4. System musi umożliwiać blokowanie manipulacji plikami przez złośliwe oprogramowanie: tworzenie, edycję, usuwanie.
   6.5. System musi umożliwiać blokowanie wykonywania się złośliwych plików wykonywalnych i bibliotek DLL.
   6.6. System musi umożliwiać zastosowanie list zezwalających dla danych:
      a) Hash (funkcji skrótu) plików w formatach MD5, SHA1, SHA2.
      b) Nazw plików.

c) Ścieżek plików - z możliwością używania (wildcard) na początku, w środku oraz na końcu nazwy folderu.
d) Aplikacji z uwzględnieniem nazwy, wersji i producenta.
e) Dla konkretnego certyfikatu, którym podpisane są pliki.

6.7. System musi umożliwiać zastosowanie list blokujących dla danych:
a) Hash (funkcji skrótu) plików w formatach MD5, SHA1, SHA2.
b) Nazw plików.
c) Ścieżek plików - z możliwością używania (wildcard) na początku, w środku oraz na końcu nazwy folderu.
d) Dla konkretnego certyfikatu, którym podpisane są pliki.

6.8. System musi umożliwiać blokowanie połączeń do znanych złośliwych stron internetowych, domen lub adresów IP. Lista ta musi być automatycznie aktualizowana przez producenta rozwiązania.

7. Analiza historyczna zagrożeń.

7.1. Dane do analizy muszą pochodzić bezpośrednio z urządzeń końcowych.

7.2. Dane historyczne metadanych zebranych z urządzeń muszą być dostępne do analizy z okresu minimum 1 miesiąca.

7.3. System musi umożliwiać wyszukiwanie oznak ataków w zebranych informacjach. Wyszukiwanie musi być możliwe w oparciu o wszystkie zebrane informacje ze stacji końcowej oraz zidentyfikowane taktyki i techniki MITRE.

7.4. Wyszukiwanie musi umożliwiać budowanie zaawansowanych zapytań z wykorzystaniem logicznych operatorów typu AND, OR, NOT, ISTNIEJE, znaków wildcard, zakresów liczb (np. adresów od 10.0.0.100 do 10.0.0.200). Wyszukiwania muszą wspierać również format STIX.

7.5. System musi w oparciu o zebrane dane samodzielnie identyfikować zachowania wg nomenklatury MITRE. Zachowanie musi być również elementem, w oparciu o który można wykonywać zapytania do zebranych informacji.

7.6. Musi istnieć możliwość zapisania utworzonych zapytań wraz z możliwością ich automatycznego uruchamiania wg określonego harmonogramu z częstotliwością minimalną 15 minut.

7.7. System musi umożliwiać tworzenie profili, które opisują, jakie informacje z urządzenia końcowego będą zbierane.

7.8. Musi istnieć możliwość tworzenia różnych profili i przypisywania ich do różnych grup komputerów.

7.9. Zbierane informacje muszą zawierać minimalnie informacje o:

a) Inwentaryzacji plików.

b) Szczegółowych operacjach na plikach (utworzenie, zapis, odczyt, zmiana nazwy, skasowanie, ustawienie czasu, bezpośredni dostęp do woluminu, bezpośredni zapis do woluminu).

c) Informacjach o procesach (utworzenie, uruchomienie, zatrzymanie, utworzenie wątków, załadowanie sterownika, załadowanie biblioteki).

d) Informacjach o połączeniach sieciowych (zapytania HTTP, zapytania DNS, zaakceptowanie połączenia, nasłuchiwanie na połączenie, zamknięcie połączenia).

e) Zdarzeniach systemowych.

f) Szczegółowych operacjach na rejestrze systemu (utworzenie, skasowanie, zmiana nazwy klucza rejestru; wpisanie, odczytanie, skasowanie wartości rejestru).

7.10. Z poziomu znalezionych informacji musi istnieć możliwość wykonywania akcji, np. dla znalezionego pliku możliwość jego ściągnięcia przez operatora, usunięcia, dodania do czarnej listy.

7.11. System musi umożliwiać integrację ze źródłami STIX/TAXII. Integracja taka ma umożliwiać automatyczne tworzenie zapytań do bazy zdarzeń historycznych na podstawie danych pobranych z kanału STIX/TAXII.

8. Zarządzanie fałszywymi alarmami (False Positives).

8.1. System musi umożliwiać ręczne zarządzanie fałszywymi alarmami poprzez możliwość oznaczania źle sklasyfikowanej aktywności, celem poprawnego wykrywania w przyszłości.

8.2. System musi posiadać mechanizm automatycznej reklasyfikacji fałszywych alarmów (False Positives) i przeciwdziałać błędnemu ich wykrywaniu w przyszłości.

9. Analiza zagrożeń.

9.1. System musi umożliwiać pobieranie fragmentów zrzutów pamięci z urządzeń końcowych.

9.2. System musi posiadać interfejs API pozwalający na śledzenie wykrytych incydentów oraz prowadzonych analiz zagrożeń z uwzględnieniem takich parametrów jak:

a) Adres IP.

b) Nazwa hosta.

c) Użytkownik.

d) Data.

e) Ilość wystąpień danego zdarzenia.

f) Klasyfikacja aktywności.

10. Reagowanie na incydenty bezpieczeństwa.

10.1. Incydenty bezpieczeństwa muszą być klasyfikowane (klasa zagrożenia) co najmniej w następujące grupy:

a) Złośliwe.
b) Podejrzane.
c) Niejednoznaczne – wymagające głębszej analizy.
d) Niechciane tzw. PUP – „Potential Unwanted Programs".
e) Prawdopodobnie bezpieczne.

10.2. W ramach każdej klasy zagrożeń musi istnieć możliwość zastosowania lub nie poniższej reakcji lub działania ograniczającego wpływ incydentu na bezpieczeństwo:

a) Możliwość zabicia/zatrzymania procesu.
b) Możliwość usunięcia pliku.
c) Możliwość przywrócenia stanu rejestru systemu przed wykonaniem się danego zagrożenia.
d) Automatyczne wprowadzenie hosta w stan izolacji sieciowej – zgodnie z konfigurowalną polityką dostępu do sieci.

10.3. W wypadku klasyfikacji zagrożenia jako niejednoznaczne, system musi umożliwiać automatyczną detonację pliku w chmurze producenta – działanie tej funkcji może zostać wyłączone przez Zamawiającego.

10.4. System musi umożliwiać dynamiczną zmianę grupy agenta na inną, gdzie zostały przypisane polityki bezpieczeństwa o większych obostrzeniach.

10.5. System musi umożliwiać zbudowanie (zaprogramowanie) własnych akcji reagujących na daną klasyfikację zagrożenia.

10.6. System musi umożliwiać automatyczne blokowanie adresu IP, z którym łączy się podejrzany proces, na zewnętrznym urządzeniu firewall.

10.7. W ramach reakcji na incydenty musi istnieć możliwość powiadamiania innych systemów za pomocą:

a) Wysłania wiadomości e-mail ze szczegółami zdarzenia.
b) Wysłania informacji za pomocą protokołu syslog.
c) Możliwości wysłania informacji do zewnętrznego systemu, zawierającego w załączeniu dane w postaci XML lub JSON umożliwiające automatyczne założenie zgłoszenia.

10.8. Wszystkie powyższe akcje opisane w pkt 10.7. muszą być konfigurowalne per każda klasa zagrożenia.

10.9. Musi istnieć możliwość zastosowania wszystkich akcji jednocześnie w ramach danej klasy zagrożenia (np. izolacja, wysłanie powiadomienia SYSLOG, usunięcie pliku i zablokowanie niebezpiecznego adresu IP na urządzeniu Firewall).

10.10. Polityka reagowania na zagrożenia i incydenty bezpieczeństwa musi umożliwiać jej rozróżnienie dla poszczególnych grup agentów.

10.11. System musi posiadać funkcjonalność zdalnego dostępu do chronionego urządzenia końcowego (remote shell) z poziomu konsoli administratora systemu.

10.12. W ramach dostępu zdalnego (remote shell access) muszą być możliwe co najmniej następujące akcje:

a) Listowanie plików w katalogach.
b) Listowanie konfiguracji adresacji IP na interfejsach.
c) Pobranie pliku z urządzenia końcowego.
d) Wgranie pliku na urządzenie końcowe.
e) Usunięcie pliku na urządzeniu końcowym.
f) Informacja o zalogowanych użytkownikach.
g) Zwracanie sumy kontrolnej (SHA1 oraz MD5) pliku na urządzeniu.
h) Lista zadań systemu operacyjnego (tasklist).
i) Zrzucenie pamięci danego procesu.
j) Uruchomienie powłoki systemowej.
k) Pobranie wartości rejestru.
l) Listowanie i usuwanie aplikacji w systemie, które są uruchamiane przy starcie z klucza rejestru RUN.

11. Zarządzanie podatnościami.

11.1. System musi umożliwiać wykrywanie i katalogowanie w czasie rzeczywistym wersji aplikacji komunikujących się za pomocą sieci.

11.2. System musi umożliwiać wykrywanie urządzeń IoT w sieci, gdzie znajdują się chronione hosty.

11.3. System musi umożliwiać wykrywanie innych hostów w sieci, gdzie nie ma zainstalowanego agenta.

11.4. System musi umożliwiać wykrywanie podatności w aplikacjach, które komunikują się za pomocą sieci z urządzeniami zewnętrznymi.

11.5. Musi istnieć możliwość ograniczenia ryzyka dla konkretnej podatnej wersji aplikacji poprzez automatyczne ograniczenie możliwości komunikacji na podstawie reguł bazujących na aktualizowanych informacjach CVE.

12. Wykrywanie zaawansowanych scenariuszy ataków.

12.1. System musi działać w oparciu o mechanizmy analizy zachowań procesów i wywołań funkcji systemowych wsparte sztuczną inteligencją, w szczególności działającymi mechanizmami opartymi o modele matematyczne algorytmów uczenia maszynowego (Machine Learning).

12.2. Uczenie maszynowe musi być wykorzystywane zarówno w analizie zachowań procesów, jak i w analizie samych plików.

12.3. System musi wykrywać i umożliwiać reakcję w locie na znane zagrożenia bazując na ich zachowaniu oraz reputacji, w szczególności:

a) Możliwość blokowania i reagowania w ramach sekwencji wykonania danego zagrożenia bazując na heurystyce zachowań (np. podczas próby szyfrowania plików przez zagrożenie typu ransomware).

b) Możliwość korzystania z komercyjnych baz reputacji plików (np. Virus Total).

c) Możliwość wykrywania zagrożeń typu RAT (Remote Access Trojan) na podstawie zachowań.

d) Wykrywanie zagrożeń musi umożliwiać konfiguracyjnie zarówno blokowania uruchomienia danego pliku, jak i możliwość blokowania złośliwych akcji po uruchomieniu się danego zagrożenia.

e) System musi umożliwiać blokowanie złośliwych urządzeń USB należących do innych niż dozwolone przez politykę klas.

f) System musi umożliwiać logowanie dostępu urządzeń USB mających interakcję z systemem operacyjnym.

g) System musi umożliwiać wykrywanie i blokowanie podejrzanej aktywności w interpreterach języków skryptowych takich jak:

I) Powershell.

II) CScript.

III) Python.

IV) Makra pakietu Microsoft Office.

13. Architektura rozwiązania.

13.1. Centralne zarządzanie musi odbywać się za pomocą przeglądarki internetowej poprzez WebUI.

13.2. System musi umożliwiać dostęp do interfejsu API.

13.3. System zarządzania musi umożliwiać integrację z usługą katalogową Active Directory oraz rozwiązaniami Two Factor Authentication i rozwiązaniami typu SSO (Single Sign On).

13.4. System zarządzania musi umożliwiać granularną kontrolę opartą o predefiniowane role oraz wsparcie dla modelu RBAC.

13.5. Agent systemu musi być zabezpieczony hasłem przed próbami deinstalacji z poziomu użytkownika oraz innych złośliwych procesów.

13.6. Rozwiązanie musi pozwalać na:

a) Centralne zarządzanie.

b) Przechowywanie zdarzeń w centralnym systemie.

c) Funkcjonowanie oprogramowania w modelu chmurowym – Zamawiający nie musi instalować po swojej stronie żadnych komponentów (z wyjątkiem instalacji agentów na chronionych końcówkach).

14. Zgodność z normami.

14.1. Dostarczony system musi posiadać zgodność z GDPR z możliwością usunięcia zapisanych informacji. Wyszukiwanie rekordów musi być możliwe poprzez nazwę użytkownika, nazwę urządzenia, adres IP, adres MAC.

14.2. Dostarczony system musi umożliwiać eksport szczegółowego audytu funkcjonowania systemu zawierającego przynajmniej informacje o tym, kto, kiedy i jakie wprowadzał zmiany w politykach, podejmował akcje, generował raport GDPR, logował się do systemu.

15. Integracja rozwiązania z innymi komponentami.

15.1. System musi udostępniać API, za pomocą którego można wykonywać operacje zarządzania konfiguracją polityki oraz wprowadzania końcówek w stan izolacji.

15.2. Wymagane jest dostarczenie dokumentacji do API.

15.3. System musi umożliwiać integrację z urządzeniami typu Firewall (co najmniej z producentami Check Point, Cisco, Fortinet, Palo Alto) co najmniej umożliwiając blokowanie adresów IP, z którymi komunikuje się złośliwe oprogramowanie.

15.4. System musi umożliwiać integrację z rozwiązaniami typu Network Access Control (NAC), umożliwiając izolację podejrzanego komputera do osobnego VLAN.

15.5. System musi umożliwiać integrację z rozwiązaniem typu sandbox działającym lokalnie (on-premises) – system sandbox nie jest przedmiotem zapytania.

15.6. System musi umożliwiać budowanie dopasowanej pod rozwiązanie („custom”) integracji z zewnętrznymi systemami/urządzeniami bezpieczeństwa poprzez wywoływanie własnych/zmodyfikowanych samodzielnie skryptów.

15.7. System musi umożliwiać integrację z systemami typu SIEM. Zdarzenie musi zawierać przynajmniej informacje:

a) Nazwa urządzenia.
b) Stan agenta na urządzeniu.
c) Adres MAC.
d) System operacyjny.
e) Źródłowe IP.
f) Nazwa procesu.
g) Ścieżka procesu.
h) Typ procesu.
i) Istotność.
j) Klasyfikacja.
k) Reguła wykrywająca zagrożenie.
l) Akcja.
m) Hash procesu.
n) Nazwa/rodzina/typ zagrożenia.
o) Techniki MITRE.
p) Cel ataku.
q) Zdarzenia audytowe systemu, wykonane akcje, zmiany w politykach itp.

15.8. System musi umożliwiać integrację z systemami typu help desk, dostarczając wszystkie informacje dostępne w incydencie, które mogą być wykorzystane w celu automatycznego utworzenia zgłoszenia.

16. Licencje oraz serwisy.

16.1. Dostarczona zostanie subskrypcja upoważniająca do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów, obejmująca co najmniej następujące funkcjonalności:

a) Całość infrastruktury zainstalowana musi być w środowisku producenta z możliwością instalacji niektórych komponentów rozwiązania (agregujący ruch z agentów do centralnego systemu zarządzania oraz umożliwiający wykonywanie akcji integracyjnych z lokalnego systemu) w infrastrukturze Zamawiającego (model chmurowo/hybrydowy).

b) Dostęp do baz zagrożeń bezpieczeństwa – Threat Intelligence.

c) Aktualizacje baz zagrożeń CVSS.

16.2. Rozwiązanie musi być dostarczone w postaci subskrypcji pozwalającej na ochronę 1000 urządzeń końcowych (bez względu na to, czy oprogramowanie zostanie zainstalowane na systemach typu PC czy systemach serwerowych) na okres 3 lat.

16.3. Wraz z subskrypcją musi zostać dostarczona usługa doradztwa technicznego dostarczana przez producenta rozwiązania, wspomagająca proces implementacji oprogramowania w oparciu o najlepsze praktyki na okres minimum jednego roku.

16.4. Na czas subskrypcji oprogramowania, dla osób administrujących oraz obsługujących oprogramowanie, musi zostać Zamawiającemu przyznany dostęp do platformy szkoleniowej producenta, na której dostępny będzie instruktaż dotyczący funkcjonowania i administracji oferowanego rozwiązania.