**Załącznik nr 2b do SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA – ZADANIE 2**

**OPIS RÓWNOWAŻNOŚCI:**

W przypadku gdy w dokumencie stanowiącym element opisu przedmiotu zamówienia pojawią się wskazania znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego dostawcę (jeżeli mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub jego produktów), należy rozumieć, zgodnie z przepisem art. 99 ust. 5 ustawy Pzp, że zamawiający nie może opisać przedmiotu zamówienia w wystarczająco precyzyjny i zrozumiały sposób i w takich okolicznościach Zamawiający dopuszcza możliwość składania w ofercie rozwiązań równoważnych, wskazując, iż minimalne wymagania, jakim mają odpowiadać rozwiązania równoważne, to wymagania nie gorsze od parametrów wskazanych w tych dokumentach, a ich kryteria w celu oceny równoważności wskazane są w opisie przedmiotu zamówienia.

W przypadku, gdy Zamawiający opisuje przedmiot zamówienia przez odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy, zamawiający dopuszcza rozwiązania równoważne opisywanym.

Wykonawcy mogą składać oferty zawierające rozwiązania równoważne w stosunku do przedmiotu zamówienia przedstawionego w SWZ – zgodnie z art. 101 ust. 4, 5 i 6 ustawy PZP, jednak są zobowiązani wykazać, że oferowane przez nich rozwiązania spełniają wymagania określone przez Zamawiającego. Równoważność pod względem parametrów technicznych, użytkowych oraz eksploatacyjnych ma w szczególności zapewnić uzyskanie parametrów nie gorszych od założonych w niniejszym SWZ

Za równoważne uznaje się rozwiązania, jak również elementy, materiały, urządzenia o właściwościach funkcjonalnych i jakościowych takich samych, które zostały określone w opisie przedmiotu zamówienia, lecz oznaczonych innym znakiem towarowym, patentem lub pochodzeniem. Przy czym istotne jest to, że produkt równoważny to produkt, który nie jest identyczny, tożsamy z produktem referencyjnym, ale posiada pewne, istotne dla Zamawiającego, zbliżone do produktu referencyjnego cechy i parametry.

Istotne dla Zamawiającego cechy i parametry, to takie, które pozwolą zachować wszystkim systemom, urządzeniom, wyrobom, parametry i cechy pozwalające przede wszystkim na prawidłową współpracę z innymi systemami i/lub urządzeniami i/lub wyrobami w sposób założony przez Zamawiającego oraz pozwalające przy tym uzyskać parametry nie gorsze od założonych w niniejszym załączniku. Ciężar udowodnienia równoważności spoczywa na Wykonawcy

Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowany przedmiot zamówienia spełnia wymagania określone przez Zamawiającego poprzez złożenie opisu zaoferowanych produktów wraz z wykazaniem cech równoważności w stosunku do wymagań opisanych przez Zamawiającego w niniejszym załączniku oraz podanie nazwy handlowej i producenta.

W celu wykazania cech równoważności Zamawiający dopuszcza załączenie do opisu etykiet, zdjęć, kart katalogowych itp., z dopiskiem której pozycji asortymentowej (jakiego sprzętu) dotyczy dana informacja z zastrzeżeniem, że z tych dokumentów muszą wynikać parametry co najmniej określone przez Zamawiającego w załącznikach do OPZ i dane identyfikujące produkt.

**PODNIESIENIE POZIOMU CYBERBEZPIECZEŃSTWA SZPITALA – PAKIET NR 2:**

Przedmiotem zamówienia jest dostarczenie i wdrożenie rozwiązania zawierającego następujące elementy:

**Zakup i wdrożenie systemu EDR**

Poniżej wyspecyfikowano minimalne parametry sprzętu, oprogramowania oraz usług, które należy dostarczyć i wdrożyć w ramach realizacji przedmiotu zamówienia. W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna.

# **Wymagania ogólne**

System ochrony i reagowania na zaawansowane zagrożenia dla urządzeń końcowych ma zapewnić 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 ma wykrywać zagrożenia na poszczególnych etapach infekcji jak i selektywnie reagować na wykryte incydenty w zależności od poziomu i klasyfikacji danego zagrożenia.

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie ma pracować w oparciu o komercyjne bazy zabezpieczeń oraz oprogramowanie dostarczane przez jednego producent.

# **Wsparcie dla systemów operacyjnych**

System ma analizować i chronić stacje robocze oraz serwery działające pod kontrolą następujących systemów operacyjnych:

1. Systemy Windows 8.x/10/Server 2016/Server 2019/Server 2022.
2. Systemy Apple MacOS.
3. Systemy Linux, minimum Redhat, Ubuntu, Oracle, SUSE

W tym zakresie producent rozwiązania ma dostarczyć „agenty” instalowane w zabezpieczanych środowiskach.

# **Zarządzanie instalacją i aktualizacją agentów**

W zakresie instalacji i aktualizacji agentów system ma zapewnić:

1. Instalacja agenta poprzez: SCCM, JAMF i Satellite.
2. Aktualizacja/Zmiana wersji agenta z poziomu konsoli zarządzania bez udziału użytkownika hosta końcowego.
3. Możliwość kreowania pakietów instalacyjnych agenta, które zawierają parametry umożliwiające min. : podłączenie się danego agenta do danej instancji systemu zarządzającego oraz – po podłączeniu – przypisanie go określonej grupy hostów.
4. Podłączanie agenta do systemu zarządzającego wymaga podania hasła jako parametru. System ma uniemożliwiać podłączenie agenta bez podania poprawnego hasła.
5. Możliwość zarządzania aktualizacją agentów w oparciu o grupy, do których przynależą.

# **Wpływ agenta na zasoby chronionego hosta**

Działanie agenta ma wywierać niewielki wpływ na obciążenie zasobów urządzenia końcowego:

1. Poziom zużycia pamięci RAM dla procesów agenta ma wynosić średnio poniżej 200MB.
2. Poziom średni zużycia procesora (CPU) dla procesów agenta ma wynosić średnio do 1%.
3. Wielkość paczki instalacyjnej nie większa niż 100MB.

# **Określanie powierzchni ataku**

System ma umożliwiać określanie potencjalnej powierzchni ataku poprzez:

1. Wykrywanie i katalogowanie w czasie rzeczywistym wersji aplikacji lokalnych komunikujących się za pomocą sieci.
2. Wykrywanie innych hostów w sieci, gdzie nie ma zainstalowanego agenta.

# **Wykrywanie i reagowanie na zagrożenia**

System ma posiadać następujące funkcje w zakresie wykrywania i reagowania na zagrożenia:

1. Agent wykrywa i reaguje na zagrożenia również w przypadku odłączenia hosta od sieci Internet (tryb offline) oraz przy braku kontaktu z systemem zarządzania.
2. System identyfikuje podejrzane zachowanie użytkownika jak i samej stacji końcowej.
3. Agent wykrywa podejrzane aktywności dla: działających, uruchamianych i zatrzymywanych procesów oraz w ramach interakcji pomiędzy procesami.
4. System ma zapewnić analizę i prezentowanie informacji o parametrach z jakimi został wykonany dany proces (np. parametry z linii poleceń).
5. Agent wykrywa nieautoryzowane zmiany w rejestrach, w szczególności wykonywane przez śledzone procesy.
6. Agent wykrywa i monitoruje wszystkie zapytania DNS generowane z chronionego hosta.
7. Agent wykrywa i blokuje podejrzane aktywności związane z użyciem dynamicznie ładowanych bibliotek DLL oraz uruchamianiem potencjalnie niebezpiecznych plików.
8. System ma umożliwiać blokowanie manipulacji plikami przez złośliwe oprogramowanie: tworzenie, edycję, usuwanie).
9. System ma umożliwiać zastosowywanie białych i czarnych list przy analizie danych, co najmniej na podstawie:

* Hashy (funkcji skrótu) plików w formatach MD5, SHA1, SHA256.
* Nazw plików.
* Ścieżek plików.
* Aplikacji z uwzględnieniem nazwy, wersji oprogramowania i producenta.

1. System ma uzupełniać informacje analityczne o dodatkowe dane dostarczane w ramach tzw. Threat Intelligence. Bazując na informacjach o klasyfikacji zagrożenia, dostarczanych przez serwisy producenta, ma realizować bardziej dokładną, rozszerzoną analizę zagrożenia.
2. Do wykrywania zagrożeń - jako dodatkową funkcję - agent ma wykorzystywać silnik NGAV (analiza statyczna w oparciu o sygnatury). W tym zakresie administrator systemu musi mieć możliwość definiowania wykluczeń, tzn. wskazania w jakich sytuacjach skanowanie przez silnik NGAV nie jest realizowane.
3. System ma stosować matrycę MITRE™ ATT&CK dla wykrywanych naruszeń polityki bezpieczeństwa.

# **Reagowanie na incydenty bezpieczeństwa**

System musi umożliwiać selektywne reagowanie na wykryte incydenty bezpieczeństwa:

1. Incydenty bezpieczeństwa są klasyfikowane w oparciu o min. następujące klasy (poniższe klasy mogą być odzwierciedlone inną nomenklaturą nazewnictwa, np.: Critical, High, Medium, Low, Info):
   1. Złośliwe.
   2. Podejrzane.
   3. Niestandardowe – wymagające głębszej analizy.
   4. Niechciane tzw. PUP – Potential Unwanted Programs.
   5. Prawdopodobnie bezpieczne zachowanie.
2. W ramach każdej klasy zagrożeń musi istnieć możliwość zastosowania (lub nie) poniższej reakcji lub działania ograniczającego wpływ incydentu na bezpieczeństwo:
   1. Zabicie/Zatrzymanie procesu.
   2. Usunięcie pliku.
   3. Przywrócenie konfiguracji rejestru systemu do stanu sprzed wystąpienia danego zagrożenia.
   4. Automatyczne lub ręczne wprowadzenie hosta w stan izolacji sieciowej – zgodnie ze zdefiniowaną (skonfigurowaną) polityką dostępu do sieci.
3. W wypadku klasyfikacji zagrożenia jako niejednoznaczne, system ma umożliwiać automatyczną detonację pliku w chmurze producenta – działanie tej funkcji może zostać określone konfiguracyjnie.
4. Możliwość zbudowania (zaprogramowania) własnych akcji reagowania na daną klasyfikację zagrożenia.
5. Możliwość dynamicznej lub manualnej zmiany grupy, do której należy agent na inną, gdzie zostały przypisane polityki bezpieczeństwa o większych obostrzeniach.
6. Automatyczne blokowanie adresu IP, z którym łączy się podejrzany proces – poprzez API call - na zewnętrznym urządzeniu firewall.
7. W ramach reakcji na incydenty bezpieczeństwa ma istnieć możliwość powiadamiania innych systemów poprzez:
   1. Wysłanie wiadomości pocztowej e-mail ze szczegółami zdarzenia.
   2. Wysłanie informacji za pomocą protokołu SYSLOG.
   3. Wysłanie powiadomienia (zawierającego dane w postaci XML lub JSON) do zewnętrznego systemu w celu automatycznego założenia ticketu.
8. Wszystkie powyższe akcje maja być konfigurowalne per każda klasa zagrożenia – określona w punkcie 1.
9. System ma umożliwiać zastosowanie wszystkich akcji jednocześnie w ramach danej klasy zagrożenia (np. izolacja, wysłanie powiadomienia SYSLOG, usunięcie pliku i zablokowanie niebezpiecznego adresu IP na urządzeniu Firewall).
10. Polityka reagowania na zagrożenia i incydenty bezpieczeństwa ma umożliwiać jej rozróżnienie dla poszczególnych grup agentów.
11. System ma posiadać funkcję zdalnego dostępu do chronionego hosta (remote shell), z poziomu konsoli administratora systemu.
12. W ramach dostępu zdalnego (remote shell access) mają być możliwe co najmniej następujące akcje:
    1. Listowanie plików w katalogach.
    2. Listowanie konfiguracji adresacji IP na interfejsach.
    3. Pobranie pliku z urządzenia końcowego.
    4. Wgranie pliku na urządzenie końcowe.
    5. Usunięcie pliku na urządzeniu końcowym.
    6. Pozyskanie informacji o zalogowanych użytkownikach.
    7. Uzyskanie sumy kontrolnej (SHA1 oraz MD5) pliku na urządzeniu.
    8. Pobranie listy zadań systemu operacyjnego (tasklist).
    9. Zrzucenie pamięci danego procesu.
    10. Uruchomienie powłoki systemowej.
    11. Pobranie wartości rejestru.
    12. Listowanie i usuwanie aplikacji w systemie, które są uruchamiane przy starcie (z klucza rejestru RUN).

# **Analiza historyczna zagrożeń**

System ma umożliwiać przeprowadzanie czynności śledczych oraz przeszukiwanie danych pozyskanych z urządzeń końcowych.

1. System ma umożliwiać pobieranie zrzutów pamięci z urządzeń końcowych.
2. System ma posiadać interfejs API pozwalający na dostęp do informacji o wykrytych incydentach oraz prowadzonych analizach zagrożeń z uwzględnieniem takich parametrów jak:
3. Adres IP
4. Nazwa hosta
5. Użytkownik
6. Data
7. Ilość wystąpień danego zdarzenia
8. Klasyfikacja aktywności

System musi umożliwiać przekazanie powyższych danych do systemu ticketowego.

1. System ma możliwość wyszukiwania oznak ataków w zebranych informacjach. Wyszukiwanie musi być możliwe w oparciu o wszystkie informacje zebrane ze stacji końcowej oraz zidentyfikowane taktyki i techniki MITRE.
2. Dane do analizy historycznej muszą pochodzić bezpośrednio z urządzeń końcowych.
3. Historyczne metadane zebrane z urządzeń muszą być dostępne do analizy z okresu minimum 1 miesiąca.
4. Wyszukiwanie jest możliwe poprzez 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).
5. System wykorzystując mechanizmy AI (lub równoważne) ma samodzielnie identyfikować i analizować zachowania na hostach według nomenklatury MITRE. Dla skutecznej analizy, zachowanie musi być elementem, w oparciu o który można przeszukiwać zgromadzone informacje.
6. System ma umożliwiać zapisywanie utworzonych zapytań wraz z możliwością ich automatycznego uruchamiania wg określonego harmonogramu z częstotliwością minimalną - 15 minut.
7. System ma pozwalać tworzyć profile, które opisują jakie informacje z urządzenia końcowego mają być gromadzone.
8. System ma umożliwiać tworzenie wielu różnych profili i przypisywanie ich do różnych grup monitorowanych hostów.
9. Gromadzone dane mają zawierają co najmniej: informacje o inwentaryzacji plików, szczegółowe operacje na plikach (utworzenie, zapis, odczyt, zmiana nazwy, skasowanie, ustawienie czasu, bezpośredni dostęp do woluminu, bezpośredni zapis do woluminu), informacje o procesach (utworzenie, uruchomienie, zatrzymanie, utworzenie wątków, załadowanie sterownika, załadowanie biblioteki), informacje o połączeniach sieciowych (zapytania http, zapytań DNS, zaakceptowania połączenia, oczekiwanie na połączenie, zamknięcie połączenia), zdarzeń systemowych, szczegółowe operacje na rejestrze systemu (utworzenie, skasowanie, zmiany nazwy klucza rejestru, wpisanie, odczytanie, skasowanie wartości rejestru).
10. Z poziomu zgromadzonych danych ma istnieć możliwość wykonywania akcji, np.: dla znalezionego pliku, możliwość jego ściągnięcia przez operatora, usunięcia, dodania do czarnej listy.

# **Wykrywanie zaawansowanych scenariuszy ataków:**

System ma umożliwiać wykrywanie zaawansowanych scenariuszy ataków, w szczególności:

1. System ma 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).
2. Uczenie maszynowe ma być wykorzystywane zarówno w analizie zachowań procesów jak i w analizie samych plików.
3. System ma wykrywać i analizować zachowania związane z nieautoryzowanym podniesieniem uprawnień podczas ich wykonywania oraz w związku ze zmianą parametrów systemu operacyjnego.
4. System musi wykrywać i reagować w czasie rzeczywistym na znane zagrożenia bazując na ich zachowaniu oraz reputacji, w szczególności:
   1. Blokowanie i reagowanie w ramach sekwencji wykonania danego zagrożenia bazując na heurystyce zachowań (np. podczas próby szyfrowania plików przez zagrożenie typu ransomware).
   2. Możliwość korzystania z komercyjnych baz reputacji plików (np. Virus Total lub równoważnych dostarczanych przez producenta).
   3. Możliwość wykrywania zagrożeń typu RAT (Remote Acces Trojan) na podstawie zachowań.
   4. Możliwość blokowania uruchomienia danego pliku, jak blokowania złośliwych akcji po uruchomieniu się danego zagrożenia.
   5. Blokowanie urządzeń USB należących do innych niż dozwolone przez politykę klas.
   6. Możliwość logowania użycia urządzeń USB, które mają interakcję z systemem operacyjnym.
   7. Wykrywanie i blokowanie podejrzanej aktywności w interpreterach języków skryptowych dla co najmniej:
      1. Powershell.
      2. CScript.
      3. Python.
      4. Makra pakiety Microsoft Office.

# **Zarządzanie fałszywymi alarmami (False Positives)**

W tym zakresie system ma zapewnić:

1. Ręczne zarządzanie fałszywymi alarmami poprzez możliwość oznaczania źle sklasyfikowanych zdarzeń, celem poprawnego ich interpretowania w przyszłości.
2. System ma posiadać mechanizmy automatycznej reklasyfikacji fałszywych alarmów (False Positives) w celu przeciwdziałania błędnej interpretacji zdarzeń w przyszłości.

# **Zarządzanie podatnościami**

System ma umożliwiać zarządzaniem podatnościami i reagowaniem na wykryte podatności na kontrolowanych hostach w zakresie:

1. Wykrywanie podatności w aplikacjach, które komunikują się za pomocą sieci z urządzeniami zewnętrznymi.

# **Architektura systemu zarządzania**

Architektura rozwiązania ma zapewnić:

1. Centralne zarządzanie.
2. Przechowywanie zdarzeń w systemie centralnym.
3. Funkcjonowanie systemu w modelu chmurowym – nie jest wymagane instalowanie po stronie lokalnej żadnych komponentów (z wyjątkiem instalacji agentów na chronionych hostach).
4. Dostęp do interfejsu konfiguracyjnego za pomocą przeglądarki internetowej poprzez WebUI.
5. Dostęp do/z systemu zarządzającego poprzez interfejs API.
6. Integrację z usługa katalogową Active Directory (user, group), rozwiązaniami typu Multi Factor Authentication oraz rozwiązaniami typu SSO (Single sign On).
7. Granularne zarządzanie funkcjami konfiguracyjnymi w oparciu o role (RBAC).
8. Zabezpieczenie przed próbami deinstalacji agenta z poziomu użytkownika oraz innych złośliwych procesów.

# **Zgodność z normami**

W tym zakresie system ma zapewnić:

1. Zgodność z normą PCI DSS.
2. Zgodność z normą GDPR, z możliwością usunięcia zapisanych informacji. Przeszukiwanie rekordów jest możliwe w oparciu o co najmniej: nazwę użytkownika, nazwę urządzenia, adres IP, adres MAC.
3. Eksport szczegółowego audyty funkcjonowania sytemu, zawierającego przynajmniej informacje o tym kto, kiedy i jakie wprowadzał zmiany w politykach, podejmował akcje, generował raport GDPR, logował się do systemu.

**Integracja z innymi rozwiązaniami**

1. System ma udostępniać API, za pomocą którego można wykonywać operacje: zarządzania, konfiguracji polityk oraz wprowadzania końcówek w stan izolacji.
2. Producent rozwiązania ma dostarczyć dokumentację interfejsu API, która jest niezbędna na etapie konfiguracji systemu.
3. System ma umożliwiać integrację z rozwiązaniami typu Network Access Control (NAC), umożliwiając zablokowanie lub izolację podejrzanego hosta, np. poprzez przeniesienie go do osobnego VLAN’u (kwarantanna).
4. System ma umożliwiać integrację z rozwiązaniem typu sandbox działającym lokalnie (on-premises) lub w chmurze.
5. System ma umożliwiać budowanie dopasowanej pod rozwiązanie („custom”) integracji z zewnętrznymi systemami/urządzeniami bezpieczeństwa poprzez wywoływanie własnych/zmodyfikowanych samodzielnie skryptów.
6. System ma możliwość integracji z systemami typu SIEM. Rejestrowane zdarzenie ma zawierać co najmniej następujące informacje:
   1. Nazwa urządzenia.
   2. Stan agenta na urządzeniu.
   3. Adres MAC.
   4. System operacyjny.
   5. Źródłowe IP.
   6. Nazwa procesu.
   7. Ścieżka procesu.
   8. Typ procesu.
   9. Istotność.
   10. Klasyfikacja.
   11. Reguła wykrywająca zagrożenie.
   12. Akcja.
   13. Hash procesu.
   14. Nazwa/rodzina/typ zagrożenia.
   15. Techniki MITRE.
   16. Cel ataku.
   17. Zdarzenia audytowe systemu, wykonane akcje, zmiany w politykach, itp.
7. System ma umożliwiać integrację z systemami ticketowymi, dostarczając wszystkie informacje dostępne w incydencie, które mogą być wykorzystane w celu automatycznego utworzenia zgłoszenia.

# **Testy wydajnościowe oraz funkcjonalne**

Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta.

# **Serwisy i licencje**

Wymagane są wszystkie niezbędne serwisy oraz licencje niezbędne do uruchomienia powyższych funkcji oraz do dostępu do baz zabezpieczeń dostarczanych przez producenta systemu. W szczególności powinny one obejmować:

1. Dostęp do centralnego systemu zarządzania działającego 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 lokalnej (model chmurowo/hybrydowy) **na okres [36] miesięcy**.
2. **Ochronę 500 hostów** (bez względu na to, czy oprogramowanie zostanie zainstalowane na systemach typu PC, czy serwerowych) **na okres [36] miesięcy**.
3. Usługę doradztwa technicznego świadczona przez producenta rozwiązania, wspomagająca proces implementacji oprogramowania w oparciu o najlepsze praktyki oraz szkolenie online producenta dotyczące funkcjonowania i administracji systemem dla 500, na okres minimum jednego roku.

# **Gwarancja oraz wsparcie**

1. System musi być objęty serwisem producenta **przez okres [36] miesięcy**, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.