Nr referencyjny nadany sprawie przez Zamawiającego	**TP 13/2023**

Podniesienie poziomu bezpieczeństwa systemów teleinformatycznych poprzez dostawę i wdrożenie systemu bezpieczeństwa klasy EDR dla Powiatowego Centrum Zdrowia w Kamiennej Górze Sp. z o.o.

1.Przedmiotem zamówienia jest podniesienie poziomu bezpieczeństwa systemów teleinformatycznych poprzez dostawę i wdrożenie systemu bezpieczeństwa klasy EDR dla Powiatowego Centrum Zdrowia w Kamiennej Górze Sp. z o.o

2.Zamówienie realizowane jest w ramach środków pochodzących z Funduszu Przeciwdziałania COVID-19 - podniesienie poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców dla potrzeb Powiatowego Centrum Zdrowia w Kamiennej Górze Sp. z o.o.

3. W ramach przedmiotu zamówienia Wykonawca jest zobowiązany:

a)Dostarczyć system bezpieczeństwa zgodne z opisem zawartym w Załączniku 1A do siedziby Zamawiającego w Kamiennej Górze przy ul. Bohaterów Getta 10
b)Udzielić licencji na dostarczony system
c)Wdrożyć wyznaczonych pracowników Zamawiającego zgodnie z wytycznymi w Załączniku 1A do formularza oferty

4. Wymagane właściwości/cechy użytkowe systemu bezpieczeństwa:

Lp.	Właściwości/cechy	Wymagane
1.	Wsparcie producenta	Minimum 5 Lat
2.	System bezpieczeństwa EDR (dalej system) musi być dostarczony w formie SaaS. Zamawiający wymaga, aby usługi SaaS były przechowywane i przetwarzane (włącznie z sandboxingiem) na terenie Polski, a producent systemu musi posiadać certyfikację SOC 2 type 2 oraz gwarantować dostępność usługi w ramach SLA co najmniej na poziomie 99,9%. – W przypadku wątpliwości Zamawiający może wezwać Wykonawcę do przedłożenia certyfikatu SOC 2 type 2 Producenta zaoferowanego rozwiązania.	TAK
3.	System wg ewaluacji MITRE Engenuity: Mitre Attack z 2022 musi posiadać skuteczność na poziomie minimum 95% w następujących kategoriach: a. widoczności zagrożeń (sekcja Visibility) b. analityki zagrożeń (sekcja Analytics Coverage)	TAK
4.	Wszystkie dane telemetryczne muszą być przechowywane przez system w centralnym i przeszukiwalnym repozytorium danych.	TAK
5.	System musi umożliwiać przeszukiwanie danych telemetrycznych przy pomocy kreatorów lub manualnie z wykorzystaniem kwerend. Reguły tworzenia kwerend muszą być opisane w dokumentacji systemu.	TAK
6.	System musi umożliwiać przekształcenie kwerendy do danych telemetrycznych w uruchamianą zgodnie z zadanym harmonogramem regułę korelacyjną generującą alarmy, jeśli kwerenda zwróciła jakiekolwiek rekordy.	TAK
7.	System musi umożliwiać definiowanie atomowych wskaźników kompromitacji w formie: SHA256, nazwy domenowej, adresu IPv4, adresu IPv6, ścieżki, nazwy pliku. Musi istnieć możliwość dodania znacznika ręcznie, zaimportowania znaczników z pliku i via REST API oraz oznaczenia reputacji, wiarygodności i okresu wygaśnięcia znacznika.	TAK
8.	System musi umożliwiać definiowanie złożonych wskaźników kompromitacji opisujących zachowanie procesu co najmniej w zakresie: operacji plikowych, uruchamianych procesów i ich parametrów, operacji sieciowych i operacji na rejestrze (tylko windows).	TAK
9.	System dla każdego wprowadzonego atomowego i złożonego wskaźnika kompromitacji musi wygenerować alarm(-y): a. jeśli znacznik został odszukany w historycznych danych telemetrycznych (zgromadzonych przed dodaniem wskaźnika) b. jeśli znacznik zostanie odszukany w nowych danych telemetrycznych	TAK
10.	System musi umożliwiać przekształcanie złożonych wskaźników kompromitacji w reguły prewencyjne co najmniej dla agenta dla Windows, macOS i Linux.	TAK
11.	System musi umożliwiać integrację z VirusTotal.	TAK

12.	System musi umożliwiać globalne blokowanie uruchamiania/ładowania plików binarnych o określonych SHA256.	TAK
13.	System w ramach odpowiedzi na incydent musi umożliwiać: a. Remediację ze wskazaniem kroków, które mogą być podjęte automatycznie i kroków, które należy zrealizować manualnie. Musi istnieć możliwość wyboru kroków remediacyjnych, które zostaną wykonane automatycznie. b. Uruchomienie skryptu python na endpointcie. c. Nawiązanie interaktywnego połączenia do linii poleceń na endpoitcie. d. Wstrzymanie procesu na endpointcie. e. Wyłączenie procesu na endpointcie. f. Izolację sieciową hosta. g. Dodanie adresu IP do listy publikowanej po https z uwierzytelnieniem w celu integracji z firewallami i innymi systemami bezpieczeństwa. h. Dodanie nazwy domenowej do publikowanej po https z uwierzytelnieniem w celu integracji z firewallami i innymi systemami bezpieczeństwa. i. Zmianę w rejestrze (tylko systemy Windows). j. Usunięcie pliku na endointcie. k. Przeniesienie pliku na endpointcie do kwarantanny. l. Wyszukanie pliku na innych hostach.	TAK
14.	System musi posiadać mechanizm wykrywania anomalii w ruchu sieciowym i w zachowaniu użytkownika i procesów.	TAK
15.	System musi obsługiwać co najmniej następujące poziomy powagi alarmów: informacyjny, niski, średni, wysoki i krytyczny.	TAK
16.	System musi automatycznie grupować powiązane alarmy w celu przyspieszenia i ułatwienia triażu i analizy incydentu.	TAK
17.	W ramach incydentu system musi grupować: a. Powiązanych z incydentem użytkowników b. Endpointy c. Pliki d. Domeny e. Adresy IP	TAK
18.	System dla alarmów zgrupowanych w ramach incydentu musi automatycznie tworzyć łańcuchy przyczynowo skutkowe reprezentujące zależności pomiędzy procesami wykorzystywanymi w trakcie ataku i powiązane dane telemetryczne, tak aby analityk mógł w łatwy sposób przeanalizować wykorzystywane techniki, określić zakres ataku, ustalić potencjalny cel ataku i zweryfikować czy cel został osiągnięty.	TAK
19.	System musi umożliwiać wgląd w raport z sandboxa dla plików powiązanych z incydentem i eksport tego raportu.	TAK
20.	Agent dla systemów Windows: a. Musi zbierać i wysyłać do systemu co najmniej następujące dane telemetryczne: i. Utworzenie nowego procesu i zakończenie procesu ii. Wszystkie operacje na plikach: tworzenie, zapisywanie, kasowanie, zmiana nazwy, przesunięcie, modyfikacja, link symboliczny iii. Ładowanie bibliotek DLL iv. Wstrzykiwanie do procesu v. Wszystkie operacje na socketach sieciowych dla TCP i UDP: accept, connect, create, listen, close, bind vi. Statystyki połączeń sieciowych vii. Praca z rejestrem: skasowanie wartości, ustawienie wartości, utworzenie klucza, kasowanie klucza, zmiana nazwy klucza b. Musi zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu poprzez wykrywanie prób wykorzystania co najmniej następujących technika eksploitacji: i. Przekierowanie APC ii. Obejście Data Execution Prevention iii. DLL Hijacking iv. Exploit Kit Fingerprinting v. JIT vi. Null Dereference vii. ROP viii. Structures exception handler hijackings ix. Heap Spray x. Kernel Privilege Escalation	TAK

	c. Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi umożliwiając skonfigurowanie co najmniej następujących mechanizmów: i. Weryfikacja sha256 w bazie threat intelligence producenta systemu ii. Analiza dynamiczna w sandboxie chmurowym producenta systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym hoście) iii. Lokalna analiza statyczna iv. Weryfikacja podpisu pliku binarnego v. Przeniesienie pliku binarnego do kwarantanny vi. Zablokowanie uruchomienia/załadowania złośliwego pliku binarnego vii. Zablokowanie uruchomienia pliku z przenośnej pamięci masowej USB viii. Zablokowanie uruchomienia pliku z innych lokalizacji sieciowych niż wskazane ix. Weryfikację i wykrycie groźnego zachowania procesu powstałego w wyniku uruchomienia/załadowania pliku binarnego x. Wykrywanie shellcodu'u ładowanego do pamięci xi. Wykrycie i przerwanie próby szyfrowania plików na dysku (ochrona przeciw ransomware). d. Musi wykrywać i blokować próbę wyłączenia Volume Shadow Copy Service (VSS). e. Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi makrami co najmniej w plikach Microsoft Word i Microsoft Excel umożliwiając skonfigurowanie co najmniej następujące mechanizmy: i. Weryfikacja sha256 w bazie threat intelligence producenta systemu ii. Analiza dynamiczna w sandboxie chmurowym producenta systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym hoście) iii. Lokalna analiza statyczna f. Musi zapewnić ochronę przed atakami wykorzystującymi legalne narzędzia systemowe w groźny sposób poprzez analizę złożonych łańcuchów przyczynowo-skutkowych i wykrywanie technik i taktyk stosowanych przez cyberprzestępców. g. Musi umożliwiać zablokowanie całego ruchu sieciowego (izolacji sieciowej) poza połączeniem do systemu. h. Musi posiadać możliwość manualnego wyłączenia izolacji sieciowej w przypadku, gdy agent utracił łączność z systemem. Wyłączenie izolacji sieciowej musi być zabezpieczone hasłem. Każdy endpoint musi posiadać własne hasło, tak aby można było je podać bezpiecznie użytkownikowi bez obawy, że inni użytkownicy zaczną wyłączać agenta. Hasło musi być automatycznie rotowane przez system nie rzadziej niż co dwa tygodnie.	

5.Usługa konfiguracji oraz instalacji

Zakres wdrożenia systemu typu EDR:
a)Aktywacja licencji dla systemu
b)Podstawowa konfiguracja systemu – dostęp dla administratorów
c)Konfiguracja mechanizmów i polityk wykrywania oraz reakcji na zagrożenia
d)Instalacja aplikacji klienckiej na przykładowych stacjach roboczych
e)Optymalizacja działania polityk z uwzględnieniem aplikacji używanych w środowisku Zamawiającego
f)Wykonanie schematu i opisu podłączenia systemu w infrastrukturze Zamawiającego

6.Oferowane rozwiązanie, oprócz spełnienia odpowiednich parametrów funkcjonalnych, winno zagwarantować bezpieczeństwo danych pacjentów i personelu medycznego oraz zapewnić wymagany poziom usług medycznych podczas eksploatacji.

7.Wykonawca winien zapewnić ciągłość pracy Szpitala (PCZ w Kamiennej Górze Sp. z o.o.) podczas prac wdrożeniowych. Jeżeli przerwa jest konieczna, to Wykonawca winien z minimum 2-dniowym wyprzedzeniem zgłosić ten fakt Zamawiającemu z podaniem czasu i daty przerwy, do akceptacji przez Zamawiającego.

8. Potwierdzeniem zrealizowania przez Wykonawcę całego zakresu objętego umową będzie protokół odbioru podpisany przez upoważnionych przedstawicieli stron.

9. Wykonawca na zakupione licencje udziela gwarancji na okres 5 lat.

10. Pracownicy wykonujący prace wdrożeniowe winni posiadać niezbędną wiedzę oraz doświadczenie w pracy z systemami informatycznymi.

11. Podana w Formularzu oferty cena musi uwzględniać dostarczenie licencji systemu bezpieczeństwa, instalacje oraz wdrożenie.

II. Informacje ogólne

12. Opis przedmiotu zamówienia opracowano zgodnie z zasadami określonymi w art. 99 ustawy Prawo zamówień publicznych (tj. Dz.U. z 2023 r., poz.1605 z późn.zm.). Jednakże w przypadku, gdy opis przedmiotu zamówienia zawiera wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty dostarczane przez konkretnego wykonawcę należy uznać, iż wskazaniu temu towarzyszą wyrazu „lub równoważny".

13. Zgodnie z art. 101 ust. 4 ustawy Prawo zamówień publicznych ilekroć w opisie przedmiotu zamówienia - przedmiot zamówienia opisany został przez odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych – Zamawiający dopuszcza zastosowanie rozwiązań równoważnym opisywanym a odniesieniu takiemu towarzyszą wyrazu „lub równoważne".

14. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego przedmiot zamówienia spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów, uwiarygodniających te rozwiązania.