Poznań dnia: 2025-10-31

Szpital Wojewódzki w Poznaniu
Dział Zamówień Publicznych
Juraszów 7/19
60-479 Poznań

WYKONAWCY
ubiegający się o zamówienie

Dotyczy: postępowania o udzielenie zamówienia publicznego:

Nazwa zamówienia:	Przedmiotem zamówienia jest zakup z wdrożeniem produkcyjnym:- infrastruktury cyberochrony transmisji danych; - narzędzi cyberochrony oraz usługi szkoleń dla personelu Szpitala Wojewódzkiego w Poznaniu z zakresu cyberbezpieczeństwa środowiska informatycznego i danych medycznych w tym środowisku..
Numer referencyjny:	SZW/DZP/118/2025

WYJAŚNIENIA TREŚCI SWZ

Zamawiający, **Szpital Wojewódzki w Poznaniu**

Dział Zamówień Publicznych, działając na podstawie art. 135 ust. 6 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2024 poz. 1320), udostępnia poniżej treść zapytań do Specyfikacji Warunków Zamówienia (zwanej dalej ”SWZ”) wraz z wyjaśnieniami:

Opis przedmiotu zamówienia - zadanie 2
5. EDR musi automatycznie reagować na pojawiające się zagrożenia, definiowane przez politykę w czasie zbliżonym do rzeczywistego, w autonomiczny sposób z komunikatami odpowiedzi bezpieczeństwa:
5.1 Zabij proces: Zatrzymuje procesy. Aktywna zawartość w dokumentach, plikach wykonywalnych i procesach podrzędnych jest zatrzymywana. Agent włącza funkcję zabicia procesu dla procesów, które działają wbrew normalnemu zachowaniu stacji końcowej lub nie pasują do działań aplikacji, w której ukrywa się proces.
5.2 Kwarantanna: zatrzymuje procesy, szyfruje plik wykonywalny i przenosi go na ograniczoną ścieżkę. Jeśli zagrożenie jest znane, agent automatycznie je unieszkodliwia, zanim będzie można je wykonać.
5.3 Odłącz się od sieci: (kwarantanna sieciowa lub izolacja sieciowa) Agent musi komunikować się tylko z konsolą zarządzającą. Stacja końcowa nie może komunikować się z innymi elementami w sieci. Wszystkie działania na konsoli zarządzania muszą działać niezależnie od stanu izolacji sieci agenta.
5.4 Napraw: Zatrzymuje procesy, poddaje kwarantannie pliki binarne, usuwa połączone biblioteki, usuwa pliki źródłowe i przywraca konfigurację systemu operacyjnego, aplikacji i ustawień użytkownika do stanu sprzed rozpoczęcia ataku.

5.5 Przywróć: przywraca stan stacji końcowej do stanu z momentu utworzenia migawki VSS (Volume Shadow Copy), cofając zmiany wprowadzone przez złośliwy proces i skojarzone z nim zasoby. Agent powinien autonomicznie i w czasie zbliżonym do rzeczywistego przywrócić dane z chronionego hosta w przypadku ataku z wykorzystaniem szkodliwego oprogramowania typu ransomware.

Pytanie nr 1

Czy Zamawiający dopuszcza rozwiązanie, którego system EDR nie podejmuje działań automatycznych oraz nie oferuje automatycznej izolacji punktów końcowych i działań napraw i przywróć. Działania automatyczne podejmuje agent oprogramowania antywirusowego. Izolacja dostępna jest tylko na żądanie. Działanie napraw podejmuje próbę dezynfekcji pliku.

6. EDR musi wspierać co najmniej następujące modele wdrożenia: SaaS (agent, usługa SaaS w chmurze), wdrożenie lokalne (urządzenie wirtualne) lub wdrożenie hybrydowe.

Stanowisko (wyjaśnienie) Zamawiającego: Zamawiający dopuszcza rozwiązanie którego agent oprogramowania antywirusowego dokonuje działań automatycznych, a izolacja jest dostępna na żądanie

Pytanie nr 2

Czy Zamawiający dopuszcza rozwiązanie, które nie oferuje wdrożenia hybrydowego? Rozwiązanie można wdrożyć z wykorzystaniem konsoli w chmurze lub konsoli lokalnej, jednocześnie korzystać można tylko z jednej konsoli.

14. EDR musi obsługiwać następujące formaty syslog: CEF, CEF2, RFC-5424, STIX i IOC. Rozwiązanie powinno obsługiwać certyfikaty SSL i X.509 do szyfrowania i uwierzytelniania transportu syslog.

Stanowisko (wyjaśnienie) Zamawiającego: Tak zamawiający dopuszcza.

Pytanie nr 3

Czy Zamawiający dopuszcza rozwiązanie, które nie obsługuje wymienionych formatów syslog? Obsługiwany jest format JSON.

15. EDR musi zapewniać możliwość wysyłania wiadomości tekstowych do użytkownika stacji końcowej, bezpośrednio z konsoli zarządzania, nawet kiedy agent pracujący na stacji, znajduje się w trybie izolacji sieci / kwarantanny sieciowej.

Stanowisko (wyjaśnienie) Zamawiającego: Tak zamawiający dopuszcza rozwiązanie które obsługuje format JSON.

Pytanie nr 4

Czy Zamawiający dopuszcza rozwiązanie, które nie oferuje dedykowanej funkcjonalności wysyłania komunikatów na stacje robocze? Z wykorzystaniem funkcji Remote Shell istnieje możliwości wysyłania komunikatów na stacje poprzez PowerShell.

16. EDR musi umożliwiać zintegrowane z usługą Active Directory, aby możliwe było automatyczne przypisywanie agentów do grup, w celu powiązania ich z zasadami AD. Konsola zarządzania NIE powinna łączyć się z usługą Active Directory bezpośrednio za pośrednictwem

programu ADFS ani żadnej innej metody uzyskiwania atrybutów usługi Device i User AD. Serwer zarządzania rozwiązaniem nie powinien mieć żadnych zależności od stanu usługi AD.

- distinguishedName
- dnshostname
- objectGUID
- name
- samaccountname
- objectSid

Wykorzystywane są powyższe atrybuty.

17. EDR musi zawierać dashboard pokazujący wszystkie komputery, oraz możliwość ich filtrowania na podstawie atrybutów takich jak: OS, typ stacji końcowej, wersja agenta, występujące podatności, atrybuty AD, informacyjne telemetryczne, adresacja IP, charakterystyki hardware, ilości CPU, adresy MAC, interfejsy, nazwa hosta, nazwa grupy, domena). Lista powinna być dostępna do przeglądania w celu inwentaryzacji hostów, stosowania akcji dla podzbioru stacji końcowych lub mapowania stacji końcowych do grup. Musi zapewniać opcję wyświetlenia szczegółów stacji, takie jak aspekty telemetrii, stan stacji, aplikacje oraz zapewniać następujące opcje działania: Odłącz/Połącz się od sieci (kwarantanna sieciowa, Uruchom ponownie OS, Zamknij system, Wyślij wiadomość do użytkownika, Odinstaluj agenta, Wyświetl zagrożenia.

Stanowisko (wyjaśnienie) Zamawiającego: Zamawiający dopuszcza możliwość wysłania komunikatów na stacje poprzez PowerShell

Pytanie nr 5

Czy Zamawiający dopuszcza rozwiązanie, które nie oferuje narzędzi do inwentaryzacji oraz działań takich jak zamknij system, wyślij wiadomość do użytkownika.

18. Polityka ochrony stacji musi umożliwiać odpowiedź na wykryte zagrożenie w oparciu o kwalifikację zdarzenia (zagrożenie: Malicious Threat czy podejrzane działanie: Suspicious Threat). Odpowiedź na zagrożenie powinna umożliwiać wybranie opcje alert-only lub opcje aktywnej ochrony w oparciu o klasyfikację zagrożenia. Aktywna odpowiedź na zagrożenie, powinna być wykonywana przez autonomicznego agenta, nawet jeśli chroniona stacja nie jest podłączona do sieci.

Stanowisko (wyjaśnienie) Zamawiającego: Zamawiający dopuszcza rozwiązanie bez funkcjonalności zamykania systemu, wysyłania wiadomości do użytkownika oraz narzędzi inwentaryzacji.

Pytanie nr 6

Czy Zamawiający dopuszcza rozwiązanie, które nie pozwala na dostosowanie reakcji w zależności od kwalifikacji zagrożenia?

19. EDR musi wytwarzać funkcjonalność lokalnej zapory ogniowej dla chronionej stacji końcowej. Ochrona firewall musi umożliwiać realizację unikalnych polityk dla każdej

chronionej grupy hostów. Reguły firewalla powinny umożliwiać uwzględnienie następujących parametrów: FQDN, IP, CIDR. Funkcjonalność musi być obsługiwana dla następujących systemów operacyjnych: Windows, Linux i MacOS.

Stanowisko (wyjaśnienie) Zamawiającego: Zamawiający dopuszcza rozwiązanie bez opcji dostosowania reakcji w zależności do zagrożenia

Pytanie nr 7

Czy Zamawiający dopuszcza rozwiązanie, którego zapora nie umożliwia uwzględnienia FQDN i CIDR oraz nie obsługuje systemów macOS i Linux?

25. EDR musi posiadać możliwość szczegółowego definiowania meta danych które będą zbierane z chronionych hostów (np. tylko informacje o procesach i zmianach w rejestrze bez kolekcjonowania informacji o operacjach na plikach).

Stanowisko (wyjaśnienie) Zamawiającego: Zamawiający dopuszcza rozwiązanie którego zapora nie umożliwia uwzględnienia FQDN i CIDR oraz nie obsługuje systemów macOS i Linux

Pytanie nr 8

Czy Zamawiający dopuszcza rozwiązanie, które nie pozwala na definiowanie meta danych zbieranych z punktów końcowych?

30. EDR musi pozwalać na dodawanie własnych skryptów do centralnego repozytorium wykorzystujących języki min. Powershell (Windows) i Bash (Linux, Mac).

31. EDR musi pozwalać na zdalne uruchomienie skryptów z centralnego repozytorium na wybranych stacjach końcowych. Wynik działania skryptów musi być dostępny lokalnie na stacji końcowej lub w konsoli centralnej.

32. Konsola centralna musi zapewniać śledzenie stanu działania poszczególnego wywołania skryptu (sukces/porażka/w toku).

Stanowisko (wyjaśnienie) Zamawiającego: Zamawiający dopuszcza rozwiązanie które nie pozwala na definiowanie meta danych zbieranych z punktów końcowych

Pytanie nr 9

Czy Zamawiający dopuszcza rozwiązanie, które nie pozwala na dodawanie i uruchamianie własnych skryptów z poziomu konsoli? Z wykorzystaniem Remote Shella można wysłać skrypt na stację roboczą, natomiast nie ma możliwości weryfikacji czy prawidłowo on się wykonał.

35. EDR musi mieć możliwość filtrowania zebranych informacji na temat podatności z wykorzystaniem co najmniej:
a) Nazwy stacji końcowej,
b) Nazwy aplikacji,
c) Producenta aplikacji,
d) Numeru CVE,
e) Ilości dni od detekcji,
f) Czy dana podatność jest w tym momencie wykorzystywana,
g) Poziom dojrzałości dostępnego exploita dla konkretnej podatności.

h) Poziom rekomendacji
Stanowisko (wyjaśnienie) Zamawiającego: Zamawiający dopuszcza rozwiązanie wykorzystujące Remote Shella do wysłania skryptu na stację roboczą.

Pytanie nr 10

Czy Zamawiający dopuszcza rozwiązanie, które nie oferuje filtrów takich jak: producent aplikacji, ilość dni od detekcji, czy dana podatność jest wykorzystywana, poziom dojrzałości exploita, poziom rekomendacji – zamiast poziomu rekomendacji dostępny filtr z oceną ryzyka.

36. EDR musi prezentować informacje o wszystkich wykrytych podatnością z podaniem co najmniej następujących informacji:

a) Numer CVE,

b) Poziom Severity,

c) NVD Base Score,

d) Czy dana podatność jest w tym momencie wykorzystywana,

e) Poziom dojrzałości dostępnego exploita dla konkretnej podatności,

f) Data publikacji danej podatności.

Stanowisko (wyjaśnienie) Zamawiającego: Tak zamawiający dopuszcza rozwiązanie które nie oferuje filtrów takich jak: producent aplikacji, ilość dni od detekcji, czy dana podatność jest wykorzystywana, poziom dojrzałości exploita,a zamiast poziomu rekomendacji dostępny jest filtr z oceną ryzyka.

Pytanie nr 11

Czy Zamawiający dopuszcza rozwiązanie, które nie podaje: NVD Base Score, czy dana podatność jest aktualnie wykorzystywana, poziomu dojrzałości oraz daty publikacji?

Stanowisko (wyjaśnienie) Zamawiającego: Tak zamawiający dopuszcza rozwiązanie które nie podaje NVD Base Score, czy dana podatność jest aktualnie wykorzystywana, poziomu dojrzałości oraz daty publikacji

Pytanie nr 12

W Funkcjach konsoli zdalnej punkt 37 OPZ, funkcjonalności z punktów od 1-42 mogą być realizowane przez konsolę chmurową, natomiast funkcjonalności z punktów 43-54 wyłącznie dla konsoli lokalnej. Konsola lokalna nie oferuje natomiast modułu zarządzania podatnościami. Niektóre funkcje są ekskluzywne dla konkretnego typu konsoli w rozwiązaniu, które chcielibyśmy zaoferować. Czy zamawiający dopuszcza konsolę która spełnia wszystkie wymagania z punktów funkcjonalności wymienionych w punktach od 1 – 42?

Stanowisko (wyjaśnienie) Zamawiającego: Tak zamawiający dopuszcza rozwiązanie, które spełnia wymagania konsoli opisane w podpunktach 1-42, w założeniu, że funkcjonalności dostępne, są z poziomu konsoli chmurowej.

Zamawiający
/-/ I Z-ca Dyrektora
ds. Administracyjnych
Krystyna Piątkowska