Centrum Usług Informatycznych we Wrocławiu
ul. Namysłowska 8, 50-304 Wrocław
Telefon: 0717779032
Adres email: cui@cui.wroclaw.pl

Wrocław, 09.11.2023

Dotyczy: postępowania prowadzonego w trybie przetargu nieograniczonego pn.: „**Dostawa licencji oprogramowania antywirusowego i oprogramowania EDR dla stacji roboczych i systemów zarządzanych przez CUI i Jednostki Gminy Wrocław wraz z wdrożeniem i wsparciem**”, sygnatura sprawy CUI-ZZ.3201.16.2023

Zamawiający, na podstawie art. 135 ust. 2 ustawy Prawo zamówień publicznych (t.j. Dz. U. z 2023 r. poz. 1605 ze zm.) – dalej ustawa Pzp, przekazuje odpowiedzi na wnioski o wyjaśnienie treści SWZ.

Ochrona stacji roboczych - specyfikacja równoważna

Wniosek nr 1:

Pytanie do pkt. 1:
Czy Zamawiający dopuści rozwiązanie, które oferuje zaawansowaną ochronę proaktywną oraz funkcjonalność XDR dla platform Windows 8.1 i nowszych oraz macOS Mojave 10.14 i nowszych?

Odpowiedź:

Zamawiający nie dopuszcza rozwiązania które oferuje zaawansowaną ochronę proaktywną oraz funkcjonalność XDR tylko dla platform Windows 8.1 i nowszych oraz macOS Mojave 10.14 i nowszych.

Oprogramowanie musi wspierać system Windows 7 (systemy 32 i 64 bitowe).

Wniosek nr 2:

Pytanie do pkt. 2:
Czy zamawiający dopuści rozwiązanie, które zapewnia agenta instalowanego na chronionej stacji w języku angielskim lub polskim, natomiast konsola centralna oraz dokumentacji dostępna jest w języku angielskim?

Odpowiedź:

Zamawiający dopuszcza przedstawione w pytaniu rozwiązanie.

Wniosek nr 3:

Pytanie do pkt. 5:
Czy Zamawiający dopuści rozwiązanie, które skanuje w „locie" pocztę przychodzącą POP3. Natomiast dla pozostałych przypadków, w tym ruchu zaszyfrowanego, niezależnie od protokołu skanowanie i analiza odbywa się podczas próby dostępu do odnośnika lub pliku stanowiącego załącznik wiadomości email. Takie podejście dzięki możliwość wykorzystania zaawansowanych silników analitycznych gwarantuje dużo wyższą skuteczność detekcji niż skanowanie „w locie".

Odpowiedź:

Zamawiający nie wyraża zgody na brak analizy „ w locie" dla ruchu zaszyfrowanego. Zamawiający wymaga, aby rozwiązanie sprawdzało zagrożenia przed potencjalną próbą dostępu przez użytkownika.

Wniosek nr 4:

Pytanie do pkt. 12:
Czy Zamawiający dopuści rozwiązanie, gdzie wysyłanie nowych zagrożeń do laboratoriów producenta odbywa się przez dedykowany portal na jawną prośbę Zamawiającego. System proaktywnej ochrony nigdy automatycznie nie wysyła plików (które mogą zawierać dane wrażliwe) do laboratoriów producenta.

Odpowiedź:

Zamawiający nie dopuszcza rozwiązania, w którym wysyłanie zagrożeń do laboratoriów producenta odbywa się przez dedykowany portal na jawną prośbę Zamawiającego

Wniosek nr 5:

Pytanie do pkt. 14:
Czy Zamawiający dopuści rozwiązanie, które posiada mechanizm kontroli aplikacji (tzw. Application Control), ale nie posiada funkcjonalności kontroli dostępności aktualizacji do danego oprogramowania. System koncentruje się na zabezpieczeniu użytkownika przed próbami uruchomienie aplikacji niebezpiecznych lub takich które nie są dozwolone wewnętrzną polityką organizacji.

Odpowiedź:

Zamawiający wymaga, aby przedstawiony system kontroli aktualizacji dotyczył systemu operacyjnego. Zamawiający nie przedstawił wymagań odnośnie kontroli aplikacji.

Wniosek nr 6:

Pytanie do pkt. 15:
Czy Zamawiający dopuści rozwiązanie, które posiada zaawansowaną funkcjonalność Device Control, ale nie posiada jawnie wyspecyfikowanej opcji blokowania urządzenia typu „Drukarka USB" – istnieje możliwość zablokowania portu USB, lub np. zablokowania portu USB i skonfigurowania wyjątków dla określonych pamięci przenośnych USB (bazując na numerze seryjnym), zamiast polityki blokującej Firewire, umożliwia blokowanie nowszego i bardziej powszechnego standardu – Thunderbolt.

Odpowiedź:

Zamawiający nie dopuszcza rozwiązania przedstawionego przez Wykonawcę. Rozwiązanie musi umożliwiać administratorowi kontrolowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

Wniosek nr 7:

Pytanie do pkt. 16:

Czy Zamawiający dopuści rozwiązanie, które najważniejsze informacje dotyczące parametrów chronionego systemu jak status polityki, przypisana polityka, adres IP, system operacyjny itp. prezentuje w czytelny sposób w centralnej konsoli zarządzającej, a generowane raportu uwzględniają informacje o detekcjach oraz wykrytych zagrożeniach.

Odpowiedź:

Zamawiający wymaga, aby rozwiązanie było wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, ostatniego połączenia do systemu zarządzania, daty ostatniego skanowania.

Wniosek nr 8:

Pytanie do pkt. 18:
Czy Zamawiający dopuści rozwiązanie, które umożliwia na zdefiniowanie zadania aktualizacji w oparciu o harmonogram, informacja o nieaktualnym silniku detekcji jest niezależna od jego maksymalnego wieku, system aktualizacje pobiera z sieci Internet? Dystrybucja aktualizacji może być wykonywania za pośrednictwem wskazach agentów (tzw. Upadate Agents), jednak wskazani agenci muszą mieć dostęp do sieci Internet. Oferowane rozwiązania jest systemem klasy SaaS gdzie wszystkie elementy centralne rozwiązania hostowane są w chmurze producenta, w związku z tym dostęp do sieci Internet w celu zarządzania ochroną na stacji (pośredni lub za pomocą proxy) jest wymagany. Producent zapewnia wysoką dostępność, skalowalność i aktualizację rozwiązania.

Odpowiedź:

Zamawiający nie wyraża zgody na rozwiązanie klasy SaaS gdzie wszystkie elementy centralne rozwiązania hostowane są w chmurze producenta.

Wniosek nr 9:

Pytanie do pkt. 19:
Czy Zamawiający dopuści rozwiązanie, które posiada mechanizm zapory ogniowej, ale nie umożliwia pracy w trybie: „tryb interaktywny – rozwiązanie

pyta się o każde nowo nawiązywane połączenie” oraz trybie „tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.” Rozwiązanie również nie posiada możliwości oceniania reguł zapory systemu Windows.

Odpowiedź:

Zamawiający wymaga, aby rozwiązanie posiadało zaporę osobistą oraz pracowało w jednym z czterech trybów:

a. tryb automatyczny,

b. tryb interaktywny,

c. tryb oparty na regułach,

d. tryb uczenia się.

Ochrona stacji roboczych – zarządzanie specyfikacja równoważna

Wniosek nr 10:

Pytanie do pkt. 2:
Czy Zamawiający dopuści rozwiązanie klasy SaaS, gdzie wszystkie elementy centralne rozwiązania hostowane są w chmurze producenta. Producent zapewnia wysoką dostępność, skalowalność i aktualizację rozwiązania?

Odpowiedź:

Zamawiający nie wyraża zgody na rozwiązanie klasy SaaS gdzie wszystkie elementy centralne rozwiązania hostowane są w chmurze producenta.

Wniosek nr 11:

Pytanie do pkt. 3:
Czy Zamawiający dopuści rozwiązanie klasy SaaS, gdzie wszystkie elementy centralne rozwiązania hostowane są w chmurze producenta. Producent zapewnia wysoką dostępność, skalowalność i aktualizację rozwiązania?

Odpowiedź:

Zamawiający nie wyraża zgody na rozwiązanie klasy SaaS gdzie wszystkie elementy centralne rozwiązania hostowane są w chmurze producenta.

Wniosek nr 12:

Pytanie do pkt. 12:
Czy Zamawiający dopuści rozwiązanie, w którym istnieje możliwość pełnego zarządzania agentem bezpieczeństwa zainstalowanym na stacjach, ale system nie umożliwia tworzenie skategoryzowanych szablonów zadań i tworzenie nowych zadań w obrębie szablonów.

Odpowiedź:

Zamawiający wymaga, aby rozwiązanie posiadało pełne zarządzanie stacjami z zainstalowanym klientem antywirusowym/agentem poprzez skategoryzowane szablony zadań oraz pozwalać na tworzenie nowych zadań w ramach danej kategorii.

Wniosek nr 13:

Pytanie do pkt. 13:
Czy Zamawiający dopuści rozwiązanie, które nie umożliwia wysłanie do systemu operacyjnego komend: wyłącz komputer, uruchom ponownie komputer, wyloguj, zainstaluj aktualizacje systemowe.

Odpowiedź:

Zamawiający nie wyraża zgody. Zamawiający podtrzymuje, że system musi pozwalać na wysyłanie komend do systemu operacyjnego, co najmniej: wyłącz komputer, uruchom ponownie komputer, wyloguj, zainstaluj aktualizacje systemowe

Wniosek nr 14:

Pytanie do pkt. 18:
Czy Zamawiający dopuści rozwiązanie klasy SaaS, gdzie wszystkie elementy centralne rozwiązania hostowane są w chmurze producenta. Producent zapewnia wysoką dostępność, skalowalność i aktualizację rozwiązania? Takie podejście

umożliwia łatwe zarządzenie stacjami znajdującymi się zarówno wewnątrz sieci organizacji jak i poza nią.

Odpowiedź:

Zamawiający nie wyraża zgody na rozwiązanie klasy SaaS gdzie wszystkie elementy centralne rozwiązania hostowane są w chmurze producenta.

EDR/XDR - specyfikacja równoważna

Wniosek nr 15:

Pytanie do pkt. 1:
Czy Zamawiający dopuści rozwiązanie, które oferuje zaawansowaną ochronę proaktywną oraz funkcjonalność XDR dla platform Windows 8.1 i nowszych oraz macOS Mojave 10.14 i nowszych?

Odpowiedź:

Zamawiający nie dopuszcza rozwiązania które oferuje zaawansowaną ochronę proaktywną oraz funkcjonalność XDR tylko dla platform Windows 8.1 i nowszych oraz macOS Mojave 10.14 i nowszych. Oprogramowanie musi wspierać system Windows 7 (systemy 32 i 64 bitowe).

Wniosek nr 16:

Pytanie do pkt. 2:
Czy zamawiający dopuści rozwiązanie, które zapewnia agenta instalowanego na chronionej stacji w języku angielskim lub polskim, natomiast konsola centralna oraz dokumentacji dostępna jest w języku angielskim?

Odpowiedź:

Zamawiający dopuszcza przedstawione w pytaniu rozwiązanie.

Wniosek nr 17:

Pytanie do pkt. 5:

Czy Zamawiający dopuści rozwiązanie klasy SaaS, gdzie wszystkie elementy centralne rozwiązania hostowane są w chmurze producenta. Producent zapewnia wysoką dostępność, skalowalność i aktualizację rozwiązania?

Odpowiedź:

Zamawiający nie wyraża zgody na rozwiązanie klasy SaaS gdzie wszystkie elementy centralne rozwiązania hostowane są w chmurze producenta.

Z wyrazami szacunku,

Dariusz Dauksz

Zastępca Dyrektora

Dokument podpisano podpisem elektronicznym w dniu:09.11.2023

Sprawę prowadzi:
Gabriela Nowak-Piechota

Informacje na temat przetwarzania danych osobowych przez CUI znajdują się na stronie BIP CUI