

Nr sprawy: RZP.271.48.2024.ZP3

Białe Błota, dnia 05.12.2024 r.

Dotyczy postępowania pn.:

Rozwiązanie antywirusowe XDR wraz z wdrożeniem w ramach Cyberbezpieczny Samorząd.

WYJAŚNIENIA ZAPYTANIA OFERTOWEGO

- I. W związku ze zwróceniem się Wykonawców do Zamawiającego o wyjaśnienie, Zamawiający przekazuje treść zapytań wraz z wyjaśnieniami:

Pytania- zestaw 2

Pytanie 1.

Zamawiający stosując nazewnictwo 1-Click Remediation oraz 1-Click Rollback, wskazuje na rozwiązanie SentinelOne, co jest jasno opisane na stronie producenta oraz stronach/ulotkach partnerów, którzy zajmują się dostarczaniem tej technologii.

<https://www.sentinelone.com/blog/rapid-response-with-xdr-one-click-remediations/>

https://sprint.pl/_default/ulotki/SPRINT_ulotka-sentinelone_WEB%20%28003%29_1.pdf -

strona nr 2

<https://lintusolutions.com/sentinelone/> - Patented 1-Click Remediation & Rollback.

Powoduje to ograniczenie konkurencji tylko i wyłącznie do tego rozwiązania. W związku z tym prosimy o wykreślenie tego punktu albo nadanie mu brzmienia: Za pomocą mechanizmów i możliwości konsoli skutki ataku są szybko usuwane, a użytkownicy mogą wrócić do pracy w ciągu kilku minut.

Odpowiedź 1.

Zamawiający nie wyraża zgody na zmianę.

Podkreślamy, że wymóg ten nie ogranicza konkurencji, lecz stanowi precyzyjne określenie oczekiwanego poziomu funkcjonalności systemu, wynikającego z potrzeb Zamawiającego. Naszym celem jest zapewnienie maksymalnej ochrony i szybkiej reakcji w sytuacjach kryzysowych, takich jak usuwanie skutków złośliwego zaszycrowania plików.

Należy zaznaczyć, że wskazane funkcjonalności, choć nazwane „1-Click Remediation” i „1-Click Rollback” w materiałach promocyjnych niektórych producentów, są dostępne również

w innych technologiach spełniających wymagania OPZ. Zamawiający nie odnosi się do konkretnych rozwiązań czy producentów, a jedynie do oczekiwanej funkcjonalności, którą można zaimplementować w różnych technologiach dostępnych na rynku.

Pytanie 2.

Czy Zamawiający punkt: Firewall Control (kontrola zapory firewall) - poprzez kontrolowanie połączeń urządzeń z siecią w obu kierunkach, z rozpoznaniem lokalizacji; uzna za spełniony w przypadku kiedy: System pozwala na zarządzanie firewallem wbudowanym w system operacyjny, definiowanie polityk, które są w następnej kolejności implementowane na określonej grupie hostów. Polityki te pozwalają na ujednolicenie reguł w kontekście ruchu wychodzącego lub przychodzącego w odniesieniu do tych grup, dzięki temu możemy w łatwy sposób zarządzać konfiguracją firewall na urządzeniach końcowych. Ponadto system pozwala na izolację hosta - po wykryciu infekcji jedną z czynności (wykonana manualnie lub automatycznie za pomocą wbudowanego SOARa) może być odcięcie hosta od sieci celem zaniechania rozprzestrzeniania się infekcji. Jeżeli nie, to prosimy o informację co Zamawiający ma na myśli.

Odpowiedź 2.

Zamawiający wyjaśnia, iż zaproponowane rozwiązanie nie spełni warunków wskazanych w OPZ.

Wymóg dotyczący „kontrolowania połączeń urządzeń z siecią w obu kierunkach, z rozpoznaniem lokalizacji” został sformułowany w sposób celowy, aby zapewnić, że rozwiązanie umożliwi precyzyjne zarządzanie ruchem sieciowym oraz wgląd w lokalizację urządzeń, co jest istotne dla zapewnienia bezpieczeństwa środowiska IT.

Wskazane przez Państwa rozwiązanie, które polega na zarządzaniu firewallem wbudowanym w system operacyjny oraz definiowaniu polityk stosowanych na grupach hostów, nie w pełni odpowiada wymaganiom OPZ. W szczególności:

- 1. Kontrola kierunków ruchu: OPZ wymaga aktywnej kontroli połączeń w obu kierunkach (przychodzących i wychodzących) w czasie rzeczywistym, a nie jedynie zarządzania politykami z poziomu hosta.*
- 2. Rozpoznanie lokalizacji: Wymóg OPZ obejmuje rozpoznanie lokalizacji połączeń, co jest niezbędne do pełnego monitorowania i ochrony sieci. Zarządzanie regułami na*



poziomie hosta nie zapewnia tej funkcjonalności w sposób, który spełnia nasze potrzeby.

- 3. Izolacja hosta: Chociaż funkcja izolacji hosta jest cenna, stanowi ona jedynie dodatkowy element ochrony, a nie podstawowy wymóg dotyczący kontroli zapory firewall.*

W związku z powyższym zaproponowana przez Państwa funkcjonalność nie spełnia określonych wymagań.

- II.** Wyjaśnienia, stają się obowiązujące dla wszystkich Wykonawców ubiegających się o udzielenie przedmiotowego zamówienia z dniem ich zamieszczenia na dedykowanej platformie zakupowej oraz stronie internetowej Zamawiającego w miejscu udostępnienia zapytania ofertowego.

z up. Wójta
Zastępcy Wójta

Natalia Zielińska

INSPIKTOR

Claudia Jesi - Skorzeńska

p.o. Kierownika Referatu
Zamówień Publicznych
i Pozyskiwania Funduszy

Katarzyna Robojnikowska

