

Kamienna Góra, 06.02.2024 r.

WYJAŚNIENIA I ZMIANA TREŚCI SWZ

Nazwa postępowania: **Zakup, dostarczenie i wdrożenie w środowisku informatycznym Dolnośląskiego Centrum Rehabilitacji i Ortopedii Sp. z o.o. w Kamiennej Górze systemu przeciwdziałającego cyberzagrożeniom, umożliwiającego ich wykrywanie przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi**

Nr referencyjny nadany sprawie przez Zamawiającego: **DI-Z.26.3.2024**

- I. Działając na podstawie art.284 ust.2 i 6 oraz art.286 ust.1 i 7 ustawy z dnia 11 września 2019 roku Prawo Zamówień Publicznych (tj. Dz.U. z 2023 r., poz.1605 z późn.zm. – dalej ustawa Pzp) Zamawiający informuje, że wpłynęły zapytania o następującej treści:

Pytanie nr 2:

W punkcie 3 załącznika A „Logi pozyskiwane z systemów Microsoft Windows nie mogą wymagać instalowania dedykowanego oprogramowania bezpośrednio na tych systemach.”

Pytanie:

Czy dopuszczalna jest zastosowanie pozyskiwanie logów z systemów Microsoft Windows poprzez zastosowanie agenta ? Jest szczególnie korzystne, gdy potrzebna jest głęboka widoczność i kontrola nad procesami systemowymi, na przykład w punktach końcowych lub systemach o znaczeniu krytycznym. Systemy te często wymagają takiego poziomu szczegółowego monitorowania, zarządzania i kontroli, jaki może zapewnić jedynie rozwiązanie oparte na agentach.

Na przykład możliwość szczegółowego filtrowania zdarzeń systemu Windows przy użyciu wyrażeń WEF takich jak XPath.

Odpowiedź na pytanie nr 2:

Oferowane rozwiązanie musi obsługiwać pełną telemetrię, dlatego dla komputerów, na których nie ma możliwości zainstalowania agenta, musi być możliwość pełnej analizy zdarzeń, np: poprzez przekierowanie dziennika zdarzeń do oferowanego rozwiązania. W związku z tym nie ma możliwości, aby z tego wymagania zrezygnować.

Pytanie nr 3:

W punkcie 8 załącznika A „Proces normalizacji musi wspierać następujące typy składni: CEF, LEEF, URI, SYSLOG (zgodny z RFC 3164) i automatycznie tworzyć na ich podstawie pola i ich wartości zgodne z zasadami określonymi przez te składnie. Parsowanie powyższych składni nie może być realizowane za pomocą wyrażeń regularnych.”

Pytanie:

Czy zgodność ze standardem dla Syslog można rozszerzyć na Syslog RFC 5424 ?

Odpowiedź na pytanie nr 3:

Tak. Oferowane rozwiązanie musi wspierać oba standardy, zarówno RFC 3164, jak i RFC 5424, ze względu na złożoność środowiska Zamawiającego.

Pytanie nr 4:

W punkcie 143 załącznika A „Funkcjonowanie rozwiązania musi umożliwiać konfigurację „on-premise”, w której wszystkie funkcjonalności oraz przetwarzanie danych będzie się odbywać całkowicie w infrastrukturze zamawiającego, zapewniając tym samym możliwość konfiguracji systemu w strefie odseparowanej od sieci Internet.”

Pytanie:

Czy zamawiający dopuści zmianę warunku w pkt. 143 załącznika A dopuszczając rozwiązanie w oparciu o konfigurację „cloud and proxy analytics gateway on-premise” ? Zmiana z zastosowania rozwiązania z wykorzystaniem kolektora proxy i brak możliwości zapewnienia wszystkich funkcjonalności przetwarzania danych przy parametrach sprzętowych serwera on-promise opisanych sekcji „Wymagania dla serwera dla systemu” załącznika A.

Odpowiedź na pytanie nr 4:

Nie, Zamawiający wymaga architektury która umożliwi osiągnięcie pełnej funkcjonalności w konfiguracji "on-premise". Podejście to umożliwia zapewnienie elastyczności związanej z późniejszymi kosztami utrzymania, wówczas Zamawiający - gdy będzie taka potrzeba - będzie mógł przenieść część komponentów do dowolnej chmury, która będzie opłacalna kosztowo. Natomiast jeżeli zmieni się model rozliczeniowy na inny, który nie jest już korzystny, to będzie miał możliwość przeniesienia do innej chmury albo powrotu do przetwarzania w modelu on-premise. Dodatkowo z punktu widzenia bezpieczeństwa wymagalność konfiguracji w chmurze wiąże się z dodatkowym ryzykiem, zarówno w kontekście dostępności, jak i poufności. Uwzględniając powyższe uzasadnienie, Zamawiający nie dopuszcza zmiany wymogu.

Pytanie nr 5:

W punkcie 109 załącznika A " Architektura rozwiązania musi w pełni wspierać konfigurację niezawodnościową, zapewniającą zarówno pełną redundancję w zakresie, odbierania logów i ich przechowywania, korelacji oraz reakcji na zagrożenia jak i możliwość zastosowania konfiguracji o ograniczonej redundancji do najważniejszych dla zamawiającego źródeł danych."

Pytanie.

Czy zamawiający dopuszcza rozwiązanie wykorzystujące konfigurację „cloud and proxy analytics gateway on-premise” ?

Odpowiedź na pytanie nr 5:

Uwzględniając Odpowiedź na pytanie nr 4, Zamawiający nie dopuszcza rozwiązania wskazanego w pytaniu.

-
- II. Zamawiający informuje, że na podstawie art. 284 ust.3 ustawy Pzp zmienia terminy składania i otwarcia ofert określone w pkt 26.1. i 27.1. Części I SWZ w następujący sposób:

Nowy termin składania ofert: 09.02.2024 r. godz.10:00

Nowy termin otwarcia ofert: 09.02.2024 r. godz.11:00

Skutkiem powyższej zmiany, zmianie ulega brzmienie pkt 24.1. Części I SWZ, który przyjmuje następujące brzmienie:

„24.1. Wykonawca jest związany złożoną ofertą od dnia upływu terminu składania ofert do dnia 09.03.2024 r.”

-
- III. Zamawiający informuje, że pytania i odpowiedzi oraz zmiany stają się integralną częścią specyfikacji warunków zamówienia i będą wiążące przy składaniu ofert. Pozostałe warunki nie ulegają zmianie.

Prezes Zarządu

Artur Mazur