

Włodawa dnia 13.06.2024 r.

Znak postępowania: WO.272.2.4.2024

UCZESTNICY POSTĘPOWANIA

Dotyczy: odpowiedzi dotyczących postanowień Specyfikacji Warunków Zamówienia w postępowaniu pt.: *Dostawa rozwiązań podnoszących poziom cyberbezpieczeństwa systemów teleinformatycznych oraz usługa audytu bezpieczeństwa systemów IT w Starostwie Powiatowym we Włodawie.*

Na podstawie art. 284 ust. 2 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tj. Dz.U.2023.poz. 1605 z późn. zm.), Zamawiający udziela odpowiedzi na pytania zadane przez uczestników postępowania.

Pytania i odpowiedzi

Pytanie nr 1

Dotyczy załącznika nr 2, Punkt 3: Oprogramowanie antywirusowe

Obecny zapis:

"Należy skonfigurować konsolę w chmurze, podłączyć do konsoli wszystkie stacje robocze, skonfigurować konsolę wg zaleceń producenta,..."

Pytanie:

Czy zamawiający dopuszcza, aby w ramach wdrożenia podłączyć tylko "przykładowe (maks. 3) stacje robocze"?

Uzasadnienie pytania:

Wdrożenie tylko przykładowych stacji pozwoli zamawiającemu w łatwy i efektywny sposób dokonać wdrożenia na pozostałych stacjach natomiast obniży koszty oferty.

Odpowiedź: Zamawiający wyraża zgodę, aby w ramach wdrożenia podłączyć tylko "przykładowe (maks. 3) stacje robocze".

Pytanie nr 2

Dotyczy załącznika nr 2, Punkt 3: Oprogramowanie antywirusowe

Obecny zapis: "System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit."

W związku z końcem wsparcia dla systemów Windows 7 i 8.x, oraz polityką EOL producenta ESET (obecnego rozwiązanie zamawiającego) czy zamawiający dopuszcza "wsparcie instalacji aplikacji klienckiej tylko w środowisku MS Windows 10/11"

Odpowiedź: Zamawiający wyraża zgodę.

Pytanie nr 3

Dotyczy załącznika nr 2, Punkt 4: Oprogramowanie DLP.

Obecny zapis: "Wymagane jest dostarczenie licencji bezterminowej dla 100 urządzeń..."

Czy zamawiający dopuszcza aby licencjonowanie dla oprogramowania DLP bazowało na użytkownikach, a nie na urządzeniach?

Uzasadnienie: Chcielibyśmy zaoferować oprogramowanie DLP (Safetica), które w takim właśnie modelu jest licencjonowane.

Odpowiedź: Zamawiający wyraża zgodę.

Pytanie nr 4

Dotyczy załącznika 2, punkt 8.17 Opcjonalny moduł EDR:

Ze względu na to, iż chcielibyśmy złożyć ofertę na rozwiązanie EDR z pakietu ESET, którego zamawiający używa, proszę o informację:

Czy zamawiający zgadza się aby licencja była licencją terminową, której ważność pokrywa się z ważnością wsparcia.

Odpowiedź: Zamawiający wyraża zgodę.

Pytanie nr 5

Dotyczy załącznika 2, punkt 8.17 Opcjonalny moduł EDR:

Zapis obecny:

"Rozwiązanie musi umożliwiać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy."

Czy zamawiający dopuszcza rozwiązanie, które posiada możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający.

Odpowiedź: Zamawiający wyraża zgodę.

Pytanie nr 6

Zamawiający podzielił przedmiotowe zamówienia na dwie części:

- Część 1 (Pakiet nr 1): Dostawa sprzętu i oprogramowania wraz z wdrożeniem i świadczeniem usług gwarancyjnych;
- Część 2 (Pakiet nr 2): Audyt bezpieczeństwa systemów IT.

Natomiast opis przedmiotu zamówienia nie wskazuje które czynności dotyczą części nr 1 a które części nr 2 przedmiotowego postępowania. Tym samym proszę o dokładne określenie które zapisy załącznika nr 2 (OPZ) dotyczą części nr 1 przedmiotowego postępowania, a które części nr 2

Odpowiedź: Zamawiający wyjaśnia, że Część 2 zamówienia dotyczy jedynie realizacji zakresu zgodnie z OPZ rozdział 2 Ogólny opis przedmiotu zamówienia pozycja nr 17: *Audyt bezpieczeństwa – końcowy. Analiza poziomu bezpieczeństwa po zakończeniu projektu. Weryfikacja osiągnięcia założonych celów projektu.*

Pytanie nr 7

Czy zamawiający w ramach świadczenia usługi SOC wymaga pełnienia roli osoby odpowiedzialnej za kontakt z odpowiednim CSIRTem?

Odpowiedź: Zamawiający wymaga pełnienia roli osoby odpowiedzialnej za kontakt z odpowiednim CSIRTem

Pytanie nr 8

Czy zamawiający oczekuje świadczenia usługi SOC na rozwiązaniu komercyjnym czy dopuszcza wykorzystanie rozwiązania opensource?

Odpowiedź: Zamawiający dopuszcza wykorzystanie rozwiązania opensource.

Pytanie nr 9

Czy czas podjęcia i realizacji zdarzenia obejmuje jedynie okres dostępności usługi tj. godziny 8.00 - 17.00 w dni robocze czy zamawiający wymaga zapewnienia opisanych warunków SLA w trybie 24/7/365?

Odpowiedź: Zamawiający wymaga zapewnienia opisanych warunków SLA w trybie 24/7/365.

Pytanie nr 10

W związku z bardzo szerokim zakresem wdrożenia obejmującym bardzo różnorodne produkty zwracamy się z prośbą o wydłużenie terminu składania ofert. Prośbę swoją motywuję faktem iż w celu prawidłowego i racjonalnego oszacowania ceny wymagana jest współpraca ekspertów z wielu dziedzin IT, cyberbezpieczeństwa i systemów zarządzania, a ilość dokumentacji zarówno technicznej jak i cenowej do przygotowania w ramach niniejszego postępowania jest bardzo duża. Wnoszę o wydłużenie terminu składania ofert do 21 czerwca 2024 roku.

Odpowiedź: Zamawiający nie wyraża zgody na wydłużenie terminu składania ofert.

Pytanie nr 11

Czy dopuszczają Państwo zmianę wzoru umowy na wzór Wykonawcy ?

Odpowiedź: Zamawiający nie wyraża zgody na zmianę wzoru umowy.

Pytanie nr 12

Czy dopuszczają Państwo zmianę § 9 Prawa autorskie na Licencja w zakresie wykorzystania dokumentów ?

Odpowiedź: Zamawiający nie wyraża zgody.

Pytanie nr 13

W związku z podzieleniem Państwa zamówienia na dwie części, chciałabym uzyskać odpowiedź, co dokładnie znajduje się w części drugiej Państwa zamówienia, ponieważ z załącznika SWZ wynika tylko Audyt Bezpieczeństwa Informacji, zaś w załączniku nr 2 - OPZ, są również szkolenia z Cyberbezpieczeństwa, aktualizacja dokumentacji SZBI oraz dwa Audytu wstępny i końcowy, czy te usługi składają się na część drugą zamówienia ?

Odpowiedź: Zamawiający wyjaśnia, że Część 2 zamówienia dotyczy jedynie realizacji zakresu zgodnie z OPZ rozdział 2 Ogólny opis przedmiotu zamówienia, pozycja nr 17: *Audyt bezpieczeństwa – końcowy. Analiza poziomu bezpieczeństwa po zakończeniu projektu. Weryfikacja osiągnięcia założonych celów projektu.*

Pytanie nr 14

Zapytanie jest modyfikacją wcześniejszego zapytania:

Dotyczy załącznika nr 2, Punkt 3: Oprogramowanie antywirusowe

Obecny zapis:

"System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit."

W związku z końcem wsparcia dla systemów Windows 7 i 8.x, oraz polityką EOL producenta ESET (obecnego rozwiązanie zamawiającego), czy zamawiający dopuszcza rozwiązanie, które będzie wspierało instalację aplikacji klienckiej pod systemem Windows 10 oraz Windows 11 za pomocą najnowszej wersji produktu oraz będzie wspierało systemy Windows 7, 8 oraz 8.1 za pomocą starszej wersji produktu?

Odpowiedź: Zamawiający dopuszcza rozwiązanie, które będzie wspierało instalację aplikacji klienckiej pod systemem Windows 10 oraz Windows 11 za pomocą najnowszej wersji produktu oraz będzie wspierało instalację aplikacji klienckiej pod systemy Windows 7, 8 oraz 8.1 za pomocą starszej wersji produktu.

SEKRETARZ

mgr Jadwiga Szaprańska

