

Warszawa, 20 października 2023 roku

Wszyscy Wykonawcy

Uprzejmie informujemy, że do Zamawiającego wpłynęły zapytania dotyczące Specyfikacji Warunków Zamówienia w postępowaniu przetargowym na Dostawa wraz z wdrożeniem klastra sprzętowego wysokiej dostępności w postaci dwóch urządzeń sieciowych o funkcjonalności load balancera”, nr referencyjny: **BZzp.261.118.2023** Przekazujemy Państwu wyjaśnienia na otrzymane zapytania:

Pytanie 1:

Zamawiający w wymaganiach OPZ pkt 1.37: "Klucze prywatne zapisywane na dysku urządzenia muszą być zaszyfrowane" opisał funkcjonalność, która polega na szyfrowaniu haseł i kluczy SSL przechowywanych na oferowanej platformie. Czy ze względów bezpieczeństwa i ochrony prywatności Zamawiający wymaga, aby wymagana funkcjonalność była realizowana w oparciu o unikalny klucz przechowywany na dedykowanym układzie sprzętowym (np EPROM) na oferowanej platformie sprzętowej?

Odp.

Tak zamawiający wymaga unikatowego klucza przechowywanego na dedykowanym układzie np. eprom.

Pytanie 2:

W związku z szeregiem technologii bezpieczeństwa oczekiwanych przez Zamawiającego (m.in. firewall stanowy, web applicaiton firewall) i wymaganej z tego powodu eksperckiej wiedzy jaką powinien posiadać Wykonawca w odniesieniu do zaoferowanego w postępowaniu przedmiotu zamówienia, prosimy o doprecyzowanie zapisów SWZ i tym samym: Czy Zamawiający wymaga, aby Wykonawca posiadał referencje wskazujące na co najmniej jedną dostawę urządzeń sieciowych tego samego producenta, jak zaoferowane w tym postępowaniu przez Wykonawcę urządzenia sieciowe, o wartości co najmniej 1 000 000 PLN brutto (słownie: jeden milion złotych).

Odp.:

Zamawiający nie dokonuje zmiany treści warunku udziału w postępowaniu. Warunek jest opisany precyzyjnie i jego wykładnia sprowadza się do spełnienia wymogu dostarczenia

urządzeń sieciowych o funkcjonalności Load Balancera w ramach jednej dostawy. Treść warunku nie dotyczy kwestii produkcyjnej, czy też powiązań produktowych.

Pytanie 3:

Zamawiający w OPZ opisał funkcjonalność "Rozwiązanie powinno zawierać system sztucznej inteligencji analizujący na bieżąco ruch i wykrywające ilościowe anomalie ruchu". W związku z wielowektorowym charakterem cyberataków, niezwykle trudne jest ich blokowanie przy jednoczesnym braku wpływu na prawidłowy (legalny) ruch pochodzący od prawdziwych użytkowników.

Czy Zamawiający wymaga, aby w ramach tej funkcjonalności algorytmy sztucznej inteligencji dynamicznie generowały sygnatury ataków zarówno dla warstwy sieciowej (L3/4) jak i aplikacyjnej (w szczególności dla DNS oraz HTTP) i na ich podstawie precyzyjnie blokowały ataki?

Odp.:

Tak, zamawiający potwierdza.

Pytanie 4:

W środowiskach aplikacyjnych obecnie obserwujemy dużą zmienność i dynamikę. Czy w związku z tym Zamawiający wymaga bardziej zaawansowanych i przez to dostosowanych do dynamicznych środowisk aplikacyjnych metod load balancingu takich jak:

- dynamiczna ważona dla usługi
- dynamiczna ważona dla serwera
- obserwowana
- przewidywana

Odp.:

Zamawiający wskazuje, że nie jest to objęte podstawowym wymaganiem, ale jest to dodatkowo punktowane w ramach kryterium oceny ofert.

**z up. Kierownik
Działu Zamówień Publicznych
Grzegorz Śledziwski**

/podpis na oryginale/