Marszałek
Województwa Lubelskiego

Lublin, 22.10.2020 r.

OP-IV.272.84.2020.BRP

Wykonawcy

Wyjaśnienia oraz zmiana treści Specyfikacji Istotnych Warunków Zamówienia

Zamawiający: Województwo Lubelskie z siedzibą w Lublinie, na podstawie art. 38 ust. 2 i 4 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (tj. Dz. U. z 2019 r. poz. 1843 z późn. zm.) w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego na **Wdrożenie systemu do zarządzania bezpieczeństwem teleinformatycznym wraz z 36-miesięcznym wsparciem serwisowym**, dokonuje następujących wyjaśnień oraz zmian treści Specyfikacji Istotnych Warunków Zamówienia:

Zmianie ulega termin składania i otwarcia ofert:

Termin składania ofert: do dnia 16 listopada 2020 r., do godz. 11:00
Termin otwarcia ofert: dnia 16 listopada 2020 r., o godzinie 11:30

Powyższe zmiany stają się integralną częścią SIWZ.
Zamawiający wprowadza adekwatne zmiany w ogłoszeniu.

Pytanie 1: Dot. punktu nr 3 OPZ z załącznika nr 1. Czy zamawiający zapewni systemy operacyjne na potrzeby oferowanego rozwiązania np. Windows 2019 Standard Server pod bazę danych i poszczególne komponenty oferowanego systemu?

Odp: Zamawiający nie dysponuje licencjami Windows 2019 Standard Server pod poszczególne komponenty oferowanego systemu.
Zamawiający dysponuje następującym środowiskiem na realizację oferowanego rozwiązania:
Klastrem zbudowanym z VMWare składającym się z 5 serwerów fizycznych HP ProLiant BL460c, posiadającym licencje MS Windows 2012 Datacenter w poniższej konfiguracji:
Serwer HP ProLiant BL460c Gen8 z dwoma procesorami Intel(R) Xeon(R) CPU E5-2650 v2 @ 2.60GHz ,8 rdzeni fizycznych każdy – 2 szt..

W związku z powyższym w Załączniku nr 1 do SIWZ - Opis Przedmiotu zamówienia, Zamawiający wprowadza zmianę treści pkt 3.

Urząd Marszałkowski Województwa Lubelskiego w Lublinie
20-029 Lublin, ul. Artura Grottgera 4, tel. 81 44 16 600, fax 81 44 16 602
marszalek@lubelskie.pl

Pkt 3 otrzymuje brzmienie:

„3. Zainstalowanie i skonfigurowanie Systemu w środowisku Zamawiającego - środowisko wirtualne. Wykonawca dostarczy licencję na niezbędny do działania systemu silnik bazy danych oraz system operacyjny dla środowiska złożonego z 2 serwerów dwuprocesorowych 8 rdzeniowych działających w klastrze VMWare. Wykonawca odpowiada za właściwe sparametryzowanie zarówno systemu operacyjnego jak i silnika bazy danych.”.

Pytanie 2: Dot. punktu 106A OPZ z załącznika nr 1.
Jeśli oferowany system ma być systemem nadrzędnym do zarządzania incydentami to czy zamawiający dopuszcza wysyłanie alertów lub incydentów z systemu SIEM do oferowanego systemu poprzez syslogi.

Odp: Zamawiający dopuszcza wysyłanie alertów i incydentów z systemu SIEM do oferowanego systemu poprzez syslogi.

Pytanie 3: Dot. punktu 106 B / D OPZ z załącznika nr 1.
W niniejszym postepowaniu Zamawiający planuje zakup nowego systemu do zarządzania incydentami i z naszego doświadczenia i praktycznych implementacji u klientów wynika, iż nie ma sensu prowadzenia dwóch systemów do zarządzania incydentami, bo komplikuje to tylko proces obsługi incydentów. W związku z tym czy zamawiający dopuszcza spełnienie tych wymagań poprzez wystawienie API w oferowanym systemie zarządzania bezpieczeństwem, które będą mogły być pobierane jeżeli jest taka możliwość do obecnego systemu SIEM. W innym przypadku trzeba będzie budować 3 system, który będzie integrował statusy obsługi incydentów oraz komentarzy między obecnym systemem SIEM a oferowanym w postępowaniu, co znacznie podniesie koszty wdrożenia i skomplikuje obsługę incydentów nie dając efektywnych korzyści Zamawiającemu.

Odp: Zamawiający dopuszcza spełnienie wymagań określonych w punkcie 106b) opisu przedmiotu zamówienia poprzez wystawienie API w oferowanym systemie zarządzania bezpieczeństwem.
W związku z powyższym w Załączniku nr 1 do SIWZ – Opis przedmiotu zamówienia, Zamawiający wprowadza następujące zmiany w treści pkt 106 i pkt 107.

„106. System do zarządzania bezpieczeństwem teleinformatycznym musi umożliwiać integrację z używanym przez Zamawiającego systemem SIEM Splunk Enterprise Security w zakresie pobierania i aktualizowania incydentów. Integracja powinna być jednokierunkowa w zakresie:

a) pobrania nowych incydentów z systemu SIEM za pomocą m.in. syslog,
b) możliwości wykonywania zapytań w systemie SIEM w celu wzbogacenia informacji w trakcie prowadzenia śledztwa w Systemie zarządzania bezpieczeństwem,
c) możliwości synchronizacji komentarzy.”

Realizacja powyższych funkcjonalności może zostać zrealizowana za pomocą API.

Punkt 107 Załącznika nr 1 – Opis przedmiotu zamówienia, o treści: „System do zarządzania bezpieczeństwem teleinformatycznym powinien umożliwiać synchronizację bazy zasobów (assets) w systemie SIEM na podstawie danych z Systemu zarządzania bezpieczeństwem.” wykreśla się.

W związku z powyższymi zmianami, Zamawiający wprowadza Zmieniony załącznik nr 1 – Opis przedmiotu zamówienia.

z up. MARSZAŁKA WOJEWÓDZTWA
/-/ Jerzy Kaczmarski
Z-ca Dyrektora Departamentu
Organizacyjno-Prawnego