Urząd Miejski w Słupsku
pl. Zwycięstwa 3
76-200 Słupsk

Słupsk, dnia 16.12.2022 r.

AT.ZP.271.37.2022.PK

WYJAŚNIENIE TREŚCI SWZ

Dotyczy postępowania o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym bez negocjacji, o którym mowa w art. 275 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710 z późn. zm.), zwanej dalej „ustawą Pzp" – pn. **„Rozbudowa istniejącego systemu bezpieczeństwa sieci dla Urzędu Miejskiego w Słupsku"**

WYJAŚNIENIE TREŚCI SWZ

Zamawiający, Miasto Słupsk informuje, iż wpłynęły zapytania dotyczące wyjaśnienia treści Specyfikacji Warunków Zamówienia w zakresie części II postępowania.
Działając na podstawie art. 284 ust. 6 ustawy Pzp udostępnia się treść zapytania wraz z wyjaśnieniami:

Pytanie 1

Proszę o odpowiedź na następujące w sprawie postępowania AT.ZP.271.37.2022.PK pytania

1. Z treści wymagań nie wynika jednoznacznie, czy wykonawca ma dostarczyć system SIEM razem z hardware, czy też system na funkcjonować na hardware Zamawiającego. Zapewne bardziej prawdopodobna jest druga opcja, stąd pytanie 2.
2. Jakie są podstawowe parametry wydajności hardware Zamawiającego, przeznaczonego na działanie zamówionego systemu SIEM.
3. Wymaganie 1.4: w jaki sposób Wykonawca ma udokumentować spełnienie wymogu kompresji logów w skali co najmniej 50-1?

Odpowiedź:

Ad. 1 i 2

System SIEM będzie uruchamiany na istniejącym środowisku wirtualizacyjnym Zamawiającego. Możliwe maksymalne parametry maszyny wirtualnej (CPU: 2 - 10 core @ 2,1 GHz; RAM: do 48 GB; LAN: 1 Gbit; Dysk: 1 TB)

Ad. 3

Informacja o współczynniku kompresji logów musi znajdować się na oficjalnej stronie producenta dotyczącej oferowanego systemu. Jeśli nie ma takiej informacji należy przesłać poświadczone oświadczenie producenta oprogramowania z wymaganą informacją.

Pytanie 2

W związku z określeniem w wymaganiu 1.13 ze dostarczone Licencja rozwiązania monitorującego musi obejmować obsługę minimum 100 urządzeń/systemów Proszę o określenie orientacyjnie jaka ilość analizowanych danych np. w GB na dzień lub EPS ma być obsługiwana przez system dla posiadanych 100 uradzeń. Stwierdzenie potrzeby analizy z milionów plików i zdarzeń jest niejednoznaczne / nieścisłe i niepowalające na dobranie odpowiedniej technologii spełniającej wymagania.

Odpowiedź:

Zamawiający nie posiada obecnie informacji jaka ilość danych podlegałaby analizie.

Pytanie 3
Prosimy uszczegółowienie co wchodzi w skład całej infrastruktury zamawiającego podając ilości urządzeń i ich typy np.:
Serwery windows 10 sztuk
Serwery linux 10 sztuk ..ipt

Odpowiedź:

Zamawiającemu w tym zapisie chodzi o to by system był w stanie monitorować całą infrastrukturę IT a nie tylko jej wybrane elementy. W chwili uruchomienia system ma monitorować wymagane minimum urządzeń/systemów.

Obecna infrastruktura to orientacyjnie:
Serwery Windows: 6szt
Serwery Linux: 40szt
Przełączniki sieciowe: 60szt
UTM: 1szt

Pytanie 4

Prosimy o określenie jaka ilość zdarzeń w sieci obecnie występuje u Zmawiającego (w postaci Flow Per Minute (FPM)
Określenie że system
Musi być w stanie skorelować miliony zdarzeń z sieci, systemów, aplikacji, maszyn wirtualnych i infrastruktury pamięci masowej przy użyciu funkcji korelacji w czasie rzeczywistym jest niejednoznaczne / nieścisłe i niepowalające na dobranie odpowiedniej technologii spełniającej wymagania

Odpowiedź:

Zamawiający nie posiada obecnie informacji jaka ilość zdarzeń podlegałaby analizie.

Pytanie 5

Prosimy o uszczegółowienie jaka wielość przechowywanych danych ma być obsłużona przez system. Dodatkowo to wymaganie może być odczytane aby dostarczyć rozwiązanie SIEM sprzętowe (tak zwany appliance)
Prosimy o wyraźne określenie czy Zamawiający oczekuje systemu SIEM w postaci sprzętowej APPLIANCE lub w postaci software– a sprzęt zapewni we własnym zakresie

Odpowiedź:

Zamawiający zaakceptuje dostarczenie systemu SIEM w postaci software a sprzęt zapewni we własnym zakresie. System będzie uruchamiany na istniejącym środowisku wirtualizacyjnym Zamawiającego. Możliwe maksymalne parametry maszyny wirtualnej
CPU: 2 – 10 core @ 2,1 GHZ
RAM: do 48 GB
LAN: 1 Gbit
Dysk: 1TB
Zamawiający nie posiada obecnie informacji jaka wielość przechowywanych danych ma być obsłużona przez system.

Pytanie 6

Licencjonowanie musi być oparte jedynie na ilości monitorowanych urządzeń/systemów - Wymaganie to preferuje jedynie technologie które licencjonowane są na ilość urządzeń – obecnie na rynku taką ofertą dostarczają jedynie 2 firmy. Zamawiający tym samym ogranicza ilość wykonawców, którzy mogą przystąpić do tego postepowania tym samym łamiąc ustawę i tryb tego Zamówienia które jest prowadzone na podstawie: art. 275 pkt 1 ustawy Inne sposoby licencjonowania np. GB/ dzień czy EPS czy Nody systemu SIEM **są równoważne do licencjonowania na ilość monitorowanych urządzeń/systemów** i powinny być uwzględnione jako rozwiązanie równoważne.
Prosimy o zmianę tego wymagania

Odpowiedź:

Zamawiający nie posiada obecnie informacji jaka ilość zdarzeń, GB/ dzień czy EPS podlegałaby analizie dlatego wybrany został model licencyjny oparty jedynie na ilości monitorowanych urządzeń/systemów.

Pytanie 7

Prosimy o uszczegółowienie co dla zamawiającego oznacza wiele wbudowanych reguł **<10 < 100 <1000 < 1 Milion reguł**

Odpowiedź:

Chodzi o min. 100 reguł.

Pytanie 8

Proponowane rozwiązanie monitorujące nie może być specyficzne dla producenta - Prosimy o uszczegółowienie tego wymagania. Każdy producent SIEM posiada specyficzne dla siebie rozwiązanie wyróżniające go na ryknu. Np. ilość gotowych raportów , obsługiwane standardy formaty – gotowe konektory itp. Czy to wymaganie należy traktować jako potrzebę zakupu systemu SIEM zbudowanego tylko z kodu Open Source -

Odpowiedź:

Chodzi o to by rozwiązanie monitorujące można było zainstalować na różnych rozwiązaniach sprzętowych oraz by nie obsługiwało tylko sprzętu jednego producenta (ma obsługiwać sprzęt i systemy wielu różnych producentów).

Pytanie 9

Ponadto, dla obliczenia niezbędnych danych systemu prosimy o podanie bardziej szczegółowych danych obejmujących ilości sprzętu (komputerów, serwerow, urządzeń sieciowych etc.).

Zasoby IT TOTAL	**Ilość (Odpowiedź)**
Windows Servers - HIGH EPS (10% of total)	**Brak danych**
Windows Servers - MED EPS (50% of total)	**Brak danych**
Windows Servers - LOW EPS (40% of total)	**Brak danych**
Windows Servers	**6**
Windows Desktops (Laptops / tablets / POS)	**400**
Linux / Unix Servers	**40**
Mainframe / Midrange	**0**
Network Routers	**5**
Network Switches	**60**
Network Flows (NetFlow / Jflow / S-Flow)	**Brak danych**
Network Wireless LAN	**6**
Network Load-Balancers	**0**
WAN Accelerator	**0**
Other Network Devices	**Ok 200 drukarek sieciowych**
Network Firewalls (Check Point - Internal)	**0**
Network Firewalls (Check Point - DMZ)	**0**
Network Firewalls (Cisco - Internal)	**0**
Network Firewalls (Cisco - DMZ)	**0**
Network Firewall (Palo Alto)	**0**
Network IPS/IDS	**1 (zintegrowany w UTM)**
Network VPN / SSL VPN	**1 (zintegrowane w UTM)**
Network AntiSpam	**1 (zintegrowane w UTM)**
Network Web Proxy	**1 (zintegrowane w UTM)**
Other Security Devices	**0**
Web Servers (IIS, Apache, Tomcat)	**5**
Database (MSSQL, Oracle, Sybase)	**7**
Email Servers (Exchange, Sendmail, BES, etc)	**1**
AntiVirus / DLP Server	**1**
Other Applications (ERP, Inhouse, etc)	**3**

Pytanie 10

Wykonawca wnosi o zmikanę tyerminu wykonania umowy. Biorąc pod uwagę termin złożenia oferty 21.12.2022, okres dni wolnych od pracy, okres na wniesienie ewentualnych odwołań od decyzji Zamawiającego, uważamy że pozostający do końca 2022r. kilkudniowy termin na wykonanie umowy jest nierealny,

Odpowiedź:

Zamawiający nie ma możliwości zmiany terminu realizacji umowy. Zadanie finansowane jest z budżetu 2022 roku.

Z up. PREZYDENTA
Irena Tkaczuk - Kawalerowicz
DYREKTOR
Wydziału Administracyjno - Technicznego