Znak: WAG.261.1.2016
OL.261.1.9.JP

Lublin, dnia 15 września 2016 r.

O F E R E N C I

wszyscy

Dotyczy przetargu nieograniczonego na zakup systemu zarządzania zdarzeniami i bezpieczeństwem informacji opublikowanego w Biuletynie Zamówień Publicznych w dniu 06.09.2016 r. pod numerem 305446-2016.

Działając na podstawie art. 38 ust. 1 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych Lubelski Oddział Wojewódzki Narodowego Funduszu Zdrowia przekazuje wyjaśnienia dotyczące treści specyfikacji istotnych warunków zamówienia:

Pytanie 1

W pkt 1.39 Opisu przedmiotu zamówienia (Załącznik nr 5 do SIWZ) wśród wymogów, które musi spełniać system SIEM znajduje się parametr:
dyski twarde - min 6TB (użytkowej RAID-5)
W związku z powyższym prosimy uprzejmie o odpowiedź na pytanie:

Czy Zamawiający zaakceptuje rozwiązanie typu appliance jednego z największych światowych producentów systemów SIEM obsługujące 1.200 EPS i wyposażone w system dyskowy o pojemności 3TB + 480GB SSD?

Rozwiązanie powyższe zostało przez producenta przewidziane pod kątem wykorzystania pamięci masowej dla licencji 1.200 EPS, a więc o 20% przewyższającego Państwa wymogi. System składowania danych został przez producenta zoptymalizowany i w jego ocenie dla ww. liczby zdarzeń podana pojemność powinna być wystarczająca.
Możemy oczywiście zaoferować Państwu produkt spełniający z naddatkiem wymaganie w zakresie pojemności systemu dyskowego (np. 8TB surowej pojemności), jednak taki system producent zaleca dla 3.000 EPS, czyli trzykrotnie większej niż przewidywana przez Państwa liczba zdarzeń i tak nadmiarowe rozwiązanie znacząco podniesie cenę oferty.

Odpowiedź 1

Zamawiający podtrzymuje zapisy siwz.

Pytanie 2:

Proszę o podanie ilości systemów źródłowych, z których będą wysyłane informacje do systemu SIEM, w rozbiciu na ich rodzaj, wg poniższego zestawienia:

Nazwa systemu ilość

a. MS Domain Controler + DNS -
b. MS Windows Servers (2003-2012) -
c. Vmware vCenter -

d. Cisco Ironport (web proxy) -
e. Juniper J series -
f. Fortinet FortiGate -
g. Microsoft Exchange Server -
h. Linux Servers -
i. HP-UX -
j. Apache web server -
k. Cisco Router (NetFlow) -
l. Cisco switches

Odpowiedź 2
Zamawiający nie widzi potrzeby wykazywania ilości poszczególnych systemów, a wymaga aby powyższe systemy źródłowe były wspierane przez oferowany system SIEM, a ilość źródeł logów powinna wynosić min.750

Pytanie 3:
Prosimy o podanie liczby użytkowników, którzy będą korzystali z systemu – logowali się do niego i wykorzystywali funkcjonalności dostępne w GUI.
Odpowiedź 3
System powinien umożliwiać równoczesną pracę nieograniczonej liczbie użytkowników interfejsu bez wpływu na wydajność systemu SIEM.

Pytanie 4
Proszę o podanie liczby użytkowników korzystających z państwa sieci, która będzie podlegać monitorowaniu i rejestracji zdarzeń przez system SIEM.
Odpowiedź 4
Zamawiający nie przewiduje monitorowania i rejestracji zdarzeń użytkowników pracujących w sieci bezpośrednio w związku z czym ich liczba nie ma żadnego znaczenia. Minimalne parametry opisujące wydajność urządzenia są przedstawione w Załączniku nr 5 do SIWZ.

Pytanie 5
W jakich przypadkach i do przesyłania jakich logów oraz informacji ma być używany agent do systemów Windows, Unix i Linux?
Odpowiedź 5
Zamawiający oczekuje, aby producent systemu SIEM zapewniał możliwość wykorzystania opcjonalnych agentów do zbierania zdarzeń z systemów Windows, Unix, Linux w zakresie identycznym jak system bezagentowy. Zakres ten zawarty jest i opisany w Załączniku nr 5 SIWZ. Zamawiający może wykorzystać „agenta" np. w celu poprawienia wydajności systemu.

Z-ca Przewodniczącego Komisji Przetargowej

Wiesław Czyżyk