Warszawa, 23 listopada 2020 r.

DAZ.262.69.2020

Wszyscy zainteresowani

Dotyczy: postępowania o udzielenie zamówienia publicznego (nr 57/20/PN/N) *zakup systemu klasy "SIEM", wraz z kompletem niezbędnych licencji oraz usług, w modelu tradycyjnym z wykorzystaniem infrastruktury Zamawiającego.*

Działając na podstawie art. 38 ust. 2 ustawy Prawo zamówień publicznych (t.j. Dz. U. 2019 r. poz. 1843. z póź. zm.), uprzejmie informuję, iż do Zamawiającego wpłynęły wnioski o wyjaśnienie treści SIWZ. Poniżej przedstawiam ich treść wraz z wyjaśnieniem udzielonym przez Zamawiającego

Pytanie 1:
Czy Zamawiający w punkcie 1.1 SOPZ dopuszcza sprzedaż licencji w modelu perpetual z okresem wsparcia 24 miesiące?
Odpowiedź 1:
Zamawiający podtrzymuje wskazany w SIWZ termin realizacji umowy określony na 18 miesięcy od dnia jej zawarcia. Zamawiający dopuszcza licencje w modelu perpetual z okresem wsparcia określonym w SOPZ i SIWZ.

Pytanie 2:
Rozumiemy, że termin 10 dni odnosi się wyłączne do fizycznego dostarczenia licencji, zaś termin wdrożenia ma zostać określony przez Zamawiającego w ofercie?

Odpowiedź 2:
Zgodnie z zapisami pkt 4 SIWZ dostawa i wdrożenie systemu w terminie 10* dni kalendarzowych od dnia podpisania umowy;
*Lub krócej – zgodnie z ofertą Wykonawcy
Wskazany termin 10 dni kalendarzowych jest terminem maksymalnym, w którym mieści się zarówno dostawa jak i wdrożenie systemu.

Pytanie 3:
W punkcie 4.5 SOPZ Zamawiający określił, że: „System musi zapewnić mechanizm identyfikacji zapisywanych danych, który pozwoli na unikanie duplikacji danych". Prosimy o rezygnację z wymagania, w naszej ocenie jest to ograniczenie konkurencyjności oferowanych rozwiązań i może w znaczącym zakresie ograniczyć liczbę producentów spełniających to wymaganie.

Odpowiedź 3:
Zamawiający podtrzymuje parametry określone w SOPZ. Dla Zamawiającego jest to kluczowa funkcjonalność umożliwiająca dużą oszczędność przestrzeni dyskowej.

Pytanie 4:
W punkcie 4.12 SOPZ Zamawiający określił wymagania dotyczące sposobu komunikacji użytkownika z systemem. Prosimy o rezygnację z zapisu: „nie jest dopuszczalne wymaganie instalacji jakiegokolwiek

dedykowanego oprogramowania klienckiego na stacjach roboczych użytkowników, w tym wtyczek i środowisk uruchomieniowych w rodzaju Adobe Flash, Java lub Microsoft Silverlight" i zastąpienie go zapisem „lub dedykowanego oprogramowania klienckiego na stacjach roboczych użytkowników". W naszej ocenie pozostawienie tego zapisu w niezmienionej formie jest ograniczeniem konkurencyjności oferowanych rozwiązań i może w znaczącym stopniu ograniczyć liczbę producentów spełniających to wymaganie.

Odpowiedź 4:
Zamawiający podtrzymuje parametry określone w SOPZ. Dla Zamawiającego jest to kluczowa funkcjonalność. Zamawiający wymaga, aby oprogramowanie było mobilne oraz nie wymagało instalacji dodatkowych programów do jego obsługi.

Pytanie 5:
Czy Zamawiający dopuszcza w punkcie 4.15 wykreślenie punktu b. trap SNMP oraz f. NetFlow v5, sFlow, jFlow, IPFIX ?

Odpowiedź 5:

Zamawiający podtrzymuje parametry określone w SOPZ. Są to kluczowe, a zarazem bardzo podstawowe protokoły do obsługi strumieni sieci, które Zamawiający chce używać przy analityce ruchu sieciowego w oprogramowaniu klasy SIEM.

Pytanie 6:
Prosimy o rezygnację z wymagania w punkcie 4.16 o treści: „agent musi mieć możliwość równoważenia obciążenia (wysyłanych danych) pomiędzy kilka serwerów centralnych rozwiązań działających w klastrze lub niezależnie". W naszej ocenie jest to ograniczenie konkurencyjności oferowanych rozwiązań i może w znaczącym stopniu ograniczyć liczbę producentów spełniających to wymaganie.

Odpowiedź 6:
Zamawiający podtrzymuje parametry określone w SOPZ. Jest to dla Zamawiającego kluczowa funkcjonalność, która pozwala na utworzenie architektury HA (wysokiej dostępności) dla usług, co w przypadku bezpieczeństwa jest rzeczą istotną. Zamawiający wymaga, aby dane wysyłane przez agentów były obsługiwane bez przestojów i kolejek – równoważenie obciążenia gwarantuje spełnienie tego wymogu.

Pytanie 7:
Prosimy o rezygnację z wymagań z punktu 4.17 o treści „System musi posiadać interfejs programowania aplikacji (API) w postaci bibliotek programistycznych dla języków: Java, Python, JavaScript, PHP, Ruby oraz C#". W naszej ocenie jest to ograniczenie konkurencyjności oferowanych rozwiązań i może w znaczącym stopniu ograniczyć liczbę producentów spełniających to wymaganie.
Odpowiedź 7:
Zamawiający podtrzymuje parametry określone w SOPZ. Dla Zamawiającego jest to kluczowa funkcjonalność, dzięki której będzie możliwa integracja systemów rozwijanych przez NCBR z oprogramowanie klasy SIEM.

Pytanie 8:
Prosimy o rezygnację z punktu 4.18 :
System musi umożliwiać pozyskiwanie danych z nasłuchu sieci. Zbierane informacje muszą obejmować wartości wszystkich nagłówków połączeń do warstwy 4 ISO/OSI, oraz do warstwy 7, dla następujących protokołów:
a. DHCP,
b. DNS,
c. HTTP,
d. IMAP,
e. SIP,
f. SMB,
g. SMTP.
Prowadzenie nasłuchu musi być możliwe z dedykowanego serwera, jak również musi być możliwe z agenta zainstalowanego na stacji roboczej lub serwerze.
W naszej ocenie jest to ograniczenie konkurencyjności oferowanych rozwiązań i może w znaczącym stopniu ograniczyć liczbę producentów spełniających to wymaganie.

Odpowiedź 8:
Zamawiający podtrzymuje parametry określone w SOPZ. Jest to podstawowa, a zarazem pożądana przez Zamawiającego funkcjonalność oprogramowania klasy SIEM.

Pytanie 9:
Czy w punkcie 4.26 Zamawiający dopuszcza usunięcie zapisu dotyczącego akceleracji dla raportów definiowanych przez użytkownika?

Odpowiedź 9:
Zamawiający podtrzymuje parametry określone w SOPZ. Dla zamawiającego jest to kluczowa funkcjonalność, dzięki której Zamawiający będzie mógł szybciej dotrzeć do pożądanych informacji dot. bezpieczeństwa (incydentów, zdarzeń itp.).

Pytanie 10:
Czy Zamawiający dopuszcza usunięcie w punkcie 4.31 zapisu: *dane geolokalizacyjne (np. kraj) dla zdarzeń mają służyć w narzędziu do prezentacji na mapie, jak również umożliwiać ich wykorzystanie w wyszukiwaniu wartości pól oraz w regułach korelacyjnych?* W naszej ocenie jest to ograniczenie konkurencyjności oferowanych rozwiązań i może w znaczącym stopniu ograniczyć liczbę producentów spełniających to wymaganie.

Odpowiedź 10:
Zamawiający usuwa zapis „dane geolokalizacyjne (np. kraj) dla zdarzeń mają służyć w narzędziu do prezentacji na mapie, jak również umożliwiać ich wykorzystanie w wyszukiwaniu wartości pól oraz w regułach korelacyjnych?" znajdujący się w punkcie 4.31 SOPZ

Pytanie 11:
Prosimy o rezygnację z zapisu w punkcie 4.36.

Odpowiedź 11:

Zamawiający podtrzymuje parametry określone w SOPZ. Jest to kluczowa funkcjonalność dla Zamawiającego. Zamawiającemu zależy, aby ustrukturyzowane dane w plikach XML i JSON były obsługiwane przez oprogramowanie klasy SIEM „w locie" bez tworzenia dodatkowych parserów. Przy dużej ilości logów otrzymywanych w formacie XML i JSON jest to duża oszczędność czasu.

Pytanie 12:
Czy w punkcie 4.37 Zamawiający może usunąć zapis „*bez konieczności tworzenie parserów. Nazwy pól powinny być wierszem nagłówkowym CSV*", w naszej ocenie jest to ograniczenie konkurencyjności oferowanych rozwiązań i może w znaczącym stopniu ograniczyć liczbę producentów spełniających to wymaganie.

Odpowiedź 12:
Zamawiający podtrzymuje parametry określone w SOPZ. Jest to kluczowa funkcjonalność dla Zamawiającego. Zamawiającemu zależy aby ustrukturyzowane dane w plikach CSV były obsługiwane przez oprogramowanie klasy SIEM „w locie" bez tworzenia dodatkowych parserów. Przy dużej ilości logów otrzymywanych w formacie XML i JSON jest to duża oszczędność czasu.

Pytanie 13:
Czy Zamawiający może zrezygnować z zapisu w punkcie 4.44: „*oraz tworzyć statystyki występowania poszczególnych wartości tych pól*". W naszej ocenie jest to ograniczenie konkurencyjności oferowanych rozwiązań i może w znaczącym stopniu ograniczyć liczbę producentów spełniających to wymaganie.

Odpowiedź 13:
Zamawiający usuwa zapis „oraz tworzyć statystyki występowania poszczególnych wartości tych pól" z punktu 4.44 SOPZ

Pytanie 14:
Czy w punkcie 4.48 SOPZ zamawiający dopuszcza rezygnację z zapisu o wykorzystaniu składni REGEX, bądź czy Zamawiający dopuszcza możliwość wykorzystania własnej składni w proponowanym systemie.

Odpowiedź 14:
Zamawiający podtrzymuje parametry określone w SOPZ. Wyrażenia regularne są podstawową funkcjonalnością oprogramowania klasy SIEM i Zamawiający wymaga tej funkcjonalności. Jest ona kluczowa do obsługi oprogramowania przez pracowników Działu Bezpieczeństwa.

Pytanie 15:
Czy Zamawiający dopuszcza możliwość odstąpienia od zapisu w punkcie 4.53: „musi istnieć możliwość zastosowania bez modyfikacji reguł korelacyjnych dla danych historycznych, w celu wykrycia podobnych zdarzeń w przeszłości".

Odpowiedź 15:
Zamawiający podtrzymuje parametry określone w SOPZ. Dla Zamawiającego reguły korelacyjne sięgające do danych historycznych są kluczową funkcjonalnością i niezbędną dla prawidłowej analizy zdarzeń bezpieczeństwa.

Pytanie 16:
Czy Zamawiający dopuszcza możliwość rezygnacji z zapisów punktu 4.56 podpunkt a, b i c. W naszej ocenie jest to ograniczenie konkurencyjności oferowanych rozwiązań i może w znaczącym stopniu ograniczyć liczbę producentów spełniających to wymaganie.

Odpowiedź 16:
Zamawiający podtrzymuje parametry określone w SOPZ. Z oprogramowania będą korzystać inne komórki organizacyjne, które wymagają takowych funkcjonalności (np. obszar IT).

Pytanie 17:
Czy Zamawiający dopuszcza rezygnację z zapisu w punkcie 4.57 SOPZ? W naszej ocenie jest to ograniczenie konkurencyjności oferowanych rozwiązań i może w znaczącym stopniu ograniczyć liczbę producentów spełniających to wymaganie.

Odpowiedź 17:
Zamawiający podtrzymuje parametry określone w SOPZ. Rozliczalność działań użytkowników jest jednym z filarów bezpieczeństwa (obok dostępności, integralności, poufności, niezaprzeczalności i autentyczności) i Zamawiający wymaga aby oprogramowanie umożliwiało rozliczalność działań użytkowników – zwłaszcza w zakresie dostępu do przetwarzanych logów/danych.

Pytanie 18:
Prosimy o rezygnację z zapisu w punkcie 6.1.1 „zawierającego dostęp do bazy wiedzy".

Odpowiedź 18:
SOPZ nie posiada takiego zapisu. Zamawiający wymaga dostępu do bazy wiedzy oprogramowania, w ramach świadczonego wsparcia producenta.

Pytanie 19:
Czy mógłbym prosić o przesłanie załączników 1-6 do SIWZ w wersji edytowalnej, jeśli takie Państwo posiadają?

Odpowiedź 19:
Zamawiający w załączeniu udostępnia edytowalne wersje załączników 1-6 do SIWZ.

Załączniki:

1. Załączniki nr 1-6 do SIWZ – wersje edytowalne

Grzegorz Mroczek

Dyrektor

Działu Bezpieczeństwa