Szczecin, dnia 6 lipca 2018 r.

WAG.261.2.**4**.9.2018

- Wykonawcy -

Dotyczy: Przetarg nieograniczony w zakresie zakupu i wdrożenia systemu wykrywania zagrożeń typy SIEM.

Działając w oparciu o normę art. 38 ust. 1 pkt 3 i ust. 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jedn. Dz. U. z 2017 r. poz. 1579, z późn. zm.), Zachodniopomorski Oddział Wojewódzki Narodowego Funduszu Zdrowia jako Zamawiający w zorganizowanym postępowaniu o udzielenie zamówienia publicznego, w trybie przetargu nieograniczonego w powyższym zakresie, w związku z otrzymanymi prośbami o wyjaśnienie treści siwz z dnia 26 czerwca 2018 r. podaje, co następuje:

Pytanie 1.
Czy Zamawiający uzna za spełniony warunek jeśli łączna wartość :
1. dostawy i wdrożenia wraz z dwuletnią asystą techniczną systemu SIEM wraz z
2. kontynuacją asysty technicznej dla tego samego systemu SIEM i tego samego Klienta na kolejne dwa lata jest nie mniejsza niż 250 000,-?

Odpowiedź:
Zamawiający uzna, że wykonawca spełnia warunek zdolności technicznej lub zawodowej, jeśli dostawa opisana w pytaniu miała miejsce w okresie ostatnich trzech lat przed upływem terminu składania ofert.

Pytanie 2.
I.9 - System SIEM zapewni zbieranie wybranych surowych logów i przepływów sieciowych.
Przez surowe logi Zamawiający rozumie logi w oryginalnej postaci, zapisane w płaskim pliku tekstowym, opatrzonym podpisem cyfrowym, w celu zapewnienia ich niezaprzeczalności.
Wymaganie podpisania podpisem cyfrowym logów ogranicza istotnie zakres możliwych rozwiązań.
Czy Zamawiający zgadza się na zbieranie logów w plikach płaskich niepodpisanych cyfrowo?

Odpowiedź:
Zamawiający nie wyraża zgody na zbieranie logów w płaskich plikach tekstowych, nieopatrzonych podpisem cyfrowym.

Pytanie 3.
I.13 - System SIEM pozwoli włączyć opatrywanie każdego zdarzenia sumą kontrolną obliczaną według jednego z wybranych algorytmów: MD2; MD5; SHA-1; SHA-256; SHA-384; SHA-512.
Wymaganie opatrywania każdego zdarzenia sumą kontrolną ogranicza istotnie zakres możliwych rozwiązań.
Czy Zamawiający zgadza się to, by zdarzenia nie były opatrywane sumą kontrolną?

Odpowiedź:
Zamawiający nie wyraża zgody na to, by zdarzenia nie były opatrywane sumą kontrolną obliczaną według jednego z powszechnie stosowanych algorytmów, a wymienionych powyżej.

Pytanie 4.
I.30 - Rozwiązanie pozwoli na zdefiniowanie ustawienia dla uwierzytelnienia i samego działania sesji konsoli, takie jak:
30.1. czas wygaśnięcia sesji,

30.2. maksymalna liczba nieudanych prób zalogowania i okres trwania interwału gdy one wystąpiły,
30.3. czas zablokowania konta po przekroczeniu nieudanej liczby logowań.
Wymaganie ogranicza istotnie zakres możliwych rozwiązań nie zwiększając poziomu bezpieczeństwa w istotny sposób.
Czy Zamawiający zgadza się na pominięcie takiego zapisu?

Odpowiedź:
Zamawiający stoi na stanowisku, że zdefiniowanie ustawienia dla uwierzytelnienia i samego działania sesji konsoli wpływa istotnie na poprawę poziomu bezpieczeństwa. W związku z powyższym Zamawiający nie zgadza się na pominięcie wyżej cytowanego zapisu .

Pytanie 5.
I.33 - Rozwiązanie zapewni możliwość separacji ról i przywilejów poszczególnych użytkowników systemu SIEM (np. dostęp administracyjny, dostęp do konkretnych raportów, dostęp do danych zgromadzonych z konkretnych źródeł) oraz wskazać pule adresowe IP dotyczące zawartości zdarzeń i przepływów rejestrowanych przez system. W ten sposób wewnątrz tej samej roli można dać użytkownikom dostęp do logów z tych samych systemów, ale dotyczących różnych adresacji IP (można uzyskać w ten sposób wybór tylko części logów firewall i przypisać tę część do konta użytkownika)
Wymaganie ogranicza istotnie zakres możliwych rozwiązań.
Czy Zamawiający zgadza się na granulację uprawnień bazująca na rolach i grupach w zakresie akacji wykonywanych na typach obiektów (np. export, zapis, odczyt, modyfikacja, tworzenie, kasowanie itd.): dostępu administracyjnego, uprawnień do alertów, incydentów, uprawnień do reguł, uprawnień do zdarzeń, uprawnień do iwestygacji, dashbordów, chartów oraz raportów.

Odpowiedź:
Zamawiający nie zgadza się na granulację uprawnień, bazującą jedynie na grupach i rolach w zakresie wykonywanych akcji, na wyżej wymienionych typach obiektów. W ramach tej samej roli musi istnieć możliwość dania użytkownikom dostępu do logów z tych samych systemów, ale dotyczących różnych adresacji IP, co będzie skutkowało tym, że tylko wybrana część logów z urządzenia będzie przypisana do konta użytkownika.

Pytanie 6.
Dotyczy punktu 1.18.
Czy Zamawiający dopuści rozwiązanie SIEM, które pozwala określić sposób retencji przechowywanych zdarzeń oraz przepływów, natomiast nie ma możliwości wyznaczenia innego miejsca ich przechowywania w systemie plików poza miejscem wyznaczonym przez producenta rozwiązania?

Odpowiedź:
Zamawiający dopuści rozwiązanie SIEM pozwalające na określenie sposobu retencji przechowywanych zdarzeń i przepływów jedynie w miejscu wyznaczonym przez producenta rozwiązania.

Pytanie 7.
Dotyczy punktu 1.18.
Prosimy o potwierdzenie, że Zamawiający oczekuje, aby reguły retencji i przechowywania danych dotyczyły danych pierwotnych (raw data) oraz danych znormalizowanych w zależności od zdefiniowanych polityk retencji.

Odpowiedź:
Zamawiający potwierdza, iż oczekuje, aby reguły retencji i przechowywania danych dotyczyły „raw data" oraz danych znormalizowanych, w zależności od ustawionych polityk retencji.

Pytanie 8.
Dotyczy punktu I. 20.
Czy Zamawiający dopuści rozwiązanie SIEM, dla którego producent rozwiązania nie udostępnia opcjonalnych agentów dla system Unix/Linux? W przypadku odmowy czy Zamawiający uzna za spełnienie powyższego wymagania jeżeli zaoferowane rozwiązanie zapewni powyższą funkcjonalność poprzez zastosowanie serwisów syslog dla tych systemów (traktowanych jako agent)?

Odpowiedź:
Zamawiający uzna serwisy syslog jako agentów na systemach Unix/Linux.

Pytanie 9.
Dotyczy punktu I 52.
Prosimy o wykreślenie punktu 52 jako wskazującego na rozwiązanie oferowane przez jednego producenta, mianowicie McAfee.

Odpowiedź:
Zamawiający nie zgadza się na wykreślenie punktu 1.52. Jednocześnie Zamawiający dokonuje zmiany brzmienia tego punktu na poniższe:
„Interfejs systemu SIEM może dawać możliwość tworzenia łańcucha zależnych widoków, gdzie wybranie jednego elementu widoku dynamicznie aktualizuje widoki zależne".
W związku z powyższą odpowiedzią zmianie ulega treść załącznika do *Formularza oferty*, tzw. check lista, poprzez wykreślenie z załącznika poz. 91, a tym samym zmniejszenie liczby pozycji ze 109 do 108.

Pytanie 10.
Dotyczy punktu 32.
Większość rozwiązań typu "appliance" opiera się na tym, że producent danego oprogramowania wybiera dostawcę sprzętu i dopasowuje rozwiązanie do własnego oprogramowania pod względem wydajnościowym.
Czy Zamawiający dopuści rozwiązanie, w którym producent oprogramowania nie jest jednocześnie producentem sprzętu, z zastrzeżeniem spełnienia wymagań Zamawiającego dotyczących parametrów technicznych jak i spełnienia wymagań stawianych platformie sprzętowej.

Odpowiedź:
Zamawiający wyraża zgodę na rozwiązanie, w którym producent oprogramowania nie jest jednocześnie producentem sprzętu, z zastrzeżeniem spełnienia wymagań Zamawiającego dotyczących parametrów technicznych, jak i spełnienia wymagań stawianych platformie sprzętowej przez producenta oprogramowania względnie, aby takie urządzenie było określane przez producenta oprogramowania jako rekomendowane.

Przewodniczący komisji przetargowej
Elżbieta Stypuła-Krotecka