WAG-ZP.261.7.2015

Rzeszów, dnia 25 września 2015 r.

Do wiadomości Wykonawców

Dotyczy: postępowania przetargowego prowadzonego w trybie przetargu nieograniczonego pod nazwą : „Dostawa systemu zarządzania zdarzeniami i bezpieczeństwem informacji SIEM wraz z asystą techniczną na oferowany system".

ODPOWIEDZI NA PYTANIA

Podkarpacki Oddział Wojewódzki Narodowego Funduszu Zdrowia w Rzeszowie na podstawie art. 38 ust. 1 i 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2013 r. poz. 907 z późn. zm.) zwanej dalej „ustawą Pzp" przekazuje treść pytań wraz z wyjaśnieniami:

Treść pytania nr 1:

1.Rozwiązanie powinno zapewniać generowanie dynamicznych linii trendu oraz - wykrywanie anomalii w oparciu o wyznaczone linie trendu.

Czy zamawiający pod pojęciem wykrywania anomalii w oparciu o wyznaczone linie trendu rozumie wykrywanie zdarzeń polegających na przekroczeniu przez parametry ilościowe zbierane na urządzeniu z monitorowanych urządzeń pewnych modyfikowalnych przez użytkownika założeń dotyczących wielkości tych parametrów?
Treść odpowiedzi na pytanie nr 1:

Zamawiający dopuszcza taką interpretację zapisu.

Treść pytania nr 2:

2. Rozwiązanie powinno umożliwiać tzw. analizę behawioralną

Czy zamawiający pod pojęciem analizy behawioralnej dopuszcza funkcjonalność wyświetlania wykresów dotyczących zdarzeń bezpieczeństwa, adresu IP, przepływu sieciowego, lub użytkownika z bazy Active Directory w zadanym przez użytkownika okresie czasu?
Treść odpowiedzi na pytanie nr 2:

Zamawiający dopuszcza taką interpretację zapisu.

Treść pytania nr 3:

3.System powinien mieć możliwość wykrywania anomalii w sieci, niewłaściwego wykorzystania usług i protokołów sieciowych, malware i aktywności P2P, na podstawie przepływów sieciowych, poprzez np. wyznaczenie linii bazowych dla każdego zdarzenia, adresu IP, przepływu sieciowego, lub użytkownika z bazy Active Directory.

Czy pod pojęciem linii bazowej Zamawiający rozumie konfigurowalne wartości dotyczące ilości zdarzeń, lub innych parametrów systemowych lub ruchowych dotyczących zdarzenia do którego odnosi się dany alarm?
Treść odpowiedzi na pytanie nr 3:

Zamawiający dopuszcza taką interpretację zapisu.

Treść pytania nr 4:

4. System SIEM musi zapewnić dostarczanie powiadomień. Powiadomienia muszą bazować na co najmniej dwóch warunkach, w tym: poziom alertu (ilość zdarzeń w zdefiniowanym przedziale czasu) i konfigurowane odchylenie od linii bazowej.

Czy pod pojęciem konfigurowane odchylenie od linii bazowej Zamawiający rozumie, że można w systemie SIEM skonfigurować, że dany parametr ma wyzwalać alarm w momencie przekroczenia jakiejś zadanej wartości?
Treść odpowiedzi na pytanie nr 4:

Zamawiający dopuszcza taką interpretację zapisu.

Treść pytania nr 5:

5. System SIEM powinien umożliwić wysyłanie powiadomień o incydentach poza System SIEM na podstawie następujących kryteriów: ilość zdarzeń w zadanym okresie czasu; odchylenia od linii bazowych tworzonych dynamicznie dla wszystkich nazw użytkowników z bazy Active Directory, adresów IP, Hostów, Domen, portów, protokołów.

Czy pod pojęciem linii bazowej Zamawiający rozumie konfigurowalne wartości dotyczące ilości zdarzeń, lub innych parametrów systemowych lub ruchowych dotyczących zdarzenia do którego odnosi się dany alarm?
Treść odpowiedzi na pytanie nr 5:

Zamawiający dopuszcza taką interpretację zapisu.

Treść pytania nr 6:

6. Interfejs systemu SIEM ma umożliwiać tworzenie łańcucha zależnych widoków, gdzie wybranie jednego elementu widoku dynamicznie aktualizuje widoki zależne.

Czy Zamawiający dopuszcza alternatywne działanie systemu w obszarze widoków, polegające na zwiększaniu dokładności raportów poprzez pojawianie się ich w nowym oknie przeglądarki?
Treść odpowiedzi na pytanie nr 6:

Zamawiający dopuszcza takie rozwiązanie.

Pismo to stanowi integralną część SIWZ i jest wiążące dla wszystkich wykonawców ubiegających się o udzielenie zamówienia.

Działając zgodnie z art. 27 ust. 2 ustawy Pzp Zamawiający żąda niezwłocznego potwierdzenia faktu otrzymania niniejszego pisma. Potwierdzenie należy przesłać na nr faksu 017 86 04 228 lub drogą elektroniczną na adres: anna.jez@nfz-rzeszow.pl

Przewodniczący Komisji Przetargowej
Podkarpackiego Oddziału Wojewódzkiego
NARODOWEGO FUNDUSZU ZDROWIA
z siedzibą w Rzeszowie

Z poważaniem

Bartłomiej Kapica