|  |  |
| --- | --- |
| Poznań, 31 października 2023 r. |  |

K-292-4-1217/2023

**DO WSZYSTKICH WYKONAWCÓW**

Uniwersytet Ekonomiczny w Poznaniu informuje, że do postępowania o udzielenie
zamówie­nia publicznego o nr **ZP/055/23** na **System analizy logów i zdarzeń typu Security Information and Event Management** prowadzonego w trybie podstawowym wpłynęło pytanie, na które Zamawiający niniejszym odpowiada.

*Pytanie 1:*

*Zwracamy się z uprzejma prośba o zmianę brzmienia punktu 8.*

*W obecnej formie punkt narzuca wymaganie dla dostarczanego systemu o możliwość*

*tworzenia miedzy innymi raportów takich jak:*

*- HIPAA -amerykański standard dotyczący amerykańskich placówek służby zdrowia*

*przetwarzających dane pacjentów w sposób elektroniczny*

*- SOX - amerykański standard. Objęte są nim przedsiębiorstwa notowane na rynkach*

*kapitałowych kontrolowanych przez amerykański nadzór giełdowy (Securities and Exchange*

*Commission -SEC).*

*- NERC- amerykański standard dotyczący raportowania niezawodności systemów*

*elektroenergetycznych*

*- FISMA-raport bezpieczeństwa rządu amerykańskiego dotyczący jednostek federalnych*

*-GLBA- raport wynikający z amerykańskiego rozporządzenia "Gramm-Leach-Bliley Act'*

*dotyczący organizacji oferujących klientom końcowym usługi finansowe takie jak pożyczki,*

*porady finansowe, inwestycyjne lub ubezpieczeniowe.*

*GPG13 - standard kierowany wyłącznie dla jednostek administracji publicznej Wielkiej*

*Brytanii*

*Zwracamy uwagę, iż wymienione raporty:*

*- są raportami o charakterze nadmiarowym dla przedmiotowego postępowania*

*- nie dotyczą żadnych ze stosowanych standardów bezpieczeństwa w polskim*

*prawie*

*- dotyczą jednostek administracji amerykańskiej oraz wielkiej Brytanii*

*- nie dotyczą obszarów na jakich funkcjonuje Zamawiający*

*Wszystkie wymienione raporty dostarczane są przez jednego producenta systemu SIEM :*

*https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSIEM.pdf*

*Sugerujemy zasadność wprowadzenia wymagania dotyczącego posiadania przez*

*system SIEM predefiniowanych raportów związanych z GDPR oraz NIST. Są to*

*standardy posiadające odniesienia w regulacjach prawa obowiązującego w Polsce oraz*

*UE.*

*Prosimy o zmianę wymagania na:*

*Rozwiązanie SIEM musi dostarczać bez dodatkowych opłat następujące rodzaje raportów:*

*- GDPR*

*- NIST*

Odpowiedź:

W odpowiedzi Zamawiający zmienia zapis SWZ i tak:

W FORMULARZ SPECYFIKACJI TECHNICZNO-CENOWEJ ZAMAWIANEGO/OFEROWANEGO SYSTEMU w kolumnie 3 „Wymagania minimalne(charakterystyka)” pozycja 8 „Raporty”

pkt 2 zapis:

” 2.Rozwiązanie SIEM musi dostarczać bez dodatkowych opłat następujące rodzaje raportów:

- PCI-DSS

- HIPAA

- SOX

- NERC

- FISMA

- ISO

- GLBA

- GPG13

- SANS Critical Controls” otrzymuje brzmienie „bateria o pojemności min 595mAh.”

Otrzymuje brzmienie:

„2. Rozwiązanie SIEM musi dostarczać bez dodatkowych opłat następujące rodzaje raportów: GPDR, PN-EN ISO/IEC 27001, SANS Critical Controls.”

Pytanie 2:

Dotyczy: 1. System SIEM musi pozwalać na eksportowanie i importowanie pulpitów administracyjnych (dashboards), raportów oraz reguł w formacie XML Zwracamy uwagę, iż wymaganie nie mówi o funkcjonalności, której Zamawiający oczekuje, a narzuca jej rozwiązanie. Narzędzia SIEM dostarczają funkcję eksportowania i importowania wymienionych obiektów za pomocą optymalnych formatów danych. Narzucenie wykorzystania formatu XML jednoznacznie ogranicza konkurencję wskazując na rozwiązanie Forti SIEM i stanowi naruszenie zasad postępowań publicznych. Prosimy o zmianę wymagania. Proponowana nowa treść: System SIEM musi pozwalać na eksportowanie i importowanie pulpitów administracyjnych (dashboards), raportów oraz reguł.

Odpowiedź:

Według wiedzy Zamawiającego format plików XML jest standardem otwartym i powszechnie używanym. Możliwość wykorzystywania go do wymiany danych (eksportowania/importowania) jest dostępna także w innych produktach niż tylko wskazany w pytaniu (np. Splunk). Dodatkowo możliwość przetwarzania plików XML w innych narzędziach niż tylko system producenta rozwiązania zwiększa możliwości dostosowywania rozwiązania do potrzeb własnych Zamawiającego.

Pytanie 3:

Dotyczy wymagania: 9.4 Dane w ramach pulpitów administracyjnych muszą pozwalać na następujące formy prezentacji: - Bar - Pie - Line - Table - Combination (line and table view) - Treemap - Scatter graph - Single values - Gauges - Geographical Map Zwracamy uwagę, iż wymaganie nie mówi o funkcjonalności, której Zamawiający oczekuje, a

narzuca jej rozwiązanie. Narzędzia SIEM dostarczają funkcję tworzenia wykresów, jednak

zastosowana przez Zamawiającego terminologia nie wyjaśnia jakiej funkcji oczekuje.

Ponieważ lista stanowi jednoznaczne odniesienie do dokumentacji produktu FortiSIEM,

wymaganie to stanowi ograniczenie konkurencyjności.

https://help.fortinet.com/fsiem/5-2-5/OnlineHelp/HTML5\_Help/FortiSIEM\_charts\_and\_maps.htm

Zwracamy się z uprzejmą prośbą o zmianę treści wymagania na:

Dane w ramach pulpitów administracyjnych muszą pozwalać na następujące formy prezentacji:

- Wykres kołowy

- Wykres liniowy

- Mapa

- Inne

Odpowiedź:

3. Zamawiającemu zależy na jak największej elastyczności systemu i możliwości prezentacji danych w różnych formatach. Podane typy wykresów są dostępne także w innych produktach niż wskazany w pytaniu (np. Splunk).

Pytanie 4:

Dotyczy wymagania: 1. 11.1 System SIEM musi mieć możliwość: - wyszukiwania zdarzeń (events) w czasie rzeczywistym bez konieczności indeksowania oraz używania wyrażeń logicznych takich jak AND, OR, NOT czy też cudzysłowów - zagnieżdżania wyników wyszukiwań w oparciu o operatory IN oraz NOT IN - wyszukiwania w oparciu o słowa kluczowe oraz w oparciu o sparsowane atrybuty zdarzeń względem analizowanych danych - wyszukiwania historycznego z zastosowaniem kwerend zagnieżdżonych, ze wsparciem dla filtrowania typu Boolean, grupowaniem w oparciu o agregację danych, filtry czasowe, wyrażenia regularne, wyrażenia matematyczne. - wyszukiwania w oparciu o zapytania wstępne uruchamiane zgodnie harmonogramem - wyszukiwania w oparciu o nie mniej niż następujące operatory: include, =,!=, , IS NULL, IS NOT NULL, contains, not contains, contains regex, not contains regex - podejmowania w czasie rzeczywistym działań w oparciu o złożone wzorce zdarzeń - w przypadku prostych zapytań musi na przykład być możliwe określenie wartości granicznej (threshold) ilości zdarzeń X w określonym przedziale czasowym Y z Z wybranych wartości - w przypadku zapytań przekrojowych wspierających filtry typu Boolean musi być możliwe: a) stworzenie wzorców zapytań za określony przedział czasu z wykorzystaniem operatorów takich jak: AND, OR, FOLLOWED BY, AND NOT, and NOT FOLLOWED BY b) każdy z wzorców może być filtrowany i agregowany z wykorzystaniem operatorów takich jak: AVG, MAX, MIN, COUNT and COUNT DISTINCT c) ustalane wartości graniczne (thresholds) mogą być statyczne lub też mogą być otrzymywane jako rezultat analizy statystycznej - analiza statystyczna i alarmowanie w oparciu o zdarzenia musi mieć możliwość działania w oparciu o: a) średnie kroczące (moving averages) b) odchylenia standardowe (standard deviations) - w wypadku przekroczenia statystycznej wartości granicznej (statistical threshold) musi zostać wygenerowany alert w czasie zbliżonym do rzeczywistego - wykorzystywania obiektów wykrytych i znajdujących się bazie urządzeń (CMDB), użytkowników i ich tożsamości oraz lokalizacji podczas wyszukiwania i tworzenie reguł - tworzenia harmonogramu raportów i dostarczania ich pocztą elektroniczną - możliwości eksportowania raportów do formatów CSV i PDF - wyszukiwania zdarzeń poprzez pryzmat całej organizacji lub też w ujęciu fizycznego lub logicznego obszaru raportującego - wykorzystania dynamicznych list pozwalających na obserwację źródeł generujących zdarzenia krytyczne, wraz z możliwością wykorzystania tychże list w dowolnej regule raportującej - skalowania możliwości analitycznych poprzez dodawanie do systemu SIEM kolejnych maszyn wirtualnych bez konieczności wyłączania całego klastra SIEM - automatycznego korelowania użytkownika z jego lokalizacją i adresem IP:

- musi istnieć możliwość tworzenia raportów i wyszukiwania użytkownika w połączeniu z jego adresem IP

oraz lokalizacją. Lokalizacja może oznaczać port na switch'u, adres MAC lub połączenie VPN

- musi istnieć możliwość wzbogacania zdarzeń (events) przy których dane użytkownika pozbawione są

informacje o adresie IP

- wykorzystanie funkcjonalności Geo IP w oparciu o bazę pochodzącą od tego samego producenta

- możliwość wykrywania zdarzeń IPS false positive w oparciu o integrację z zewnętrznymi skanerami

podatności

Zwracamy uwagę, iż punkt jednoznacznie wskazuje produkt FortiSIEM.

https://www.fortinetguru.com/2017/06/fortisiem-rules/

Zamawiający wprost cytuje w ogłoszeniu dokumentację tego producenta:

a) „AND, OR, FOLLOWED BY, AND NOT, and NOT FOLLOWED BY”

Zamawiający nie opisuje oczekiwanej funkcji detekcji, a wskazuje konkretną realizację –

która dostarczana jest przez produkt FortiSIEM. Stanowi to naruszenie zasad

konkurencyjności.

Wnosimy o usunięcie tego wymagania

Odpowiedź:

Według wiedzy Zamawiającego nierelacyjne bazy danych np. noSQL wykorzystują te same typy operatorów. Możliwość ich wykorzystania znajduje się u dużej ilości producentów systemów SIEM dostępnych na rynku. W związku z czym literalnie identyczne zapisy można znaleźć w dokumentacji innych producentów niż wskazany w pytaniu, np.: <https://synoptek.com/wp-content/uploads/2020/05/sd-siem-as-a-service.pdf>.

 Jednocześnie Uniwersytet Ekonomiczny w Poznaniu informuje, że zmienia termin składania ofert, działając na podstawie art 286 ust. 1 ustawy Prawo zamówień publicznych (tj. Dz. U. z 2023 poz. 1605) dokonuje zmiany treści SWZ i tak:

- pkt. XVIII.1 otrzymuje brzmienie:

1. „Ofertę wraz z wymaganymi dokumentami należy umieścić na platformazakupowa.pl pod adresem: https://platformazakupowa.pl/pn/uep w myśl Ustawy PZP na stronie internetowej prowadzonego postępowania do dnia 7 listopada 2023 r. do godziny 9:30.

- pkt. XVII.1 otrzymuje brzmienie:

1. Wykonawca będzie związany ofertą przez okres 30 dni, tj. do dnia 6 grudnia 2023 r.

Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.