Ministerstwo Zdrowia

e usługi w zdrowiu

Łódź, dn. 04.02.2021 roku

Do wszystkich zainteresowanych,

Dotyczy przetargu na: **„Dostawę i instalację infrastruktury teleinformatycznej i architektury technicznej dla Instytutu Medycyny Pracy im. prof. dra med. Jerzego Nofera z siedzibą w Łodzi w ramach realizacji projektu pn. *„Wprowadzenie nowoczesnych e-usług w podmiotach leczniczych nadzorowanych przez Ministra Zdrowia”*”** . Nr ref. postępowania: ***AZAPUZA/64/20/PN***

Szanowni Państwo

Zgodnie z art. 38 ust. 1 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t. j. Dz.U.z 2019 poz. 1843 ze zm.) dalej Pzp, Zamawiający przesyła wyjaśnienia dotyczące specyfikacji istotnych warunków zamówienia:

Pytanie nr 1

Pytanie nr 1 - pakiet numer 2
Jakiego okresu licencyjnego dla elementów pakietu 2 wymaga Zamawiający?
Czy licencja na rozwiązania może być dostarczona w formie subskrypcyjnej tj. w przypadku jej wygaśnięcia produkt przestaje funkcjonować czy ma mieć formę "na własność" tj. wygaśnięcie licencji wsparcia producenta nie spowoduje zaprzestania działania rozwiązania lecz nie będzie ono otrzymywać poprawek, wsparcia technicznego producenta oraz dostępu do nowszych wersji systemu?

Odpowiedź nr 1

Zamawiający wymaga licencji w formie „na własność” wraz z minimum 3 letnim okresem wsparcia

Pytanie nr 2

Pytanie nr 2 - pakiet numer 2

Jakiego okresu licencyjnego dla możliwości korzystania z zewnętrznych baz sygnatur wymaga Zamawiający - dotyczy punktu 22. System do zarządzania informacją i zdarzeniami bezpieczeństwa SIEM (Security Information and Event Management) "Musi istnieć integracji z zewnętrznymi bazami o zagrożeniach (Threat Inteligence feeds - TI)" (...) w szczególności:

"d. wraz z systemem SIEM musi być dostarczony, już zintegrowany, zestaw komercyjnych baz zagrożeń

e. wraz z systemem SIEM musi być dostarczony, już zintegrowany, zestaw baz zagrożeń niekomercyjnych (open source)”

Odpowiedź nr 2

Zamawiający wymaga minimum 3 letniego okresu licencyjnego

Pytanie nr 3

Pytanie nr 3 - pakiet numer 2

Odnośnie zapisu: "System musi mieć możliwość anonimizacji zebranych danych w zakresie nie mniejszym niż: adresy IP, nazwy hostów, adres MAC, adresy email, nazwy użytkowników. Proces ten ma być możliwy w oparciu o role/profile użytkowników administracyjnych. Ujawnienie danych (deanonimizacja) ma sie odbywać z wykorzystaniem użytkownika udzielającego lub zabraniającego jej wykonania. W przypadku zatwierdzenia wspomnianego żądania, dane są ujawniane na określony czas, po którym powtórnie ulegają anonimizacji."

Czy Zamawiający zgodzi się na wykreślenie wymogu anonimizacji adresów MAC?

Odpowiedź nr 3

Zamawiający wyraża zgodę na wykreślenie tego wymogu

Pytanie nr 4

Pytanie nr 4 - pakiet numer 2

System DAM (Database Activity Monitoring) - Jakiego okresu licencyjnego systemu DAM wymaga Zamawiający?

Odpowiedź nr 4

Zamawiający wymaga licencji bezterminowej wraz z minimum 3 letnim okresem wsparcia

Pytanie nr 5

Zwracamy się z uprzejmą prośbą o wyjaśnienie wspólnego znaczenia punktów 2 oraz 4e.

Cytując:
pkt.2
„System musi zapewniać minimum 1000 EPS, minimum 100 urządzeń jako źródeł zdarzeń, w tym minimum 50 komputerów Windows z wykorzystaniem dostarczonego w ramach systemu oprogramowania typu agent".
Zważywszy na dopuszczenie licencjonowania w oparciu o przestrzeń dyskową przeznaczoną na zdarzenia bezpieczeństwa zwracamy się z uprzejmym pytaniem, czy Zamawiający dopuści jako równoważny model licencjonowania w oparciu o **sumaryczną liczbę dokumentów** będących zdarzeniami bezpieczeństwa. Liczba dokumentów pomnożona przez średnią wielkość dokumentu wynoszącą 600 bajtów przekłada się na sumaryczną przestrzeń dyskową dla systemu.

Pkt. 4e

„Klaster SIEM nie może posiadać ograniczeń licencyjnych związanych z ilością gromadzonych i przechowywanych zdarzeń i/lub danych. Jedynym ograniczeniem w tym zakresie może być rozmiar przestrzeni dyskowej".

Punkt 4e jasno wskazuje, iż przedmiotem licencjonowania może być tylko rozmiar przestrzeni dyskowej przeznaczonej na zdarzenia bezpieczeństwa. Punkt 2 wymienia kilka warunków brzegowych, jednakże z żadnym z nim nie jest podany jedyny parametr dopuszczonego wymiarowania systemu. Z uwagi na dopuszczenie licencjonowania jedynie w zakresie rozmiaru przestrzeni dyskowej zwracamy się z uprzejmą prośbą o wyspecyfikowanie oczekiwanej licencjonowanej przestrzeni dyskowej.

Odpowiedź nr 5

W odpowiedzi na pytanie, Zamawiający informuje, iż nie dopuszcza ograniczania licencyjnego przestrzeni dyskowej. Przestrzeń dyskowa zgodnie z zapisem specyfikacji nie podlega licencjonowaniu, a rozmiar przestrzeni dyskowej będzie alokowany i zwiększany w zależności od rozrostu baz danych.

Pytanie nr 6

pkt. 24
Zwracamy się z uprzejmą prośbą o zmianę brzmienia punktu 24. W obecnej formie punkt narzuca wymaganie dla dostarczanego systemu o możliwość tworzenia między innymi raportów takich jak:
- HIPAA – amerykański standard dotyczący amerykańskich placówek służby zdrowia przetwarzających dane pacjentów w sposób elektroniczny
źródło:
https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act
https://www.manageengine.com/products/eventlog/help/StandaloneManagedServer-UserGuide/ComplianceReports/hipaa-compliance-reports.html
- SOX – amerykański standard. Objęte są nim przedsiębiorstwa notowane na rynkach kapitałowych kontrolowanych przez amerykański nadzór giełdowy (*Securities and Exchange Commission - SEC*).
Źródło:
https://www2.deloitte.com/pl/pl/pages/technology/articles/czym-jest-SOX.html
https://www.manageengine.com/products/eventlog/help/StandaloneManagedServer-UserGuide/ComplianceReports/sox-compliance-reports.html
- NERC – amerykański standard dotyczący raportowania niezawodności systemów elektroenergetycznych
Źródło:
https://en.wikipedia.org/wiki/North_American_Electric_Reliability_Corporation
https://www.manageengine.com/products/eventlog/help/StandaloneManagedServer-UserGuide/ComplianceReports/nerc-compliance-reports.html
- FISMA – raport bezpieczeństwa rządu amerykańskiego dotyczący jednostek federalnych
Źródło:
https://www.blackstratus.com/compliance/fisma/
https://www.manageengine.com/products/eventlog/help/compliance-reports/eventlog-analyzer-fisma-compliance-reports.html

- 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.
Źródło:
https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act
https://www.manageengine.com/products/eventlog/help/StandaloneManagedServer-UserGuide/ComplianceReports/glba-compliance-reports.html
- GPG13 – standard kierowany wyłącznie dla jednostek administracji publicznej Wielkiej Brytanii
Źródło:
https://www.huntsmansecurity.com/solutions/cyber-security-compliance/gpg13/
https://www.manageengine.com/products/eventlog/help/StandaloneManagedServer-UserGuide/ComplianceReports/gpg13-compliance.html
Zwracamy uwagę, iż:
- wymienione raporty nie dotyczą żadnych ze stosowanych standardów bezpieczeństwa w polskim prawie
- wymienione raporty dotyczą jednostek administracji amerykańskiej oraz wielkiej Brytanii (gpg13)
- wymienione raporty nie dotyczą obszarów na jakich funkcjonuje Zamawiający
- wszystkie wymienione raporty dostarczane są przez jednego z producentów systemów SIEM

Proponujemy zmianę punktu 24. tak, aby dostarczane raporty miały związek z polskim prawem i polskimi standardami. Raportowaniem proponujemy objąć standard GDPR/RODO oraz PCI-DSS.

Odpowiedź nr 6

W odpowiedzi na pytanie Zamawiający informuje, iż posiadanie przez dane rozwiązanie raportów predefiniowanych zgodnych z przedstawioną w wymaganiu listą, świadczy o dojrzałości danej platformy. Ich dostępność ułatwia pracę zespołowi administratorów i operatorów. Krytyczne z punktu widzenie Zamawiającego jest to aby szablony raportów były dostępne bez konieczności stosowanie dodatkowej licencji.

Wybrane wytyczne dotyczące wyżej wymienionych norm oraz same raporty je implementujące mogą zostać wykorzystane przez dział bezpieczeństwa/CISO jako źródło najlepszych praktyk i obszarów, które powinny być monitorowane. Tym samym posiadanie tego typu raportów opartych na najlepszych standardach branżowych, pozwala na prostsze i szybsze stworzenie inspirowanych nimi, a jednocześnie adekwatnych do potrzeb danej organizacji sposobów analizy danych.

Wymienione w wymaganiu szablony raportów również dotykają kwestii związanych z GDPR.

Pytanie nr 7

pkt. 25
„System SIEM musi pozwalać na eksportowanie i importowanie pulpitów administracyjnych dashboards), raportów oraz reguł w formacie XML".
Zwracamy się z uprzejmą prośbą o wyjaśnienie, dlaczego Zamawiający narzuca na dostarczany system konkretny format exportu obiektów, zważywszy że są to obiekty wewnętrzne aplikacji nie przeznaczone do edycji przez użytkownika ? Operacje export i import są zadaniami wewnętrznymi i systemy SIEM posiadają własne mechanizmy obsługi tego procesu. Format danych dla zadania export / import nie ma wpływu na jakość systemu i jego funkcjonalność i nie posiada uzasadnienia w zakresie eksploatacji SIEM.

Z uwagi na brak wartości merytorycznej tego wymagania oraz fakt spełnienia tego wymagania przez system Manage Engine https://www.manageengine.com/products/eventlog/help/StandaloneManagedServer-UserGuide/AdminSettings/report-profiles-2.html zwracamy się z prośbą o rezygnację z narzuconego formatu XML lub równoległe dopuszczenie formatu JSON.

Odpowiedź nr 7

W odpowiedzi na pytanie Zamawiający informuje, iż korzysta z formatu XML i znajomość jego struktury pozwala na łatwe przearanżowanie pulpitów administracyjnych raportów lub reguł. Szczególnie, mając na uwadze poprzednie pytanie o wymagane predefiniowane raporty, format XML pozwoli zamawiającemu w łatwy sposób wykorzystać ich części w utworzeniu, własnych raportów.

Pytanie nr 8

pkt.34
„Użyteczność oraz dojrzałość technologiczna zaoferowanego rozwiązania musi być potwierdzona obecnością producenta rozwiązania w Magicznym Kwadrancie Gartnera (MQ) dla Security Information and Event Management (SIEM) z 2020 roku".
Na rynku istnieją rozwiązania, które realizują wymagania stawiane przed nimi w ramach przedmiotowego postępowania, ale nie są one obecne w rankingach takich jak Magiczny Kwadrant Gartnera czy Forrester. Dotyczy to chociażby polskich producentów rozwiązań klasy SIEM, którzy ze względów czysto finansowych nie są objęci kwadratem Gartnera. Należy pamiętać, że powyższe rankingi mają obecnie głównie charakter marketingowy, są kosztowne dla producenta i nie powinno się ich traktować jako narzędzie do weryfikacji dojrzałości rozwiązań informatycznych. W związku z powyższym wnosimy o usunięcie zapisu z SIWZ jako rażąco ograniczającego konkurencję w niniejszym postepowaniu uniemożliwiającego start w postępowaniu polskim producentom systemów SIEM.

Odpowiedź nr 8

W odpowiedzi na pytanie Zamawiający informuje, iż Zgodnie z wyrokiem Krajowej Izby Odwoławczej z dnia 27 sierpnia 2019 r. Sygn. akt: KIO 1567/19 „Posłużenie się jako punktem odniesienia raportem firmy Gartner ze względu na możliwość odniesienia się do obiektywnej oceny sporządzonej przez niezależnych ekspertów, pozwalającej ocenić dojrzałość technologiczną rozwiązania oferowanego przez wykonawcę należy ocenić jako uzasadnione. Gartner Inc. to uznana firmą analityczno-doradcza, która specjalizuje się w tematyce doradztwa strategicznego i wykorzystywania technologii informatycznych i zarządzania nimi w znacznej części udostępniająca wyniki niekomercyjnie, w tym dotyczy to opracowań użytych przez zamawiającego, z których popularnymi i uważanymi za wiarygodne są publikowane coroczne raporty z badań rynku rozwiązań IT, zwane Gartner Magic Quadrant ukazujące rynek IT w kontekście dostępnych na rynku technologii w danej kategorii będącej przedmiotem zainteresowania potencjalnego zamawiającego. W ocenie składu orzekającego decyzja zamawiającego o wykorzystaniu raportów Gartner do oceny jakościowej proponowanych przez oferentów rozwiązań znajduje uzasadnienie w jego rzeczywistych potrzebach i nie narusza zasad uczciwej konkurencji oraz równości wykonawców. Tym samym kryterium zakwestionowane nie narusza przepisów ustawy pzp wskazanych przez odwołującego. Należy przy tym zauważyć, że nie ma podstaw do twierdzenia, że potencjalny wykonawca powinien mieć zapewnione takie warunki udziału w postępowaniu, tak przedmiotowe, jak i podmiotowe, oraz tak sformułowane kryteria

pozacenowe, które zapewnią mu najlepszą pozycję przy ocenie ofert. Teza taka z założenia jest błędna."
Zamawiający podtrzymuje zapis dot. obecności w Magicznym Kwadrancie Gartnera (MQ) dla Security Information and Event Management (SIEM) z 2020 roku.

Z poważaniem,

DYREKTOR
Instytutu Medycyny Pracy
im. prof. dra med. Jerzego Nofera
Prof. dr hab. med. Jolanta Walusiak-Skorupa