TP/33/2022

Sandomierz, 2022-10-13

Szpital Specjalistyczny Ducha Świętego
ul. Schinzla 13
27-600 Sandomierz

ZAWIADOMIENIE O WYBORZE NAJKORZYSTNIEJSZEJ OFERTY

dot.: postępowania o udzielenie zamówienia publicznego. Numer sprawy: *TP/33/2022*. Nazwa zadania: *Dostawa systemu do zarządzania bezpieczeństwem IT oraz zarządzania ryzykiem cyber-zagrożeń klasy SIEM-SOAR*

1. Działając na podstawie art. 253 ust. 1 pkt. 1) Prawa zamówień publicznych Zamawiający informuje, że w prowadzonym postępowaniu wybrano do realizacji zamówienia najkorzystniejszą ofertę złożoną przez Wykonawcę:

VECTO Sp. z o.o., Al. Lotników 32/46, 02-668 Warszawa

Uzasadnienie wyboru:
Oferta najkorzystniejsza wybrana została zgodnie z art. 239 i następne ustawy Pzp, na podstawie kryterium oceny ofert określonego w Specyfikacji Warunków Zamówienia tj. kryterium najniższej ceny. Za najkorzystniejszą ofertę uznana została oferta z najniższą ceną.

W prowadzonym postępowaniu złożono następujące oferty niepodlegające odrzuceniu
---

Lp.: 1
Nazwa wykonawcy: VECTO Sp. z o.o.
Adres wykonawcy: Al. Lotników 32/46, 02-668 Warszawa
Cena oferty brutto: 242.556,00 zł.

2. Działając na podstawie art. 253 ust. 1 pkt. 2) ustawy Pzp Zamawiający informuje o odrzuceniu z udziału w postępowaniu oferty:

W prowadzonym postępowaniu odrzucono następujące oferty

Lp.: 1
Nazwa wykonawcy: Blue Energy Sp. z o.o.
Adres wykonawcy: ul. Towarowa 35, 61-896 Poznań
Cena oferty brutto: 232.470,00 zł.

Uzasadnienie faktyczne odrzucenia: Zgodnie z Załącznikiem nr 1 do Specyfikacji Warunków Zamówienia - Szczegółowy Opis Przedmiotu Zamówienia (dalej: SOPZ), Zamawiający wymagał:
1) W poz. 2 SOPZ „System musi zawierać bazę wiedzy eksperckiej (tzw. Knowledge Base) uwzględniającej wiedzę, która pozwoli ocenić poprawność projektu zabezpieczeń, identyfikując efektywność zastosowanych mechanizmów sieciowych oraz lokalnych w stosunku do potencjalnych wektorów ataków oraz w przypadku ich niezastosowania zidentyfikować ryzyka, które się z tym wiążą".
Dane zawarte w dokumentacji producenta zaoferowanego systemu:
Risk calculation a/gorithrm
The risk calculation mechanism performs the aggregation of the risk field values. We have the following algorithms for calculating the alert risk (Aggregation type):
• min - returns the minimum value of the risk values from selected fields;
• max - returns the maximum value of the risk values from selected fields;

• avg - returns the average of risk values from selected fields;
• sum - returns the sum of risk values from selected fields;
• custom - returns the risk value based on your own algorithm

Wynik porównania wymagań Zamawiającego z ofertą Wykonawcy:

Zaoferowany przez Wykonawcę sposób zarządzania ryzykiem, bazuje tyko na wartościach wyszukiwanych w logach (także zagregowanych), obejmujących gotowe funkcje oraz funkcje custom, na podstawie których wyliczany jest poziom ryzyka. Rozwiązanie to nie umożliwia oceny poprawności projektu zabezpieczeń, gdyż zastosowany w produkcie EnergyLogServer algorytm jest bardzo uproszony i nie posiada bazy wiedzy eksperckiej przez co nie umożliwia szacowania poprawności projektu zabezpieczeń. Brak tej funkcjonalności nie pozwala na realną ocenę zagrożenia występującego w logach względem zastosowanej architektury zabezpieczeń, ocena ryzyka nie uwzględnia elementów bazy wiedzy np.: zastosowanych zabezpieczeń lokalnych oraz sieciowych.

2) W poz. 6 SOPZ „Kod źródłowy dostarczonego rozwiązania musi być wyłączną własnością producenta systemu klasy SIEM i SOAR. Kod źródłowy musi być zamknięty"

Dane zawarte w dokumentacji producenta zaoferowanego systemu:

„ Elasticsearch is a NoSQL database solution that is the heart of our system. "

„The Elsasticsearch engine allows building a database in witch large amounts of data are stored in ordered indexes. The Logstash module is responsible for load data into Indexes, whose function is to collect data on specific tcp/udp ports, filter them, normalize them and place them in the appropriate index. Additional plugins, that we can use in Logstash reinforce the work of the module, increase its efficiency, enabling the module to quick interpret data andparse it."

Post installation steps

- configure Elasticsearch cluster settings

```
vi /etc/elaticserach/elasticsearch.yml
```

  - add all IPs of Elasticsearch node in the following directive:

```
discovery.seed_hosts: [ "172.10.0.1:9300", "172.10.0.2:9300" ]
```

- start Elasticsearch service

```
systemc start elasticsearch
```

- start Logstash service

```
systemctl start logstash
```

- start Cerebro service

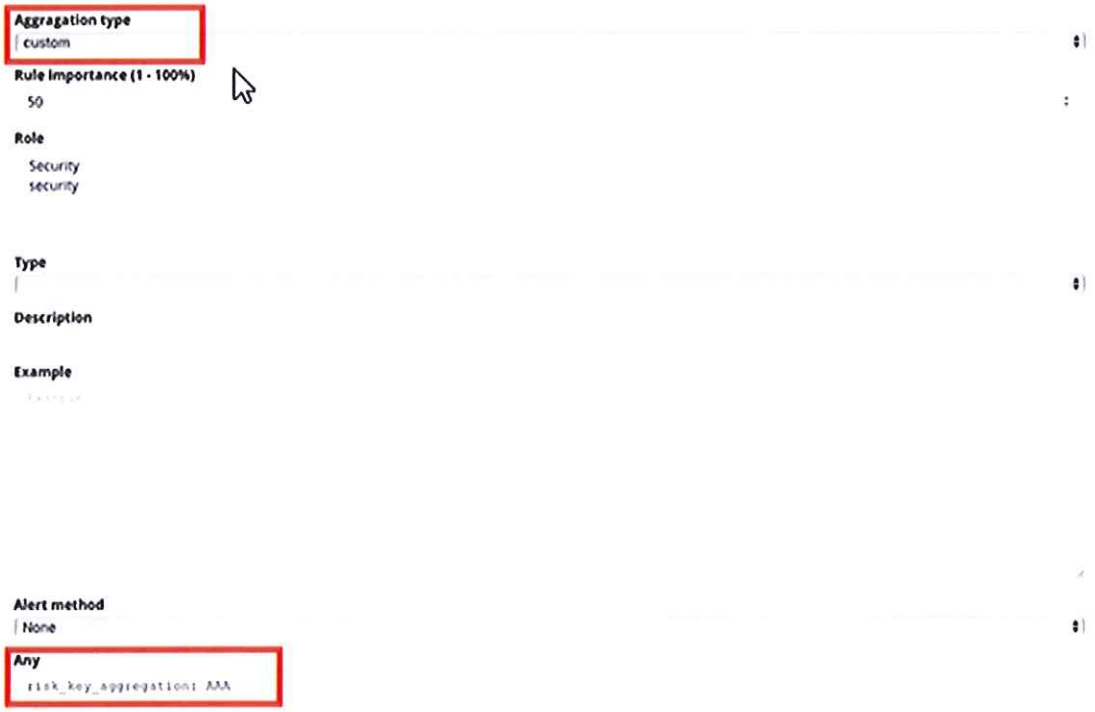
```
systemctl start cerebro
```

- start Kibana service

```
systemctl start kibana
```

Wynik porównania wymagań Zamawiającego z ofertą Wykonawcy:
Zgodnie ze specyfikacją zaoferowanego produktu oficjalnie publikowaną na stronie internetowej jego producenta:
https://kb.energylogserver.com/en/latest/02-Configuration/02-Configuration.html
https://kb.energylogserver.com/
stwierdzamy, iż produkt „Energy Log Server" nie spełnia warunku określonego w punkcie 6, bowiem producent oprogramowania nie jest właścicielem całości kodu i jest on zależny od innych licencji, które w przyszłości uniemożliwią rozwiązywanie zgłoszonych błędów ze względu na brak możliwości ich poprawy np.: przez wykorzystywanie części oprogramowania należącego do innego podmiotu lub wykorzystaniem darmowego oprogramowania (np.: na licencji GPL).W dokumentacji wyraźnie jest wskazane, że produkt EnergyLogServer bazuje na oprogramowaniu Elasticsearch (https://www.elastic.co/), którego producent zaoferowanego systemu nie jest właścicielem oraz jego zainstalowanie jest wymagane podczas instalacji produktu. Jednoznacznie wynika, że EnergyLogServer bazuje na oprogramowaniu ELK (Usługi: elasticsearch, logstash, kibana), co jest sprzeczne z wymaganiem Zamawiającego wyrażonym w punkcie 6 OPZ, gdzie wiele funkcjonalności zdefiniowanych w pozostałych wymaganiach (m.in. filtrowanie, normalizacja logów) jest realizowane przez oprogramowanie ELK (którego producent nie jest właścicielem), a jedynie opiera na nim swój produkt EnergyLogServer.
3) W poz. 19 SOPZ „System musi pozwalać na zautomatyzowaną ocenę wpływu incydentu bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej (np: utrata wizerunku, związana z zagrożeniem przełamania zabezpieczeń serwera webowego organizacji dostępnego z sieci Internet)".
Dane zawarte w dokumentacji producenta zaoferowanego systemu:

The following figure shows the places where you can call your own algorithm:



Wynik porównania wymagań Zamawiającego z ofertą Wykonawcy:
Przedstawiony powyżej algorytm szacowania ryzyka w rozwiązaniu EnergyLogServer zaoferowanym przez Wykonawcę umożliwia tylko wyznaczenie ryzyka, bez możliwości oceny jego wpływu na organizacje np.: na utratę wizerunku, ponieważ takie informacje nie znajdują się w logach i wymagają zastosowania dodatkowych algorytmów. W oprogramowaniu EnergyLogServer wyraźnie jest wskazana jako jedyna możliwość opcja „Custom" umożliwiająca tylko ocenę ryzyka jako odpowiedź na zagrożenie.

Nie ma żadnej funkcjonalności związanej z oceną skutków zagrożenia, np.: możliwy wyciek danych czy utrata reputacji, a jedynie poziom ryzyka co nie pozwala właściwie ocenić rzeczywistego priorytetu zagrożenia i nie jest zgodne z wymaganiem Zamawiającego.
4) W poz. 53 SOPZ „System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów".
Wynik porównania wymagań Zamawiającego z ofertą Wykonawcy:
Zamawiający w swoim wymaganiu wyraźnie wskazał, że chodzi mu o oprogramowanie UEBA (ang: User and entity behavior analytics), czyli takie które umożliwia budowanie i utrzymanie modelu danych zarówno dla użytkowników UBA (ang: User behavior analytics) jak i dla komputerów EBA (ang: Entity behavior analytics). Zgodnie z dokumentacją produktu system Energy-LogServer posiada tylko moduł UBA, czyli umożliwia tylko analizę zachowania użytkowników, nie posiadając równocześnie możliwości uczenia się zachowań komputerów (EBA).

Przedstawione powyżej informacje, przesądzają o niezgodności oferty Wykonawcy Blue Energy Sp. z o.o z treścią warunków zamówienia tj. Szczegółowego Opisu Przedmiotu Zamówienia stanowiącego zał. nr 1 do SWZ, a w konsekwencji powodują ziszczenie się określonej w art. 226 ust. 1 pkt 5) ustawy Pzp przesłanki odrzucenia oferty. W związku z powyższym Zamawiający działając na podstawie art. 226 ust. 1 pkt 5) ustawy Prawo zamówień publicznych odrzucił w/w ofertę, ponieważ jej treść jest niezgodna z warunkami zamówienia.

Uzasadnienie prawne odrzucenia: art. 226 ust. 1 pkt 5) ustawy Pzp.

3. Podpisanie umowy możliwe będzie po dopełnieniu wszelkich formalności. Miejsce i termin podpisania umowy zostaną uzgodnione z wyłonionym Wykonawcą.

Środki ochrony prawnej

Od niniejszej decyzji Zamawiającego, Wykonawcy przysługują środki ochrony prawnej (Odwołanie, Skarga do Sądu).
Termin wniesienia odwołania: 5 dni od dnia przesłania niniejszego pisma przy użyciu środków komunikacji elektronicznej (poczta elektroniczna), lub 10 dni od dnia przesłania niniejszego zawiadomienia, jeżeli zostało ono przesłane w inny sposób.
Informacje dotyczące środków ochrony prawnej znajdują się w Specyfikacji Warunków Zamówienia oraz w Dziale IX Prawa zamówień publicznych "Środki ochrony prawnej", art. od 505 do 590.

Z-ca Dyrektora ds. Zabiegowo-Operacyjnych
Szpitala Specjalistycznego Ducha Świętego
w Sandomierzu
dr Jerzy Kuliński

Kierownik Zamawiającego

Korgulemia