DOLNOŚLĄSKIE CENTRUM REHABILITACJI I ORTOPEDII Sp. z o.o.
58-400 Kamienna Góra, ul. Janusza Korczaka 1
tel.: +**48 75 645 9600** e-mail: ***dcro@dcro.org.pl*** ***www.dcro.org.pl***

Kamienna Góra dnia 16.02.2024 r.

WYJAŚNIENIA TREŚCI SWZ

Nazwa postępowania: **Zakup, dostarczenie i wdrożenie w środowisku informatycznym Dolnośląskiego Centrum Rehabilitacji i Ortopedii Sp. z o.o. w Kamiennej Górze systemu przeciwdziałającemu cyberzagrożeniom, umożliwiającego ich wykrywanie przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi**

Nr referencyjny nadany sprawie przez Zamawiającego: **DI-Z.26.4.2024**

I. Działając na podstawie art.284 ust.2 i 6 ustawy z dnia 11 września 2019 roku Prawo Zamówień Publicznych (tj. Dz.U. z 2023 r., poz.1605 z późn.zm. – dalej ustawa Pzp) Zamawiający informuje, że wpłynęły zapytania o następującej treści:

Pytanie nr 4:
W punkcie 140 załącznika A w sekcji Platforma przeciwdziałania cyberzagrożeniom „Zamawiający na obecnym etapie nie jest w stanie zmierzyć ilości danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz nie zna wymagań związanych z architekturą proponowanego rozwiązania, dlatego oferowana licencje nie może nakładać limitów w tym zakresie.”
Pytanie:
Czy zamawiający zmieni punkt 140 załącznika A? Wymaganie to jest w sprzeczności z wymaganiami w punktach 102 oraz 103 załącznika A, gdzie zamawiający określił wymagania na kolektory parsujace 20k zdarzeń na sekundę oraz 10k zdarzeń dla kolektora logów. Określenie wymagania że oferowana licencje nie może nakładać limitów w ilości EPS ogranicza możliwość spełnienia warunków tylko przez jednego producenta.

Odpowiedź na pytanie nr 4:
Zgodnie z odpowiedzią na pytanie nr 1.

Pytanie nr 5:
W punkcie 139 załącznika A w sekcji Platforma przeciwdziałania cyberzagrożeniom „W związku z tym, że obsługa systemu ma objąć także użytkowników nieposługujących się biegle językiem angielskim, interfejs użytkownika musi umożliwiać obsługę w języku polskim lub posiadać możliwość wgrania plików językowych tłumaczących interfejs na język polski. Pliki tłumaczące interfejs na język polski muszą zostać wgrane w trakcie wdrożenia systemu, przed jego zakończeniem.”
Pytanie:
Czy zamawiający dopuści zmianę warunku w pkt. 139 załącznika A dopuszczając interfejs w języku angielskim ze względu na fakt że definicje w języku angielskim nie przekładają się na język polski pojęciowo jeśli chodzi o słownictwo związane z zagadnieniami używanymi w systemach przeciwdziałających cyberzagrożeniom przy wsparciu mechanizmów uczenia maszynowego. Większy zakres wsparcia ze względu na dostępność dokumentacji ze szczegółowymi instrukcjami są napisanymi w jednym lub obu językach. Ograniczenie do jednej wersji językowej wskazuje na jednego producenta który spełnia wszystkie wymagania.

Odpowiedź na pytanie nr 5:
Zgodnie z odpowiedzią na pytanie nr 2.

Pytanie nr 6:
W punkcie 33 załącznika A w sekcji Platforma przeciwdziałania cyberzagrożeniom „System musi posiadać wbudowaną bazę wskaźników kompromitacji, która umożliwi zbieranie, przechowywanie oraz przypisywanie wskaźników kompromitacji (IOC) do incydentów. Baza powinna obsługiwać protokół TLP w wersji 2.0 oraz obsługiwać następujące typy wskaźników:
a. fqdn,
b. e-mail,
c. nazwa pliku,
d. ścieżka do pliku,
e. hash,
f. adres IP,
g. klucz rejestru,
h. cmd."
Pytanie:
Czy zamawiający dopuści zmianę warunku w pkt. 33 załącznika A dopuszczając zapis wykreślający protokół TLP jeśli zastosowanie protokołu TLP względem wskaźników kompromitacji IOC jeśli wykorzystanie protokołu TLP względem wskaźników kompromitacji IOC ogranicza się tylko do jednej klasyfikacji TLP: AMBER na równi z logami systemowymi, podatnościami oraz informacjami DDoS?

Odpowiedź na pytanie nr 6:
Zgodnie z odpowiedzią na pytanie nr 3.

Pytanie nr 7:
W punkcie 141 załącznika A w sekcji Platforma przeciwdziałania cyberzagrożeniom „Produkt musi umożliwiać równoczesną pracę co najmniej 10 operatorów oraz obsługiwać 150 źródeł logów dotyczących wszystkich zdarzeń związanych z komputerami oraz serwerami wykorzystywanymi w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cybersecurity w ramach wszystkich oferowanych w tym postępowaniu funkcjonalności."
Pytanie:
Czy zamawiający zapewni uszczegółowienie informacji o posiadanej infrastrukturze poprzez wskazanie typów urządzeń generujący logi na które składa się wymagane minimum 150 urządzeń?
Dostawca na bazie powszechnie dostępnych metod i praktyk przeliczy wymaganą ilość licencji, która oparta będzie na innym modelu licencjonowania niż ilość urządzeń i będzie równoważna do wymagań Zamawiającego. Zaznaczamy, że przeliczniki dla różnych modeli licencjonowania (ilość urządzeń, GB/Dzień , EPS) są proporcjonalne (większa ilość urządzeń to większa ilość GB/Dzień i większa ilość ESP) i ostatecznie większa ilość gromadzonych logów w systemie SIEM .
Prośba o wypełnienie przez Zamawiającego:

Zasoby/źródła logów IT TOTAL	150
Windows Servers – HIGH bardzo mocno obciążany Np DNS, AD (typowo 10% wszystkich zasobów Windows)	
Windows Servers – średnio obciążany (typowo 50% wszystkie serwerów Windows	
Windows Servers – mało obciążany (typowo 40% wszystkich serwerów Windows)	
Windows Desktops (Laptops / tablets / POS)	
Linux / Unix Servers	
Mainframe / Midrange	
Network Routers	
Network Switches	
Network Flows (NetFlow / Jflow / S-Flow)	

Network Wireless LAN	
Network Load-Balancers	
WAN Accelerator	
Other Network Devices	
Network Firewalls (Check Point - Internal)	
Network Firewalls (Check Point - DMZ)	
Network Firewalls (Cisco - Internal)	
Network Firewalls (Cisco - DMZ)	
Network Firewall (Palo Alto)	
Network IPS/IDS	
Network VPN / SSL VPN	
Network AntiSpam	
Network Web Proxy	
Other Security Devices	
Web Servers (IIS, Apache, Tomcat)	
Database (MSSQL, Oracle, Sybase)	
Email Servers (Exchange, Sendmail, BES, etc)	
AntiVirus / DLP Server	
Other Applications (ERP, Inhouse, etc)	

Odpowiedź na pytanie nr 7:
Zamawiający dąży do zapewnienia analizy cyberzagrożeń w oparciu o pełną telemetrię zarówno w odniesieniu do stacji roboczych, serwerów jak i systemów zabezpieczeń. W zaproponowanej przez Wykonawcę tabeli są jedynie podane ogólnie systemy, co nie odzwierciedla rzeczywistego zapotrzebowania. Przykładowo inny poziom logowania będzie miał serwer czy stacja robocza, na której przekierowany będzie tylko dziennik zdarzeń "Security", a zupełnie inne zapotrzebowanie będzie w stosunku do źródła z którego będą przekierowane dodatkowo zainstalowane aplikację oraz rozszerzenie logowania poprzez narzędzie Sysmon. W związku z powyższym Zamawiający podtrzymuje wymaganie i nie dopuszcza innych modeli licencjonowania, chyba że w wersji "Unlimited", ponieważ generuje to dla Zamawiającego ryzyko nieprzewidzianych opłat dodatkowych np.: po instalacji sysmona lub innych zmian w architekturze.

Pytanie nr 8:
W punkcie 10 załącznika A w sekcji Wymagania dla serwera dla systemu „Zainstalowany system operacyjny Windows Server Standard 2022 posiadający licencje na obsługę wszystkich wymaganych rdzeni, dodatkowo wymaga się ilości licencji, która zapewni możliwość uruchomienia minimum 6 maszyn wirtualnych."
Pytanie:
Czy zamawiający uzupełni uszczegółowienie informacji w zakresie przeznaczenia serwera systemu? Jakie ma być przeznaczenie serwera w odniesieniu wymagań opisanych w punktach 102, 102, 144 załącznika A w sekcji Platforma przeciwdziałania cyberzagrożeniom?

Odpowiedź na pytanie nr 8:
Zamawiający oszacował zapotrzebowanie następująco:
- Pierwszy serwer
  - Parsowanie logów
  - Reakcja na zagrożenia
- Drugi serwer
  - Zapis logów

  - Indeksowanie
- Trzeci serwer
  - Mechanizm sztucznej inteligencji
- Czwarty serwer
  - Korelacja
- Piąty serwer
  - Zapis zdarzeń
- Szósty serwer
  - Serwer aplikacji
  - Bazy danych

Jednakże Zamawiający zgodnie z punktem 101 który definiuje funkcjonalności, które muszę mieć możliwość instalacji na oddzielnych maszynach wirtualnych. Zamawiający chce mieć możliwość, w przypadku gdy będzie taka potrzeba, późniejszego dostosowania architektury proponowanego rozwiązania poprzez realokację funkcjonalności oraz zmianę parametrów fizycznych przydzielonych do zainstalowanych maszyn wirtualnych.

Pytanie nr 9:
W punkcie 1 załącznika A w sekcji Wymagania dla serwera dla systemu „Pamięć RAM 128GB w kościach DDR4, o taktowaniu minimum 3200MHz, kości pamięci wyposażone w system kodowania korekcyjnego ECC, możliwość rozszerzenia pamięci RAM maksymalnie do 12TB (6TB na procesor)"
Pytanie:
Czy zamawiający uzupełni uszczegółowienie informacji w zakresie przeznaczenia serwera systemu? Jakie ma być przeznaczenie serwera w odniesieniu wymagań opisanych w punktach 102, 102 załącznika A w sekcji Platforma przeciwdziałania cyberzagrożeniom ? Wymagania określone przez zamawiającego na kolektory parsujące 20k zdarzeń na sekundę oraz 10k zdarzeń dla kolektora logów.

Odpowiedź na pytanie nr 9:
Wymagania określone przez Zamawiającego: na kolektory parsujące 20k zdarzeń na sekundę oraz 10k zdarzeń dla kolektora logów. Przedstawione wymaganie dotyczy całości proponowanego rozwiązania, czyli serwera wirtualizacji, na którym zostaną wydzielone maszyny wirtualne (min. 6 szt.). Platforma ta musi mieć możliwość zapewnienia zasobów na parsowanie 20k zdarzeń na sekundę oraz zapewnić ciągłość zapisu na poziomie 10 tys. logów na sekundę.

Pytanie nr 10:
W punkcie 2 załącznika A w sekcji Wymagania dla serwera dla systemu „Zainstalowane dwa procesory 16 rdzeni/32 wątki każdy, o taktowaniu minimalnym 2.4GHz i TDP typowym 135W, pamięć cache minimum 24MB, każdy procesor powinien osiągać wynik minimum 29300 pkt benchmark w teście https://www.cpubenchmark.net/high_end_cpus.html, wyniki z dnia 22.01.2024r."
Pytanie:
Czy zamawiający uzupełni uszczegółowienie informacji w zakresie przeznaczenia serwera systemu? Jakie ma być przeznaczenie serwera w odniesieniu wymagań opisanych w punktach 102, 102 załącznika A w sekcji Platforma przeciwdziałania cyberzagrożeniom ? Wymagania określone przez zamawiającego na kolektory parsujące 20k zdarzeń na sekundę oraz 10k zdarzeń dla kolektora logów.

Odpowiedź na pytanie nr 10:
Zgodnie z odpowiedzią na pytanie nr 9.

Pytanie nr 11:
W punkcie 117 załącznika A w sekcji Platforma przeciwdziałania cyberzagrożeniom „Rozwiązanie nie może Przechowywanie logów oraz zdarzeń nie może wykorzystywać klasycznej relacyjnej bazy danych (w tym, choć nie tylko: MS SQL, Postgresql, MySQL, Oracle, itp.) celem gromadzenia i przechowywania danych związanych ze zbieranymi zdarzeniami. Rozwiązanie musi wykorzystywać w tym celu nowoczesną bazę taką jak na przykład noSQL lub OLAP lub autorskie rozwiązanie producenta."
Pytanie:

Czy zamawiający dopuści zmianę warunku w pkt. 117 załącznika A dopuszczając wykorzystanie bazy optymalizowanej bazy MySQL w systemie Linux do gromadzenia i przechowywania logów? Obecny zapis wyklucza produkty firm wykorzystujące optymalizowane bazy MySQL i wskazuje na tylko jedna produkt jednego producenta.

Odpowiedź na pytanie nr 11:
Większość rozwiązań na rynku oparta jest o bazy NoSQL, w tym Splunk, Elastic, ArcSight Logger, LogRhythm czy AlienVault, co potwierdza że jest to standard, dlatego Zamawiający odrzuca możliwość zastosowania bazy relacyjnej.

Pytanie nr 12:
W punkcie 45 załącznika A w sekcji Platforma przeciwdziałania cyberzagrożeniom „Modele zachowania użytkowników (UBA) i komputerów (EBA) muszą być tworzone automatycznie na bazie zdarzeń historycznych ze skonfigurowanego (wskazanego) okresu lub zdefiniowanej ilości zdarzeń wymaganych do ukończenia procesu nauczania. Algorytm nauczania musi mieć możliwość konfiguracji sposobu odrzucania wartości skrajnych mogących wpłynąć negatywnie na wyniki procesu nauczania oraz umożliwić odrębne uczenie w ramach zdefiniowanych zakresów czasowych (np.: rozdzielenie zdarzeń do nauczania w godzinach pracy od zdarzeń po godzinach pracy).”
Pytanie:
Czy zamawiający dopuści zmianę warunku w pkt. 45 wyłączając warunek maszynowego uczenia dla modułu EBA ? Zgodnie z dobrymi praktykami zastosowanie maszynowego uczenia względem EBA nie przynosi zamierzonych rezultatów. Zgodnie z dobrymi praktykami zalecane jest stosowanie statycznych reguł względem bazy assetów.

Odpowiedź na pytanie nr 12:
Zamawiający nie zgadza się z argumentacja Wykonawcy, gdyż EBA jest niezwykle efektywnym rozwiązaniem, które umożliwia m.in. wykrywanie zmian w zachowaniu serwerów czy stacji roboczych, w przypadku złośliwego oprogramowania lub nieautoryzowanych aktywności, których nie da się wykryć regułami statycznymi. Dlatego Zamawiający wymaga, aby EBA była elementem proponowanego rozwiązania.

Pytanie nr 13:
W punkcie 127 załącznika A w sekcji Platforma przeciwdziałania cyberzagrożeniom „System musi mieć możliwość realizacji funkcjonalności UEBA (User Entity Behaviour Analysis) zarówno w oparciu o dedykowanego Agenta na systemy Windows oraz w oparciu o logi z systemu Windows. Metadane lub logi dotyczące funkcji UEBA nie mogą podlegać licencjonowaniu ze względu na EPS lub rozmiar.”
Pytanie:
Czy zamawiający dopuści zmianę warunku w pkt. 127 rezygnując z określenia „rozmiar” w treści wskazujący na liczbę użytkowników oraz komputerów. Obecnie tylko jeden producent spełnia łącznie wymagania w punktach 117, 127, 139, 140, 141.

Odpowiedź na pytanie nr 13:
Zamawiający wyraźnie określił wymogi związane z licencjonowaniem; wprowadzenie dodatkowych opłat na ilość zgromadzonych danych może doprowadzić do konieczności ponoszenia dodatkowych opłat w trakcie użytkowania systemu, czego Zamawiający chce uniknąć. Dlatego Zamawiający nie zgadza się na zmianę modelu licencjonowania.

Punkt 117 – jest wiele rozwiązań klasy SIEM, które wykorzystuje bazy NoSQL lista w odpowiedziach powyżej
Punkt 127 – UEBA jest standardowym mechanizmem bezpieczeństwa i jest wiele takich rozwiązań na rynku, np:

- Exabeam
- Securonix
- Varonis
- SecureVisio

- Gurucul
- Splunk (Uptycs)

Punkt 139
Dostarczanie plików tłumaczeń jest powszechną praktyką rynkową stosowaną przez czołowych producentów, jak:
Splunk: Splunk umożliwia dostosowanie języka interfejsu poprzez pliki tłumaczeń. Użytkownicy mogą modyfikować lub dodawać pliki tłumaczeń, aby dostosować interfejs do swoich potrzeb językowych.
AlienVault USM (Unified Security Management): AlienVault USM oferuje możliwość dostosowania języka interfejsu poprzez pliki tłumaczeń. Użytkownicy mogą zmieniać język interfejsu, dodając odpowiednie pliki tłumaczeń.
LogRhythm: umożliwia dostosowanie języka interfejsu do potrzeb użytkownika poprzez pliki tłumaczeń. Można modyfikować istniejące pliki tłumaczeń lub dodawać nowe, aby zmienić język interfejsu.
Securonix: pozwala użytkownikom dostosować język interfejsu poprzez pliki tłumaczeń. Użytkownicy mogą zmieniać język interfejsu, dodając odpowiednie pliki tłumaczeń do systemu.

Punkt 140, oraz 141 dotyczy licencjonowania i jest wiele rozwiązań licencjonowanych inaczej niż ilość zdarzeń na sekundę lub ilość gromadzonych danych, np.:

LogRhythm: LogRhythm oferuje licencjonowanie oparte na liczbie źródeł logów.

Securonix: Securonix oferuje elastyczne modele licencjonowania, które mogą obejmować liczbę użytkowników, urządzeń lub zdarzeń.

SecureVisio: SecureVisio oferuje licencjonowanie oparte na liczbie źródeł logów.

II. Zamawiający informuje, że pytania i odpowiedzi stają się integralną częścią specyfikacji warunków zamówienia i będą wiążące przy składaniu ofert. Pozostałe warunki nie ulegają zmianie.

Prezes Zarządu

Artur Mazur