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 15.02.2024 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 1:
W punkcie 140 załącznika A „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 wykreśli punkt 140 załącznika A ze względu na sprzeczny zapis z punktami 102 oraz 102 w załączniku A określający wydajność pojedynczego kolektora logów na co najmniej 10 tyś zdarzeń na sekundę?

Odpowiedź na pytanie nr 1:
Zamawiający informuje, iż punkty te w żadnym wypadku nie są sprzeczne, gdyż wyraźnie jest napisane, że punkt 140 dotyczy całej architektury rozwiązania, natomiast punkt 102 dotyczy jedynie pojedynczego kolektora. Zamawiający wymaga, aby zaproponowana architektura systemu była elastyczna, przez co rozumie się możliwość zainstalowania więcej niż jednego kolektora co nie może wpływać na koszty licencji. Ważne jest w tym przypadku, aby pojedynczy kolektor umożliwiał przyjęcie co najmniej 10 tyś zdarzeń na sekundę, co jest szczególnie istotne np.: w przypadku zdarzeń z systemów klasy Firewall, które są w stanie wygenerować bardzo dużą ilość zdarzeń związanych z ruchem sieciowym oraz włączeniu pełnej telemetrii na stacjach roboczych i serwerach.
W związku z powyższym Zamawiający pozostawia zapisy treści SWZ bez zmian.

Pytanie nr 2:
W punkcie 8 załącznika A „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. 8 załącznika A dopuszczając interfejs w języku angielskim ze względu na fakt że język polski jest uboższy pojęciowo jeśli chodzi o słownictwo związane z zagadnieniami używanymi w cyber security, machine learning i jednocześnie sprzeczny. Innym uzasadnieniem przemawiającym za zastosowaniem interfejsu w języku angielskim jest dokumentacja w języku angielskim, wszystkie instrukcje są napisane w języku angielskim.

Odpowiedź na pytanie nr 2:
Zamawiający chce wykorzystać oferowane rozwiązanie do podniesienia efektywności cyberodporoności organizacji co wiąże się także z zaangażowaniem ludzi, którzy nie mają kompetencji w zakresie cyberbezpieczeństwa oraz biegłej znajomości języka angielskiego. Planujemy objąć ich playbook'ami w zakresie autoryzacji wiedzy i czynności, za które są odpowiedzialni oraz aktualizacji i budowy bazy cmdb, która podniesie poziom zrozumienia oraz automatyzacji.

W związku z powyższym Zamawiający wymaga aby interfejs użytkownika posiadał możliwość wgrania plików językowych tłumaczących interfejs na język polski – tj. dopuszcza wszystkie rozwiązania klasy Enterprise, w których wgranie plików językowych jest powszechnie stosowaną praktyką.

Pytanie nr 3:
W punkcie 33 załącznika A „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 ogranicza się do jednej klasyfikacji TLP: AMBER na równi z logami systemowymi, podatnościami oraz informacjami DDoS?.

Odpowiedź na pytanie nr 3:
Zamawiający nie zgadza się z przedstawioną argumentacją, gdyż klaryfikacja TLP dotyczy zasad wymiany informacji oraz grup docelowych z którymi ta informacja będzie wymienia. Zamawiający planuje wykorzystać wszystkie typy klasyfikacji, w tym TLP:CLEAR do wymiany informacji o domenach i adresach IP, stanowiących potencjalne zagrożenie z sieci Internet, czy TLP: GREEN dla zagrożeń sektorowych dla Polski. Klasyfikacja TLP: AMBER, ogranicza jej użycie tylko do organizacji oraz zewnętrznych struktur bezpieczeństwa i tylko w przypadku, gdy wiąże się z ryzykiem dla prywatności, reputacji lub innych działań, co przekłada się w praktyce na jej nieudostępnianie.

W związku z powyższym Zamawiający pozostawia warunek określony w pkt. 33 (Załącznik A) bez zmian.

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