NARODOWY INSTYTUT ZDROWIA PUBLICZNEGO
PAŃSTWOWY INSTYTUT BADAWCZY

Warszawa, dnia 03.08.2023 r.

WYJAŚNIENIE i ZMIANA TREŚCI
SPECYFIKACJI WARUNKÓW ZAMÓWIENIA

Dotyczy: znak postępowania: **O.OZP.260.24.5.2023**

Na podstawie art. 284 ust. 2 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych, Zamawiający Narodowy Instytut Zdrowia Publicznego PZH – Państwowy Instytut Badawczy zawiadamia, że w postępowania **na świadczenie kompleksowych usług z zakresu cyberbezpieczeństwa (SOC),** wpłynęły wnioski o wyjaśnienie treści Specyfikacji Warunków Zamówienia następującej treści:

1. Pkt 1.2 i 1.3 - ile szacunkowo w chwili obecnej obsługują Państwo alertów i incydentów w ciągu doby/tygodnia/miesiąca?
   Odpowiedź: Ilość alertów zależy od sposobu wdrożenia systemu NDR przez Wykonawcę. Dotychczasowa ilość alertów to kilka alertów na dobę.

2. Pkt 1.5 - czy Zamawiający posiada opracowane i wdrożone procedury i procesy obsługi incydentów?
   Odpowiedź: Proces obsługi incydentu leży po stronie Wykonawcy. Incydent obsługiwany jest na podstawie automatycznych alertów z systemu NDR dostarczonego przez Wykonawcę oraz incydentów zgłaszanych przez Zamawiającego.

3. Pkt 1.14 Czy Zamawiający oczekuje wdrożenia systemów bezpieczeństwa typu NDR, EDR, SIEM itp.? W pkt. 1.14 jest mowa o "systemach bezpieczeństwa **dostarczonych** w ramach usług"
   Odpowiedź: Zamawiający oczekuje wdrożenia systemów bezpieczeństwa typu NDR.

4. Pkt 1.17. Czy Zamawiający posiada wdrożony system ticketowy (prowadzący rejestr prac wykonywanych w ramach procesu obsługi incydentów) czy taki system w ramach usługi ma zostać wdrożony/udostępniony?
   Odpowiedź: Zamawiający posiada wdrożony system ticketowy, jednak nie udostępni go Wykonawcy. System obsługi incydentów jest narzędziem Wykonawcy, służącym do obsługi zgłoszeń Zamawiającego.

5. Pkt 1.19 - Czy oczekiwaniem zamawiającego jest wykonanie i utrzymanie inwentaryzacji jego zasobów IT?
   Odpowiedź: Zamawiający nie oczekuje wykonania inwentaryzacji zasobów IT.

6. Pkt 1.20 - jakiego rodzaju zgłoszenia mają być przyjmowane przez podane kanały komunikacji? Od użytkowników/pracowników systemów NIZ czy może od podmiotów zewnętrznych?
   Odpowiedź: Zamawiający informuje, że przez podane kanały komunikacji mają być przyjmowane zgłoszenia związane z incydentami lub podejrzeniami wystąpienia incydentów cyberbezpieczeństwa od pracowników IT Zamawiającego.

7. Pkt 1.23 - Jaki rejestr ma na myśli Zmawiający? Informacje o alertach są przechowywane w dedykowanych systemach (możliwość eksportu) oraz systemie ticketowym.
   Odpowiedź: Zamawiający informuje, że prowadzony rejestr musi obejmować szczegółowe informacje o alertach ze szczególnym uwzględnieniem: czasu wystąpienia alertu, osób zaangażowanych w proces obsługi, przebiegu i wyników analizy, historii podjętych czynności i komunikacji. Jeżeli system ticketowy Wykonawcy umożliwia gromadzenie i udostępnienie wymaganych informacji, to wymaganie zostanie spełnione.

8. Pkt 1.43 - Czy Zamawiający dysponuje personelem zdolnym do przeprowadzania zmian w konfiguracji ustalonych systemów bezpieczeństwa? Jakiego rodzaju technologie są wykorzystywane w tym zakresie przez Zamawiającego? Jak często (szacunkowo) mogą być przez Zamawiającego zlecane takie zmiany?
   Odpowiedź: Tak, Zamawiający dysponuje zespołem IT o odpowiednich kompetencjach. Wykorzystywane są technologie Fortinet. Zmiany w konfiguracji są incydentalne, głównie na początku usługi podczas dostrajania systemów.

9. Pkt 1.44 - Logi systemów operacyjnych, aplikacji i urządzeń bezpieczeństwa to odrębne źródła danych. Prosimy o wskazanie liczby aplikacji i urządzeń bezpieczeństwa z których będą kolekcjonowane logi. Prosimy również o wskazanie liczby urządzeń z podziałem na systemy operacyjne z których będą kolekcjonowane logi?

   Odpowiedź: Usługi monitoringu zdarzeń realizowane będą w oparciu o min. 2 źródła danych: Wdrożony przez Wykonawcę system NDR oraz FortiAnalyzer będący w posiadaniu Zamawiającego.

   W związku z udzieloną odpowiedzią Zamawiający dokonuje zmiany Rozdział III SWZ (Opis przedmiotu zamówienia) w zakresie pkt. 1.44.
   W załączeniu Rzodział III SWZ po zmianie.

10. Pkt 1.51 - w jakim zakresie czasowym ma być prowadzona usługa?
    Odpowiedź: Zamawiający informuje, że zgodnie z punktem 1.51 OPZ w zakresie monitoringu systemów bezpieczeństwa oraz analizy i selekcji zdarzeń *dostawca* zagwarantuje dostępność min. 3 osób w godzinach 7:00 - 21:00 w dni robocze, min. 2 osób w godzinach 7:00 - 21:00 w dni wolne od pracy oraz min. 2 osób w godzinach 21:00 - 7:00,
    co oznacza konieczność prowadzenia usługi przez 24 godziny na dobę przez 7 dni w tygodniu przez cały okres trwania umowy.

11. Jakie jest uzasadnienie posiadania przez zespół świadczący usługę SOC certyfikatu CRTP (Certified Red Team Professional) w takiej liczbie? To samo dotyczy certyfikatu PNTP (Professional Network Penetration Tester). Pentesty oraz redteaming nie wchodzą w zakres usługi.
    Odpowiedź: Wymagane certyfikaty lub równoważne mają na celu potwierdzenie kompetencji zespołu zaangażowanego w obsługę incydentów w całym okresie trwania umowy.

12. **Pytanie ogólne:**
    Zwracamy się z prośbą do Zamawiającego, o wydłużenie terminu składania ofert do 04.08.2023r. w celu szczegółowego i rzetelnego przygotowania oferty oraz do zapoznania i odniesienia do wyjaśnień poniżej wymienionych pytań.
    Biorąc pod uwagę powyższe, wydłużenie przedstawionego terminu wydaje się być uzasadnione.
    Odpowiedź: Zamawiający wydłuża termin składania ofert do dnia 08.08.2023r.

13. **Dotyczy: punkt 1.44 z OPZ:**

Usługi monitoringu zdarzeń muszą być realizowane co najmniej na podstawie trzech źródeł danych: zdarzeń z punktów końcowych o poziomie szczegółowości systemów klasy EDR (Endpoint Detection and Response), informacji o ruchu sieciowym na poziomie szczegółowości systemów klasy NTA (Network Traffic Analysis), logów systemów operacyjnych, aplikacji, urządzeń bezpieczeństwa.
Z umowy wynika, że Zamawiający zamierza udostępnić system Fortigate 500E, oraz wymaga od wykonawcy wdrożenia systemu NDR.

a) Czy Zamawiający posiada system EDR ? Jeżeli tak, czy Zamawiający zamierza go udostępnić Wykonawcy Usługi SOC ? Jeżeli tak, prosimy o podanie producenta oraz wersji systemu EDR.

Odpowiedź: Zamawiający nie posiada systemu EDR.

b) Jakie funkcje bezpieczeństwa są uruchomione na systemie Fortigate 500E (IPSEC VPN, SSL VPN, IPS/IDP; Antivirus; Antispam, Detekcja aplikacji; integracja z Active Directory; inne)

Odpowiedź: Zamawiający informuje że w systemie Fortigate 500E są włączone następujące funkcje, tj. IPSEC VPN, SSL VPN, IPS/IDP; Antivirus; Antispam, Detekcja aplikacji; integracja z Active Directory.

c) Jakie systemy Zamawiający zamierza objąć Usługą SOC w zakresie monitorowania logów systemów operacyjnych oraz aplikacji ?

Odpowiedź: Usługi monitoringu zdarzeń realizowane będą w oparciu o min. 2 źródła danych: Wdrożony przez Wykonawcę system NDR oraz FortiAnalyzer będący w posiadaniu Zamawiającego.

W związku z udzieloną odpowiedzią Zamawiający dokonuje zmiany Rozdział III SWZ (Opis przedmiotu zamówienia) w zakresie pkt. 1.44.
W załączeniu Rzodział III SWZ po zmianie.

14. Dotyczy: punkt 1.22 z OPZ

"Stały monitoring alertów i zdarzeń, o priorytecie wskazanym przez zamawiającego (ograniczenie dziennej liczby alertów) / o ustalonym priorytecie (jeśli nie ma ograniczania alertów), występujących w ustalonych systemach bezpieczeństwa"

a) Co to znaczy o priorytecie wskazanym przez Zamawiającego?

Odpowiedź: Oznacza alerty o poziomie Critical z systemu FortiAnalyzer

b) Jaka jest szacowana dzienna ilość zdarzeń zgłaszanych przez Zamawiającego?

Odpowiedź: Ilość alertów zależy od sposobu wdrożenia systemu NDR przez Wykonawcę. Dotychczasowa ilość alertów to kilka alertów na dobę

15. Dotyczy: punkt 1.33 z OPZ

„Raz w miesiącu / raz na kwartał w pierwszym tygodniu kolejnego miesiąca / kwartału wykonawca prześle zamawiającemu raport zawierający co najmniej..."
Jaki jest cel tworzenia raportów kwartalnych ?

Odpowiedź: Celem jest dostarczenie Zamawiającemu zagregowanych informacji o stanie bezpieczeństwa

16. Dotyczy: punkt 1.34. z OPZ:

"Przegląd i omówienie procedur, ścieżek eskalacji, konfiguracji systemów, parametrów usługi w ramach kwartalnych spotkań warsztatowych. Spotkania będą odbywały się w siedzibie zamawiającego lub, za zgodą zamawiającego, on-line"
Jak jest planowany wymiar godzinowy spotkań warsztatowych?

Odpowiedź: Zamawiający nie precyzuje wymiaru godzinowego spotkań warsztatowych, jednakże nie przewiduje dłuższych niż 8h.

17. **Dotyczy: punkt 1.36. z OPZ:**

"Realizowanie działań związanych z reakcją na incydenty w siedzibie **zamawiającego** oraz w lokalizacjach wskazanych przez **zamawiającego** gdzie znajdują się systemy **zamawiającego** dotknięte incydentem, zgodnie z **ustalonymi** czasami reakcji, w **zatwierdzonym** zakresie oraz zgodnie z **ustaloną** autoryzacją"

a) Gdzie znajdują się systemy Zamawiającego, które mogą zostać wskazane przez Zamawiającego?
Odpowiedź: Zamawiający informuje, że systemy Zamawiającego znajdują się w siedzibie Zamawiającego: Warszawa, ul. Chocimska 24

b) Co oznacza w pkt 1.36 "zgodnie z **ustalonymi** czasami reakcji"?
Odpowiedź: Czasy reakcji określone są w załączniku nr 1 Zakres Usług

18. **Dotyczy: punkt 1.39. z OPZ:**

"Zarządzanie konfiguracją **ustalonych** systemów bezpieczeństwa **zamawiającego** zgodnie z **ustalonym** procesem wprowadzania zmian oraz w ramach **ustalonej** autoryzacji i poziomów dostępów: Przeprowadzanie aktualizacji oprogramowania, wprowadzanie zmian w regułach i mechanizmach wykrywania zagrożeń w celu podniesienia efektywności wykrywania, rozwiązywanie problemów."
Ile i jakie są systemy bezpieczeństwa posiada Zamawiający?
Odpowiedź: Zamawiający posiada urządzenia Fortigate - 2 szt. w konfiguracji HA.

19. **Dotyczy: punkt 1.41 z OPZ:**

"Mapowanie sieci w oparciu o informacje przekazane przez zamawiającego oraz uzyskane w ramach procesów analizy zdarzeń i reakcji na incydenty. Utrzymywanie aktualnej bazy wiedzy o zasobach i architekturze sieci zamawiającego na poziomie umożliwiającym określenie roli, typu oraz priorytetu zasobów..."
Czy Zamawiający posiada oprogramowanie typu CMDB?
Odpowiedź: Zamawiający posiada oprogramowanie typu CMDB.

20. **Dotyczy: punkt 1.42. z OPZ:**

"Skanowanie podatności zasobów zamawiającego z wykorzystaniem automatycznych narzędzi. Skanowanie zasobów dostępnych z sieci Internet musi być realizowane co najmniej...."
Czy Zamawiający posiada oprogramowanie do skanowania podatności?
Odpowiedź: Zamawiający posiada oprogramowanie do skanowania podatności systemów końcowych.

21. Pytanie ogólne:
Czy Zamawiający dopuszcza zastosowanie do świadczenia Usługi systemu SIEM Wykonawcy, kolekcjonującego logi i alerty z systemów objętych Usługą SOC
Odpowiedź: Tak

Pytania dot. Umowy

26. Dotyczy §7 ust.2 zwracamy się z prośbą o zmniejszenie wysokości kary umownej z 20% wynagrodzenia brutto na 5% wynagrodzenia netto.

Odpowiedź: Zamawiający informuje, że nie wyraża zgody na zmniejszenie wysokości kary umownej z 20% wynagrodzenia brutto na 5% wynagrodzenia netto

27. Dotyczy §7 ust. 4 zwracamy się z prośbą o zmianę zwłoki w niedotrzymaniu terminów realizacji poszczególnych etapów prac z 500 zł do kwoty 250 zł.

Odpowiedź: Zamawiający informuje, że nie wyraża zgody na zmianę zwłoki w niedotrzymaniu terminów realizacji poszczególnych etapów prac z 500 zł do kwoty 250 zł

28. Odnośnie §7 ust. 5 prosimy o zmianę kary umownej z 500 zł do wysokości 250 zł.

Odpowiedź: Zamawiający informuje, że nie wyraża zgody na zmianę kary umownej z 500 zł do wysokości 250 zł.

29. Dotyczy §7 ust. 6 zwracamy się z prośbą o zmianę kary związanej z odstąpieniem od umowy przez Zamawiającego na wysokość 20% ceny netto.

Odpowiedź: Zamawiający informuje, że nie wyraża zgody na zmianę kary związanej z odstąpieniem od umowy przez Zamawiającego na wysokość 20% ceny netto

30. Zwracamy się z prośbą o zmianę w §7 ust. 8 zmniejszenia łącznej wysokości kar umownych na 30% łącznego wynagrodzenia netto.

Odpowiedź: Zamawiający informuje, że nie wyraża zgody na zmniejszenie łącznej wysokości kar umownych na 30% łącznego wynagrodzenia netto.

31. Proponujemy wykreślenie § 11 ust. 1-3 z uwagi na fakt, iż umowa zawarta na czas określony powinna wskazywać przyczyny wypowiedzenia.

Odpowiedź: Zamawiający nie wyraża zgody na wykreślenie wskazanych punktów.

Na podstawie art. 286 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych, Zamawiający Narodowy Instytut Zdrowia Publicznego PZH – Państwowy Instytut Badawczy informuje, że w postępowaniu **na świadczenie kompleksowych usług z zakresu cyberbezpieczeństwa (SOC)** dokonuje następującej zmiany treści Specyfikacji Warunków Zamówienia:

I**.** Rozdział III SWZ (Opis przedmiotu zamówienia) pkt. 1.44.**:**

Jest:

1.44. Usługi monitoringu zdarzeń muszą być realizowane co najmniej na podstawie trzech źródeł danych: zdarzeń z punktów końcowych o poziomie szczegółowości systemów klasy EDR (Endpoint Detection and Response), informacji o ruchu sieciowym na poziomie szczegółowości systemów klasy NTA (Network Traffic Analysis), logów systemów operacyjnych, aplikacji, urządzeń bezpieczeństwa. W ramach analizy procesu obsługi incydentów dla wszystkich zdarzeń zakwalifikowanych jako potencjalny incydent*dostawca* dokona krzyżowego sprawdzenia danych w powyższych źródłach informacji.

otrzymuje on następujące brzmienie:

1.44. Usługi monitoringu zdarzeń muszą być realizowane co najmniej na podstawie dwóch źródeł danych: informacji o ruchu sieciowym na poziomie szczegółowości dostarczonego systemu NDR, urządzeń bezpieczeństwa (FortiAnalyzer). W ramach analizy procesu obsługi incydentów dla wszystkich zdarzeń zakwalifikowanych jako potencjalny incydent*dostawca* dokona krzyżowego sprawdzenia danych w powyższych źródłach informacji.

W załączeniu Rozdział III SWZ po zmianie.

II. W SPECYFIKACJI WARUNKÓW ZAMÓWIENIA pkt. 16 – Miejsce i termin składania ofert oraz ppkt 16.1 oraz 16.2

16.1. Ofertę wraz z załącznikami należy złożyć za pośrednictwem platformy zakupowej pod adresem: https://www.platformazakupowa.pl/pn/pzh **do dnia 04.08.2023 r. do godz. 09.00.**
Celem prawidłowego złożenia oferty Zamawiający zamieścił na stronie platformy zakupowej pod adresem: https://www.platformazakupowa.pl/pn/pzh plik pn. Instrukcja składania oferty dla Wykonawcy.

16.2. Otwarcie ofert nastąpi **w dniu 04.08.2023 r. o godz. 09:30.**

Zamawiający zmienia treść przytaczanego zapisu i nadaje mu nowe brzmienie:

16.1. Ofertę wraz z załącznikami należy złożyć za pośrednictwem platformy zakupowej pod adresem: https://www.platformazakupowa.pl/pn/pzh **do dnia 08.08.2023 r. do godz. 09.00.**
Celem prawidłowego złożenia oferty Zamawiający zamieścił na stronie platformy zakupowej pod adresem: https://www.platformazakupowa.pl/pn/pzh plik pn. Instrukcja składania oferty dla Wykonawcy.

16.2. Otwarcie ofert nastąpi **w dniu 08.08.2023 r. o godz. 09:30.**

IV. W SPECYFIKACJI WARUNKÓW ZAMÓWIENIA pkt. 13 – Termin, do którego Wykonawca będzie związany złożoną ofertą. ppkt. 13.1 jest:

13.1. Wykonawca jest związany ofertą przez okres 30 dni, tj. **do dnia 02.09.2023 r**., przy czym pierwszym dniem terminu związania ofertą jest dzień, w którym upływa termin składania ofert.

Zamawiający zmienia treść przytaczanego zapisu i nadaje mu nowe brzmienie:

13.1. Wykonawca jest związany ofertą przez okres 30 dni, tj. **do dnia 06.09.2023 r**., przy czym pierwszym dniem terminu związania ofertą jest dzień, w którym upływa termin składania ofert.

Zamawiający informuje, iż w wyniku niniejszej zmiany treści SWZ, dokonał zmiany treści ogłoszenia o zamówieniu jak również modyfikuje termin składania i otwarcia ofert.

ZATWIERDZIŁ:

Dyrektor Narodowego Instytutu Zdrowia Publicznego PZH

–Państwowego Instytutu Badawczego

Bernard Waśko