Główny Inspektorat Ochrony Środowiska

Inspekcji Ochrony Środowiska

Departament Informatyzacji

tel. + 48 22 36 92 329 e-mail: sekretariatdinf@gios.gov.pl ul. Bitwy Warszawskiej 1920 r. 3, 02–362 Warszawa

Warszawa, dnia: 29 lipca 2022 r.

DINF-SBT.26.5.2022

Zapytanie w sprawie rozeznania rynku na zamówienie

pt.: „Usługa zdalnego monitorowania cyberbezpieczeństwa”

Zamawiający - Główny Inspektorat Ochrony Środowiska, ul. Bitwy Warszawskiej 1920 r. 3, 02-362 Warszawa, zamierza wszcząć zamówienie publiczne na usługę przeprowadzenia audytu bezpieczeństwa sieci i rozwiązań IT na potrzeby Zamawiającego - Głównego Inspektoratu Ochrony Środowiska (w skr. GIOŚ), ul. Bitwy Warszawskiej 1920 r. nr.3, 02-362 Warszawa.

W związku z tym zwracamy się do potencjalnych Wykonawców o przedłożenie wstępnego oszacowania kosztów, terminu dostawy oraz czasu realizacji zamówienia.

Główny Inspektorat Ochrony Środowiska informuje, że niniejsze zapytanie nie stanowi oferty w rozumieniu art.66 Kodeksu Cywilnego, ani nie jest ogłoszeniem o zamówieniu w rozumieniu ustawy Prawo Zamówień Publicznych. Informacja ta ma na celu wyłącznie ustalenie wartości szacunkowej poszczególnych zadań. Ostateczny opis przedmiotu zamówienia może się różnić od przedstawionego poniżej.

Kod CPV:
48000000-8 Pakiety oprogramowania i systemy informatyczne

1. **Cel zamówienia:**
   Celem zamówienia będzie usługa **zdalnego monitorowania cyberbezpieczeństwa infrastruktury IT na potrzeby GIOŚ** w opisanym poniżej zakresie.
2. **Przewidywany zakres zamówienia:**
   Ww. usługa monitorowania będzie realizowana zdalnie, w oparciu o rozwiązanie techniczne Wykonawcy dostarczone i zainstalowane w sieci i na urządzeniach Zamawiającego, umożliwiając Zamawiającemu podejmowanie decyzji o sposobie reakcji na zagrożenia i incydenty bezpieczeństwa na podstawie informacji dostępnych z konsoli systemu. W ramach usługi „Monitoringu bezpieczeństwa”, prowadzone będą analizy bezpieczeństwa na podstawie logów możliwych do pozyskania z urządzeń i rozwiązań funkcjonujących

w ramach adresacji IP sieci GIOŚ, dostępnych wewnątrz sieci WAN (rozumianej jako lokalizacje widoczne i zarządzane centralnie), Zamawiającego mającego główna siedzibę na ul. Bitwy Warszawskiej 1920 r. 3 w Warszawie.

3. **Założenia techniczne oczekiwanego rozwiązania**

Zamawiający dla realizacji usługi monitoringu bezpieczeństwa oczekuje uruchomienia lokalnego modelu instalacji i funkcjonowania systemu klasy SIEM (system bezpieczeństwa zainstalowany na urządzeniach i w lokalizacji klienta). Monitorowanie zdarzeń i zarządzanie systemem powinno odbywać się zdalnie przez Zespół Wykonawcy przy wykorzystaniu zabezpieczonego połączenia. Optymalne dla Zamawiającego rozwiązanie techniczne to instalacja na pojedynczej maszynie wirtualnej (jednak nie więcej niż na dwóch) zawierająca w sobie wszystkie niezbędne komponenty oraz elementy potrzebne do tego, aby we właściwy sposób zbierać, przetwarzać i analizować logi oraz zdarzenia.

W ramach zaoferowanego rozwiązania Wykonawca winien być uruchomiony system umożliwiający zbieranie logów na poziomie co najmniej 1500 EPSów (Events Per Second). Zakres modułów zaoferowanego rozwiązania, powinien obsługiwać co najmniej funkcje:

a. pobierania danych,
b. przechowywania, wyszukiwania i zarządzania bazą zebranych logów,
c. obsługi warstwy analitycznej i interfejsu użytkownika

Monitoring zdarzeń powinien odbywać się przy wykorzystaniu konsoli operatorskiej systemu, do której wysyłane są same alarmy o ewentualnych zagrożeniach poprzez bezpieczne połączenie VPN. Analiza powinna być realizowana w lokalnym systemie, również dane przechowywane musza być lokalnie i nie mogą być wysyłane poza infrastrukturę Zamawiającego.

4. **Model czasowy świadczenia usług**

Zaoferowany zakres świadczonych usług może dotyczyć dwóch modeli czasowych realizowanego monitoringu:

- całodobowy w trybie 24/7,
- realizowany w godzinach popołudniowych i nocnych (16:00-8:00) oraz w dni wolne i weekendy.

5. **Zaoferowana usługa monitorowania cyberbezpieczeństwa infrastruktury IT winna obejmować:**

a) usługę „Monitoring bezpieczeństwa”, w ramach której system SIEM i operatorzy Wykonawcy monitorują i alarmują o incydentach bezpieczeństwa, wykrytych w infrastrukturze Zamawiającego. Operatorzy obserwują logi, procesy i systemy klienta oraz stosują odpowiednie techniki do zbieranych i porównywania danych z różnych źródeł/urządzeń, w celu wykrycia nietypowej aktywności w infrastrukturze. Zespół

operatorów Wykonawcy ma za zadnie: wstępną klasyfikację poziomu incydentu/zagrożenia, komunikacje z Zamawiającym w zakresie obsługi zagrożeń i incydentów oraz zapewnienie dostępu i porównane tych informacji z danymi o rejestrowanych incydentach z sektorowego CSIRT/CERT w zakresie potrzebnym do realizacji postawionych zadań.

b) dodatkowe elementy usługi – tj. pulę godzin (wskazaną w ofercie) obejmującą pracę dedykowanego zespołu analityków (tzw. 2 linii wsparcia), których zakresem działania są zaawansowane usługi bezpieczeństwa obejmujące wszystkie zadania analityczne związane z obsługą incydentów bezpieczeństwa jak i proaktywne działania mające na celu jak najlepsze zabezpieczenie infrastruktury Zamawiającego przed ewentualnymi zagrożeniami, w tym konfiguracje i rekonfiguracje zainstalowanego rozwiązania Wykonawcy w zakresie zidentyfikowanego lub wskazanego zakresu zmieniających się potrzeb.

c) Zespoły Wykonawcy będą też odpowiedzialne za współdziałanie Zamawiającego z sektorowym CSIRT w zakresie ew. obsługi incydentu jak i późniejszą koordynację działań mających na celu usunięcie skutków incydentu i przywrócenie poprawnego działania infrastruktury Zamawiającego. Usługa powinna dawać możliwość prowadzenia i systematycznego szacowania ryzyka zdarzeń lub incydentów łącznie z obsługą procesu zarządzania ryzykiem pojawiających się incydentów w oparciu o najbardziej aktualny stan wiedzy.

Zakres obsługi i analiz monitorowania cyberbezpieczeństwa infrastruktury IT zawarty w ramach usługi:

1) **Obsługa zdarzeń (incydentu/zagrożenia)**

a) Zdalna analiza zgłoszenia, zebranie wszystkich niezbędnych informacji do poprawnej obsługi incydentu, weryfikacja poprawności i kompletności uzyskanych danych źródłowych;

b) Dla zdarzeń o wysokim priorytecie: opracowanie/realizacja scenariusza obsługi incydentu lub zagrożenia oraz wsparcie pracowników Zamawiającego przy realizacji przygotowanego scenariusza;

c) Przygotowanie i realizacja wspólnie z zespołem Zamawiającego scenariusza działań naprawczych mających na celu niedopuszczenie do materializacji zagrożenia ew. usunięcie skutków incydentu;

d) Opracowanie wniosków z incydentu mających na celu ograniczenie możliwości powtórzenia się danego typu incydentu w przyszłości lub ograniczenia skutków występującego zagrożenia wynikającego z obsługi procesu zarzadzania ryzykiem.

2) **Zakres analiz:**

a) Analiza logów pod kątem zabezpieczenia klienta przed pojawiającymi się nowymi zagrożeniami nie objętymi dotychczasowymi regułami zaimplementowanymi w systemie SIEM jak i procedurami reakcji;
b) Konfiguracja/rekonfiguracja reguł korelacyjnych (nowych scenariuszy) bezpieczeństwa do wdrożenia w zainstalowanym systemie SIEM i propozycje optymalizacji aktualnie działających scenariuszy bezpieczeństwa. Analiza logów pod kątem zoptymalizowanych reguł i informacji o zagrożeniach;
c) Analiza potrzeb Zamawiającego w zakresie rozszerzenia monitorowania o kolejne elementy systemów teleinformatycznych Zamawiającego.

3) **Zakres konsultacji i raportowania:**
a) Propozycja zabezpieczenia systemu przed przyszłymi podobnymi przypadkami, identyfikacji przyczyn problemu oraz jego ew. źródeł. Dodatkowo opracowanie instrukcji/wytycznych w zakresie powiadomienia odpowiednich służb, o ile jest to wymagane przepisami;
b) Przygotowanie kwartalnych raportów podsumowujących stan godzinowej realizacji umowy oraz zakresu merytorycznego zdarzeń bezpieczeństwa z ostatniego kwartału (określenie możliwości optymalizacji funkcjonowania monitorowania bezpieczeństwa);
c) Raport powinien zawierać informacje o wykrytych zagrożeniach oraz działaniach zapobiegawczych zaleconych do natychmiastowego podjęcia (w uzgodnieniu z Zamawiającym), a także działań korygująco-naprawczych oraz zaleceń w zakresie koniecznych do podjęcia samodzielnie przez Zamawiającego działań wzmacniających i rekonstrukcyjnych rozwiązania bezpieczeństwa.

6. Dodatkowe informacje i wymagania:

a) o zamówienie będzie mógł się ubiegać Wykonawca, który w ciągu ostatnich dwóch lat (w okresie od styczeń 2020r. do lipiec 2022r.) realizował podobne co do zakresu usługi na określonym przez Zamawiającego łącznym poziomie kwot tych zamówień. Ponadto Zamawiający zastrzega, że wszelkie prowadzone w ramach usługi prace instalacyjne/rekonfiguracyjne mogą być realizowane w godzinach 8:00-16:00 pod warunkiem uzgodnienia wsparcia ze strony Zamawiającego.
b) umowa na realizacje usługi monitorowania bezpieczeństwa zostanie zawarta na 6 miesięcy i będzie płatna comiesięcznie z opcją przedłużenia na kolejne 12 miesięcy pod warunkiem deklaracji (opcja) podjęcia przez Wykonawcę obsługi rozwiązania SIEM zakupionego przez Zamawiającego i realizacji powyższej usługi z jego wykorzystaniem. Konieczne jest wskazanie w przedłożonej ofercie ceny realizacji

usługi z wykorzystaniem własnego rozwiązania SIEM i ceny realizacji usługi przy wykorzystaniu rozwiązania zakupionego przez Zamawiającego. W przypadku braku specjalistów i/lub możliwości obsługi rozwiązania zakupionego przez Zamawiającego umowa ulega rozwiązaniu po 6 miesiącach bez żadnych wzajemnych roszczeń Stron.

7. **Termin składania szacunkowej ofert:**

   Szacunkowe oferty należy złożyć elektronicznie na adres oferty.dinf@gios.gov.pl do dnia 12-08-2022 r. do godziny 14:00, w formie opisu i/lub ew. uwag do zakresu wskazanego w niniejszym Zapytaniu.

   W ramach szacunkowej wyceny należy podać wartość netto, stawkę podatku VAT, wartość brutto wyrażone w polskich złotych. Wycena powinna obejmować wszystkie koszty związane z realizacją pełnego zakresu przedmiotu zamówienia (z uwzględnieniem opcji) i w miarę możliwości odnosić się do każdego ze wskazanych zakresów.

8. **Osoby wskazane do kontaktu:**

   Osoba uprawniona do kontaktu z potencjalnymi Wykonawcami:

(imię i nazwisko)	Jerzy Goraziński
(Wydział / Departament)	Departament Informatyzacji
(telefon)	22 396 22 98 w godzinach 9:00 – 15:00
(adres e-mail)	j.gorazinski@gios.gov.pl

Marcin Stalpiński
Dyrektor Departamentu

/podpisano kwalifikowanym podpisem elektronicznym/