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: 21 października 2022 r.

DINF-SBT.26.6.2022

Zapytanie w sprawie rozeznania rynku na zamówienie

pt.: „Usługa zdalnego monitorowania cyberbezpieczeństwa IT – Zdalny SOC”

Zamawiający, Główny Inspektorat Ochrony Środowiska (w skr. GIOŚ), ul. Bitwy Warszawskiej 1920 r. nr. 3, 02-362 Warszawa, zamierza wszcząć zamówienie publiczne i dokonać zakupu usługi „Zdalnego monitorowania cyberbezpieczeństwa IT - Zdalny SOC”, na potrzeby Zamawiającego.

W związku z koniecznością dokonania precyzyjnego i odniesionego do aktualnych warunków rozeznania rynku, zwracamy się do potencjalnych Wykonawców o odniesienie się do przedstawionego zakresu usługi i przedłożenie wstępnego oszacowania kosztów, terminu rozpoczęcia świadczenia usługi 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 i możliwości realizacji opisanych zadań. Ostateczny opis przedmiotu zamówienia może się różnić od przedstawionego poniżej.

Kod CPV:

72510000-3 Usługi zarzadzania wspierane komputerowo
72590000-7 Profesjonalne usługi komputerowe
48219000-6 Pakiety oprogramowania do różnych operacji sieciowych

1. **Cel zamówienia:**
   Celem zamówienia będzie zakupienie usługi **Zdalnego monitorowania cyberbezpieczeństwa infrastruktury IT na potrzeby GIOŚ** – „Zdalny SOC”, 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

(aplikacja), umożliwiając Zamawiającemu podejmowanie decyzji o sposobie reakcji na zagrożenia i incydenty bezpieczeństwa na podstawie informacji dostępnych z konsoli systemu i informacji przekazywanych przez Zespół SOC Wykonawcy. W ramach usługi Zdalny SOC, prowadzone będą analizy zagrożeń na podstawie logów możliwych do pozyskania z urządzeń i rozwiązań funkcjonujących w ramach adresacji IP sieci GIOŚ, dostępnych w sieci WAN Zamawiającego (rozumianej jako lokalizacje i urządzenia widoczne i zarządzane centralnie), mającego główna siedzibę na ul. Bitwy Warszawskiej 1920 r. nr. 3 w Warszawie.

A. OPIS OCZEKIWANEGO ROZWIĄZANIA

a) podstawowa usługa to monitorowanie bezpieczeństwa, w ramach której opierając się co najmniej o wskazania systemu klasy SIEM, operatorzy Wykonawcy monitorują i alarmują o zagrożeniach i incydentach bezpieczeństwa, wykrytych w infrastrukturze Zamawiającego. Operatorzy obserwują logi, procesy i systemy Zamawiającego oraz stosują odpowiednie techniki do zbieranych i porównywania danych z różnych źródeł/urządzeń, w celu wykrycia nietypowej lub ewidentnie wrogiej aktywności w infrastrukturze. Zespół operatorów Wykonawcy ma za zadnie: dokonać wstępnej klasyfikacji poziomu incydentu/zagrożenia, podjąć komunikację z Zamawiającym w zakresie obsługi zagrożeń i incydentów oraz zapewnić dostęp i porównane tych informacji z danymi o rejestrowanych incydentach z sektorowego CSIRT/CERT w zakresie potrzebnym do realizacji prowadzonych ustaleń.

b) dodatkowe elementy usługi – tj. pula godzin (powinna zostać określona w ofercie Wykonawcy) obejmująca pracę dedykowanego zespołu analityków (tzw. 2 linii wsparcia), których zakresem działania są zaawansowane usługi bezpieczeństwa obejmujące zadania analityczne związane z obsługą zidentyfikowanych incydentów bezpieczeństwa, jak i późniejsze proaktywne zalecenia i działania mające na celu jak najlepsze zabezpieczenie infrastruktury Zamawiającego przed ewentualnymi zagrożeniami.

   W tym zakresie mieści się również raportowanie i rekonfiguracja (update) rozwiązania Wykonawcy zainstalowanego u Zamawiającego w zakresie zidentyfikowanego i zmieniającego się zakresu potrzeb.

c) Zespoły Wykonawcy będą odpowiedzialne za wsparcie Zamawiającego w zakresie współdziałania Zamawiającego z sektorowym CSIRT przy obsłudze incydentów, jak i późniejszą koordynację działań mających na celu usunięcie skutków incydentu i przywrócenie poprawnego działania infrastruktury Zamawiającego. Usługa powinna dawać możliwość prowadzenia szacowania ryzyka zdarzeń lub incydentów łącznie

z obsługą procesu zarządzania ryzykiem pojawiających się incydentów w oparciu o najbardziej aktualny stan wiedzy.

B. OCZEKIWANY SPOSÓB REALIZACJI USŁUG

Zamawiający dla realizacji usługi monitoringu bezpieczeństwa oczekuje co najmniej instalacji i uruchomienia lokalnego rozwiązania systemu bezpieczeństwa klasy SIEM zainstalowanego na urządzeniach i w lokalizacji klienta. Monitorowanie zdarzeń i zarządzanie systemem powinno odbywać się zdalnie przez Zespół Wykonawcy przy wykorzystaniu bezpiecznego połączenia. Optymalne dla Zamawiającego rozwiązanie techniczne to instalacja rozwiązania na platformie wirtualnej, zawierająca w sobie wszystkie niezbędne komponenty oraz elementy potrzebne do tego, aby we właściwy sposób zbierać, przetwarzać i analizować logi zdarzeń w tym zagrożeń i incydentów bezpieczeństwa.

Rozwiązanie powinno również zapewniać prezentacje informacji nt. zagrożeń i/lub incydentów u Zamawiającego w formie aktualizowanych na bieżąco dashboardów.

Zadaniem Zespołu operatorów Wykonawcy będzie wskazanie oraz klasyfikacja poziomu zagrożenia/incydentu oraz zapewnienie dostępu do informacji pozwalających na sprawne zarządzenie zarejestrowanymi zdarzeniami. Zespół Wykonawcy będzie też odpowiedzialny za współdziałanie z sektorowym CSIRT podczas obsługi incydentu jak i późniejszą koordynację działań i komunikacji partnerów zaangażowanych w usuwanie skutków incydentu.

Zespół Wykonawcy powinien zapewnić dostęp do informacji o rejestrowanych incydentach w zakresie potrzebnym do realizacji postawionych zadań związanych z identyfikowaniem i zapobieganiem incydentom wykrywanym na bazie systemu klasy SIEM.

Usługa realizowana przez Zdalny SOC powinna umożliwiać prowadzenie i systematyczne szacowania ryzyka zdarzeń lub incydentów włącznie z procesem zarządzania ryzykiem oraz incydentami w oparciu o aktualny stan wiedzy.

Podział na I i II linię/zespoły wsparcia jest podziałem wymagającym zaangażowania (wskazania w umowie) innych wykonawców do każdego z Zespołów.

a. Zakres zadań I linii wsparcia usługi Zdalny SOC:

   Monitoring:

   - Bieżące monitorowanie zgłoszeń i incydentów wykrytych przez system monitorowania bezpieczeństwa,
   - Ustalenie typu i poziomu zagrożenia ze strony wykrytego zdarzenia,
   - Wstępna analiza zagrożeń uznanych za incydenty, zgodnie z ustalonymi procedurami i scenariuszami uzgodnionymi z Zamawiającym.

   Zarządzanie incydentami:

- Samodzielna obsługa zagrożeń uznanych za incydenty o niskim priorytecie, które zostały opisane w procedurach uzgodnionych z Zamawiającym i nie kończą się eskalacją.

Raportowanie:

- Realizacja okresowych raportów podsumowujących ilość incydentów i czasy obsługi, w terminach ustalonych w zależności od wpływu i wagi zagrożeń na bezpieczeństwo Zmawiającego.

Czas reakcji:

- Usługa świadczona zgodnie z zaproponowanym w ofercie SLA uzgodnionym z Zamawiającym,
- Czas reakcji operatorów wskazany w SLA jest liczony jako czas od pojawienia się zdarzenia w systemie SIEM do uznania go za ryzyko bądź incydent wymagający działania, do podjęcia przez operatorów pierwszych działań ograniczających ryzyko lub likwidujących incydent.

b. Dodatkowe elementy usługi – zakres II linii wsparcia SOC:
   - wskazana pula godzin obejmująca pracę dedykowanego zespołu analityków (II Linii Zdalny SOC), których zakresem działania jest Zarządzanie Incydentami Bezpieczeństwa Informatycznego mające na celu analizy w tym:
     - pomoc I Linii usług SOC w zapobieganiu zidentyfikowanym incydentom
     - zadania analityczne związane z obsługą incydentów bezpieczeństwa w tym działania mające na celu wykrycie źródeł ataku i jak najlepsze zabezpieczenie infrastruktury Zamawiającego przed powtórzeniem się incydentów
     - zapobieganie potencjalnym zagrożeniom cybernetycznym wynikającym z aktualnego stanu wiedzy w zakresie cyberbezpieczeństwa, w tym nowych rodzajów ataków i ich scenariuszy do implementacji/aktualizacji w narzędziach wykorzystywanych przez I Linię wsparcia.

C. ZAKRES ZADAŃ DO REALIZACJI W RAMACH USŁUGI ZDALNY SOC

1) Zadanie obsługi 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 i współpraca przy realizacji przygotowanego scenariusza;

c) Przygotowanie i realizacja wspólnie z zespołem Zamawiającego scenariuszy działań naprawczych mających na celu niedopuszczenie do materializacji zagrożeń 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 (w tym automatyzacji) 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 na zagrożenia;
b) Konfiguracja/rekonfiguracja reguł korelacyjnych (nowych scenariuszy) bezpieczeństwa do wdrożenia w zainstalowanym u Zamawiającego systemie SIEM i/lub propozycje optymalizacji aktualnie działających scenariuszy bezpieczeństwa. Analiza logów pod kątem zoptymalizowanych reguł i śledzenia informacji o zagrożeniach;
c) Analiza potrzeb Zamawiającego w zakresie rozszerzenia monitorowania na kolejne elementy systemów teleinformatycznych Zamawiającego.

3) Zakres konsultacji i raportowania:

a) Propozycja zabezpieczenia systemów Zamawiającego przed powtórzeniem podobnych do już zidentyfikowanych zdarzeń oraz identyfikacji przyczyn problemu i wskazanie jego ew. źródeł. Dodatkowo opracowanie instrukcji/wytycznych w zakresie obsługi incydentów w tym powiadomienia odpowiednich służb, o ile jest to wymagane przepisami;
b) Przygotowanie kwartalnych raportów podsumowujących stan godzinowej realizacji umowy (II Linii SOC) oraz zakresu merytorycznego wykrytych zdarzeń bezpieczeństwa z ostatniego kwartału (określenie możliwości optymalizacji funkcjonowania systemów i zasad 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 w tym zaleceń w zakresie koniecznych do podjęcia samodzielnie przez Zamawiającego działań wzmacniających i rekonstruujących rozwiązania bezpieczeństwa.

4) Założenia techniczne:

W ramach zaoferowanego rozwiązania Wykonawca winien uruchomić system klasy SIEM umożliwiający zbieranie logów co najmniej na poziomie:

- 1500 stacji roboczych,
- 200 serwerów (maszyn wirtualnych, urządzeń aktywnych),
- docelowo, po pełnym wdrożeniu i skonfigurowaniu scenariuszy oczekiwana wydajność rozwiązania klasy SIEM do 1500 EPS (Events Per Second) bez zmiany ceny świadczenia usługi.

Zakres modułów zaoferowanego rozwiązania, powinien co najmniej umożliwiać obsługę funkcji:

- pobierania danych,
- przechowywania, wyszukiwania i zarządzania bazą zebranych logów,
- obsługi warstwy analitycznej i interfejsu użytkownika w tym prezentacji na dashboardach.

Monitoring zdarzeń przez personel Zdalnego SOC powinien odbywać się przy wykorzystaniu konsoli operatorskiej systemu, do której wysyłane są jedynie alarmy o ewentualnych zagrożeniach poprzez bezpieczne połączenie VPN. Analiza powinna być realizowana w oparciu o lokalnie zainstalowany u Zamawiającego system, a dane nie mogą być przechowywane poza infrastrukturę Zamawiającego.

5) Model czasowy świadczenia usług

Zaoferowany zakres świadczonych usług może odnosić się do dwóch możliwych modeli czasowych realizowanego monitoringu przez Zdalny SOC:

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

D. DODATKOWE INFORMACJE I WYMAGANIA

a) o zamówienie będzie mógł się ubiegać Wykonawca, który w ciągu ostatnich dwóch lat kalendarzowych realizował zadania i/lub usługi podobne co do zakresu określonego przez Zamawiającego w zapytaniu, posiada odpowiednie rozwiązania techniczne i personel.

b) Zamawiający zastrzega, że wszelkie prowadzone w ramach instalacji i uruchomienia usługi prace instalacyjne/rekonfiguracyjne oprogramowania u urządzeń mogą być realizowane w godzinach 8:00-16:00 w dni robocze, pod warunkiem uzyskania zgody ze strony Zamawiającego.

c) umowa na realizacje usługi monitorowania bezpieczeństwa „Zdalny SOC” może zostać zawarta na 12 miesięcy z opcją przedłużenia na kolejne 12 miesięcy.

d) w przypadku dokonania przez Zamawiającego zakupu własnego systemu odpowiadającego klasie SIEM umowa będzie umożliwiać jej rozwiązanie w okresie 3

miesięcy od uruchomienia przez Zamawiającego własnego systemu klasy SIEM bez żadnych wzajemnych roszczeń Stron.

e) oferta nie może zawierać innych zobowiązań finansowych lub opłat (wstępnych, zależnych od rozbudowy elementów technicznych itp.) poza równą stawką opłaty miesięcznej (ryczałt) przez okres 12 miesięcy.

f) dla realizacji płatności zastosowana zostanie opłata miesięczna (ryczałt), który musi mieć stałą wartość i nie może być uzależniony od modelu SLA i kwota zmienna miesięcznie wynikająca z ilości godzin wsparcia/konsultacji/usług II linii wsparcia SOC i stawki godzinowej, która zostanie skalkulowana w umowie ale nie musi zostać wykorzystana w całości.

g) usługi II linii wsparcia musza mieć określony: stały koszt godzinowy, stałą miesięczną ilość godzin (lub ilość godzin określoną dla całej umowy, która nie może być mniejsza niż 600 godzin w okresie 12 miesięcy) i możliwość realizowania/grupowania godzin w okresie całej umowy.

h) miesięczna faktura za realizację usługi Zdalny SOC powinna składać się ze stałej wartości ryczałtu oraz zmiennej, zależnej od ilości wykorzystanych godzin, wartości wynikającej z ceny za godzinę razy ilość godzin w danym miesiącu.

i) z uwagi na konieczność uzyskania porównywalnych ofert załączony został Formularz zawierający elementy niezbędne do prawidłowego oszacowania przez Zamawiającego ceny usługi.

3. Termin składania szacunkowej ofert:

Szacunkowe oferty należy złożyć elektronicznie na adres oferty.dinf@gios.gov.pl do dnia 31-10-2022 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.

4. Osoby wskazane do kontaktu:

Osoba uprawniona do kontaktu z potencjalnymi Wykonawcami:

(imię i nazwisko)	Jerzy Goraziński
(Wydział / Departament)	Departament Informatyzacji
(telefon)	22 369 17 10 w godzinach 9:00 – 15:00
(adres e-mail)	j.gorazinski@gios.gov.pl

Załączniki:

- Formularz szacowania ceny

Marcin Stalpiński
Dyrektor Departamentu

/*podpisano kwalifikowanym podpisem elektronicznym*/

GŁÓWNY INSPEKTORAT OCHRONY ŚRODOWISKA
M: gios@gios.gov.pl
W: www.gios.gov.pl
A: ul. Bitwy Warszawskiej 1920 r. nr 3
02-362 Warszawa
T: +48 22 369 22 26
F: +48 22 825 04 65