Ministerstwo Rozwoju i Technologii

ul. Plac Trzech Krzyży 3/5

00-507 Warszawa

ZAPYTANIE O WYCENĘ DO OSZACOWANIA WARTOŚCI ZAMÓWIENIA

Ministerstwo Rozwoju i Technologii planuje uruchomić postępowanie przetargowe o udzielenie zamówienia publicznego na zakup i wdrożenie usług SOC (Security Operations Center).

Uprzejmie prosimy o wycenę, poniżej opisanych minimalnych wymagań stanowiących przedmiot planowanego zamówienia do wszczęcia postępowania przetargowego na zakup i wdrożenie usług SOC (Security Operations Center). W tym celu uprzejmie prosimy o wypełnienie załączonego Formularza Ofertowego.

I. PRZEDMIOT ZAMÓWIENIA

Przedmiotem Zamówienia jest zakup i wdrożenie usług SOC (Security Operations Center) który zostanie zrealizowany poprzez wykonanie następujących zadań:

1) wdrożenie i świadczenie usług SOC przez okres 24 miesięcy;
2) świadczenie usługi asysty technicznej na podstawie dodatkowych zleceń Zamawiającego.

II. TERMIN REALIZACJI ZAMÓWIENIA

Przedmiot zamówienia zostanie zrealizowany w terminie:

1) maksymalnie **do 30 dni** od daty podpisania przez strony umowy w zakresie wdrożenie i rozpoczęcie świadczenia usług SOC
2) 24 miesięcy od daty podpisania przez strony umowy w zakresie usługi asysty technicznej lub do wyczerpania liczby roboczogodzin, w zależności co nastąpi w pierwszej kolejności.

III. MINIMALNE WYMAGANIA DOTYCZĄCE REALIZACJI PRZEDMIOTU ZAMÓWIENIA

1) W ramach realizacji przedmiotu zamówienia Wykonawca dostarczy i wdroży usługę SOC (Security Operations Center) w oparciu o systemy SIEM oraz SOAR będące własnością Zamawiającego.
2) Zamawiający wymaga, aby podmiot świadczący usługi SOC znajdował się na liście Trusted Introducer oraz posiadał aktywny stan „akretydowany” (ang. acredited). Link - https://www.trusted-introducer.org/trusted-introducer/
3) Zamawiający wymaga, aby podmiot świadczący usługi SOC posiadał, utrzymywał i aktualizować system zarządzania bezpieczeństwem informacji spełniający wymagania Polskiej Normy PN-EN ISO/IEC 27001 w zakresie obejmującym co najmniej świadczone usługi.
4) Zamawiający wymaga uruchomienia usługi opartej o 3 linie wsparcia. L1 – Monitoring, L2 – Zespół reagowania L3 – Zespół ekspercki
5) W ramach 1-szej linii tj. L1 zamawiający wymaga:
   a. Prowadzenia monitoringu w trybie ciągłym 24/7/365
   b. Prowadzenia w trybie ciągłym analizy i weryfikacji zdarzeń z systemu SIEM
   c. Analiza prowadzona jest w oparciu o wcześniej zaimplementowane reguły korelacyjne w systemie SIEM
   d. Wykonanie oceny stopnia niebezpieczeństwa dla stwierdzonego wystąpienia incydentu (Krytyczny, Wysoki, Średni, Niski)
   e. Analizę danych incydentu i potwierdzenie, że zawierają wszystkie niezbędne dane tj. data wystąpienia incydentu, stopień niebezpieczeństwa, sposób/miejsce przełamania

zabezpieczeń, wzkaźniki kompromitacji (ang. IoC – Indicators of Compromise) (w zależności od dostępności danych w Systemie SIEM)

f. Poinformowanie wyznaczonej osoby z zespołu Zamawiającego o wystąpieniu incydentu o poziomie krytycznym i wysokim wraz z przekazaniem uzyskanych we wstępnej analizie, celem dalszej analizy i mitygacji skutków zdarzenia przez Zamawiającego
g. Koordynowanie obsługi incydentów rozumianej jako nadzór nad procesem obsługi incydentu polegająca na dystrybucji zadań w zakresie prowadzonej analizy, informowanie osób upoważnionych.
h. Przygotowywanie i dostarczanie raportów okresowych.

6) W ramach 2-giej linii tj. L2 Zamawiający wymaga:
   a. Prowadzania szczegółowej analizy incydentów bezpieczeństwa na poziomie krytycznym i wysokim.
   b. Szczegółowa analiza polega na dostarczeniu pełnego obrazu wraz ze szczegółami analizowanego incydentu wraz z przekazaniem osobie upoważnionej po stronie Zmawiającego rekomendacji w jaki sposób zidentyfikowany problem powinien zostać rozwiązany
   c. W ramach szczegółowej analizy powinny zostać przekazane minimum poniższe informacje:
      i. Data i godzina wykrycia incydentu
      ii. Poziom niebezpieczeństwa
      iii. Sposób i miejsce przełamania zabezpieczeń
      iv. Wskaźniki kompromitacji
      v. Opis incydentu zawierający wyjaśnienia na podstawie jakich danych dane działanie zostało uznane za niebezpieczne
      vi. Identyfikacja atakującego (Adres IP, Dane właściciela adresu IP, Miasto. Kraj, ASN)
      vii. Cel atakującego (Adres IP, Nazwa systemu lub usługi)
      viii. Rodzaj skompromitowanych danych (Kradzież, modyfikacja, skasowanie, upublicznienie)
      ix. Opis wykorzystanych narzędzi i podjętych kroków w śledztwie
      x. Rekomendowana metoda rozwiązania problemu
7) W ramach 3-ciej linii tj. L3 Zamawiający wymaga:
   a. Prowadzenia aktywnego poszukiwania incydentów bezpieczeństwa poza zdefiniowanymi regułami korelacyjnymi (ang. Threat Hunting) z użyciem ustalonych wcześniej narzędzi i technik np. SIEM, SOAR, XDR, OSINT
   b. Zamawiający wymaga, aby w ramach Threat Hunting 3-cia linia poświęciła przynajmniej 16 roboczogodzin w miesiącu.
   c. W ramach wykonanych prac sporządziła raport z analizy zawierający:
      i. opis stwierdzonych nieprawidłowości, incydentów bezpieczeństwa, braków w danych systemów
      ii. rekomendacje na temat implementacji nowych reguł korelacyjnych w systemie SIEM
      iii. rekomendacje na temat implementacji dodatkowych narzędzi analitycznych w systemie SOAR
      iv. rekomendacje na temat rozbudowy zbieranego zakresu danych do analizy w systemie SIEM
8) Zamawiający posiada wdrożone systemy SIEM, SOAR oraz XDR klasy Enterprise.
9) Dla każdego z systemów Zamawiający posiada aktywną umowę serwisową wraz z dostępnymi usługami asysty technicznej w celu dostosowania ich do wymagań usługi SOC.
10) System SIEM jest zasilany na poziomie ok. 20 0000 zapisywanych zdarzeń na sekundę
11) System SIEM w maksimum przyjmuje zdarzenia na poziomie ok. 50 000 zapisywanych zdarzeń na sekundę
12) Średni dobowy wolumen logów to 125GB
13) Zamawiający zakłada ok. 5 aktywnych użytkowników SIEM
14) Zamawiający posiada około 250 aktywnych reguł korelacyjnych, które w momencie uruchomienia usługi muszą zostać objęte obsługą.
15) Zamawiający na podstawie ostatniego okresu przewiduje wystąpienie około 30 incydentów bezpieczeństwa.

IV. MINIMALNE WYMAGANIA W ZAKRESIE WDROŻENIA SYSTEMU WRAZ Z INSTRUKTAŻEM

1) Wykonawca wdroży usługi SOC nastąpi poprzez:
   a) Przygotowanie planu wdrożenia w uzgodnieniu z Zamawiającym
   b) Uzgodni zasady dostępu i bezpieczeństwa pracy SOC (konta, RBAC, MFA/VPN/jump, audyt działań, zasady zgód)
   c) Przeprowadzi inwentaryzację i analizę stanu SIEM/SOAR (co już jest, jakość danych, integracje, luki)
   d) Przygotuje projekt operacyjny usługi SOC (proces obsługi incydentu, eskalacje, klasyfikacja, SLA)
   e) Przeprowadzi wraz z Zamawiającym uruchomienie obsługi SIEM w tym bazowych detekcji i dashboardów (MVP monitoringu, kolejka alertów/incydentów)
   f) Przeprowadzi wraz z Zamawiającym uruchominienie obsługi SOAR w tym uruchomienie podstawowych playbooków (automatyzacje z kontrolą zgód)
   g) Przeprowadzi pilotaż oraz optymalizację procesów (testy scenariuszy, redukcja false positive, dopięcie braków)
   h) Przeprowadzi wraz Zamawiającym Go-Live i uruchomi usługę produkcyjnie.

V. MINIMALNE WYMAGANIA W ZAKRESIE ASYSTY TECHNICZNEJ

1) Wykonawca przez cały okres trwania umowy zobowiązany będzie do świadczenia usługi asysty technicznej na każde żądanie Zamawiającego, tj. każdorazowo na podstawie pisemnego zlecenia asysty technicznej, wystawianego przez Zamawiającego.
2) Zakres, sposób oraz termin realizacji zostaną uzgodniony na etapie przedstawienia wymagań przez Zamawiającego i wyceny pracochłonności przez Wykonawcę, poprzedzających zlecenie.
3) Zlecenia będą obejmować ekspercie wsparcie w zakresie cyberbezpieczeństwa m. in.:
   - Analiza śledcza (ang. forensic analysis)
   - Testy penetracyjne (ang. penetration tests)
   - Symulacje ataku (ang. Redteaming)
   - Audyt cyberbezpieczeństwa
   - Systemowy przegląd i optymalizacja reguł SIEM
4) Szczegółowy zakres usługi asysty technicznej uwzględniać będzie każdorazowo zlecenie.
5) Usługi asysty technicznej Wykonawca zobowiązuje się realizować w dwóch formach:
   a) w siedzibie Zamawiającego;
   b) zdalnie.
6) Po wykonaniu usług Wykonawca przedłoży Zamawiającemu protokół z wykonania usług asysty zawierający ich rodzaj, zakres oraz termin.
7) Maksymalna liczba roboczogodzin w trakcie trwania umowy wskazana jest w Formularzu Ofertowym.
8) Zamawiający zastrzega sobie prawo do nieudzielania zleceń na usługi asysty technicznej.