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 umowy, zwanym dalej także „zamówieniem", jest świadczenie usługi SOC (Security Operations Center) polegającej na monitorowaniu, analizowaniu i reagowaniu na incydenty związane z cyberbezpieczeństwem.

Zamówienie zostanie zrealizowane poprzez:

1) wdrożenie usługi SOC
2) świadczenie usługi SOC przez okres 12 miesięcy
3) usługi asysty technicznej.

II. TERMIN REALIZACJI ZAMÓWIENIA

Przedmiot zamówienia zostanie zrealizowany w terminie:

1) maksymalnie **do 60 dni** od daty podpisania przez strony umowy w zakresie wdrożenia usługi SOC
2) 12 miesięcy świadczenie usługi SOC od dnia wdrożenia tych usług
3) 12 miesięcy od daty wdrożenia usługi SOC 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, SOAR oraz XDR 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 (Poważnym, Wysoki, Średni, Niski)

e. Analizę danych incydentu i potwierdzenie, że zawierają wszystkie niezbędne dane tj. data wystąpienia incydentu, stopień niebezpieczeństwa, sposób/miejsce przełamania zabezpieczeń, wskaźniki 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 poważnym 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 poważnym i wysokim.
   b. Szczegółowa analiza polega na dostarczeniu pełnego obrazu wraz ze szczegółami analizowanego incydentu wraz z przekazaniem osobie upoważnionej po stronie Zamawiającego 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 klasy Enterprise rozumiejąc przez to rozwiązanie czołowych producentów takich jak Fortinet, IBM, Cisco.
9) Zamawiający posiada system XDR TrendMicro Vision One w wersji SaaS.
10) Dla każdego z systemów Zamawiający posiada aktywną umowę serwisową wraz z dostępnymi usługami asysty technicznej w celu dostosowania ich do wymagań zespołu usługi SOC.
11) System SIEM jest zasilany na poziomie ok. 20 0000 zapisywanych zdarzeń na sekundę
12) System SIEM w maksimum przyjmuje zdarzenia na poziomie ok. 50 000 zapisywanych zdarzeń na sekundę
13) Średni dobowy wolumen logów to 150GB
14) Zamawiający wskazuje, że średnio 5 użytkowników aktywnie pracuje w systemie SIEM. Wartość ta została podana wyłącznie w celu zobrazowania skali zmian konfiguracyjnych oraz liczby osób

zaangażowanych w pracę w systemie i nie oznacza ograniczenia liczby użytkowników mogących równocześnie pracować w systemie.

15) Zamawiający posiada około 250 aktywnych reguł korelacyjnych, które w momencie uruchomienia usługi muszą zostać objęte obsługą. Reguły generują około 100-150 zdarzeń dziennie.
16) Zamawiający na podstawie ostatniego okresu przewiduje wystąpienie około 30 incydentów bezpieczeństwa miesięcznie wymagających analizy, reakcji i wdrożenia zabezpieczeń.
17) Zamawiający na moment prowadzenia postępowania ma zaimplementowane następujące źródła danych systemu SIEM
    a. Stacje robocze użytkowników za pomocą systemu XDR – 1600 sztuk
    b. Serwery z systemem operacyjnym Linux za pomocą agenta SIEM – 300 sztuk
    c. Serwery z systemem operacyjnym Windows za pomocą agenta SIEM – 300 sztuk
    d. Urządzenia sieciowe (Routery, Przełączniki, Bramy głosowe) – 100 sztuk
    e. Zapory sieciowe – 10 sztuk
    f. Serwery www – 50 sztuk
    g. Oprogramowanie Web Application Firewall w formie SaaS
    h. Oprogramowanie biurowe dostarczane w formie SaaS
18) Zamawiający dopuszcza świadczenie usług poprzez integrację usług SIEM z systemem Wykonawcy.
19) Zamawiający obecnie korzysta z ogólnodostępnych narzędzi OSINT, natomiast nie wyklucza zakupu i udostępnienia Wykonawcy takowych, jeżeli będą one wynikały z potrzeb realizacji usług SOC.

IV. MINIMALNE WYMAGANIA DOTYCZĄCE CZASÓW OBSŁUGI INCYDENTÓW

1) Zamawiający w ramach usług SLA definiuje następujące priorytety incydentów:
    a. **Poważny** - Incydent spełnia kryteria Priorytetu Wysokiego oraz jednocześnie dotyczy systemu, zasobu albo zbioru danych, którego naruszenie może skutkować uruchomieniem obowiązków ustawowych Zamawiającego w zakresie cyberbezpieczeństwa lub ochrony danych osobowych. Zakwalifikowanie incydentu do Priorytetu Poważnego skutkuje niezwłocznym uruchomieniem po stronie Zamawiającego procedury eskalacyjnej i notyfikacyjnej. Do Priorytetu Poważnego zalicza się w szczególności incydent:
        i. dotyczący systemu lub zasobu przetwarzającego albo przechowującego dane osobowe w znacznej skali, w tym powyżej 50 rekordów danych osobowych;
        ii. mogący powodować obowiązek zgłoszenia incydentu właściwemu CSIRT lub innemu właściwemu organowi na podstawie ustawy o krajowym systemie cyberbezpieczeństwa;
        iii. mogący powodować obowiązek zgłoszenia naruszenia ochrony danych osobowych Prezesowi UODO lub zawiadomienia osób, których dane dotyczą, na podstawie RODO.
    b. **Wysoki** - Incydent spełnia kryteria Priorytetu Średniego oraz dodatkowo wskazuje na potwierdzone lub wysoce prawdopodobne przełamanie zabezpieczeń, aktywne działanie atakującego albo realne zagrożenie dla poufności, integralności lub dostępności monitorowanego systemu. Do Priorytetu Wysokiego zalicza się w szczególności:
        i. utrzymywanie przez co najmniej 30 minut aktywnego kanału komunikacji z infrastrukturą dowodzenia i kontroli złośliwego oprogramowania;
        ii. potwierdzone przełamanie zabezpieczeń aplikacji lub systemu;
        iii. ujawnienie nieautoryzowanych procesów, wątków, usług, binariów, skryptów lub mechanizmów trwałości;
        iv. potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów;
        v. nieuprawnione uzyskanie lub wykorzystanie uprawnień umożliwiających dalszą eskalację, utrzymanie dostępu, podsłuch transmisji albo wykorzystanie podatności;

vi. potwierdzone ujawnienie lub transfer danych z monitorowanego systemu z użyciem protokołów sieciowych albo nieautoryzowanych nośników;
vii. ujawnienie nieautoryzowanego oprogramowania administracyjnego, narzędzi ofensywnych, grayware lub złośliwego oprogramowania umożliwiającego zdalne wykonanie kodu lub poleceń;
viii. celowany atak na personel Zamawiającego ukierunkowany na pozyskanie danych uwierzytelniających lub uzyskanie dostępu do systemów;
ix. potwierdzona informacja o incydencie pochodząca od właściwego CSIRT, innego uprawnionego podmiotu publicznego albo od uprawnionego przedstawiciela Zamawiającego.

c. **Średni** - Incydent wskazuje na naruszenie bezpieczeństwa albo wysokie prawdopodobieństwo takiego naruszenia, ale na moment klasyfikacji brak jest potwierdzenia przesłanek kwalifikujących incydent do Priorytetu Wysokiego albo Poważnego. Do Priorytetu Średniego zalicza się w szczególności:
i. potwierdzone wskaźniki kompromitacji lub inne wiarygodne dowody naruszenia wykryte przez systemy monitoringu bezpieczeństwa;
ii. nieautoryzowane dysponowanie uprawnieniami administracyjnymi albo użycie kont uprzywilejowanych niezgodnie z przeznaczeniem;
iii. częściowo spersonalizowany atak socjotechniczny na personel Zamawiającego, którego celem jest pozyskanie danych uwierzytelniających lub dostępu do systemu;
iv. wykrycie złośliwego oprogramowania na monitorowanym systemie, jeżeli zostało ono rozpoznane, lecz nie zostało zablokowane lub odizolowane przez inny mechanizm bezpieczeństwa;
v. potwierdzone naruszenie poufności, integralności lub dostępności wykryte przez system bezpieczeństwa, jeżeli użytkownik lub właściciel systemu nie potwierdzi autoryzowanego charakteru działania.

d. **Niski** - Zdarzenie bezpieczeństwa zostało wykryte zgodnie ze scenariuszem reakcji, lecz po analizie potwierdzono, że było skutkiem działań służbowych wykonanych przez osobę uprawnioną, z naruszeniem zasad, standardów albo procedur obowiązujących u Zamawiającego, bez potwierdzenia przełamania zabezpieczeń i bez potwierdzenia naruszenia poufności, integralności lub dostępności systemu.

2) System SIEM nadaje incydentowi wstępny priorytet operacyjny w ramach czasu reakcji. Wstępny priorytet operacyjny służy uruchomieniu właściwego trybu obsługi incydentu oraz zastosowaniu odpowiednich parametrów SLA.
3) Przez czas reakcji należy rozumieć czas liczony od momentu zarejestrowania incydentu w systemie SIEM Zamawiającego do chwili, w której Wykonawca potwierdzi zauważenie incydentu oraz nada mu kategorię priorytetu w systemie SIEM Zamawiającego.
4) Wykonawca zapewni następujące maksymalne czasy reakcji:
a. dla incydentu o priorytecie Poważnym – do 1 godziny
b. dla incydentu o priorytecie Wysokim – do 2 godzin
c. dla incydentu o priorytecie Średnim – do 4 godzin
d. dla incydentu o priorytecie Niskim – do 8 godzin
5) Czasy reakcji objęte SLA mają zastosowanie do maksymalnie 100 incydentów zarejestrowanych w danym dniu kalendarzowym. Po przekroczeniu tego wolumenu kolejne incydenty będą obsługiwane w trybie Best Effort, to znaczy bez gwarancji zachowania wskazanych czasów reakcji.
6) Incydenty o priorytecie Poważnym nie podlegają ograniczeniu ilościowemu 100 incydentów dziennie i podlegają obsłudze zgodnie z czasem reakcji określonym dla tego priorytetu niezależnie od liczby innych incydentów zarejestrowanych w danym dniu.
7) Jeżeli incydent pierwotnie zakwalifikowany do priorytetu Wysokiego, Średniego albo Niskiego zostanie w toku analizy przekwalifikowany do priorytetu Poważnego, od chwili przekwalifikowania incydent podlega obsłudze na zasadach właściwych dla priorytetu Poważnego. Od chwili przekwalifikowania dalsza obsługa incydentu prowadzona jest w trybie

właściwym dla priorytetu Poważnego, uwzględniając ponowne rozpoczęcie biegu parametru czas realizacji.

8) W przypadku ujawnienia nowych okoliczności w toku obsługi incydentu Wykonawca jest uprawniony i zobowiązany do zmiany priorytetu incydentu na wyższy albo niższy, odpowiednio do ustalonego stanu faktycznego. Każda zmiana powinna być uzgodniona z Zamawiającym.
9) Przez czas realizacji należy rozumieć czas liczony od momentu zakończenia czasu reakcji do chwili przekazania Zamawiającemu analizy incydentu oraz rekomendacji dalszych działań.
10) Wykonawca zapewni następujące maksymalne czasy realizacji:
    a. Poważny – do 8 godzin,
    b. Wysoki – do 16 godzin,
    c. Średni – do 40 godzin.
11) Dla incydentów o priorytecie Niskim nie ustala się gwarantowanego czasu realizacji obejmującego przekazanie analizy i rekomendacji, chyba że obowiązek taki zostanie przewidziany w uzgodnionych procedurach operacyjnych.
12) Gwarantowane czasy realizacji mają zastosowanie do maksymalnie 5 incydentów dziennie, dla których Wykonawca zobowiązany jest przygotować i przekazać analizę oraz rekomendacje.
13) Po przekroczeniu wolumenu 5 incydentów dziennie kolejne analizy i rekomendacje będą przygotowywane i przekazywane w trybie Best Effort, bez gwarancji zachowania wskazanych czasów realizacji.
14) Incydenty o priorytecie Poważnym nie podlegają ograniczeniu ilościowemu 5 analiz dziennie. Dla incydentów o priorytecie Poważnym Wykonawca jest zobowiązany przekazać analizę i rekomendacje w czasie właściwym dla tego priorytetu niezależnie od liczby innych incydentów obsługiwanych w danym dniu.
15) W przypadku jednoczesnego wystąpienia kilku incydentów Wykonawca jest zobowiązany organizować obsługę w sposób zapewniający pierwszeństwo incydentom o wyższym priorytecie, przy czym nie może to prowadzić do nieuzasadnionego zaniżania priorytetów incydentów ani do obchodzenia parametrów SLA.

V. MINIMALNE WYMAGANIA W ZAKRESIE WDROŻENIA SYSTEMU WRAZ Z INSTRUKTAŻEM

1) Wykonawca, w terminie do 60 dni kalendarzowych od dnia podpisania Umowy, przeprowadzi wdrożenie usługi SOC w środowisku Zamawiającego oraz przygotuje usługę do świadczenia w trybie produkcyjnym.
2) Wdrożenie obejmuje co najmniej następujące działania:
    a. Wykonawca opracuje i przekaże Zamawiającemu plan wdrożenia, obejmujący co najmniej harmonogram prac, podział odpowiedzialności Stron, zależności organizacyjne i techniczne, wymagane działania po stronie Zamawiającego, ryzyka wdrożeniowe oraz terminy realizacji poszczególnych etapów
    b. Wykonawca,wspólnie z Zamawiającym, uzgodni zasady dostępu do systemów i zasady bezpieczeństwa realizacji usługi SOC, obejmujące co najmniej: sposób realizacji dostępu, wymagania dla kont, zakres uprawnień, zasady RBAC, stosowanie MFA, wykorzystanie VPN i/lub jump host, zasady rejestrowania i audytu działań operatorów SOC oraz przypadki, w których działanie Wykonawcy wymaga uprzedniej zgody Zamawiającego. Za uzgodnione uznaje się wyłącznie zasady potwierdzone przez obie Strony.
    c. Wykonawca przeprowadzi inwentaryzację i analizę stanu początkowego środowiska SIEM i SOAR, obejmujące co najmniej: wykaz istniejących integracji, źródeł logów i telemetrii, ocenę jakości i kompletności danych, przegląd istniejących reguł detekcyjnych, dashboardów, playbooków i mechanizmów eskalacji oraz identyfikację braków, ograniczeń i ryzyk wpływających na uruchomienie usługi.
    d. Wykonawca opracuje i przedstawi Zamawiającemu do akceptacji projekt operacyjny usługi SOC, obejmujący co najmniej: sposób obsługi zdarzeń i incydentów, klasyfikację zdarzeń i incydentów, ścieżki eskalacji, role i odpowiedzialności, zasady współpracy Stron, czasy reakcji i obsługi, zasady komunikacji oraz zakres czynności, które Wykonawca może realizować samodzielnie, i czynności wymagających

uprzedniej zgody Zamawiającego. Przejście do kolejnych etapów wdrożenia w zakresie operacyjnym wymaga akceptacji tego projektu przez Zamawiającego.

e. Wykonawca przeprowadzi pilotaż operacyjny, obejmujący co najmniej testy uzgodnionych scenariuszy obsługi, weryfikację poprawności działania detekcji i playbooków, strojenie reguł w celu ograniczenia liczby zdarzeń false-positive, usunięcie błędów krytycznych oraz uzupełnienie braków uniemożliwiających rozpoczęcie świadczenia usługi w trybie produkcyjnym.

f. Po zakończeniu pilotażu i usunięciu braków krytycznych Wykonawca, wspólnie z Zamawiającym, rozpocznie świadczenie usług SOC produkcyjnie. Rozpoczęcie świadczenia usług nastąpi po potwierdzeniu przez Zamawiającego gotowości do rozpoczęcia świadczenia usługi.

VI. 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.