Ministerstwo
Aktywów Państwowych

Departament Informatyzacji i
Cyberbezpieczeństwa

DIC.I.045.2.2025

IK: 1061314
Warszawa, 16 kwietnia 2025 r.

Protokół z przeprowadzonych wstępnych konsultacji rynkowych w zakresie zakupu i wdrożenie usługi SOC (Security Operations Center) w Ministerstwie Aktywów Państwowych

Cel protokołu

Protokół publikowany jest w celu zapewnienia, że podmioty, które będą uczestniczyć w ewentualnym postępowaniu o udzielenie zamówienia publicznego, będą dysponować tą samą wiedzą, co podmioty uczestniczące we wstępnych konsultacjach rynkowych, zgodnie z art. 84 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. z 2024 r. poz. 1320).

W protokole zawarto kluczowe informacje uzyskane podczas konsultacji, w tym zagadnienia poruszane z uczestnikami, mające na celu doprecyzowanie zakresu zamówienia, czasu realizacji oraz określenie optymalnego podejścia do wdrożenia SZBI.

Lista podmiotów uczestniczących we wstępnych konsultacjach rynkowych

Nr	Firma	Adres
1	Blue Energy sp. z o.o.	ul. Towarowa 35, 65-189 Poznań
2	COIG S.A.	ul. Mikołowska 100, 40-065 Katowice
3	DAGMA Sp. z o.o.	ul. Pszczyńska 15, 40-478 Katowice
4	Efigo Sp. z o.o.	ul. Mikołaja Kopernika 8/6, 40-064 Katowice
5	EPROM Sp. z o.o.	ul. Piękna 15/12, 00-549 Warszawa
6	Exatel S.A	ul. Perkuna 47, 04-164 Warszawa
7	MEDIA Sp. z o.o.	ul. Kościuszki 65, 40-047 Katowice
8	NASK Spółka Akcyjna	ul. 11 Listopada 23, 03-446 Warszawa
9	Nomios Poland sp. z o.o.	ul. Puławska 537, 02-844 Warszawa
10	Operator Chmury Krajowej sp. z o.o.	ul. Grzybowska 62, 00-844 Warszawa
11	SOC360 Sp. z o.o.	Al. Jerozolimskie 146C, 02-305 Warszawa

Konsultacje odbyły się w okresie od 4 lutego do 8 kwietnia 2025 r. w formie spotkań stacjonarnych oraz wideokonferencji, prowadzone przez Departament Informatyzacji i Cyberbezpieczeństwa, wydział Analiz i Cyberbezpieczeństwa i wydział Administratorów.

Kwestie omawiane w trakcie wstępnych konsultacji rynkowych

Spotkania odbywały się zgodnie z ustaloną agendą, która obejmowała:

1. Otwarcie spotkania,
2. Prezentacja wykonawcy – omówienie doświadczenia, kompetencji, zrealizowanych wdrożeń SOC oraz referencji,
3. Opis usługi SOC – kluczowe źródła danych, architektura rozwiązania, integracja z infrastrukturą Zamawiającego, proces obsługi incydentów oraz dobre praktyki,
4. Proces wdrożenia – etapy, harmonogram, typowe wyzwania i rekomendacje wykonawców,
5. Elementy kosztotwórcze – czynniki wpływające na koszty wdrożenia i utrzymania, warianty cenowe i modele świadczenia usługi,
6. Informacje niezbędne do wyceny – dane wymagane od Zamawiającego, dostęp do zasobów, wsparcie organizacyjne,
7. Bezpieczeństwo usługi – zabezpieczenia techniczne i organizacyjne, standardy, certyfikacje,
8. Zespół wykonawcy – skład, role, kwalifikacje, doświadczenie i metodyki zarządzania projektem.

Podsumowanie wpływu wstępnych konsultacji rynkowych na planowane postępowanie

Na podstawie przeprowadzonych konsultacji rynkowych, Zamawiający zdecydował o ujęciu w dokumentacji postępowania kierunkowych wymagań:

1) Opis przedmiotu zamówienia

- Przedmiotem zamówienia jest świadczenie przez Usługodawcę na rzecz Zamawiającego Security Operations Center (SOC) w modelu usługowym, realizowanej w trybie ciągłym (24/7/365), przez okres od 24 do 36 miesięcy, który zostanie ostatecznie określony na etapie przygotowania dokumentacji do postępowania.
- Usługa obejmuje stałe monitorowanie wskazanej infrastruktury IT, wykrywanie, analizę i korelację zdarzeń bezpieczeństwa oraz identyfikację nietypowych i podejrzanych aktywności.
- Usługa obejmuje reagowanie na incydenty, prowadzenie analizy i weryfikacji zdarzeń, klasyfikacja incydentów, oraz podejmowanie działań ograniczających skutki incydentów.
- W ramach zarządzania podatnościami Usługodawca będzie przeprowadzał cykliczne skany podatności w infrastrukturze Zamawiającego.

- Zamawiający oczekuje cyklicznego opracowywania rekomendacji dotyczących zmian konfiguracyjnych i organizacyjnych mających na celu zwiększenie poziomu bezpieczeństwa środowiska IT, wraz ze wskazaniem krytycznych luk oraz zaleceń dotyczących ich usunięcia.
- Usługa obejmuje również wsparcie Zamawiającego w przygotowywaniu zgłoszeń incydentów do właściwego CSIRT.
- Zamawiający udostępni system zgłoszeniowy, który będzie wykorzystywany jako główny kanał komunikacji operacyjnej pomiędzy Zamawiającym a Usługodawcą.
- W ramach realizacji usługi, na etapie wdrożenia, Wykonawca będzie zobowiązany do przeprowadzenia tzw. „audytu zerowego", obejmującego przegląd środowiska IT, modelowanie zagrożeń, ustalenie i weryfikację źródeł danych oraz określenie sposobu ich podłączania.

2. Model realizacji

Zamawiający udostępni do wykorzystania informacje pochodzące z posiadanych źródeł zdarzeń rejestrowanych na infrastrukturze, obejmujących systemy IT oraz systemy bezpieczeństwa. Lista źródeł danych zostanie wskazana na etapie przygotowania dokumentacji do postępowania.

Jeżeli architektura rozwiązania zaproponowana przez Wykonawcę będzie wymagała zastosowania dodatkowych komponentów w celu realizacji usługi w wymaganym zakresie – takich jak urządzenia klasy SIEM, sondy do zbierania informacji lub elementy wchodzące w interakcję z infrastrukturą Zamawiającego – dane generowane lub przetwarzane przez te komponenty, które zawierają informacje dotyczące Zamawiającego, muszą być przetwarzane wyłącznie w infrastrukturze znajdującej się pod jurysdykcją Rzeczypospolitej Polskiej.

Dopuszcza się przetwarzanie danych zanonimizowanych, tj. takich, które nie pozwalają na identyfikację Zamawiającego ani na odtworzenie kontekstu jego środowiska, poza jurysdykcją Rzeczypospolitej Polskiej – na przykład w celu analizy zdarzeń oraz rekomendacji działań mitygujących.