ZAPYTANIE O INFORMACJĘ

1. Zamawiający i cel zapytania

1.1 Państwowy Instytut Medyczny MSWiA, ul. Wołoska 137, 02-507 Warszawa, NIP: 5214004558, zwany dalej „Zamawiającym", planuje zakup, wdrożenie i utrzymanie systemu klasy SIEM (Security Information and Event Management), zwanego dalej „Systemem".

1.2 Celem niniejszego zapytania o informację (Request for Information - RFI) jest:

- Rozpoznanie rozwiązań dostępnych na rynku i ich możliwości.
- Zebranie informacji o modelach licencjonowania, architekturze i wymaganiach infrastrukturalnych.
- Oszacowanie orientacyjnego kosztu zakupu, wdrożenia i utrzymania.
- Weryfikacja, czy zakres planowanych wymagań jest realistyczny, jednoznaczny i nie ogranicza konkurencji.
- Zebranie uwag do planowanego opisu przedmiotu zamówienia.

1.3 RFI stanowi wstępne konsultacje rynkowe, o których mowa w art. 84 ustawy Prawo zamówień publicznych (dalej: Pzp). Zebrane informacje zostaną wykorzystane wyłącznie do przygotowania opisu przedmiotu zamówienia, określenia warunków zamówienia oraz oszacowania jego wartości.

1.4 Niniejsze zapytanie nie stanowi ogłoszenia o zamówieniu ani oferty w rozumieniu przepisów prawa. Udział w konsultacjach nie daje wykonawcy żadnych roszczeń i nie zobowiązuje Zamawiającego do wszczęcia postępowania. Informacje udostępnione Wykonawcom biorącym udział w konsultacjach zostaną przekazane wszystkim zainteresowanym w dokumentach zamówienia.

1.5 Zapytanie zostało opublikowane na stronie internetowej Zamawiającego: Zapytania ofertowe - Państwowy Instytut Medyczny MSWiA - Portal Gov.pl

1.6 Wyniki konsultacji zostaną odnotowane w protokole postępowania i uwzględnione przy szacowaniu wartości zamówienia (art. 28 i n. ustawy PZP), łącznie z opcjami, wydłużeniem wsparcia oraz powiązanym zamówieniem na usługę SOC.

2. Opis potrzeb Zamawiającego

2.1 System ma służyć do monitorowania bezpieczeństwa infrastruktury teleinformatycznej Zamawiającego, w szczególności do: centralnego gromadzenia logów, korelacji i analizy zdarzeń bezpieczeństwa, wykrywania incydentów w czasie rzeczywistym lub zbliżonym do rzeczywistego, wsparcia reagowania na incydenty, prowadzenia analiz powłamaniowych i audytowych oraz spełnienia wymagań prawnych i regulacyjnych.

3. Zakres informacji oczekiwanych od Wykonawców

Zamawiający prosi o przekazanie informacji w poniższym zakresie. Odpowiedzi należy przedstawić zwięźle, z odwołaniem do dokumentacji producenta, jeśli to możliwe.

3.1 Dane Wykonawcy

- Pełna nazwa, adres, NIP, osoba kontaktowa.
- Status wobec producenta proponowanego rozwiązania (partner, dystrybutor, producent) oraz poziom autoryzacji.
- Doświadczenie we wdrożeniach SIEM, w tym w sektorze ochrony zdrowia i administracji publicznej (bez ujawniania danych poufnych klientów).
- Certyfikaty zespołu i firmy (np. ISO/IEC 27001, certyfikaty producenta).

3.2 Proponowane rozwiązanie

- Nazwa, producent i wersja Systemu, data wydania najnowszej wersji oraz planowane daty końca sprzedaży i wsparcia.
- Rekomendowana architektura (komponenty, kolektory, magazyn danych, HA, DR) oraz jej schemat.
- Dostępne modele wdrożenia (on-premises, chmura prywatna, SaaS, hybryda) wraz z lokalizacją przetwarzania danych i zgodnością z wymaganiem przechowywania danych w EOG.
- Kraj siedziby producenta oraz podmiotów mających dostęp do danych, a także informacja o możliwości dostępu organów państw trzecich do przetwarzanych danych.
- Wymagania infrastrukturalne dla modelu on-premises (CPU, RAM, dyski, system operacyjny, sieć).
- Zakres funkcjonalności dostępnych w standardzie oraz wymagających dodatkowych modułów lub licencji (UEBA, SOAR, Threat Intelligence, case management).

3.3 Funkcjonalność

- Prosimy o wypełnienie kwestionariusza stanowiącego Załącznik nr 1 (oznaczenie: spełnia w standardzie / spełnia po dodatkowej konfiguracji / wymaga dodatkowego modułu / nie spełnia) wraz z krótkim opisem.

3.4 Integracje

- Wsparcie dla źródeł logów wskazanych w Załączniku nr 1 (parsery fabryczne, konektory, agent, API).
- Sposób monitorowania urządzeń medycznych (np. syslog, SPAN, NetFlow).
- Sposób dodawania nowych źródeł niewspieranych fabrycznie oraz czas i koszt takiej usługi.
- Integracja z systemami ticketowymi, EDR/XDR, firewallami i narzędziami Threat Intelligence.

- Dostępne API oraz możliwości eksportu danych i konfiguracji w formatach otwartych, wraz z formatami i kosztem eksportu przy zmianie dostawcy.

3.5 Wydajność i skalowalność

- Maksymalna obsługiwana liczba EPS i GB/dobę na jednym węźle i w klastrze.
- Sposób i granice skalowania, wpływ przyrostu wolumenu na koszt licencji.
- Skutki przekroczenia licencjonowanego wolumenu.
- Typowy czas odpowiedzi na zapytania dla danych z ostatnich 7, 30 i 90 dni.
- Mechanizmy retencji, kompresji i archiwizacji oraz koszty magazynowania danych przy retencji 12 i 24 miesięcy.

3.6 Bezpieczeństwo i zgodność

- Uwierzytelnianie (SSO, MFA), RBAC, dziennik audytowy, szyfrowanie transmisji i danych w spoczynku.
- Mechanizmy zapewniające integralność zgromadzonych logów.
- Gotowe raporty i reguły wspierające zgodność z ustawą o krajowym systemie cyberbezpieczeństwa (KSC), RODO i ISO/IEC 27001.
- Polityka producenta w zakresie aktualizacji bezpieczeństwa i zarządzania podatnościami; certyfikacje produktu lub usługi chmurowej (np. ISO/IEC 27001, SOC 2).

3.7 Wdrożenie

- Proponowana metodyka i etapy wdrożenia, typowy czas realizacji.
- Zakres prac po stronie Wykonawcy i po stronie Zamawiającego, niezbędne zaangażowanie personelu Zamawiającego.
- Liczba wdrożonych fabrycznie reguł detekcji, mapowanie na MITRE ATT&CK, proces strojenia reguł i ograniczania fałszywych alarmów.
- Ryzyka i założenia, które wpływają na harmonogram i koszt.

3.8 Wsparcie, SLA i szkolenia

- Dostępne poziomy wsparcia (godziny, kanały, język), proponowane czasy reakcji i usunięcia awarii.
- Zakres aktualizacji treści detekcyjnych w ramach subskrypcji.
- Oferta szkoleń dla administratorów i analityków oraz możliwość prowadzenia ich w języku polskim.
- Dostępne opcje usługi SOC (SOC as a Service, MDR), w tym wariant z dostępem do Systemu Zamawiającego oraz model hybrydowy (bez dostawy platformy SIEM), wraz z orientacyjnym kosztem.

3.9 Orientacyjny koszt

- Prosimy o podanie szacunkowych kosztów według struktury z Załącznika nr 2, w ujęciu na 36 miesięcy (zakres podstawowy) oraz odrębnie dla opcji wydłużenia wsparcia o 24 miesiące, z wyodrębnieniem kosztów

jednorazowych i cyklicznych oraz wskazaniem modelu licencjonowania (np. według wolumenu danych, EPS, liczby źródeł).
- Prosimy także o podanie cen jednostkowych: za 1GB/dobę lub 1000 EPS, za dodatkowe źródło logów oraz za roboczogodzinę integracji. Podane kwoty mają charakter orientacyjny.

3.10 Uwagi do planowanych wymagań

- Prosimy o wskazanie wymagań, które w opinii Wykonawcy: mogą ograniczać konkurencję lub faworyzować określone rozwiązanie, są niejednoznaczne albo nieproporcjonalne, generują nadmierne koszty bez istotnej korzyści dla bezpieczeństwa, lub mogą być zastąpione rozwiązaniami równoważnymi. Prosimy też o wskazanie dobrych praktyk i sugerowanych kryteriów oceny ofert.

4. Termin, sposób i forma odpowiedzi

4.1 Odpowiedzi należy przesłać do dnia 30.10.2026, godz. 14:00, na adres magdalena.kaczorowska@pimmswia.gov.pl. Pytania do Zamawiającego można kierować do dnia 27.10.2026 na adres magdalena.kaczorowska@pimmswia.gov.pl.

4.2 Odpowiedź powinna być sporządzona w języku polskim, w formacie PDF lub DOCX, podpisana przez osobę upoważnioną do reprezentowania Wykonawcy lub upoważnionego przedstawiciela.

4.3 Zamawiający zastrzega prawo do zadawania pytań uzupełniających oraz do zaproszenia Wykonawców na spotkania lub prezentację.

5. Informacje poufne

5.1 Informacje stanowiące tajemnicę przedsiębiorstwa należy wyraźnie oznaczyć. Zamawiający wykorzysta je wyłącznie do szacowania wartości zamówienia i przygotowania dokumentów zamówienia.

6. Ochrona danych osobowych

6.1 Administratorem danych osobowych osób kontaktowych jest Państwowy Instytut Medyczny MSWiA, ul. Wołoska 137, 02-507 Warszawa. Dane kontaktowe inspektora ochrony danych, Joanna Mrowicka: joanna.mrowicka@pimmswia.gov.pl.

6.2 Dane osobowe będą przetwarzane wyłącznie w celu przeprowadzenia konsultacji rynkowych, na podstawie art. 6 ust. 1 lit. f RODO. Dane pochodzą od Wykonawcy, który je przekazał w odpowiedzi na zapytanie.

6.3 Odbiorcami danych będą wyłącznie upoważnieni pracownicy Państwowego Instytutu Medycznego MSWiA w zakresie niezbędnym do realizacji ich

obowiązków służbowych. Dane nie podlegają zautomatyzowanemu podejmowaniu decyzji ani profilowaniu.

6.4 Osobom, których dane dotyczą, przysługują prawa wynikające z RODO, w tym prawo dostępu, sprostowania, ograniczenia przetwarzania, sprzeciwu oraz wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

6.5 Wykonawca zobowiązany jest przekazać niniejszą klauzulę osobom, których dane osobowe wskazuje w odpowiedzi (art. 14 RODO).

Załącznik nr 1do Zapytania o Informację

Wzór Kwestionariusza funkcjonalnego

Kwestionariusz funkcjonalny

Legenda: **S** – spełnia w standardzie; **K** – spełnia po dodatkowej konfiguracji; **M** – wymaga dodatkowego modułu lub licencji; **N** – nie spełnia.

Lp.	Obszar / wymaganie	S / K / M / N	Opis i odwołanie do dokumentacji
1	Zbieranie logów: syslog (TLS wymagany), agent Windows/Linux, WMI/WEF, API chmurowe, SNMP trap, odczyt plików, JDBC/ODBC, NetFlow/IPFIX/sFlow		
2	Buforowanie danych przy braku łączności, szyfrowanie transmisji, alarm o ustaniu logowania		
3	Normalizacja do spójnego modelu danych (np. ECS, CEF, OCSF) przy zachowaniu raw log		
4	Wzbogacanie o kontekst (AD/Entra ID, CMDB, geolokalizacja, reputacja, podatności)		
5	Tworzenie własnych parserów bez udziału producenta		
6	Gotowe reguły detekcji, mapowanie na MITRE ATT&CK, wizualizacja pokrycia		
7	Własne reguły korelacyjne (sekwencje, progi, okna czasowe, listy referencyjne)		
8	Import i eksport reguł w formacie otwartym (np. Sigma), testowanie reguł na danych historycznych		
9	UEBA / wykrywanie anomalii		
10	Integracja Threat Intelligence (STIX/TAXII, API, CSV), retrospektywne dopasowanie IoC		
11	Zarządzanie alarmami i incydentami (case management), metryki MTTD/MTTR		
12	SOAR / playbooki (blokada IP, izolacja stacji, wyłączenie konta)		
13	Wyszukiwanie pełnotekstowe i język zapytań, threat hunting		
14	Dashboardy i wizualizacja zależności, oś czasu incydentu		
15	Raporty zgodności (ustawa o KSC, RODO, ISO/IEC 27001), raporty własne i harmonogramowane		
16	Otwarte API (REST), eksport danych i konfiguracji w formatach otwartych		
17	Dokumentacja, szkolenia w języku polskim; interfejs użytkownika w języku polskim punktowany w ramach kryteriów oceny ofert		
18	Przetwarzanie, przechowywanie i dostęp do danych wyłącznie z terytorium EOG		

Załącznik nr 2 do Zapytania o informację

Wzór Arkusza kosztowego

Arkusz kosztowy (orientacyjny)

Kwoty netto w PLN. Prosimy o podanie założeń (wolumen, liczba źródeł, liczba użytkowników).

Pozycja	Koszt jednorazowy	Koszt roczny	Razem 36 miesięcy	Opcja: wydłużenie o 24 miesiące
Licencje / subskrypcja Systemu (wolumen bazowy)				
Dodatkowe moduły (UEBA, SOAR, TI, inne)				
Infrastruktura (sprzęt / zasoby chmurowe) – jeśli dotyczy				
Wdrożenie i integracja źródeł				
Szkolenia				
Wsparcie techniczne i aktualizacje				
Koszt magazynowania danych: retencja 12 miesięcy / 24 miesiące				
Cena jednostkowa: 1 GB/dobę lub 1000 EPS				
Cena jednostkowa: dodatkowe źródło logów				
Cena jednostkowa: roboczogodzina integracji				
Opcjonalnie: usługa monitorowania zdarzeń (SOC / MDR)				
RAZEM				