Kraków, **09.04.2026 roku**

DO WSZYSTKICH KOGO DOTYCZY

ODPOWIEDZI NA PYTANIA I ZMIANA TERMINU SKŁADANIA I OTWARCIA OFERT

***dot. sprawy:* 34/ZP/2026**

Szanowni Państwo,

Uprzejmie informuję, że w sprawie ogłoszonego przez 5 Wojskowy Szpital Kliniczny z Polikliniką - Samodzielny Publiczny Zakład Opieki Zdrowotnej w Krakowie postępowania na **zakup licencji SIEM - system do zarządzania informacjami i zdarzeniami zabezpieczeń na potrzeby działań zwiększających poziom cyberbezpieczeństwa 5 WSZK w Krakowie w ramach Krajowego Planu Odbudowy,** wpłynęły pytania. Treść pytań wraz z odpowiedziami na nie przedstawiam poniżej:

Pytania nr 1

1/ Zwracamy się z prośba o określenie minimalnej liczby urządzeń jakie ma obsługiwać system SIEM. O ile w ciągu 36 miesięcy może się zmienić ta wartość?

Odpowiedź: W odpowiedzi na pytanie o ilość końcówek – ok. 1300. Na chwilę obecną, Zamawiający nie jest w stanie określić, o ile zwiększy się ta liczba. W Szpitalu są planowane inwestycje, natomiast brak jeszcze konkretnych ustaleń pod kątem sprzętu IT.

Pytania nr 2

2/ Czy jest znana wartość dziennego wolumenu danych, które mają docelowo być przekazywane do SIEM?

Odpowiedź: Na potrzeby przygotowania ofert należy przyjąć, że środowisko Zamawiającego obejmuje obecnie ok. 1300 urządzeń końcowych (w tym stacje robocze oraz serwery i urzadzenia sieciowe).

Na dzień dzisiejszy Zamawiający nie jest w stanie określić o ile zwiększy się ta liczba, w Szpitalu są planowane inwestycje, natomiast brak jeszcze konkretnych ustaleń pod kątem sprzętu IT.

Środowisko obejmuje w szczególności:

- **systemy medyczne (HIS, EDM, RIS, PACS),**
- **infrastrukturę serwerową i sieciową,**
- **systemy bezpieczeństwa (np. firewall, EDR/XDR).**

Szacunkowy wolumen danych do przetwarzania przez system SIEM należy przyjąć na poziomie: od 300 GB do 400 GB logów dziennie.

3/ Wymaganie nr 4.: OT/IoT - W jakim zakresie? Czy mówimy o samym rozwiązaniu SCADA czy również o urządzeniach typu sterowniki PLC itp.?

Odpowiedź: **Zamawiający wyjaśnia, że wymaganie dotyczące obsługi środowisk OT/IoT odnosi się przede wszystkim do urządzeń medycznych funkcjonujących w infrastrukturze Zamawiającego.**
W szczególności dotyczy to urządzeń diagnostycznych i specjalistycznych, takich jak m.in.:

- **aparaty RTG,**
- **tomografy komputerowe (CT),**
- **rezonanse magnetyczne (MRI),**
- **inne urządzenia medyczne generujące zdarzenia lub logi systemowe.**

Zamawiający nie wymaga na etapie wdrożenia pełnej integracji wszystkich urządzeń tego typu, natomiast oczekuje, że oferowany system SIEM będzie posiadał możliwość integracji z tego rodzaju źródłami danych (np. poprzez syslog, API, pliki logów lub inne mechanizmy integracyjne).

Szczegółowy zakres integracji zostanie ustalony na etapie wdrożenia.

4/ Wymaganie nr 17: Co zamawiający na myśli pod nazwą "niestandardowe urządzenia"?

Odpowiedź: Zamawiający wyjaśnia, że przez „niestandardowe urządzenia" rozumie systemy oraz urządzenia, które nie posiadają natywnej integracji z oferowanym systemem SIEM lub wymagają indywidualnego dostosowania w zakresie zbierania i przetwarzania logów.

W szczególności mogą to być:

- **systemy medyczne (np. HIS, RIS, PACS, EDM),**
- **specjalistyczna aparatura medyczna,**
- **autorskie lub dedykowane aplikacje Zamawiającego,**
- **inne urządzenia lub systemy generujące logi w formatach niestandardowych lub niestrukturalnych.**

Zamawiający oczekuje, że Wykonawca zapewni możliwość integracji takich źródeł logów poprzez przygotowanie odpowiednich parserów, konektorów lub wykorzystanie dostępnych mechanizmów integracyjnych (np. syslog, API, pliki logów).

Szczegółowy zakres integracji zostanie ustalony na etapie wdrożenia.

5/ Wymaganie nr 26: Prosimy o wskazanie konkretnych rozwiązań EDR/XDR.

Odpowiedź: Zamawiający informuje, że w obecnym środowisku wykorzystuje rozwiązania klasy bezpieczeństwa, w tym:

- **system EDR/antywirus firmy ESET,**
- **urządzenia sieciowe (firewall) firmy Fortinet (FortiGate).**

Zamawiający oczekuje, że oferowany system SIEM będzie posiadał możliwość integracji z powyższymi rozwiązaniami.
Jednocześnie Zamawiający nie ogranicza się do wskazanych technologii i dopuszcza rozwiązania równoważne, pod warunkiem zapewnienia integracji z systemami klasy EDR/XDR oraz urządzeniami sieciowymi poprzez standardowe mechanizmy (np. API, syslog, konektory).
Integracja powinna umożliwiać co najmniej przekazywanie zdarzeń bezpieczeństwa, alertów oraz danych kontekstowych do systemu SIEM.

Pytania nr 3

6/

Nr	Pkt SWZ / Załącznika	Treść pytania do Zamawiającego
1	Pkt 13 Zał. nr 1	Czy wymaganie „reakcja do 1 godziny (24/7)" dla zgłoszeń krytycznych dotyczy wsparcia udzielanego przez Wykonawcę, czy przez producenta oprogramowania?
2	Pkt 35 Zał. nr 1	Czy klasyfikacja zdarzeń zgodnie z Traffic Light Protocol (TLP) musi być wbudowaną, natywną funkcjonalnością systemu SIEM, czy Zamawiający dopuszcza realizację tego wymagania poprzez konfigurację pól niestandardowych (custom fields/tags) w systemie?
3	Pkt 43 Zał. nr 1	Czy wymaganie zgodności z ISO/IEC 27001 oraz ISO/IEC 27035 dotyczy: (a) posiadania certyfikatu ISO przez producenta oprogramowania, (b) posiadania certyfikatu ISO przez Wykonawcę, (c) zdolności systemu SIEM do wspierania procesów zgodnych z tymi normami? Prosimy o doprecyzowanie, jakie dokumenty potwierdzające należy przedłożyć.
4	Pkt 17 Zał. nr 1	Czy Zamawiający może udostępnić listę źródeł logów (urządzeń, systemów, aplikacji), które mają być podłączone do systemu SIEM? Jest to niezbędne do prawidłowej wyceny prac związanych z tworzeniem niestandardowych parserów oraz do zwymiarowania infrastruktury.
5	Pkt 39 Zał. nr 1	Czy 150 reguł korelacyjnych ma być opracowanych indywidualnie dla środowiska Zamawiającego, czy Zamawiający dopuszcza wykorzystanie predefiniowanych reguł dostarczanych przez producenta, dostosowanych (ztuningowanych) do środowiska Zamawiającego?
6	Pkt 15 Zał. nr 1	Czy wymagana dostępność 99,9% dotyczy infrastruktury zapewnianej przez Wykonawcę, czy Zamawiający zapewnia infrastrukturę serwerową (on-premise) spełniającą wymagania redundancji? Czy Zamawiający dysponuje specyfikacją środowiska sprzętowego przeznaczonego pod SIEM?
7	Pkt 1 Zał. nr 1	Czy Zamawiający może podać szacowany dzienny wolumen logów (w GB/dzień) oraz liczbę źródeł logów / endpointów? Informacja ta jest niezbędna do prawidłowego zwymiarowania systemu SIEM, doboru

		licencji oraz określenia wymagań sprzętowych zapewniających retencję 12 miesięcy
8	Ogólne § 2 ust. 2 umowy	Czy w zakresie zamówienia jest dostawa sprzętu serwerowego (serwerów, macierzy, środowiska wirtualizacyjnego) do instalacji systemu SIEM, czy też Zamawiający zapewnia infrastrukturę we własnym zakresie? W przypadku gdy infrastruktura jest po stronie Zamawiającego — prosimy o podanie parametrów dostępnego środowiska.

Odpowiedź:

Ad 1) Dotyczy wsparcia udzielanego przez Wykonawcę.
Ad 2) Zamawiający dopuszcza realizację przez konfigurację pól niestandardowych w systemie.
Ad 3) Organizacja dostawcy SIEM posiada ISO 27001 i certyfikowany proces zarządzania incydentami zgodny z ISO 270354 a SIEM ma funkcjonalność umożliwiającą realizację tych procesów.
Ad 4) Nie, odpowiedź na to pytanie jest zawarta w pytaniu nr 7, ale nie udostępniamy listy źródeł logów
Ad 5) Zamawiający dopuszcza.
Ad 6) Wykonawca odpowiada tylko za software / konfigurację SIEM, 99,9% dotyczy samego systemu a nie całej infrastruktury serwerowej. Zamawiający zapewnia infrastrukturę, natomiast nie dysponuje na tę chwilę specyfikacją.
Ad 7) 300-400GB, liczba endpointów ok. 1300
Ad 8) Zamawiający zapewnia infrastrukturę we własnym zakresie

Równocześnie Zamawiający przesuwa termin składania i otwarcia ofert na dzień 17.04.2026 roku

Nowy termin składania ofert do dnia 17.04.2026 roku do godz. 08:00

Nowy termin otwarcia ofert dnia 17.04.2026 roku godz. 09:00

Załącznikiem jest Zmodyfikowany SWZ (na czerwono zmiany).

Z poważaniem,
Sekcja Zamówień Publicznych