Poznań dnia: 2026-03-03

Szpital Wojewódzki w Poznaniu
Dział Zamówień Publicznych
Juraszów 7/19
60-479 Poznań

WYKONAWCY
ubiegający się o zamówienie

Dotyczy: postępowania o udzielenie zamówienia publicznego:

Nazwa zamówienia:	Przedmiotem zamówienia jest zakup z wdrożeniem produkcyjnym: narzędzi cyberochrony;.
Numer referencyjny:	SZW/DZP/170/2025

WYJAŚNIENIA TREŚCI SWZ

Zamawiający, **Szpital Wojewódzki w Poznaniu**

Dział Zamówień Publicznych, działając na podstawie art. 135 ust. 6 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2024 r. poz. 1320 z późn. zm.), udostępnia poniżej treść zapytań do Specyfikacji Warunków Zamówienia (zwanej dalej ”SWZ”) wraz z wyjaśnieniami:

Pytanie nr 1

Wolumen logów / EPS
Prosimy o podanie szacunkowego wolumenu zdarzeń do obsłużenia w SIEM: średni EPS, peak EPS, oraz dzienny wolumen (GB/dzień) i docelową retencję (hot/warm/cold), jeśli Zamawiający posiada takie dane.
Stanowisko (wyjaśnienie) Zamawiającego: Zgodnie z opisem przedmiotu zamówienia Zamawiający wymaga dostarczenia rozwiązania o wydajności nie mniejszej niż 1 500 EPS. Dodatkowo zgodnie z opisem rozwiązanie nie może być limitowane ilością danych przesyłanych w jednostce czasu. Zamawiający zaznacza, że nie posiada systemu typu SIEM, więc nie jest w stanie podać szczegółowych danych związanych z zapytaniem o „średni EPS, peak EPS…”.

Pytanie nr 2

Liczba i typ źródeł logów

Prosimy o informację: ile jest (orientacyjnie) źródeł logów w podziale na kategorie: serwery Windows/Linux, stacje robocze, urządzenia sieciowe (FW/IDS/IPS/switche/route'ry), kontrolery domeny, systemy/aplikacje (w tym medyczne), usługi chmurowe.
Stanowisko (wyjaśnienie) Zamawiającego: Zamawiający chciałby co najmniej podłączyć do systemu podane niżej urządzenia wraz z przybliżoną ich ilością:
- 2 firewalle
- 100 switchy
- 20 serwerów
- 800 stacji roboczych
- 2 kontrolery
- 4 macierze
- 3 usługi chmurowe

Pytanie nr 3
Które źródła „obowiązkowe" na start
Prosimy o wskazanie, które systemy/źródła logów Zamawiający wymaga objąć monitoringiem w pierwszym etapie uruchomienia, a które mogą być dołączane sukcesywnie (harmonogram onboardingu).
Stanowisko (wyjaśnienie) Zamawiającego: Wszystkie systemy wskazane przez Zamawiającego w opisie przedmiotu zamówienia muszą być objęte monitoringiem od momentu zakończenia wdrożenia systemu.

Pytanie nr 4
Wymóg agentów – skala
OPZ wskazuje licencje na min. 25 agentów. Prosimy o potwierdzenie, czy to jest minimalna liczba hostów objętych agentem na start, czy tylko minimalna liczba licencji w dostawie; i jaka jest docelowa liczba hostów agentowych.
Stanowisko (wyjaśnienie) Zamawiającego: 25 szt. odnosi się do minimalnej liczby agentów w dostawie. Na start planowane jest podłączenie ok. 15-20 serwerów z wykorzystaniem agenta.

Pytanie nr 5
NetFlow / PCAP
Czy Zamawiający planuje wykorzystanie NetFlow w pełnym zakresie (z ilu urządzeń, jaki sampling, szacowany wolumen), oraz czy import PCAP ma być stały (ciągły) czy incydentalny (ad-hoc).
Stanowisko (wyjaśnienie) Zamawiającego: Zamawiający planuje wykorzystanie Netflow z klastra firewall w pełnym zakresie. Import z pliku PCAP wystarczy, aby był incydentalny.

Pytanie nr 6
Chmura

OPZ mówi o środowiskach chmurowych „jeśli używane". Prosimy o doprecyzowanie, czy Zamawiający korzysta z Microsoft Azure / Amazon Web Services / Google Cloud / Microsoft 365 i które usługi mają być logowane.
Stanowisko (wyjaśnienie) Zamawiającego: Zamawiający korzysta między innymi z środowisk chmurowych Microsoft 365, Nextcloud.

Pytanie nr 7
Retencja i wymagania prawne/organizacyjne
Prosimy o potwierdzenie oczekiwanej retencji logów (min./docelowo) oraz czy wymagany jest podział na hot/warm/cold i/lub WORM/immutability.
Stanowisko (wyjaśnienie) Zamawiającego: Zamawiający zwraca uwagę na zapis w opisie przedmiotu zamówienia, który mówi „Klaster SIEM nie może posiadać ograniczeń licencyjnych związanych z ilością przechowywanych zdarzeń i/lub danych. Jedynym ograniczeniem w tym zakresie może być rozmiar przestrzeni dyskowej."
Wymagany jest przynajmniej podział na logi typu hot/warm/cold.

Pytanie nr 8
Parametry SLA vs zakres
Prosimy o potwierdzenie, czy czasy reakcji SOC (30/60/180 min) odnoszą się do wszystkich onboardowanych źródeł od dnia uruchomienia, czy tylko do źródeł wskazanych jako krytyczne na start.
Stanowisko (wyjaśnienie) Zamawiającego: Czasy reakcji SOC odnoszą się do wszystkich źródeł od momentu zakończenia wdrożenia systemu SIEM.

Pytanie nr 9
Eksport dashboardów w XML
W OPZ znajduje się wymaganie eksportu/importu dashboardów/raportów/reguł w XML. Prosimy o wyjaśnienie uzasadnienia wymagania eksportu/importu (m.in. dashboardów/raportów/reguł) wyłącznie w formacie XML. Czy Zamawiający dopuści spełnienie wymagania poprzez eksport/import w formacie równoważnym, zapewniającym tą samą możliwość odtworzenia obiektów (np. JSON/NDJSON), ewentualnie poprzez udostępnienie przez SIEM API do przenoszenia/wersjonowania konfiguracji? Jeśli Zamawiający podtrzymuje XML – prosimy o wskazanie schematu/standardu XML albo minimalnego zakresu pól, które muszą być przenoszone.
Uzasadnienie: Wymaganie konkretnego formatu pliku może ograniczać konkurencję, jeśli nie jest niezbędne do osiągnięcia celu zamówienia; opis powinien być proporcjonalny i nieutrudniający uczciwej konkurencji.
Stanowisko (wyjaśnienie) Zamawiającego: Format XML jest standardem otwartym i szeroko stosowanym w różnych systemach SIEM. Przetwarzanie plików w tym standardzie ułatwi dostosowywanie rozwiązania do potrzeb Zamawiającego. Jednocześnie Zamawiający wyraża zgodę użycie otwartych formatów równoważnych pod warunkiem uzyskania tego samego

efektu tj. eksportowania/importowania całości konfiguracji dashbordów, raportów oraz reguł. Zamawiający nie wyraża zgody na stosowanie zamkniętych rozwiązań producenta, w tym API.

Pytanie nr 10

„Wyszukiwanie zdarzeń bez indeksowania" / wymóg technologiczny zamiast mierzalnego efektu

W OPZ jest zapis o wyszukiwaniu w czasie rzeczywistym „bez konieczności indeksowania" (wymóg technologiczny). Prosimy o doprecyzowanie wymagania „wyszukiwania zdarzeń w czasie rzeczywistym bez konieczności indeksowania": jaki efekt użytkowy Zamawiający chce w ten sposób osiągnąć (np. minimalizacja opóźnienia detekcji, możliwość przeszukiwania strumienia zanim dane zostaną utrwalone, itp.)?

Jednocześnie prosimy o określenie tego wymagania parametrami mierzalnymi, np.:

– maksymalna dopuszczalna latencja od przyjęcia logu do możliwości jego wyszukania (sekundy/minuty),

– maksymalny czas wykonania zapytań dla zadanych okien czasowych i filtrów (np. ostatnie 15 min / 24 h),

– wymagana przepustowość przyjęcia logów (EPS) przy zachowaniu ww. czasów. Pozwoli to zachować neutralność technologiczną przy zachowaniu oczekiwanej funkcjonalności i wydajności.

Uzasadnienie: Opis przedmiotu zamówienia co do zasady powinien koncentrować się na wymaganych cechach/rezultatach i być proporcjonalny; nadmierne „przywiązanie" do sposobu realizacji (technologii/procesu) może ograniczać konkurencję.

Stanowisko (wyjaśnienie) Zamawiającego: Dokładna treść wymagania brzmi: „System SIEM musi mieć możliwość: wyszukiwania zdarzeń (events) w czasie rzeczywistym bez konieczności indeksowania oraz używania wyrażeń logicznych takich jak AND, OR, NOT czy też cudzysłowów".

Systemy wyszukiwania zdarzeń bez indeksowania mają na celu przyspieszenie pracy administratorów w sytuacjach krytycznych. Pozwala na wyszukiwanie bez oczekiwania na zakończenie indeksowania oraz daje możliwość przeszukiwania po dowolnych polach, a nie tylko tych zindeksowanych. Brak używania operatorów lub cudzysłowów zmniejsza ryzyko popełniania błędów przy wyszukiwaniach, co znacząco wpływa na komfort pracy oraz szybszy czas obsługi incydentu.

Pytanie nr 11

Czy Zamawiający dopuszcza rozwiązanie, którego agent wymaga połączenia z konsolą zarządzającą?

Stanowisko (wyjaśnienie) Zamawiającego: Tak

Pytanie nr 12

Czy Zamawiający dopuszcza rozwiązanie, które przechowuje informacje o incydentach tylko przez 90 dni? Rozwiązanie które chcemy zaoferować ma możliwość zwiększenia ilości dni także do 365 dni, jednak wiąże się to ze sporym kosztem dodatkowym.

Stanowisko (wyjaśnienie) Zamawiającego: Tak dopuszczam rozwiązanie, które przechowuje informacje o incydentach 90 dni.

Pytanie nr 13
Czy Zamawiający dopuszcza rozwiązanie, które nie oferuje możliwości automatycznej izolacji w reakcji na incydent? Izolacja odbywa się ręcznie lub na podstawie własnych reguł wykrywania.
Stanowisko (wyjaśnienie) Zamawiającego: Zamawiający dopuszcza rozwiązanie w którym izolacja odbywa się ręcznie lub na podstawie własnych reguł wykrywania.

Pytanie nr 14
Czy Zamawiający dopuszcza rozwiązanie, które nie oferuje działań napraw i przywróć?
Stanowisko (wyjaśnienie) Zamawiającego: Tak

Pytanie nr 15
Czy Zamawiający dopuszcza rozwiązanie, które nie oferuje repozytorium do przechowywania skryptów oraz które nie śledzi statusu skryptów wykonywanych przez Remote Shell?
Stanowisko (wyjaśnienie) Zamawiającego: Tak

Pytanie nr 16
Czy Zamawiający jest w stanie określić jaka ilość licencji EDR powinna zostać dostarczona?
Stanowisko (wyjaśnienie) Zamawiającego: Ilość licencji to 800 szt.

Pytanie nr 17
Czy Zamawiający dopuszcza spełnienie celu w zakresie bezpieczeństwa informacji poprzez środki organizacyjne i techniczne adekwatne do zakresu wdrożenia EDR, bez formalnego wymogu certyfikacji ISO 27001? Zakres prac wdrożeniowych nie obejmuje przetwarzania danych w systemach wykonawcy i stałego dostępu do danych Zamawiającego.
Stanowisko (wyjaśnienie) Zamawiającego: Zamawiający dopuszcza taką możliwość.

Pytanie nr 18
Czy Zamawiający dopuszcza aby osoba z doświadczeniem wdrożeniowym była zatrudniona na umowę zlecenie spełniając jednocześnie pozostałe wymagania formalne wobec tej osoby**?**
Stanowisko (wyjaśnienie) Zamawiającego: Nie. Zamawiający podtrzymuje dotychczasowy zapis SWZ (umowa o pracę)

Zamawiający