Narodowy Instytut Onkologii
im. Marii Skłodowskiej-Curie –
Państwowy Instytut Badawczy
Oddział w Gliwicach

Gliwice dn. 12.02.2026r.

DO WSZYSTKICH ZAINTERESOWANYCH

Dot. zapytania cenowego nr DZ/DI-072-11/26 z dnia 3.02.2026. dot. **zakup usługi SOC i systemu SIEM**.

Zakup finansowany ze środków Instrumentu na rzecz Odbudowy i Zwiększania Odporności dla przedsięwzięć realizowanych w ramach inwestycji D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia" będącej elementem komponentu D „Efektywność, dostępność i jakość systemu ochrony zdrowia".

W związku ze złożonymi pytaniami do opublikowanej na stronie internetowej Zamawiającego dokumentacji odnośnie wyżej wymienionego zapytania cenowego, przekazujemy Państwu pytanie, jak i udzieloną odpowiedź.

Pytanie nr 8:

Prosimy o wskazanie szacowanej ilości elementów objętych zakresem monitorowania:

- Laptopy/komputery stacjonarne;
- Serwery fizyczne;
- Serwery wirtualne;
- Macierze;

Narodowy Instytut Onkologii
im. Marii Skłodowskiej-Curie –
Państwowy Instytut Badawczy
Oddział w Gliwicach

ul. Wybrzeże Armii Krajowej 15
44-102 Gliwice

Dyrekcja
Tel.: +48 32 278 96 18

dyrektor@gliwice.nio.gov.pl
www.gliwice.nio.gov.pl

Centrala
Tel.: +48 32 278 88 88
Fax: +48 32 231 35 12

NIP: 5250008057
REGON: 000288366-00028

- Serwery NAS;

Odpowiedź:

Zamawiający szacuje, iż obecnie posiada:

• laptopy i komputery stacjonarne – 2500 urządzeń,

• serwery fizyczne – 60 urządzeń,

• serwery wirtualne – 500 maszyn wirtualnych,

• macierze – 15 sztuk,

• serwery NAS – 2 sztuki.

Jednocześnie Zamawiający przewiduje, iż do końca obowiązywania umowy liczba tego typu urządzeń może wzrosnąć do około 3500.

Pytanie nr 9:
Pyt. 2.Prosimy również o odpowiedź, czy Zamawiający w odniesieniu do pkt 17., zał. Nr 3 - soc -specyfikacja techniczna- planuje udostępnić wykonawcy możliwość realizacji działania poprzez udostępnienie w infrastrukturze dostępu poprzez API, konektory i konta serwisowe? Czy zamawiający dostarczy narzędzie, którym dział SOC będzie mógł zrealizować takie działanie?
Odpowiedź:
Zamawiający rozważa kilka wariantów, w tym dostęp poprzez API, konta serwisowe imienne oraz tzw. "czarne listy", które będą aktualizowane w zadanym interwale czasowym. Szczegóły dotyczące integracji z SOC zostaną omówione po podpisaniu umowy.

Pytanie nr 10:
Czy Zamawiający potwierdza, że wymagany system SIEM do realizacji SOC, powinien być rozwiązaniem uznanym i dojrzałym rynkowo, sklasyfikowanym wśród liderów w najnowszym

Narodowy Instytut Onkologii
im. Marii Skłodowskiej-Curie – Państwowy Instytut Badawczy
Oddział w Gliwicach

ul. Wybrzeże Armii Krajowej 15
44-102 Gliwice

Dyrekcja
Tel.: +48 32 278 96 18

dyrektor@gliwice.nio.gov.pl
www.gliwice.nio.gov.pl

Centrala
Tel.: +48 32 278 88 88
Fax: +48 32 231 35 12

NIP: 5250008057
REGON: 000288366-00028

raporcie Gartner Magic Quadrant for SIEM, w celu zagwarantowania stabilności, skalowalności i długoterminowego wsparcia produktu?

Odpowiedź:

Na etapie rozeznania rynkowego Zamawiający rozważa różne opcje dostępnych rozwiązań. W odniesieniu do wymagania dotyczącego systemu SIEM do realizacji SOC, Zamawiający zakłada, że system powinien być rozwiązaniem uznanym rynkowo, stabilnym i dojrzałym, a jego klasyfikacja w najnowszym raporcie Gartner Magic Quadrant for SIEM może być jednym z kryteriów. Ostateczny wybór rozwiązania, w tym możliwość wykorzystania technologii open-source, zostanie doprecyzowany na etapie przetargu.

Pytanie nr 11:

Czy Zamawiający potwierdza, że system SIEM musi umożliwiać dalszą rozbudowę ponad wymagane minimum 150 GB danych dziennie, bez konieczności wymiany architektury ani zakłócenia działania usług SOC?

Odpowiedź:

Tak, Zamawiający potwierdza.

Pytanie nr 12:

Czy Zamawiający potwierdza, że wymagany system SIEM powinien posiadać certyfikację bezpieczeństwa zgodną z normą *Common Criteria for IT Security Evaluation* (na poziomie co najmniej EAL3)?

Odpowiedź:

Na etapie rozeznania rynkowego Zamawiający analizuje różne rozwiązania dostępne na rynku. Zamawiający oczekuje, że system SIEM będzie spełniał odpowiednie standardy bezpieczeństwa oraz posiadał mechanizmy ochrony adekwatne do realizowanych zadań. Ewentualne wymagania dotyczące certyfikacji bezpieczeństwa, w tym zgodności z normą Common Criteria for IT Security Evaluation, zostaną doprecyzowane na etapie postępowania przetargowego.

Narodowy Instytut Onkologii
im. Marii Skłodowskiej-Curie – Państwowy Instytut Badawczy
Oddział w Gliwicach

ul. Wybrzeże Armii Krajowej 15
44-102 Gliwice

Dyrekcja
Tel.: +48 32 278 96 18

dyrektor@gliwice.nio.gov.pl
www.gliwice.nio.gov.pl

Centrala
Tel.: +48 32 278 88 88
Fax: +48 32 231 35 12

NIP: 5250008057
REGON: 000288366-00028

Pytanie nr 13:
Zgodnie z Załącznikiem nr 3 pkt. 4.5 serwery pracują pod kontrolą systemów Microsoft Windows oraz Linux.

Czy serwery, o których mowa w Załączniku nr 3 pkt 4.5, są środowiskiem bare-metal, wirtualizowanym, kontenerowym, czy też mieszanym?
Odpowiedź:
Zamawiający posiada środowisko mieszane.

Pytanie nr 14:
Czy wśród źródeł logów, o których mowa w Załączniku nr 3 pkt. 4.5 znajdują się jedynie źródła pracujące w lokalnej infrastrukturze Zamawiającego (on-premise) czy też w skład źródeł przeznaczonych do objęcia usługą znajdują się również źródła w lokalizacjach zdalnych (np. usługi pracujące na zasobach dostawców zewnętrznych)?
Odpowiedź:
Zamawiający obecnie nie posiada zewnętrznych zasobów.

Pytanie nr 15:
Czy Zamawiający określi wymagania dotyczące retencji logów oraz maksymalnego czasu przechowywania danych w systemie SIEM?
Odpowiedź:
Zamawiający określa maksymalny czas retencji operacyjnej na 4,5 miesiąca przy pełnym przewidzianym obciążeniu systemu. Natomiast maksymalny czas przechowywania danych nie jest określony w przypadku dopuszczenia archiwizacji na zewnętrznych zasobach. W sytuacji, gdy taka możliwość nie jest dostępna, Zamawiający przyjmuje maksymalny czas przechowywania danych na 12 miesięcy.

Pytanie nr 16:

Czy Zamawiający doprecyzuje czy wymaganie w Załączniku nr 3 pkt. 3 oraz pkt. 4.17 obsługi Scenariuszy Reakcji (playbooków) obejmujących sterowanie elementami infrastruktury (jak modyfikacja czarnych list) oznacza konieczność dostarczenia rozwiązania SIEM oraz rozwiązania klasy SOAR (Security Orchestration, Automation and Response) czy też Wykonawca ma posiadać bezpośredni dostęp administracyjny do urządzeń, systemów lub

Narodowy Instytut Onkologii
im. Marii Skłodowskiej-Curie –
Państwowy Instytut Badawczy
Oddział w Gliwicach

ul. Wybrzeże Armii Krajowej 15
44-102 Gliwice

Dyrekcja
Tel.: +48 32 278 96 18

dyrektor@gliwice.nio.gov.pl
www.gliwice.nio.gov.pl

Centrala
Tel.: +48 32 278 88 88
Fax: +48 32 231 35 12

NIP: 5250008057
REGON: 000288366-00028

innych elementów infrastruktury Zamawiającego, które umożliwiają realizację działań konfiguracyjnych.

Odpowiedź:
Zamawiający nie wymaga dostarczenia rozwiązania klasy SOAR. Wykonawca będzie mógł realizować Scenariusze Reakcji (playbooki), w tym sterowanie elementami infrastruktury, przy ograniczonym do niezbędnego minimum dostępie do urządzeń np. poprzez czarne listy, konta serwisowe czy API. Szczegóły dotyczące sposobu realizacji tych działań oraz zakresu dostępu zostaną doprecyzowane po podpisaniu umowy.

Pytanie nr 17:

Czy dopuszczalny jest sprzęt w formie serwera i wirtualizatora dla działania SIEM? Jaki jest wymagany wirtualizator?
Odpowiedź:
Zamawiający w pierwszej kolejności rozważa wdrożenie systemu SIEM w oparciu o serwer fizyczny. Jednocześnie, z uwagi na charakter prowadzonego rozeznania rynku, dopuszcza również możliwość realizacji rozwiązania w formie maszyny wirtualnej działającej w środowisku VMware.

Pytanie nr 18:

Czy jest potrzeba monitorowania urządzeń np drukarki, przełączniki, itp?
Odpowiedź:
Zamawiający przewiduje monitoring urządzeń krytycznych dla funkcjonowania infrastruktury IT, takich jak przełączniki sieciowe. Monitoring ten może być realizowany bezpośrednio przez system SIEM lub pośrednio – za pomocą dedykowanego systemu monitorowania, z którego dane będą przekazywane do SIEM.

Pozostałe urządzenia (np. drukarki) nie będą monitorowane w sposób bezpośredni. Zamawiający oczekuje, że ich aktywność będzie analizowana na podstawie logów pochodzących z systemu UTM, w szczególności pod kątem wykrywania anomalii oraz nietypowych prób komunikacji (np. próba zestawienia połączenia SSH do serwera).

Narodowy Instytut Onkologii
im. Marii Skłodowskiej-Curie –
Państwowy Instytut Badawczy
Oddział w Gliwicach

ul. Wybrzeże Armii Krajowej 15
44-102 Gliwice

Dyrekcja
Tel.: +48 32 278 96 18

dyrektor@gliwice.nio.gov.pl
www.gliwice.nio.gov.pl

Centrala
Tel.: +48 32 278 88 88
Fax: +48 32 231 35 12

NIP: 5250008057
REGON: 000288366-00028

Pytanie nr 19:

Czy licencja subskrypcyjna czy perpetual?
Odpowiedź:
Zamawiający w pierwszej kolejności rozważa licencje perpetual, jednak na tym etapie jako dodatkową ofertę rozważy model subskrypcyjny.

Pytanie nr 20:

Czy agenty dla systemów operacyjnych mają być zarządzane centralnie z poziomu SIEM czy też lokalnie na każdym serwerze?
Odpowiedź:
Agent nie jest wymagany, ale w przypadku gdy będzie on instalowany musi być zażądany centralnie z poziomu SIEM.

Pytanie nr 21:

Dla jakich systemów operacyjnych OS i wersja ma działać agent?
Odpowiedź:
Zamawiający posiada systemy operacyjne: Windows, Linux, MAC.

Pytanie nr 22:

Czy w ramach usługi i dostarczonego systemu SIEM wymagane jest również prowadzenie monitorowania dostępności i wydajności systemów? np sprawdzanie ilości dostępnej pamięci dyskowej i alarmowanie gdy zajętość dysku jest wyższa niż wartość progowa?
Odpowiedź:
Zamawiający nie wymagał takiej funkcjonalności.

Pytanie nr 23:

Czy w przypadku awarii dysków konieczne jest pozostawienie elementu u Zamawiającego?

Narodowy Instytut Onkologii
im. Marii Skłodowskiej-Curie –
Państwowy Instytut Badawczy
Oddział w Gliwicach

ul. Wybrzeże Armii Krajowej 15
44-102 Gliwice

Dyrekcja
Tel.: +48 32 278 96 18

dyrektor@gliwice.nio.gov.pl
www.gliwice.nio.gov.pl

Centrala
Tel.: +48 32 278 88 88
Fax: +48 32 231 35 12

NIP: 5250008057
REGON: 000288366-00028

Odpowiedź:
Zgodnie z polityka bezpieczeństwa uszkodzone nośniki danych muszą zostać u Zamawiającego.

Pytanie nr 24:

Jaki jest wymagany czas wymiany urządzenia w przypadku awarii?
Odpowiedź:
Zamawiający na obecnym etapie nie określił wymaganego czasu wymiany urządzenia w przypadku awarii. Parametr ten zostanie doprecyzowany na etapie postępowania przetargowego.

Na potrzeby rozeznania rynku można przyjąć orientacyjny czas wymiany do 3 dni roboczych, z możliwością jego wydłużenia pod warunkiem dostarczenia sprzętu zastępczego umożliwiającego uruchomienie systemu, nawet z ograniczoną wydajnością lub funkcjonalnością.

Pytanie nr 25:

Ile stacji ma być objęte monitorowaniem agentowym?
Odpowiedź:
Zamawiający nie przewiduje obowiązku instalacji agentów na stacjach końcowych.

Jednocześnie, na potrzeby oszacowania kosztów oraz przygotowania oferty, należy przyjąć orientacyjną liczbę do 1000 potencjalnych agentów.

Pytanie nr 26:

Jaki jest przewidziany czas przechowywania logów?
Odpowiedź:
Zamawiający określa wymagany okres przechowywania logów w następujący sposób:

- logi dostępne do bieżącej analizy – przez okres 4,5 miesiąca,
- logi archiwalne – przez okres 12 miesięcy.

Narodowy Instytut Onkologii
im. Marii Skłodowskiej-Curie – Państwowy Instytut Badawczy
Oddział w Gliwicach

ul. Wybrzeże Armii Krajowej 15
44-102 Gliwice

Dyrekcja
Tel.: +48 32 278 96 18

dyrektor@gliwice.nio.gov.pl
www.gliwice.nio.gov.pl

Centrala
Tel.: +48 32 278 88 88
Fax: +48 32 231 35 12

NIP: 5250008057
REGON: 000288366-00028

Logi archiwalne mogą być przechowywane na zewnętrznych zasobach magazynowych, pod warunkiem zapewnienia ich integralności oraz możliwości odtworzenia w przypadku potrzeby analizy.

Pytanie nr 27:

Jaka jest przewidywana średnia wartość zdarzeń odbieranych w ciągu sekundy w najbardziej zajętej godzinie dnia?
Odpowiedź:
Zamawiający nie jest wstanie określić tego parametru.

Pytanie nr 28:

Czy wymagana jest praca w wysokiej dostępności – HA?
Odpowiedź:
Zamawiający nie wymaga wysokiej dostępności – HA.

Pytanie nr 29:

Prosimy o wskazanie liczby urządzeń, które muszą być objęte analizą UEBA?
Odpowiedź:
Zamawiający przewiduje, że analizą w ramach funkcjonalności UEBA będą objęte wyłącznie logi pochodzące z systemów i urządzeń krytycznych dla funkcjonowania infrastruktury IT.

Zakres ten obejmuje w szczególności kluczowe systemy serwerowe, systemy bezpieczeństwa oraz wybrane urządzenia sieciowe. Pozostałe urządzenia i systemy nie są planowane do objęcia analizą behawioralną UEBA.

Liczba takich urządzeń na dzień odpowiedzi nie przekroczy 250 jednak systematycznie rośnie.

Pytanie nr 30:

Prosimy o określenie liczby urządzeń sieciowych (switche), które będą przesyłały logi?
Odpowiedź:
Zamawiający szacuje liczbę urządzeń sieciowych typu switch, które będą przesyłały logi, na około 70 urządzeń logicznych.

Narodowy Instytut Onkologii
im. Marii Skłodowskiej-Curie – Państwowy Instytut Badawczy
Oddział w Gliwicach

ul. Wybrzeże Armii Krajowej 15
44-102 Gliwice

Dyrekcja
Tel.: +48 32 278 96 18

dyrektor@gliwice.nio.gov.pl
www.gliwice.nio.gov.pl

Centrala
Tel.: +48 32 278 88 88
Fax: +48 32 231 35 12

NIP: 5250008057
REGON: 000288366-00028

Należy przy tym zaznaczyć, że pojedyncze urządzenie logiczne może składać się z kilku fizycznych przełączników pracujących w stosie (stack), które z punktu widzenia zarządzania i logowania funkcjonują jako jeden przełącznik.

Pytanie nr 31:

Prosimy o potwierdzenie, czy wymienione urządzenia i systemy (WAF, UTM, PAM, VPN, DLP) posiadają możliwość przesyłania logów za pośrednictwem protokołu syslog lub udostępniają logi poprzez interfejs API?

Odpowiedź:

Zamawiający potwierdza, że wymienione systemy i urządzenia (WAF, UTM, PAM, VPN, DLP), które planowane są do integracji z systemem SIEM, posiadają możliwość przesyłania logów za pośrednictwem protokołu syslog lub udostępniają dane logów poprzez dedykowany interfejs API.

Narodowy Instytut Onkologii
im. Marii Skłodowskiej-Curie –
Państwowy Instytut Badawczy
Oddział w Gliwicach

ul. Wybrzeże Armii Krajowej 15
44-102 Gliwice

Dyrekcja
Tel.: +48 32 278 96 18

dyrektor@gliwice.nio.gov.pl
www.gliwice.nio.gov.pl

Centrala
Tel.: +48 32 278 88 88
Fax: +48 32 231 35 12

NIP: 5250008057
REGON: 000288366-00028