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

Gliwice dn. 26.1.2026r.

DO WSZYSTKICH ZAINTERESOWANYCH

Dot. zapytania cenowego nr DZ/DI-072-5/26 z dnia 20.1.2026r. dot. **zakupu i wdrożenia systemu zarządzania podatnościami**.

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 złożonym pytaniem do opublikowanej na stronie internetowej Zamawiającego dokumentacji odnośnie wyżej wymienionego zapytania cenowego, przekazujemy Państwu pytanie, jak i udzieloną odpowiedź.

Pytanie nr 5:

W związku z faktem, że projekt jest finansowany z funduszy KPO, których celem jest cyfryzacja i zwiększenie odporności systemów ochrony zdrowia, czy Zamawiający w celu maksymalizacji efektywności personelu IT przewiduje dodatkowe punktację w kryterium jakościowym lub zakłada zaoferowanie systemu wyposażonego w zintegrowany moduł automatyzacji typu low-code? Moduł ten, poprzez wsparcie dla skryptów Python/PowerShell, protokołów SSH/SNMP oraz REST API, umożliwia nie tylko identyfikację, ale i automatyczną naprawę (remediację) podatności, co znacząco wykracza poza standardowy wymóg samej integracji z systemami zgłoszeniowymi.

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:
Zamawiający informuje, że na etapie przygotowania postępowania analizuje dostępne na rynku rozwiązania, w tym funkcjonalności wykraczające poza minimalne wymagania, które mogą przyczyniać się do zwiększenia efektywności pracy personelu IT oraz realizacji celów KPO w zakresie cyfryzacji i odporności systemów ochrony zdrowia.

Zamawiający nie wyklucza uwzględnienia takich funkcjonalności w kryteriach oceny ofert, w szczególności w ramach kryteriów jakościowych, jednak ostateczny zakres wymagań oraz sposób punktacji zostaną określone w dokumentach postępowania przetargowego.

Pytanie nr 6:
Czy Zamawiający, dążąc do uzyskania jak najwyższej synergii z posiadaną infrastrukturą serwerową (VMware, Hyper-V, oVirt), przewiduje dodatkowe punktację w kryterium jakościowym lub zakłada zaoferowanie rozwiązania, które pozwalają na dwukierunkową integrację z hiperwizorami? Chodzi o funkcjonalność pozwalającą na bezpośrednią edycję parametrów maszyn wirtualnych z poziomu konsoli systemu zarządzania podatnościami, co skraca czas izolacji zagrożonych zasobów w porównaniu do systemów oferujących jedynie pasywny odczyt danych.

Odpowiedź:
Zamawiający na etapie rozeznania rynku nie zakłada wymagania dwukierunkowej integracji z hiperwizorami ani bezpośredniej edycji parametrów maszyn wirtualnych. Ewentualne dodatkowe funkcjonalności będą przedmiotem dalszych analiz na etapie przygotowania postępowania.

Pytanie nr 7:
Biorąc pod uwagę wymóg szczegółowego raportowania i klasyfikacji ryzyka , czy Zamawiający przewiduje dodatkowe punktację w kryterium jakościowym lub zakłada zaoferowanie systemów posiadających narzędzie low-code do samodzielnego definiowania struktury bazy zasobów, tzw. Inventory (możliwość dodawania własnych atrybutów bez udziału producenta)? Funkcjonalność ta pozwala na precyzyjne odzwierciedlenie specyfiki bazy sprzętowej Zamawiającego w systemie bezpieczeństwa.

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:
Zamawiający nie wyklucza uwzględnienia takich funkcjonalności w kryteriach oceny ofert, w szczególności w ramach kryteriów jakościowych, jednak ostateczny zakres wymagań oraz sposób punktacji zostaną określone w dokumentach postępowania przetargowego.

Pytanie nr 8:
Czy w ramach oceny ofert Zamawiający przewiduje dodatkowe punktację w kryterium jakościowym lub zakłada wymóg posiadania wbudowanego, graficznego kreatora integracji (typu drag-and-drop)? Narzędzie to umożliwiłoby Zamawiającemu samodzielną i szybką integrację z obecnymi oraz przyszłymi systemami klasy EDR, IAM czy Firewall bez konieczności zakupu dodatkowych usług programistycznych, co wpisuje się w cele efektywności kosztowej Inwestycji.

Odpowiedź:
Zamawiający nie wyklucza uwzględnienia takich funkcjonalności w kryteriach oceny ofert, w szczególności w ramach kryteriów jakościowych, jednak ostateczny zakres wymagań oraz sposób punktacji zostaną określone w dokumentach postępowania przetargowego.

Pytanie nr 9:
a. Czy w związku z zapisem punkt 15b: "skanowania z uwierzytelnieniem, umożliwiającego m.in.: wykrywanie komunikacji z infrastrukturą botnetową,"

zamawiający przewiduje integracje z narzędziami do analizowania ruchu sieciowego?

b. NDR/IDS? Czy zamawiający przyzna dodatkowe punktację w kryterium jakościowym lub zakłada wymóg integracji z narzędziami typu NDR/IDS oraz możliwość zintegrowania ich z procesem skanowania podatności i korelacji wyników?

c. Czy zamawiający posiada wdrożone w infrastrukturze narzędzia typu IDS/NDR z którymi przewiduje integracje?

Odpowiedź:

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

Zamawiający dopuszcza możliwość integracji oferowanego rozwiązania z zewnętrznymi narzędziami lub modułami, w tym z narzędziami do analizy ruchu sieciowego. Jednocześnie Zamawiający informuje, że nie wymaga integracji z systemami klasy NDR/IDS, gdyż nie posiada obecnie wdrożonych tego typu rozwiązań. Oferowany system powinien posiadać taką funkcjonalność.

Pytanie nr 10:
Czy wymóg funkcjonalności patch managera dotyczy tylko przypadku rozwiązania chmurowego?

Odpowiedź:
Tak Zamawiający potwierdza.

Pytanie nr 11:
Czy w punkcie 7 chodzi o zapewnienie gotowej integracji przez REST API np. z rozwiązaniem licencjonowanym? Prosimy o potwierdzenie czy w tego typu przypadkach licencja jest dostarczana przez Zamawiającego?

Odpowiedź:
Zamawiający nie przewiduje dostarczania dodatkowych licencji we własnym zakresie. Wszystkie niezbędne licencje muszą zostać dostarczone na etapie wdrożenia.

Pytanie nr 12:
Co Zamawiający rozumie przez wzorce konfiguracji w kontekście punktu 13?

Odpowiedź:
Zamawiający rozumie wzorce konfiguracji jako predefiniowane profile skanowania, obejmujące zestawy parametrów i reguł dostosowanych do określonych klas zasobów (np. aplikacje webowe, systemy operacyjne, serwery), które umożliwiają optymalizację zakresu i dokładności skanowania.

Pytanie nr 13:
Co Zamawiający rozumie przez wzorce konfiguracji w kontekście punktu 13?

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:
Zamawiający rozumie wzorce konfiguracji jako predefiniowane profile skanowania, obejmujące zestawy parametrów i reguł dostosowanych do określonych klas zasobów (np. aplikacje webowe, systemy operacyjne, serwery), które umożliwiają optymalizację zakresu i dokładności skanowania.

Pytanie nr 14:
Dotyczy punktu 7 Załącznika nr 3 – Specyfikacja techniczna zamówienia, tj.:
„*W przypadku, gdy system zarządzania podatnościami oraz skaner podatności pochodzą od różnych producentów, rozwiązanie musi zapewniać integrację z co najmniej 7 różnymi skanerami podatności*."

W związku z wymaganiem integracji systemu zarządzania podatnościami z co najmniej 7 różnymi skanerami podatności (w przypadku, gdy komponenty pochodzą od różnych producentów), prosimy o rozważenie doprecyzowania, czy Zamawiający dopuszcza możliwość wymagania, aby system zarządzania podatnościami oraz skaner podatności pochodziły od jednego producenta, tj. stanowiły jednolitą platformę, bez wykorzystania skanerów firm trzecich.

Dodatkowo prosimy o potwierdzenie, czy Zamawiający akceptuje zapis:
„*Nie dopuszcza się stosowania skanerów podatności 3rd party oraz skanerów open-source – wymagane jest dostarczenie rozwiązania w modelu jednego producenta (end-to-end).*"

Uzasadnienie:

Utrzymywanie środowiska, w którym system zbiera dane z wielu różnych skanerów podatności (w tym potencjalnie narzędzi open-source), może powodować istotne ryzyka oraz wzrost kosztów, w szczególności:

- Ryzyko supply chain / zależności od wielu dostawców

  Każdy dodatkowy skaner = kolejny komponent oprogramowania, aktualizacje, biblioteki, integracje, połączenia API oraz uprawnienia. Zwiększa to powierzchnię ataku i liczbę elementów, które muszą być stale nadzorowane i łatane.

- Ryzyko wycieku informacji o podatnościach organizacji

  Systemy zarządzania podatnościami i skanery przetwarzają dane o krytycznym znaczeniu (np. lista zasobów, wersje usług, wykryte CVE, exploity, priorytety ryzyka). Przy wielu

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

integracjach rośnie ryzyko, że podatność lub błąd w którymś komponencie umożliwi napastnikowi pozyskanie informacji o słabych punktach firmy.

– Większa złożoność i koszty utrzymania

  Integracja z wieloma skanerami oznacza: więcej konektorów, troubleshooting kompatybilności po aktualizacjach, różne formaty danych, dublowanie wyników, mapowanie reguł oraz większy nakład na utrzymanie operacyjne i administracyjne.

– Spójność procesu i odpowiedzialność jednego producenta

  Platforma jednego dostawcy upraszcza audytowanie, utrzymanie, wsparcie oraz ogranicza „przerzucanie odpowiedzialności" (system vs skaner vs integracja). W praktyce łatwiej zapewnić jednolite SLA, bezpieczeństwo i kontrolę zmian.

W związku z powyższym prosimy o wyjasnienie, czy Zamawiający preferuje model jednego producenta oraz czy dopuszcza zmianę wymagania tak, aby system zarządzania podatnościami musiał być dostarczony razem z dedykowanym skanerem tego samego producenta, bez użycia skanerów 3rd party i open-source, zgodnie z poniższym brzmieniem:

„*System zarządzania podatnościami oraz skaner podatności, które muszą pochodzić od jednego producenta i stanowić jednolitą platformę (end-to-end) i nie dopuszcza stosowania skanerów podatności firm trzecich (3rd party) ani skanerów open-source*."

Odpowiedź:
Zamawiający nie wyklucza uwzględnienia iż system w którym nie występuje ryzyko zależności od wielu dostawców będzie miało istotny wpływ na kryterium oceny ofert, w szczególności w ramach kryteriów jakościowych, jednak ostateczny zakres wymagań oraz sposób punktacji zostaną określone w dokumentach postępowania przetargowego.

Pytanie nr 15:
Dotyczy punktu 8 Załącznika nr 3 – Specyfikacja techniczna zamówienia.

Zamawiający w specyfikacji technicznej w ww. punkcie 8 wymaga:

"System musi umożliwiać integrację z systemami klasy SOC oraz SIEM."

Przez natywną integrację Wykonawca rozumie integrację, która:

□ jest dostępna jako oficjalna funkcjonalność rozwiązania (wbudowana integracja, gotowy konektor / aplikacja / wtyczka),

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

- jest opisana i udokumentowana na oficjalnych stronach producenta rozwiązania,
- nie wymaga tworzenia i utrzymywania własnych skryptów, własnego kodu ani ręcznego budowania integracji poprzez API,
- jest utrzymywana i rozwijana przez producenta oprogramowania (aktualizacje, kompatybilność wersji, poprawki bezpieczeństwa, wsparcie techniczne integracji).

W związku z powyższym, prosimy o wyjaśnienie, czy Zamawiający wymaga, aby:

„System musi zapewniać natywną integrację z platformami klasy SIEM oraz systemami do zarządzania poprawkami (Patch Management), w tym co najmniej z:

- systemem klasy SIEM,
- Jira (zarządzanie zadaniami / workflow),
- ManageEngine Patch Manager (lub równoważnym rozwiązaniem Patch Management),
- wewnętrznym / własnym systemem Zamawiającego pełniącym rolę Patch Managera (np. poprzez gotowy, wspierany przez producenta konektor integracyjny).”

Odpowiedź:
Zamawiający na dzień publikacji postępowania nie posiada wdrożonego systemu klasy SIEM ani nie korzysta z usług SOC.

Wymaganie określone w pkt 8 Specyfikacji technicznej ma charakter funkcjonalny i dotyczy zapewnienia przez oferowany System możliwości integracji z systemami klasy SOC oraz SIEM, rozumianej jako gotowość rozwiązania do takiej integracji w przypadku jej wdrożenia w przyszłości.

Zamawiający nie wymaga zapewnienia natywnej integracji z konkretnymi, wskazanymi z nazwy platformami (w tym Jira, ManageEngine Patch Manager ani innymi konkretnymi rozwiązaniami klasy Patch Management), ani nie wymaga integracji z wewnętrznym systemem Zamawiającego pełniącym rolę Patch Managera.

Spełnieniem wymagania będzie zapewnienie, że oferowany System:

- posiada natywnie wspierane przez producenta mechanizmy integracyjne umożliwiające współpracę z systemami klasy SIEM/SOC (np. w postaci gotowych konektorów, wtyczek lub obsługi standardowych protokołów i formatów wymiany danych, takich jak Syslog),

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

- umożliwia integrację w sposób utrzymywany i rozwijany przez producenta rozwiązania,
- nie wymaga tworzenia i utrzymywania własnego kodu po stronie Zamawiającego.

Pytanie nr 16:

Dotyczy punktu 9 Załącznika nr 3 – Specyfikacja techniczna zamówienia.

W nawiązaniu do powyższego wymagania:

„*System musi zapewniać ocenę ryzyka podatności, w tym ranking podatności w oparciu o powszechnie stosowane metody, np. CVSS*”,

prosimy o potwierdzenie, czy Zamawiający dopuszcza (lub preferuje) zastosowanie dynamicznego systemu klasyfikacji ryzyka, który:

wykorzystuje bazowy (statyczny) wskaźnik CVSS,

a następnie automatycznie przelicza scoring podatności w interwale nie rzadziej niż co 24 godziny na podstawie aktualnych danych kontekstowych (np. dostępność exploita, aktywne kampanie, telemetryka zagrożeń, obserwacje z Internetu / threat intelligence),

podając zaktualizowany scoring ryzyka oraz priorytety remediation dla danej podatności.

Uzasadnienie:

Statyczny scoring CVSS jest powszechnie stosowany i stanowi dobrą bazę, jednak w praktyce nie odzwierciedla dynamicznie zmieniającego się poziomu zagrożenia (np. pojawienie się publicznego exploita lub aktywne wykorzystanie danej podatności w kampaniach ataków).

Zastosowanie dynamicznej klasyfikacji ryzyka:

- zwiększa bezpieczeństwo operacyjne, ponieważ priorytety napraw są aktualizowane zgodnie z realnym ryzykiem „tu i teraz”,
- umożliwia szybszą reakcję na podatności, które stały się nagle krytyczne (np. masowo wykorzystywane),
- zmniejsza ryzyko błędnej priorytetyzacji, gdzie wysoki CVSS nie zawsze oznacza realne zagrożenie w środowisku i odwrotnie,
- jest charakterystyczne dla zaawansowanych platform klasy enterprise, a nie narzędzi niższej klasy ograniczających się wyłącznie do statycznego CVSS.

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

W związku z powyższym prosimy o wyjasnienie, czy Zamawiający dopuszcza wdrożenie systemu, który oprócz CVSS zapewnia ciągłą (min. co 24h) aktualizację oceny ryzyka podatności, tj.:

„*System, który musi zapewniać ocenę ryzyka podatności, w tym ranking podatności oparty o metody powszechnie stosowane (np. CVSS), rozszerzony o dynamiczny mechanizm oceny ryzyka, w ramach którego scoring podatności jest automatycznie przeliczany w interwale nie rzadziej niż co 24 godziny oraz aktualizowany w systemie w oparciu o bieżące informacje o zagrożeniach, co skutkuje nadaniem aktualnego priorytetu obsługi (remediation) dla danej podatności*."

Odpowiedź:
Zamawiający nie wyklucza uwzględnienia takich funkcjonalności w kryteriach oceny ofert, w szczególności w ramach kryteriów jakościowych, jednak ostateczny zakres wymagań oraz sposób punktacji zostaną określone w dokumentach postępowania przetargowego.

Pytanie nr 17:
Dotyczy punktu 10 Załącznika nr 3 – Specyfikacja techniczna zamówienia, tj.:

„*System musi umożliwiać utworzenie* ***co najmniej 10 kont użytkowników****, w tym:*

- *minimum* ***5 kont administratorów****,*
- *minimum* ***5 kont audytorów*** *z ograniczonymi uprawnieniami*."

Wprowadzenie braku limitów kont administracyjnych oraz granularnego modelu ról i uprawnień (RBAC) jest kluczowe ze względu na bezpieczeństwo, audytowalność i efektywność operacyjną systemu zarządzania podatnościami:

– Zasada najmniejszych uprawnień (Least Privilege)

  W praktyce wiele osób pracuje w procesie zarządzania podatnościami, ale nie każda powinna posiadać uprawnienia administratora. Granularne role ograniczają zakres dostępu tylko do niezbędnych funkcji, co minimalizuje ryzyko błędów oraz nadużyć.

– Redukcja ryzyka kompromitacji i skutków incydentu

  Konto administratora ma najwyższy poziom dostępu, w tym możliwość zmiany konfiguracji, integracji czy wyjątków w podatnościach. Ograniczenie liczby osób z pełnymi uprawnieniami oraz precyzyjne rozdzielenie obowiązków zmniejsza skutki ewentualnego przejęcia konta.

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

– Rozdział obowiązków (Segregation of Duties)

  Wymóg wydzielenia ról (np. zarządzanie poświadczeniami, zarządzanie skanami, analiza wyników, raportowanie, audyt) wspiera dobre praktyki bezpieczeństwa oraz zgodność z normami i wymaganiami kontrolnymi. Minimalizuje to ryzyko sytuacji, w której jedna osoba posiada pełną kontrolę nad całym procesem.

– Lepsze wsparcie pracy zespołowej i ciągłości działania

  Brak limitu kont administracyjnych eliminuje sztuczne ograniczenia licencyjne, które mogą blokować pracę w większych zespołach lub w sytuacjach zastępstw (dyżury, rotacje, urlopy). System powinien wspierać skalowanie zespołu bez barier technicznych.

– Audytowalność i zgodność z wymaganiami bezpieczeństwa

  Granularne role ułatwiają prowadzenie audytu i rozliczalność działań użytkowników, ponieważ można jednoznacznie przypisać zakres odpowiedzialności i uprawnień do roli, a nie nadawać wszystkim szerokie uprawnienia administracyjne.

– Ograniczenie kosztów operacyjnych i błędów utrzymaniowych

  Przy braku granularnych ról często stosuje się obejścia (np. wspólne konta, nadawanie admina "na chwilę"), co zwiększa ryzyko błędów oraz komplikuje zarządzanie. RBAC porządkuje proces i zmniejsza nakład administracyjny.

W związku z powyższym prosimy o potwierdzenie, czy Zamawiający dopuszcza wdrożenie:

„*Systemu, który musi umożliwiać tworzenie kont użytkowników bez ograniczeń ilościowych, w tym nie może posiadać limitu liczby kont administratorów, gdzie System musi zapewniać możliwość definiowania ról i uprawnień w modelu RBAC (Role-Based Access Control) oraz przypisywania ich użytkownikom w sposób granularny.*

Minimalny zestaw ról, które system musi umożliwiać zdefiniowanie i przypisanie, obejmuje co najmniej:

- *Administrator systemu – pełne zarządzanie konfiguracją, użytkownikami, integracjami oraz ustawieniami bezpieczeństwa,*
- *Security Manager / Kierownik bezpieczeństwa – zarządzanie politykami skanowania, priorytetami ryzyka, wyjątkami oraz raportowaniem,*
- *Administrator haseł / Credential Manager – zarządzanie wyłącznie poświadczeniami do skanowania oraz ich cyklem życia,*
- *Operator skanów / Scan Operator – uruchamianie i harmonogramowanie skanów bez możliwości zmiany konfiguracji globalnej,*

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

- *Analityk bezpieczeństwa – dostęp do wyników, klasyfikacji ryzyka, trendów i rekomendacji, bez możliwości modyfikacji ustawień systemu,*
- *Audytor (read-only) – wyłącznie podgląd raportów i historii działań (bez możliwości zmian),*
- *Użytkownik biznesowy / Viewer – ograniczony dostęp do podglądu ryzyka i stanu podatności w przypisanym zakresie.*
- *System musi umożliwiać ograniczanie dostępu do danych i funkcji co najmniej na poziomie:*
  - *organizacji / jednostek,*
  - *grup zasobów (asset groups),*
  - *projektów / środowisk (np. DEV/TEST/PROD),*
  - *typów akcji (odczyt, edycja, uruchamianie skanów, zarządzanie wyjątkami, eksport danych, integracje).”*

Odpowiedź:
Zamawiający nie wyklucza uwzględnienia takich funkcjonalności w kryteriach oceny ofert, w szczególności w ramach kryteriów jakościowych, jednak ostateczny zakres wymagań oraz sposób punktacji zostaną określone w dokumentach postępowania przetargowego.

Pytanie nr 18:
Dotyczy punktu 15 lit. b) Załącznika nr 3 – Specyfikacja techniczna zamówienia, tj.:

„*b) skanowania z uwierzytelnieniem, umożliwiającego m.in.:*
(...)

- *ocenę zgodności z regulacjami (np. PCI DSS) oraz polityką bezpieczeństwa*.”

W związku z tym, że uważamy, że skanowanie zgodności to realna kontrola bezpieczeństwa, samo stwierdzenie, że produkt „spełnia standard” jest niewystarczające. Zdaniem Wykonawcy, Zamawiający potrzebuje funkcji umożliwiającej automatyczną weryfikację konfiguracji i kontrolę zgodności w czasie (ciągłe monitorowanie), z możliwością raportowania odchyleń.

- PCI DSS nie jest „tylko dla banków”.

  PCI DSS dotyczy wszystkich organizacji, które przetwarzają, przesyłają lub przechowują dane kart płatniczych, czyli np. e-commerce, retail, platformy subskrypcyjne, operatorzy usług, integratorzy płatności, call center.

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

Nawet jeśli organizacja formalnie nie podlega PCI DSS, standard ten jest uznawany za jeden z najbardziej rygorystycznych i praktycznych zbiorów wymagań technicznych, dlatego jego stosowanie znacząco podnosi poziom bezpieczeństwa środowiska IT.

- PCI DSS jako „wysoki benchmark" dla twardych zabezpieczeń.

  Kontrole PCI DSS obejmują m.in. bezpieczeństwo konfiguracji, segmentację, twarde wymagania dla kont uprzywilejowanych, logowanie, podatności, zarządzanie aktualizacjami i testy bezpieczeństwa. Dzięki temu działa jako sprawdzony punkt odniesienia również dla organizacji spoza sektora finansowego.

- SOC 2 i ISO 27001 wspierają audyt i rozliczalność

  SOC 2 oraz ISO/IEC 27001 są często wymagane przez klientów i audyty zewnętrzne. Możliwość realizowania skanów zgodności ułatwia ciągłą ocenę stanu kontroli, skraca czas przygotowania do audytu oraz pozwala szybciej identyfikować luki w konfiguracji.

W związku z powyższym prosimy o potwierdzenie, czy System (w szczególności skaner podatności) musi umożliwiać realizację skanów zgodności (compliance scans) w odniesieniu do co najmniej następujących standardów i ram kontrolnych:

- PCI DSS
- SOC 2
- ISO/IEC 27001

Wymaganie dotyczy możliwości przeprowadzenia skanu zgodności, tj. automatycznej weryfikacji ustawień, konfiguracji i kontroli technicznych względem reguł/benchmarków wynikających z ww. standardów – a nie wyłącznie deklaracji, że produkt „jest zgodny" z danym standardem.
Wykonawca winien dostarczyć potwierdzenie spełnienia wymagania w formie co najmniej jednego z poniższych dowodów dla każdego standardu:

- certyfikat / oficjalne potwierdzenie producenta dotyczące możliwości wykonywania skanów zgodności w danym zakresie, lub
- link do oficjalnej strony organizacji/standardu lub uznanej instytucji branżowej, na której wskazano, że dane rozwiązanie może realizować skanowanie zgodności dla: PCI DSS, SOC 2, ISO/IEC 27001, 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

link do oficjalnej dokumentacji producenta (np. compliance checks/policy templates/benchmark scanning) jednoznacznie potwierdzający dostępność skanów zgodności dla ww. standardów.

Odpowiedź:
Zamawiający nie wyklucza uwzględnienia takich funkcjonalności w kryteriach oceny ofert, w szczególności w ramach kryteriów jakościowych, jednak ostateczny zakres wymagań oraz sposób punktacji zostaną określone w dokumentach postępowania przetargowego.

Pytanie nr 19:
Dotyczy punktu 15 lit. a) i b) Załącznika nr 3 – Specyfikacja techniczna zamówienia.

Zamawiający w specyfikacji technicznej w ww. punkcie 15 wymaga:

”*System musi umożliwiać wykrywanie podatności przy użyciu co najmniej dwóch metod:*

a) *skanowania sieciowego, obejmującego m.in.:*
   - *identyfikację otwartych portów,*
   - *identyfikację działających usług,*
   - *identyfikację wersji aplikacji (o ile jest możliwa),*
   - *próbę uwierzytelnienia z wykorzystaniem domyślnych danych dostępowych;*

b) *skanowania z uwierzytelnieniem, umożliwiającego m.in.:*
   - *identyfikację wersji systemu operacyjnego,*
   - *analizę uruchomionych usług i procesów,*
   - *wykrywanie komunikacji z infrastrukturą botnetową,*
   - *analizę zmian w rejestrach systemowych,*
   - *ocenę zgodności z regulacjami (np. PCI DSS) oraz polityką bezpieczeństwa*."

W związku z powyższym, prosimy o wyjaśnienie, czy Zamawiający wymaga, aby poza skanami aktywnymi i pasywnymi system musiał mieć możliwość skanowania aktywnych środowisk kontenerowych (runtime), zgodnie z poniższym brzmieniem:

„System, który musi umożliwiać skanowanie aktywnych środowisk kontenerowych (Container Runtime Security) w sposób ciągły, w tym co najmniej środowisk opartych o Kubernetes, poprzez dedykowany mechanizm zbierania danych z klastra (np. agent/connector uruchamiany w klastrze) bez konieczności ręcznego uruchamiania skanów na pojedynczych hostach.
W ramach skanowania środowisk kontenerowych system musi zapewniać co najmniej:

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

a) *Wykrywanie i inwentaryzację zasobów kontenerowych (discovery)*
   - *klastry, namespace, nody, pody, kontenery, obrazy, rejestry obrazów oraz zależności komponentów.*

b) *Identyfikację podatności w uruchomionych kontenerach oraz obrazach*
   - *wykrywanie CVE dla bibliotek i pakietów systemowych/aplikacyjnych, wraz z informacją o wersji, źródle oraz priorytecie naprawy.*

c) *Skanowanie konfiguracji bezpieczeństwa (misconfiguration / compliance)*
   - *ocena zgodności konfiguracji klastra i workloadów względem dobrych praktyk (np. benchmarków hardening), w tym uprawnień, polityk, dostępu do API, eksponowanych usług i ustawień runtime.*

d) *Detekcję niebezpiecznych ustawień i ekspozycji*
   - *kontenery uprzywilejowane (privileged), mounty hostPath, uruchomienia jako root, nadmiarowe capabilities, brak ograniczeń zasobów, zbyt szerokie uprawnienia RBAC, publiczne endpointy.*

e) *Korelację wyników z kontekstem środowiska*
   - *powiązanie podatności i błędów konfiguracji z konkretnym zasobem (namespace/pod/kontener/nod) oraz wskazanie krytyczności i priorytetu remediation.*

f) *Aktualizację wyników w trybie cyklicznym lub ciągłym*
   - *automatyczne odświeżanie wyników i ryzyka bez potrzeby ręcznego restartowania procesu skanowania (minimum raz na 24h lub częściej, jeśli dane są dostępne).*

g) *Raportowanie i eksport wyników*
   - *generowanie raportów dla zespołów bezpieczeństwa i DevOps oraz możliwość eksportu wyników (np. do SIEM/SOAR/ITSM) wraz z metadanymi zasobów kontenerowych."*

Odpowiedź:
Zamawiający wyjaśnia, że w ramach wymagań określonych w pkt 15 lit. a) i b) Załącznika nr 3 nie wymaga zapewnienia funkcjonalności ciągłego skanowania aktywnych środowisk kontenerowych (Container Runtime Security), w tym środowisk opartych o Kubernetes.

Jednocześnie Zamawiający wymaga, aby oferowany System umożliwiał wykrywanie podatności we wszystkich skanowanych zasobach IT, niezależnie od ich formy technologicznej, w tym również w zasobach kontenerowych, o ile podatności te mogą zostać wykryte w ramach skanowania sieciowego lub skanowania z uwierzytelnieniem.

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

Zamawiający nie narzuca sposobu realizacji powyższego wymagania ani nie wymaga stosowania dedykowanych mechanizmów skanowania środowisk kontenerowych w trybie ciągłym.

Zamawiający informuje jednocześnie, że na etapie postępowania może rozważyć przyznanie dodatkowej punktacji za zaoferowanie funkcjonalności ciągłego skanowania środowisk kontenerowych, o ile zostanie to przewidziane w kryteriach oceny ofert określonych w dokumentach postępowania.

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