Załącznik nr 3 – specyfikacja techniczna zamówienia do zapytania nr DZ/DI-072-5/26

Przedmiotem zamówienia jest zakup i wdrożenie systemu zarządzania podatnościami. Specyfikacja ogólna opisana jest w *„Załącznika nr 4 – Zakres realizacji przedsięwzięcia do wyboru przedsięwzięcia*" do Inwestycja D.1.1.2.

Zgodnie z wymaganiami ogólnymi określonymi w wyżej wymienionym załączniku system zapewni:

Automatyzację skanowania:

- Regularne i cykliczne skanowanie infrastruktury IT.
- Możliwość uruchamiania skanów po istotnej zmianie w systemie (np. aktualizacja, wdrożenie nowej funkcji).

Identyfikację podatności:

- Wykrywanie podatności w systemach operacyjnych, aplikacjach, bazach danych, urządzeniach sieciowych.
- Klasyfikacja podatności według poziomu ryzyka.

Raportowanie wyników:

- Generowanie szczegółowych raportów z identyfikowanymi podatnościami oraz zaleceniami naprawczymi.
- Możliwość eksportu wyników do formatów CSV, PDF

Integrację z innymi systemami:

- Możliwość komunikacji z systemami zarządzania poprawkami w celu automatycznego tworzenia zgłoszeń.

Monitorowanie i śledzenie trendów:

- Śledzenie liczby i rodzaju podatności w czasie.
- Wizualizacja wyników za pomocą wykresów i dashboardów.

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

Bezpieczeństwo:

- Dostęp do wyników skanów ograniczony rolami i uprawnieniami.
- Szyfrowanie danych związanych ze skanowaniem.

Poniżej specyfikacja szczegółowa:

1. Zakres funkcjonalny systemu musi być zgodny ze specyfikacją określoną w dokumencie **„Załącznik nr 4 – Zakres realizacji przedsięwzięcia do wyboru przedsięwzięcia”** dla **Inwestycji D.1.1.2**, wskazanym powyżej.
2. System musi umożliwiać jednoczesne skanowanie co najmniej **dwóch sieci klasy C**, tj. **minimum 512 adresów IP**.
3. Podczas wykonywania jednego skanowania system musi umożliwiać równoczesne skanowanie **co najmniej 5 adresów IP** na wielu portach.
4. System musi obsługiwać skanowanie **co najmniej 6 000 unikalnych adresów IP**.
5. System musi być dostarczony wraz z licencją i wsparciem na okres **nie krótszy niż 36 miesięcy**.
6. System musi umożliwiać **identyfikację podatności bezpieczeństwa** w skanowanych zasobach IT.
7. W przypadku, gdy system zarządzania podatnościami oraz skaner podatności pochodzą od różnych producentów, rozwiązanie musi zapewniać integrację z **co najmniej 7 różnymi skanerami podatności**.
8. System musi umożliwiać **integrację z systemami klasy SOC oraz SIEM**.
9. System musi zapewniać **ocenę ryzyka podatności**, w tym ranking podatności w oparciu o powszechnie stosowane metody, np. **CVSS**.
10. System musi umożliwiać utworzenie **co najmniej 10 kont użytkowników**, w tym:
    - minimum **5 kont administratorów**,
    - minimum **5 kont audytorów** z ograniczonymi uprawnieniami.
11. System musi zapewniać dostęp do **stale aktualizowanej bazy podatności**.
12. System musi umożliwiać **planowanie skanów** (harmonogramowanie skanowania).
13. System musi posiadać **predefiniowane polityki skanowania oraz wzorce konfiguracji**.
14. Generowane raporty muszą zawierać:
    - informacje o wykrytych podatnościach,

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

- poziom ryzyka,
- rekomendowane działania naprawcze.

15. 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.

16. Zalecenia zawarte w raportach muszą wskazywać **sposób usunięcia podatności**, o ile producent lub społeczność opublikowali takie informacje.
17. Oferta musi obejmować **szkolenie dla administratorów systemu**, umożliwiające samodzielną obsługę i konfigurację rozwiązania.
18. System powinien mieć gotowe profile dedykowane do skanowania aplikacji webowych, serwerów i innych urządzeń.
19. W przypadku rozwiązań umożliwiających wdrożenie na maszynie wirtualnej (w istniejącej infrastrukturze zamawiającego) lub na dedykowanym sprzęcie, Zamawiający prosi o wyspecyfikowanie obydwu wariantów
20. W przypadku zaoferowania rozwiązania tzw. Chmurowego, Zamawiający wymaga uwzględnienia licencji tzw. patch managera dla 500 urządzeń końcowych

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