

## OPIS PRZEDMIOTU ZAMÓWIENIA

**„DOSTAWA OPROGRAMOWANIA INFORMATYCZNEGO – SKANERA PODATNOŚCI WRAZ Z WDROŻENIEM ROZWIĄZANIA”**  
*Część 2 zamówienia na „Dostawę oprogramowania informatycznego” będącego częścią projektu pn. „Cyberbezpieczna Gmina Porąbka”*

### WYMAGANE MINIMALNE PARAMETRY JAKOŚCIOWE

<b>I.</b>	<b><i>Skaner podatności</i></b>
<b>1</b>	<b>WYMAGANIA OGÓLNE</b>
1)	Rozwiązanie musi być dostępne minimum w wersji chmurowej (SaaS).
2)	Możliwość wdrożenia sond skanujących w postaci gotowych maszyn wirtualnych, które muszą być udostępnione w postaci obrazu maszyny OVA lub dysku VHDX.
3)	Uwierzytelnianie użytkowników, za pomocą 2FA wysyłanych w postaci wiadomości SMS.
4)	Rozwiązanie musi posiadać możliwość dodania dodatkowych zestawów uprawnień (ról), które mogą być przypisane do użytkowników systemu.
5)	Możliwość zarządzania systemem przy użyciu interfejsu API.
6)	Rozwiązanie musi być dostarczone z <b>68 licencjami na stacje robocze</b>
<b>2</b>	
1)	Nieograniczona liczba skanów i nieograniczona liczba zaplanowanych skanów oraz skanów na żądanie.
2)	Nieograniczonej liczby węzłów skanowania z nieograniczoną liczbą węzłów skanowania, które umożliwiają skanowanie różnych części sieci w tym samym czasie.
3)	Możliwość skanowania całego środowiska IT z segmentowanymi i geograficznie oddzielonymi sieciami.
4)	Usługa skanowania sieci musi obsługiwać IPv6.
5)	Możliwość dodawania nowych profili skanowania sieciowego.
6)	Możliwość importu predefiniowanych przez producenta profili skanowania sieciowego.
7)	Możliwość uwzględnienia podatności o niskim prawdopodobieństwie wystąpienia w wynikach skanowania.
8)	Możliwość uwzględnienia drukarek w procesie skanowania.
9)	Możliwość uwzględnienia martwych hostów w skanach.

10)	Możliwość włączenia opcji - brutalnego wymuszania hasła - do ustawień skanowania.
11)	Profil skanowania sieciowego musi posiadać możliwość dodania uwierzytelniania na urządzeniu sieciowym, w oparciu o uwierzytelnianie Windows i/lub Linux.
12)	Profil skanowania sieciowego musi posiadać możliwość wyboru intensywności skanowania.
13)	Profil skanowania sieciowego musi posiadać możliwość wyboru testów podatności, które będą przeprowadzone w trakcie skanowania.
14)	Rozwiązanie musi posiadać co najmniej 80 tys. testów podatności aktualizowanych na bieżąco z serwera producenta rozwiązania.
15)	Podczas tworzenia zadania skanowania sieciowego, administrator musi posiadać możliwość wyboru sondy skanującej Scanner appliance zainstalowanej lokalnie, grupy sond lub sondy zewnętrznej hostowanej w chmurze producenta (tylko w wersji chmurowej).
16)	Administrator musi posiadać możliwość uruchomienia zadania skanowania sieci jednorazowo lub z harmonogramem.
17)	Rozwiązanie musi posiadać możliwość pobrania raportu CSV z modułu skanowania sieciowego w celu wyświetlenia listy zadań skanowania.
18)	Urządzenia znalezione podczas zadania skanowania muszą zostać automatycznie dodane do listy urządzeń wraz z odpowiednimi znacznikami (tagami), przypisanymi na podstawie wykrytych portów usług oraz systemu operacyjnego.
<b>3</b>	<b>MONITOROWANIE</b>
1)	Rozwiązanie musi posiadać mechanizm weryfikacji listowania na czarnych listach serwerów pocztowych i stron internetowych.
2)	Możliwość wyświetlenia listy zeskanowanych zasobów: adres IP sieci i aplikacje internetowe z następującymi informacjami: nazwa zasobu, lista wykrytych podatności.
3)	Możliwość przeglądania i analizowania stanu podatności wraz z określeniem statusu wykrytej podatności (minimum: nowa/aktywna/naprawiona) sieci oraz aplikacji internetowych.
4)	Możliwość skanowania REST API.
5)	Tworzenie i utrzymywanie tagów (grup) statycznych i dynamicznych.
6)	Możliwość wprowadzania i importowania zasobów kategorii Network IP
<b>4</b>	<b>ZARZĄDZANIE PODATNOŚCIAMI</b>
	Pulpit nawigacyjny udostępniający:
1)	<ul style="list-style-type: none"> <li>a) wyniki skanowania podatności sieci wg ważności wraz z możliwością prezentacji na wykresie słupkowym/kołowym;</li> <li>b) otwarte zgłoszenia według ważności wraz z możliwością prezentacji na wykresie słupkowym/kołowym;</li> <li>c) top 10 wyników skanowania sieci wraz z możliwością wyświetlania celu zasobu: wszystkich lub wybranych adresów IP / tagów;</li> <li>d) ostatnie skanowania;</li> <li>e) nadchodzące skanowania;</li> <li>f) ciągłe monitorowanie alertów z wyborem okresu: dzień/tydzień;</li> </ul>
2)	Możliwość sortowania, grupowania i priorytetyzacji podatności, minimum wg. stanu, statusu (nowa/aktywna/naprawiona) i ważności podatności, typu zasobu,
3)	Możliwość filtrowania listy podatności według podatności lub aplikacji internetowych / hosta.
4)	Możliwość tworzenia raportów bezpośrednio z menedżera podatności poprzez wybranie jednej lub więcej podatności.
5)	Możliwość ciągłego lub czasowego ignorowania wybranych podatności z podaniem powodu ignorowania.

6)	Możliwość ciągłego monitorowania oraz szybkiego i łatwego ustawienia profilu monitorowania zmian za pomocą powiadomień i alarmów.
7)	Możliwość utworzenia własnego widoku podatności zawierającego odfiltrowane zgodnie z konfiguracją administratora danych.
<b>5</b>	<b>RAPORTOWANIE</b>
1)	Wbudowane raporty dotyczące skanowanej sieci, w tym raporty zgodności minimum z Ustawą o ochronie danych osobowych oraz ISO 27001.
2)	Możliwość tworzenia i dostosowywania szablonów raportów sieciowych z następującymi opcjami: <ul style="list-style-type: none"> <li>a) raport oparty na określonym czasie skanowania</li> <li>b) raport oparty na wszystkich bieżących informacjach o podatnościach</li> <li>c) raport trendów z historią podatności</li> </ul>
3)	Możliwość filtrowania raportów.
<b>II.</b>	<b><i>Wymagania dodatkowe</i></b>
<b>1</b>	<b>INSTALACJA I KONFIGURACJA</b>
1)	<ol style="list-style-type: none"> <li>1. Instalacja i uruchomienie konsoli zarządzającej oraz podłączenie użytkowników.</li> <li>2. Dodanie urządzeń do skanowania</li> <li>3. Definicja profili skanowania sieciowego</li> <li>4. Konfiguracja parametrów skanowania i optymalizacja</li> <li>5. Utworzenie i konfiguracja raportów skanowania</li> <li>6. Przeprowadzenie instruktarzu stanowiskowego dla administratora obejmującego instalację, konfigurację i zarządzanie systemem, w ilości godzin pozwalających na pełne zrozumienie zagadnień administracji systemem, zakończonego podpisaniem protokołu z przeprowadzenia instruktarzu</li> </ol>
<b>2</b>	<b>DOKUMENTACJA POWYKONAWCZA</b>
1)	<p>Po zakończeniu realizacji, Zamawiający wymaga dostarczenia pełnej dokumentacji powykonawczej oraz procedur eksploatacji rozwiązań. Dokumentacja powykonawcza musi zawierać minimum:</p> <ul style="list-style-type: none"> <li>a) opis ogólnych informacji o rozwiązaniach;</li> <li>b) zestawienie loginów i haseł do rozwiązań;</li> <li>c) zestawienie ustawień;</li> <li>d) instrukcje instalacji, konfiguracji, uruchomienia;</li> <li>e) zestawienie licencji;</li> <li>f) listę autoryzowanych kontaktów serwisowych;</li> </ul>



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA