Z A P Y T A N I E O S Z A C O W A N I E

I. Informacje podstawowe:

1. Niniejsze zapytanie o szacowanie nie jest ogłoszeniem w rozumieniu ustawy Prawo zamówień publicznych a jedynie służy rozeznaniu rynku oraz oszacowaniu wartości zamówienia.
2. Zamawiający: Generalna Dyrekcja Ochrony Środowiska, Al. Jerozolimskie 136, 02-305 Warszawa, NIP: 7010151052, REGON: 141628410, www.gov.pl/gdos.

II. Przedmiot zapytania ofertowego:

1. Przedmiotem planowanego zamówienia jest:
   1) dostawa kompleksowego rozwiązania do zarządzania podatnościami i monitorowania bezpieczeństwa, w zakresie automatycznego wykrywania, oceny oraz eliminacji luk w zabezpieczeniach infrastruktury IT, aplikacji webowych ze szczególnym uwzględnieniem interfejsów API, obejmującego min. 50 licencji (umożliwiających skanowanie infrastruktury sieciowej, w tym urządzeń takich jak routery, przełączniki czy inne elementy sieci oraz aplikacji webowych i interfejsów API), wraz z instalacją, konfiguracją w infrastrukturze Zamawiającego oraz udzieleniem licencji na oprogramowanie na okres 36 miesięcy;
   2) przeprowadzenie szkolenia z obsługi oprogramowania dla wskazanych pracowników Zamawiającego.
2. Szczegółowy zakres przedmiotu planowanego zamówienia został określony w Opisie planowanego zamówienia, stanowiącym **załącznik nr 1** do zapytania.
3. Planowane postępowanie o udzielenie zamówienia publicznego realizowane jest w ramach Projektu: „Dane 3.0 – wymiana, wartość”, współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach działania FERC.02.03 Cyfrowa dostępność i ponowne wykorzystanie informacji, programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027.

III. Sposób i termin składania szacowania

1. Szacowanie – na formularzu szacowania, należy złożyć drogą elektroniczną na adres: zampub@gdos.gov.pl
2. Termin złożenia szacowania: 25.03.2025 r.
3. Adres do kontaktów z Zamawiającym: zampub@gdos.gov.pl

IV. Załączniki:

1) Opis planowanego zamówienia;
2) Formularz szacowania.

Załącznik nr 1

OPIS PLANOWANEGO ZAMÓWIENIA

1. Opis rozwiązań (wymagania minimalne) *Platforma do zarządzania podatnościami aplikacji bazodanowych, sieci i API w wersji chmurowej (SaaS), na okres 36 miesięcy*

1.1 Wymagania ogólne:

1.1.1 rozwiązanie musi być dostępne w wersji chmurowej (SaaS);
1.1.2 rozwiązanie w wersji chmurowej musi posiadać swoje centrum danych (data center) na terenie Unii Europejskiej (Wykonawca musi dostarczyć wraz z ofertą odpowiednie oświadczenie);
1.1.3 konsola centralna musi posiadać możliwość uruchomienia dodatkowego uwierzytelnienia użytkowników, za pomocą MFA;
1.1.4 rozwiązanie musi posiadać możliwość integracji z systemami ticketowymi;
1.1.5 rozwiązanie musi mieć możliwość generowania powiadomień poprzez integrację z systemami takimi jak: Exchange 2019 on-premise oraz Microsoft 365;
1.1.6 rozwiązanie musi posiadać możliwość zapewnienia nieograniczonej liczby skanów;
1.1.7 administrator w konsoli centralnej musi posiadać możliwość dodania dodatkowych użytkowników zarządzających;
1.1.8 rozwiązanie musi posiadać możliwość dodania dodatkowych zestawów uprawnień (ról), które mogą być przypisane do użytkowników systemu;
1.1.9 rozwiązanie musi zapewnić zaawansowane skanowanie API, które obejmuje min. interfejsy, takie jak REST i GraphQL;
1.1.10 skanowanie REST, GraphQL musi być godne z wytycznymi OWASP Top 10 dla bezpieczeństwa API;
1.1.11 system zakończeniu skanowania musi dostarczać szczegółowe raporty dotyczące wykrytych luk oraz rekomendacje dotyczące ich naprawy.

1.2 Zarządzanie zestawami urządzeń i aplikacji webowych

1.2.1 rozwiązanie musi posiadać możliwość dodania ręcznego urządzeń i aplikacji webowych do skanowania;
1.2.2 rozwiązanie musi posiadać możliwość importu listy urządzeń z pliku CSV;
1.2.3 dodanie urządzeń musi odbywać się za pomocą podania pojedynczego adresu IP, zakresu adresów IP oraz adresu sieci wraz z maską;
1.2.4 dodanie aplikacji webowej musi pozwalać na dodanie rodzaju autentykacji, białej i czarnej listy adresów URL oraz rozszerzeń do skanowania;
1.2.5 przy dodawaniu urządzeń i aplikacji webowych administrator musi posiadać możliwość wyboru poziomu wpływu biznesowego z jednego z 4 poziomów np.: niski, średni i wysoki;
1.2.6 przy dodawaniu urządzeń i aplikacji webowych administrator musi posiadać możliwość wyboru znaczników (tagów);
1.2.7 administrator musi posiadać możliwość dodania znaczników (tagów) statycznych wraz z odpowiednim kolorem;
1.2.8 administrator musi posiadać możliwość dodania znaczników (tagów) dynamicznych, które będą przypisywane do urządzeń po spełnieniu jednego z

warunków: nazwy zestawu urządzeń, adresu IP z podanego zakresu, otwartych portów lub systemu operacyjnego.

1.3 Skanowanie sieciowe

1.3.1 rozwiązanie musi posiadać możliwość zapewnienia nieograniczonej liczby skanów i nieograniczonej liczby zaplanowanych skanów oraz skanów na żądanie. Powiadomienia powinny być również dostępne za pośrednictwem integracji e-mail;

1.3.2 rozwiązanie musi posiadać możliwość zapewnienia nieograniczonej liczby węzłów skanowania z nieograniczoną liczbą węzłów skanowania, które umożliwiają skanowanie różnych części sieci w tym samym czasie;

1.3.3 rozwiązanie musi posiadać możliwość skanowania całego środowiska IT z segmentowanymi i oddzielonymi sieciami;

1.3.4 rozwiązanie musi posiadać możliwość dodawania nowych profili skanowania sieciowego

1.3.5 administrator musi posiadać możliwość importu predefiniowanych przez producenta profili skanowania sieciowego;

1.3.6 podczas tworzenia profilu skanowania, administrator musi posiadać możliwość wyboru trybu skanowania: np. podstawowy, pełny;

1.3.7 funkcja wykrywania urządzeń w profilu skanowania, musi pozwalać na wybór domyślnych portów, dodanie dodatkowych portów, wybór rodzaju połączenia;

1.3.8 rozwiązanie musi posiadać możliwość uwzględnienia podatności o niskim prawdopodobieństwie wystąpienia w wynikach skanowania;

1.3.9 rozwiązanie musi umożliwiać klientom wybór opcji "potencjalnie niebezpiecznych testów" i włączenia skanowania drukarek;

1.3.10 rozwiązanie musi posiadać możliwość uwzględnienia martwych hostów w skanach;

1.3.11 możliwość włączenia opcji - brutalnego wymuszania hasła - do ustawień skanowania;

1.3.12 profil skanowania sieciowego musi posiadać możliwość dodania uwierzytelniania na urządzeniu sieciowym, w oparciu o uwierzytelnianie Windows i/lub Linux;

1.3.13 profil skanowania sieciowego musi posiadać możliwość wyboru intensywność skanowania;

1.3.14 profil skanowania sieciowego musi posiadać możliwość wyboru testów podatności, które będą przeprowadzone w trakcie skanowania;

1.3.15 rozwiązanie musi posiadać co najmniej 10 tys. testów podatności aktualizowanych na bieżąco z serwera producenta rozwiązania;

1.3.16 podczas tworzenia zadania skanowania sieciowego, administrator musi posiadać możliwość wyboru sondy skanującej zainstalowanej lokalnie, grupy sond lub sondy zewnętrznej hostowanej w chmurze producenta;

1.3.17 administrator musi posiadać możliwość uruchomienia zadania skanowania sieci jednorazowo lub z harmonogramem;

1.3.18 rozwiązanie musi posiadać możliwość pobrania raportu CSV z modułu skanowania sieciowego w celu wyświetlenia listy zadań skanowania;

1.3.19 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;

1.3.20 podatności wykryte podczas skanowania sieciowego muszą automatycznie być umieszczane w menedżerze podatności.

1.4 Skanowanie aplikacji webowych

1.4.1 rozwiązanie musi posiadać możliwość dodawania nowych profili skanowania aplikacji webowych;
1.4.2 administrator musi posiadać możliwość importu predefiniowanych przez producenta profili skanowania aplikacji webowych;
1.4.3 rozwiązanie musi posiadać możliwość skanowania aplikacji internetowych (skanowanie stron internetowych);
1.4.4 rozwiązanie musi posiadać możliwość zapewnienia nieograniczonej liczby skanów i nieograniczonej liczby zaplanowanych skanów oraz skanów na żądanie. Powiadomienia powinny być również dostępne za pośrednictwem integracji e-mail;
1.4.5 rozwiązanie musi posiadać możliwość skanowania nieograniczonej liczby aplikacji internetowych;
1.4.6 rozwiązanie musi posiadać możliwość zapewnienia konfigurowalnych ustawień skanowania, takich jak ustawienia indeksowania do metody formularza: Post i Get, Post, Get;
1.4.7 rozwiązanie musi posiadać możliwość wyboru intensywności skanowania
1.4.8 rozwiązanie musi posiadać możliwość włączenia pełnego zestawu kategorii wykrywania podatności, a także dostosowania kategorii wykrywania podatności do skanowania, a także listy wykluczeni;
1.4.9 rozwiązanie musi posiadać możliwość wyboru opcji skanowania wrażliwych treści, numerów kart kredytowych i zezwalania na wprowadzanie niestandardowych treści;
1.4.10 administrator musi posiadać możliwość uruchomienia zadania skanowania aplikacji webowej jednorazowo lub z harmonogramem;
1.4.11 podatności wykryte podczas skanowania aplikacji webowych muszą automatycznie być umieszczane w wykazie podatności.

1.5 Skanowanie agentowe

1.5.1 rozwiązanie musi posiadać możliwość instalacji na systemach Windows aplikacji agentowej, która będzie przesyłać do konsoli centralnej listę zainstalowanych aplikacji;
1.5.2 systemu musi posiadać bazę podatności aplikacji zainstalowanych w systemach skanowanych przez aplikację agentową;
1.5.3 wykryte przez aplikację agentową podatności muszą automatycznie być umieszczane w menedżerze podatności;
1.5.4 pakiet instalacyjny aplikacji agentowej musi być udostępniony w postaci pliku .msi;
1.5.5 aktywacja aplikacji agentowej musi wymagać podania, wygenerowanego w konsoli centralnej, tokenu;

1.6 Skanowanie usług chmurowych

1.6.1 rozwiązanie musi posiadać możliwość wykrywania i raportowania błędnej konfiguracji usług chmurowych Microsoft Azure oraz Google Cloud;
1.6.2 rozwiązanie musi posiadać możliwość dodawania nowych profili skanowania usług chmurowych;
1.6.3 administrator musi posiadać możliwość uruchomienia zadania skanowania usługi chmurowej jednorazowo lub z harmonogramem;

1.7 Monitorowanie serwerów pocztowych i stron internetowych

1.7.1 rozwiązanie musi posiadać mechanizm weryfikacji listowania na czarnych listach serwerów pocztowych i stron internetowych.

1.8 Zarządzanie aktywami

1.8.1 rozwiązanie musi posiadać możliwość wyświetlenia listy zeskanowanych zasobów: adres IP sieci i aplikacje internetowe z następującymi informacjami:
- (a) nazwa zasobu;
- (b) liczba wykrytych podatności w zabezpieczeniach;
- (c) najwyższa wykryta podatność;
- (d) krytyczność;
- (e) informacje o systemie operacyjnym;
- (f) data wprowadzenia utworzonych zasobów i ostatnio wykryty znacznik czasu;

1.8.2 rozwiązanie musi posiadać możliwość przeglądania informacji o aktywach, takich jak:
- (a) sieć: Stan podatności - Aktywne, Ignorowane i Wyłączone;
- (b) sieć : Status podatności - Nowa, Aktywna, Ponownie otwarta i Naprawiona;
- (c) sieć: lista otwartych portów powiązanych z zasobem;
- (d) sieć: Trend zasobu - według ważności, stanu. Możliwość wyświetlania według okresu i przedziału czasu;
- (e) aplikacja internetowa : Stan podatności - Aktywne, Ignorowane i Wyłączone;
- (f) aplikacja internetowa : Status podatności - Nowa, Aktywna, Ponownie otwarta i Naprawiona;

1.8.3 Potrafi zapewnić możliwość edycji informacji o aktywach, takich jak:
- (a) sieć: Aby podać nazwę zasobu (jeśli nie jest dostępny DNS);
- (b) sieć: aby podać etykietę wpływu biznesowego;
- (c) sieć: możliwość wybrania, czy zasób przechowuje jakiekolwiek dane osobowe RODO;
- (d) aplikacja internetowa: Aby podać nazwę zasobu;
- (e) aplikacja internetowa: Aby podać etykietę wpływu biznesowego;
- (f) aplikacja internetowa: Aby zapewnić kolumnę wejściową dla opisu zasobu;
- (g) aplikacja internetowa: Rozwiązanie musi posiadać możliwość wybrania, czy zasób przechowuje jakiekolwiek dane osobowe RODO;
- (h) aplikacja internetowa: Rozwiązanie musi posiadać możliwość zapewnienia funkcji skanowania REST API;
- (i) aplikacja internetowa: Może zapewnić zakres indeksowania, taki jak nazwa hosta adresu URL i podkatalog adresu URL;
- (j) aplikacja webowa: Możliwość podawania nagłówków i plików cookie;
- (k) aplikacja internetowa: Może zapewnić elastyczność w utrzymywaniu listy wykluczających adresów URL, takich jak biała i czarna lista;
- (l) aplikacja internetowa: Rozwiązanie musi posiadać możliwość wyświetlenia listy zeskanowanych luk w zabezpieczeniach powiązanych z zasobami aplikacji internetowej;

1.8.4 rozwiązanie musi potrafić zapewnić funkcje tworzenia i utrzymywania tagów (grup) statycznych i dynamicznych;

1.8.5 rozwiązanie musi posiadać możliwość tworzenia ręcznego wprowadzania i importowania zasobów kategorii Network IP.

1.9 Menedżer podatności i panel główny

1.9.1 platforma zarządzania podatnościami musi być w stanie zapewnić funkcje pulpitu nawigacyjnego z następującymi informacjami:
- (a) wyniki skanowania podatności sieci według ważności (z opcjami wykres);
- (b) wyniki skanowania podatności aplikacji internetowych według ważności (z opcjami wykresu);
- (c) 10 największych podatności w aplikacjach sieciowych;
- (d) ostatnie skanowania;
- (e) nadchodzące skanowania;
- (f) ostatnie 10 raportów;

1.9.2 platforma zarządzania podatnościami musi mieć możliwość sortowania, grupowania i priorytetyzacji podatności:
- (a) według stanu;
- (b) według typu;
- (c) według statusu np.: nowy, aktywny, naprawiony;
- (d) według ważności np.: niski, średni, wysoki, krytyczny;
- (e) według tagów;
- (f) według pierwszego i ostatniego wykrycia;
- (g) według kategorii: podatności w skanowaniu sieci i podatności w aplikacjach internetowych;
- (h) możliwość filtrowania listy podatności;
- (i) możliwość tworzenia raportów poprzez wybranie jednej lub więcej podatności;
- (j) możliwość tworzenia notatek do celów uwag i notatek, które pojawią się w raporcie po jego wygenerowaniu;

1.9.3 rozwiązanie musi posiadać możliwość ciągłego monitorowania oraz szybkiego i łatwego ustawiania profilu monitorowania zmian za pomocą powiadomień i alarmów;

1.9.4 w widoku podatności musi istnieć możliwość utworzenia własnego widoku podatności zawierającego odfiltrowane zgodnie z konfiguracją administratora danych;

1.9.5 rozwiązanie musi posiadać możliwość zignorowania wykrytych podatności na określony czas.

1.10 System raportujący

1.10.1 system raportujący musi zawierać następujące raporty:
- (a) skanowanie sieci;
- (b) aplikacje sieciowe;
- (c) raporty zgodności musi być w stanie wygenerować następujący typ zgodności:
  1) OWASP Top 10 (2017);
  2) ustawa o ochronie danych osobowych;
  3) ISO / IEC 27001;
  4) ogólne rozporządzenie o ochronie danych;
  5) bezpieczeństwo sieci i informacji;

1.10.2 system powinien mieć możliwość dostarczania nowych niestandardowych raportów zgodności, które mogą być zalecane przez nowe regulacje prawne, gdy ma to zastosowanie;

1.10.3 rozwiązanie musi posiadać możliwość tworzenia i dostosowywania szablonów raportów sieciowych z następującymi opcjami:
(a) raport oparty na określonym czasie skanowania;
(b) raport oparty na wszystkich bieżących informacjach o podatnościach;
(c) raport trendów z historią podatności;
(d) szczegóły raportu, przegląd podatności, podsumowanie podatności, lista podatności;
(e) podatności według ważności w czasie;
(f) podatności według statusu;
(g) podatności według ważności i najbardziej narażonych kategorii;

1.10.4 potrafi utworzyć i dostosować szablon raportu aplikacji internetowej z następującymi opcjami:

1.10.5 raport oparty na określonym czasie skanowania;

1.10.6 raport oparty na wszystkich bieżących informacjach o podatnościach;

1.10.7 zawartość raportu: szczegóły raportu, przegląd podatności, podsumowanie podatności, lista podatności;

1.10.8 filtrowanie: selektywne raportowanie podatności (np. pełne i niestandardowe) i wykluczenia, uwzględnione systemy operacyjne, filtry zasobów, filtry podatności;

1.10.9 możliwość tworzenia "raportów skróconych" wysyłanych w sposób podsumowujący. Częstotliwość raportów można ustawić na: tygodniowe raporty skrócone i miesięczne raporty skrócone. Raporty są dostarczane kanałem e-mail.

1.11 Wdrożenie

1.11.1 w ramach realizacji Przedmiotu zamówienia Wykonawca dokona instalacji i konfiguracji Oprogramowania;

1.11.2 wykonawca przeprowadzi konfiguracje dostępu do platformy chmurowej;

1.11.3 wykonawca przeprowadzi konfigurację ustawień skanowania w chmurze, obejmującego infrastrukturę IaaS, SaaS i PaaS;

1.11.4 wykonawca przeprowadzi konfigurację modułów skanowania systemu i sieci dla min 20 stanowisk wskazanych przez zamawiającego;

1.11.5 wykonawca przeprowadzi konfigurację skanowania aplikacji webowej;

1.11.6 wykonawca ustali z Zamawiającym i wdroży harmonogram regularnych skanów i raportów;

1.11.7 podczas wdrożenia Wykonawca przekaże niezbędne informacje personelowi zamawiającego w zakresie korzystania z platformy i interpretacji wyników skanowania;

1.11.8 wykonawca przeprowadzi integrację z istniejącymi systemami bezpieczeństwa w organizacji;

1.11.9 wykonawca przeprowadzi Konfiguracja powiadomień o wykrytych podatnościach i zagrożeniach.

1.12 Szkolenie

1.12.1 Wykonawca zapewni Szkolenia dla 7-osobowego zespołu Zamawiającego mające na celu przekazanie wiedzy wymaganej do administrowania i zarządzania wdrożonym Oprogramowaniem;

1.12.2 Wykonawca zapewni możliwość wykorzystania przez Zamawiającego 2 dni szkoleniowych (do 6 godzin każdy);

1.12.3 szkolenia odbędą się w siedzibie Zamawiającego, przy Al. Jerozolimskich 136 w Warszawie, w godzinach 9:00 – 16:00 lub w wersji online w dni robocze (od poniedziałku do piątku), w terminach uzgodnionych z Zamawiającym.

1.12.4 Wykonawca przekaże Zamawiającemu drogą elektroniczną propozycję terminów Szkoleń na co najmniej 3 dni robocze przed zaplanowanym terminem pierwszego Szkolenia;

1.12.5 Wykonawca przeprowadzi Szkolenia w języku polskim, przez osoby posiadające wiedzę z zakresu Przedmiotu zamówienia, przy udziale osoby / osób zaangażowanych w realizację Przedmiotu zamówienia;

1.12.6 Zamawiający ma prawo do rejestracji Szkoleń w formie audiowizualnej i udostępnienia nagrania użytkownikom uprawnionym do obsługi Urządzeń oraz środowiska teleinformatycznego Zamawiającego.