Zamawiający:
Gmina Ładzice, ul. Wyzwolenia 36, 97-561 Ładzice

Załącznik nr 2

do Zapytania ofertowego nr ZPP.271.1.22.2025

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest przeprowadzenie testów podatności w Urzędzie Gminy w Ładzicach.

OGÓLNE WYMAGANIA DOTYCZĄCE ROZWIĄZANIA ZAPEWNIAJĄCEGO REALIZACJĘ USŁUGI TESTÓW PODATNOŚCI

1. Wykonawca zapewni w okresie do 30.04.2026r. dostęp do usługi zapewniającej możliwość wykonania testów podatności: 4 miesiące w roku 2025 oraz 4 miesiące w terminie do 30 kwietnia 2026r.
2. Ilość komputerów w sieci: 50; ilość serwerów i innych urządzeń sieciowych: 20.
3. Rozwiązanie typu vunlerability manager musi być dostępne w wersji: chmurowej (SaaS).
4. Rozwiązanie musi posiadać swoje centrum danych (data center) na terenie Unii Europejskiej.
5. Rozwiązanie musi oferować możliwość wdrożenia sond skanujących w postaci gotowych maszyn wirtualnych, które muszą być udostępnione w postaci obrazu maszyny OVA lub dysku VHDX.
6. Sonda skanująca musi wymagać rejestracji w konsoli centralnej, przy użyciu wygenerowanego przez administratora tokena.
7. Konsola centralna musi posiadać możliwość uruchomienia dodatkowego uwierzytelnienia użytkowników, za pomocą 2FA wysyłanych w postaci wiadomości SMS.
8. Rozwiązanie musi posiadać możliwość integracji z systemami ticketowymi.
9. Rozwiązanie musi posiadać możliwość wysyłania powiadomień do co najmniej następujących systemów: Microsoft Teams, Slack.
10. Administrator w konsoli centralnej musi posiadać możliwość dodania dodatkowych użytkowników zarządzających.
11. Rozwiązanie musi posiadać możliwość dodania dodatkowych zestawów uprawnień (ról), które mogą być przypisane do użytkowników systemu.
12. Rozwiązanie musi posiadać możliwość zarządzania systemem przy użyciu interfejsu API.

ZARZĄDZANIE ZESTAWAMI URZĄDZEŃ

1. Rozwiązanie musi posiadać możliwość dodania ręcznego urządzeń do skanowania.

2. Rozwiązanie musi posiadać możliwość importu listy urządzeń z pliku CSV.
3. Dodanie urządzeń musi odbywać się za pomocą podania pojedynczego adresu IP, zakresu adresów IP oraz adresu sieci wraz z maską.
4. Przy dodawaniu urządzeń administrator musi posiadać możliwość wyboru poziomu wpływu biznesowego z jednego z co najmniej 4 poziomów np. Neutral, Low, Medium, High.
5. Przy dodawaniu urządzeń administrator musi posiadać możliwość wyboru znaczników (tagów).
6. Administrator musi posiadać możliwość dodania znaczników (tagów) statycznych wraz z odpowiednim kolorem.
7. 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.

SKANOWANIE SIECIOWE

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, Slack.
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.
3. Rozwiązanie musi posiadać możliwość skanowania całego środowiska IT z segmentowanymi i geograficznie oddzielonymi sieciami.
4. Usługa skanowania sieci musi obsługiwać IPv6.
5. Rozwiązanie musi posiadać możliwość dodawania nowych profili skanowania sieciowego.
6. Administrator musi posiadać możliwość importu predefiniowanych przez producenta profili skanowania sieciowego.
7. Podczas tworzenia profilu skanowania, administrator musi posiadać możliwość wyboru trybu skanowania: Full, Basic lub Discovery.
8. Funkcja wykrywania urządzeń w profilu skanowania, musi pozwalać na wybór domyślnych portów, dodanie dodatkowych portów, wybór rodzaju połączenia TCP SYN lub TCP SYN ACK oraz możliwość wyłączenia lub włączenia wysłania ICMP PING.
9. Rozwiązanie musi posiadać możliwość uwzględnienia podatności o niskim prawdopodobieństwie wystąpienia w wynikach skanowania.
10. Rozwiązanie musi umożliwiać klientom wybór opcji "potencjalnie niebezpiecznych testów" i włączenia skanowania drukarek.
11. Rozwiązanie musi posiadać możliwość uwzględnienia martwych hostów w skanach.
12. Możliwość włączenia opcji - brutalnego wymuszania hasła - do ustawień skanowania.

13. Profil skanowania sieciowego musi posiadać możliwość dodania uwierzytelniania na urządzeniu sieciowym, w oparciu o uwierzytelnianie Windows i/lub Linux.
14. Profil skanowania sieciowego musi posiadać możliwość wyboru intensywność skanowania.
15. Profil skanowanie sieciowego musi posiadać możliwość wyboru testów podatności, które będą przeprowadzone w trakcie skanowania.
16. Rozwiązanie musi posiadać co najmniej 110 tys. testów podatności aktualizowanych na bieżąco z serwera producenta rozwiązania.
17. Podczas tworzenia zadania skanowania sieciowego, administrator musi posiadać możliwość wyboru sondy skanującej zainstalowanej lokalnie, grupy sond lub sondy zewnętrznej hostowanej w chmurze producenta.
18. Administrator musi posiadać możliwość uruchomienia zadania skanowania sieci jednorazowo lub z harmonogramem.
19. Rozwiązanie musi posiadać możliwość pobrania raportu CSV z modułu skanowania sieciowego w celu wyświetlenia listy zadań skanowania.
20. 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.
21. Podatności wykryte podczas skanowania sieciowego muszą automatycznie być umieszczane w menedżerze podatności.

SKANOWANIE AGENTOWE

1. Rozwiązanie musi posiadać możliwość instalacji na systemach Windows aplikacji agentowej, która będzie przesyłać do konsoli centralnej listę zainstalowanych aplikacji.
2. Systemu musi posiadać bazę podatności aplikacji zainstalowanych w systemach skanowanych przez aplikację agentową.
3. Wykryte przez aplikację agentową podatności muszą automatycznie być umieszczane w menedżerze podatności.
4. Pakiet instalacyjny aplikacji agentowej musi być udostępniony w postaci pliku .MSI.
5. Aktywacja aplikacji agentowej musi wymagać podania, wygenerowanego w konsoli centralnej, tokenu.

ZARZĄDZANIE AKTYWAMI

1. Rozwiązanie musi posiadać możliwość wyświetlenia listy zeskanowanych zasobów: adres IP sieci z co najmniej następującymi informacjami: nazwa zasobu, liczba wykrytych podatności w zabezpieczeniach, najwyższa wykryta podatność, krytyczność/istotność, informacje o systemie operacyjnym, data wprowadzenia utworzonych zasobów i ostatnio wykryty znacznik czasu.

2. Rozwiązanie musi posiadać możliwość przeglądania informacji o aktywach, takich jak stan podatności, status podatności, lista otwartych portów powiązanych z zasobem, trend zasobu (według ważności, stanu) z możliwością wyświetlania według okresu i przedziału czasu.
3. Rozwiązanie zapewni możliwość edycji informacji o aktywach, takich jak: podanie nazwy zasobu (jeśli nie jest dostępny DNS), podanie etykiety wpływu biznesowego, możliwość wybrania, czy zasób przechowuje jakiekolwiek dane osobowe.
4. Rozwiązanie musi potrafić zapewnić funkcje tworzenia i utrzymywania tagów (grup) statycznych i dynamicznych.
5. Rozwiązanie musi posiadać możliwość tworzenia ręcznego wprowadzania i importowania zasobów kategorii network IP.

MENEDŻER PODATNOŚCI I PANEL GŁÓWNY

1. Platforma zarządzania podatnościami musi być w stanie zapewnić konfigurowalne funkcje pulpitu nawigacyjnego z co najmniej następującymi widżetami: wyniki skanowania podatności sieci według ważności (wykresy: słupkowy i kołowy); otwarte zgłoszenia według ważności; Top 10 wyników skanowania sieci (możliwość ustawienia celu zasobu jako wszystkich lub wybranych adresów IP); ostatnie skanowania; nadchodzące skanowania; ostatnie 10 raportów; ciągłe monitorowanie alertów (możliwość ustawienia okresu na dzień/tydzień).
2. Platforma zarządzania podatnościami musi mieć możliwość sortowania, grupowania i priorytetyzacji podatności. Musi umożliwiać:
    a. tworzenie wielu zakładek w celu filtrowania kryteriów co najmniej wg stanu, typu, statusu, ważności, tagów, pierwszego i ostatniego wykrycia, kategorii.
    b. filtrowanie listy podatności według podatności lub hosta.
    c. tworzenie raportów bezpośrednio z menedżera podatności poprzez wybranie jednej lub więcej podatności.
    d. dalsze administrowanie / zarządzanie listą luk w zabezpieczeniach.
    e. tworzenie notatek do celów uwag i notatek, które pojawią się w raporcie po jego wygenerowaniu.
    f. tworzenie czatu konwersacyjnego do celów współpracy między użytkownikami.
    g. wyświetlanie informacji na temat podatności takich jak: wpływ, rozwiązanie, podsumowanie, wgląd, wykrywanie, odniesienie, łatki, możliwość utworzenia zgłoszenia bezpośrednio ze wskazanych luk w zabezpieczeniach, środki zaradcze.
3. Platforma powinna zapewnić wbudowany system ticketowy dla procesu naprawczego.
4. Platforma powinna umożliwić dostarczanie informacji o zgłoszeniach, takich jak:
    a. Numerowanie ich w celu łatwego śledzenia i powiadamiania za pośrednictwem poczty e-mail.

b. Możliwość podawania i aktualizowania statusu zgłoszenia.

c. Możliwość podania nazwy powiązanej podatności w zabezpieczeniach wraz z jej zasobami.

d. Możliwość podania wagi podatności w zabezpieczeniach zarejestrowanego zgłoszenia.

e. Możliwość przypisania do wyznaczonego właściciela.

f. Możliwość tworzenia wielu zakładek do utrzymywania i zarządzania zgłoszeniami.

5. Rozwiązanie musi posiadać możliwość ciągłego monitorowania oraz szybkiego i łatwego ustawienia profilu monitorowania zmian za pomocą powiadomień i alarmów.
6. W menedżerze podatności musi istnieć możliwość utworzenia własnego widoku podatności zawierającego odfiltrowane zgodnie z konfiguracją administratora danych.
7. Rozwiązanie musi posiadać możliwość zignorowania wykrytych podatności na określony czas.

SYSTEM RAPORTUJĄCY

1. System raportujący musi zawierać co najmniej raporty takie jak: skanowanie sieci, łatki, środki zaradcze, porównanie (raport Delta), zgodność.
2. System musi być w stanie wygenerować co najmniej następujące typy zgodności: ISO/IEC 27001, ogólne rozporządzenie o ochronie danych.
3. Rozwiązanie musi posiadać możliwość tworzenia i dostosowywania szablonów raportów sieciowych.
4. Rozwiązanie musi umożliwiać tworzenie "raportów skróconych" wysyłanych w sposób podsumowujący.
5. System musi posiadać możliwość ustawienia częstotliwości raportów skróconych na: tygodniowe i miesięczne oraz umożliwiać dostarczania raportów poprzez e-mail.

WYMAGANIA DO PRZEPROWADZENIA TESTÓW PODATNOŚCI

Zamawiający wymaga od osoby przeprowadzającej testy podatności w infrastrukturze Zamawiającego oraz opracowującej raporty (co najmniej jeden raport w każdym miesiącu świadczonej usługi) potwierdzenia posiadanych kompetencji poprzez dysponowanie co najmniej poniższymi lub równoważnymi im aktualnymi certyfikatami: audytora wiodącego systemu zarządzania bezpieczeństwem informacji wg normy ISO/IEC 27001:2023 oraz audytora wiodącego systemu zarządzania ciągłością działania wg normy ISO 22301:2020.

WÓJT Ewelina L...