Załącznik nr 1 do Zapytania Ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

W niniejszym dokumencie przedstawiono minimalne parametry techniczne, jakimi musi charakteryzować oprogramowanie związane z Zapytaniem Ofertowym oraz minimalny zakres szkolenia dla pracowników Działu IT.

WithSecure Elements Vulnerability Managment – 95 licencji

1. Rozwiązanie zapewnia wykrywanie oraz zarządzanie podatnościami bezpieczeństwa, w środowisku informatycznym.
2. Architektura rozwiązania składa się z systemu zarządzania oraz osobnego, dedykowanego oprogramowania wykonującego skanowania podatności, które jest zarządzane za pomocą jednej centralnej konsoli zarządzania.
3. Dostęp do konsoli centralnego zarządzania odbywa się z poziomu interfejsu WWW, niezależnie od zastosowanej platformy sprzętowej i programowej.
4. Konsola zarządzania jest dostępna w postaci usługi hostowanej na serwerach producenta
5. Konsola zarządzania oferuje dostęp za pomocą następujących wspieranych przeglądarek internetowych:
    - Microsoft Edge
    - Mozilla Firefox
    - Google Chrome
    - Safari
6. Rozwiązanie realizuje skanowania podatności za pomocą dedykowanego oprogramowania, instalowanego w środowisku, zarządzanego z poziomu konsoli centralnego zarządzania.
7. Oprogramowanie skanujące podatności, w postaci aplikacji instalowanej lokalnie, wspiera poniższe systemy operacyjne:
    - Windows Server 2012 R2 i nowsze
    - Ubuntu server 18.x LTS
8. Rozwiązanie umożliwia przeprowadzenie skanowania, wykrywającego urządzenia pracujące w skanowanej sieci komputerowej.
9. Skanowanie wykrywające urządzenia pracujące w skanowanej sieci umożliwia:
    a) wykrywanie urządzeń pracujących w skanowanej sieci na podstawie protokołów: ARP, ICMP PING, SSH, HTTP, HTTPS, RDP.
    b) wykrycie pracujących urządzeń w oparciu o analizę wszystkich dostępnych otwartych portów sieciowych.
    c) Pozwala na konfigurację parametrów skanowania takich jak:
        a. zakres przeszukiwanych portów,
        b. wydajność skanowania (ilość jednoczesnych połączeń sieciowych),
        c. liczbę jednoczesnych wątków skanowania,
        d. możliwość wykrycia wersji systemu operacyjnego.
    d) konfigurację harmonogramu uruchamiania skanu (np. dziennie, tygodniowo, w określony dzień miesiąca, kwartalnie oraz wskazanie godziny rozpoczęcia skanowania)

e) konfigurację wysyłania powiadomień na wskazany adres e-mail, informujących o rozpoczęciu skanowania oraz jego zakończeniu.

10. Konsola zarządzająca umożliwia podgląd listy skonfigurowanych skanów wykrywających dostępne hosty w sieci, wraz z informacją o zmianach w stosunku do ostatniego przeprowadzonego skanu.
11. Konsola zarządzania umożliwia eksport wyniku skanu wykrywającego dostępne urządzenia w sieci do pliku XLS oraz XML.
12. Rozwiązanie umożliwia uruchomienie skanowania wykrywającego znane podatności bezpieczeństwa na urządzeniach sieciowych.
13. Skan wykrywający znane podatności bezpieczeństwa na urządzeniach sieciowych umożliwia:
    a) określenie skanowanego celu za pomocą adresu IP, oraz grupy celów za pomocą adresu podsieci IP.
    b) masowe wprowadzenie listy skanowanych celów (adresów IP), za pomocą ustrukturyzowanego pliku z rozszerzeniem CSV.
    c) konfigurację parametrów skanowania, takich jak:
        a. zakres skanowanych portów sieciowych TCP/UDP,
        b. parametr wydajności skanowania,
        c. rodzaj uwierzytelniania na skanowanej stacji.
    d) konfigurację harmonogramu uruchamiania skanu: dziennie, tygodniowo, w określony dzień miesiąca, oraz wskazanie godziny rozpoczęcia.
    e) konfigurację wysyłania powiadomień na wskazany adres e-mail informujących o momencie rozpoczęcia skanowania oraz jego zakończeniu.
14. Konsola zarządzania umożliwia podgląd listy skonfigurowanych skanów wykrywających znane podatności bezpieczeństwa, wraz z informacją o zmianach w stosunku do ostatniego przeprowadzonego skanu.
15. Konsola zarządzania umożliwia eksport wyniku skanu wykrywającego znane podatności bezpieczeństwa do pliku.
16. Rozwiązanie umożliwia uruchomienie skanu wykrywającego luki bezpieczeństwa w aplikacjach webowych.
17. Skanowanie wykrywające luki bezpieczeństwa w aplikacjach webowych umożliwia:
    a) określenie skanowanego celu za pomocą adresu URL lub adresu IP.
    b) konfigurację parametrów skanowania takich jak:
        a. rodzaje testowanych ataków,
        b. wyjątki ze skanowania (adresy URL omijane podczas testowania aplikacji web),
        c. parametr wydajności skanowania (ilość jednoczesnych zapytań przesyłanych do skanowanej aplikacji).
    c) konfigurację uwierzytelniania w testowanej aplikacji web.
    d) konfigurację harmonogramu uruchamiania skanowania: dziennie, tygodniowo, w określony dzień miesiąca, oraz wskazanie godziny rozpoczęcia skanowania.
    e) konfigurację wysyłania powiadomień na wskazany adres e-mail informujących o momencie rozpoczęcia skanowania oraz jego zakończeniu.
18. Konsola zarządzania umożliwia podgląd listy skonfigurowanych skanów wykrywających luki w aplikacjach webowych wraz z informacją o zmianach w stosunku do ostatniego przeprowadzonego skanu.
19. Rozwiązanie umożliwia skorzystanie z narzędzia do identyfikacji zasobów informatycznych dostępnych z publicznej sieci Internet.

20. Narzędzie do identyfikacji zasobów informatycznych dostępnych z publicznej sieci Internet umożliwia:
    a) przeszukiwanie adresów internetowych, skatalogowanych przez automatyczne systemy producenta, spełniających wskazane warunki wyszukiwania.
    b) zapisywanie wskazanych warunków wyszukiwania jako szablony.
    c) podgląd listy wyników wyszukiwania z informacją o wykrytym adresie IP, nazwie oraz słowach kluczowych.
    d) dodanie wybranych wyników wyszukiwania do grupy skanowania podatności bezpieczeństwa.

21. Rozwiązanie umożliwia podgląd listy wszystkich wykrytych podatności bezpieczeństwa z wszystkich przeprowadzonych skanowań.
22. Lista wszystkich wykrytych podatności musi umożliwiać:
    a) filtrowanie podatności ze względu na ich rodzaj, przypisany znacznik (opis), urządzenie sieciowe na którym została znaleziona podatność, stopień zagrożenia, status jego naprawy.
    b) wyświetlenie szczegółów poszczególnych podatności bezpieczeństwa wraz z informacjami na jakich urządzeniach sieciowych dana podatność została wykryta.
    c) eksport listy urządzeń na których została wykryta dana podatność bezpieczeństwa do pliku CSV.
23. Rozwiązanie umożliwia podgląd listy wygenerowanych raportów.
24. Rozwiązanie umożliwia utworzenie nowego raportu podsumowującego.
25. Raport podsumowujący umożliwia:
    a) konfigurację szablonu jaki będzie wykorzystany do przygotowania raportu,
    b) wybranie grup urządzeń, które będą znajdowały się w raporcie,
    c) wybranie poszczególnych statusów oraz poziomu zagrożenia podatności, które będą znajdowały się w raporcie,
    d) personalizację danych, którymi zostanie podpisany raport.

26. Lista wygenerowanych raportów musi umożliwiać:
    a) filtrowanie raportów ze względu na ich autora, nazwę, szablon oraz opis,
    b) eksport wyniku raportu do pliku XML, DOCX, XLSX.

27. Rozwiązanie umożliwia zarządzanie wykrytymi podatności w co najmniej następujący sposób:
    a) podgląd listy utworzonych zgłoszeń,
    b) filtrowanie zgłoszeń ze względu na ich status oraz czas zamknięcia,
    c) podgląd listy szablonów dla poszczególnych rodzajów skanów,
    d) dodanie szablonu dla poszczególnych rodzajów skanów oraz wprowadzenie ich konfiguracji,
28. Wymagania w stosunku do Wykonawcy:
    a) Szkolenie dwu dniowe realizowane przez minimum 1 certyfikowanego inżyniera wraz z wdrożeniem produktu oraz konfiguracją.
    -**VuM - F-Secure Elements Vulnerability Management Technical Training (Advanced*).***
    (Na potwierdzenie Wykonawca dołączy do oferty certyfikat inżynierski ważny minimum 6 miesięcy)

b) Wykonawca spełnia warunek, jeżeli dysponuje lub będzie dysponował osobami zdolnymi do wykonania zamówienia, posiadającymi uprawnienia w danej specjalności do pełnienia samodzielnych funkcji technicznych
c) Wykonawca spełnia warunek, jeżeli wykaże, że w okresie ostatniego roku przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie wykonał minimum trzy dostawy wraz z wdrożeniem oferowanego produktu.
d) Dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego roboty budowlane zostały wykonane.
   - Jeżeli Wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów – inne odpowiednie dokumenty.
   - Okres wyrażony w latach lub miesiącach, o których mowa powyżej, liczy się wstecz od dnia w którym upływa termin składania ofert.
   - Jeżeli Wykonawca powołuje się na doświadczenie dostaw lub usług, wykonywanych wspólnie z innymi Wykonawcami: - wykaz dostaw lub usług, dotyczy dostaw lub usług, w których wykonaniu Wykonawca ten bezpośrednio uczestniczył,
   - Wykaz dostaw lub usług dotyczy dostaw lub usług, w których wykonaniu Wykonawca ten bezpośrednio uczestniczył, a w przypadku świadczeń powtarzających się lub ciągłych, w których wykonywaniu bezpośrednio uczestniczył lub uczestniczy.

SZKOLENIE DLA PRACOWNIKÓW DZIAŁU IT

Szkolenia dla pracowników Działu IT powinno trwać minimum 3 godziny lekcyjne.
Po jego zakończeniu uczestnicy powinni posiadać niezbędną wiedzę jak korzystać z zakupionego oprogramowania w celu poprawienia systemu bezpieczeństwa sieci.