

Załącznik nr 7 -7.14 do SWZ

Przedmiotem zamówienia jest dostawa rozwiązania (oprogramowania) do ochrony przed podatnościami, o następujących parametrach:

WYMAGANIA OGÓLNE

1. Rozwiązanie klasy vulnerability management musi być dostępne w dwóch wersjach: lokalnej (onpremise) oraz chmurowej (SaaS).
2. Rozwiązanie w wersji chmurowej musi posiadać swoje centrum danych (data center) na terenie Unii Europejskiej.
3. Rozwiązanie w wersji lokalnej musi być udostępnione w postaci obrazu maszyny OVA (Open Virtual Appliance), pozwalając na wdrożenie w środowisku wirtualnym VMware.
4. Rozwiązanie musi oferować możliwość wdrożenia sond skanujących w postaci gotowych maszyn wirtualnych, które muszą być udostępnione w postaci obrazu maszyny na następujące wirtualizacje: Citrix XenServer, Microsoft Hyper-V, Vmware ESX/ESXi, VirtualBox, Proxmox.
5. Sonda skanująca musi wymagać rejestracji, w centralnej konsoli zarządzającej, przy użyciu wygenerowanego przez administratora minimum sześciocyfrowego tokena.
6. Centralna konsola zarządzania musi posiadać możliwość uruchomienia dodatkowego uwierzytelnienia użytkowników, za pomocą MFA/2FA wysyłanych w postaci wiadomości SMS.
7. Rozwiązanie musi posiadać możliwość integracji z systemami ticketowymi: Jira, TopDesk i ServiceNow.
8. Rozwiązanie musi posiadać możliwość wysyłania powiadomień do następujących systemów: Slack, Microsoft Teams i Webhooks.
9. Administrator w konsoli centralnej Security Center musi posiadać możliwość dodania dodatkowych użytkowników zarządzających.
10. Rozwiązanie musi posiadać możliwość dodania dodatkowych zestawów uprawnień (ról), które mogą być przypisane do użytkowników systemu.
11. Rozwiązanie musi posiadać możliwość zarządzania systemem przy użyciu interfejsu API.

ZARZĄDZANIE ZESTAWAMI URZĄDZEŃ I APLIKACJI WEBOWYCH

12. Rozwiązanie musi posiadać możliwość dodania ręcznego urządzeń i aplikacji webowych do skanowania.
13. Rozwiązanie musi posiadać możliwość importu listy urządzeń z pliku CSV.
14. Dodawanie urządzeń musi odbywać się za pomocą podania pojedynczego adresu IP, zakresu adresów IP oraz adresu sieci wraz z maską.
15. Dodanie aplikacji webowej musi pozwalać na dodanie rodzaju autentykacji, zdefiniowania białej i czarnej listy adresów URL oraz rozszerzeń do skanowania.
16. Przy dodawaniu urządzeń i aplikacji webowych administrator musi posiadać możliwość wyboru poziomu wpływu biznesowego z jednego z 4 poziomów: Neutral, Low, Medium i High.
17. Przy dodawaniu urządzeń i aplikacji webowych administrator musi posiadać możliwość zdefiniowania i wyboru znaczników (tagów).
18. Administrator musi posiadać możliwość dodania znaczników (tagów) statycznych wraz z odpowiednim kolorem.
19. 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

20. 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 i Webhook.

21. Rozwiązanie musi posiadać możliwość zapewnienia nieograniczonej liczby węzłów skanowania z nieograniczoną liczbą węzłów skanowania, które umożliwiają skanowanie różnych części sieci w tym samym czasie.
22. Rozwiązanie musi posiadać możliwość skanowania całego środowiska IT z segmentowanymi i geograficznie oddzielonymi sieciami.
23. Usługa skanowania sieci musi obsługiwać IPv6.
24. Rozwiązanie musi posiadać możliwość definiowania i dodawania nowych profili skanowania sieciowego.
25. Administrator musi posiadać możliwość importu predefiniowanych przez producenta profili skanowania sieciowego.
26. Podczas tworzenia profilu skanowania, administrator musi posiadać możliwość wyboru trybu skanowania: pełne, podstawowe, typu discovery.
27. 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.
28. Rozwiązanie musi posiadać możliwość uwzględnienia podatności o niskim prawdopodobieństwie wystąpienia w wynikach skanowania.
29. Rozwiązanie musi umożliwiać klientom wybór opcji "potencjalnie niebezpiecznych testów" i włączenia skanowania drukarek.
30. Rozwiązanie musi posiadać możliwość uwzględnienia martwych hostów w skanach.
31. Możliwość włączenia opcji typu „brute force” do ustawień skanowania.
32. Profil skanowania sieciowego musi posiadać możliwość dodania uwierzytelniania na urządzeniu sieciowym, w oparciu o uwierzytelnianie Windows i/lub Linux.
33. Profil skanowania sieciowego musi posiadać możliwość wyboru intensywności skanowania.
34. Profil skanowania sieciowego musi posiadać możliwość wyboru testów podatności, które będą przeprowadzone w trakcie skanowania.
35. Rozwiązanie musi posiadać co najmniej 80 tys. (w wersji lokalnej) i 130 tys. (w wersji chmurowej) testów podatności aktualizowanych na bieżąco z serwera producenta rozwiązania.
36. Podczas tworzenia zadania skanowania sieciowego, administrator musi posiadać możliwość wyboru sondy skanującej zainstalowanej lokalnie, grupy sond lub sondy zewnętrznej hostowanej w chmurze producenta (tylko w wersji chmurowej).
37. Administrator musi posiadać możliwość uruchomienia zadania skanowania sieci jednorazowo lub z harmonogramem.
38. Rozwiązanie musi posiadać możliwość pobrania raportu CSV z modułu skanowania sieciowego w celu wyświetlenia listy zadań skanowania.
39. 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.
40. Podatności wykryte podczas skanowania sieciowego muszą automatycznie być umieszczane w menedżerze podatności.

SKANOWNIE APLIKACJI WEBOWYCH

41. Rozwiązanie musi posiadać możliwość dodawania nowych profili skanowania aplikacji webowych.
42. Administrator musi posiadać możliwość importu predefiniowanych przez producenta profili skanowania aplikacji webowych.
43. Rozwiązanie musi posiadać możliwość skanowania aplikacji internetowych (skanowanie stron internetowych).
44. Rozwiązanie musi posiadać możliwość zapewnienia nieograniczonej liczby skanów i nieograniczonej liczby zaplanowanych skanów oraz skanów na żądanie. Powiadomienia muszą być również dostępne za pośrednictwem integracji e-mail, Slack i Webhook.
45. Rozwiązanie musi posiadać możliwość skanowania nieograniczonej liczby aplikacji internetowych.
46. Rozwiązanie musi posiadać możliwość zapewnienia konfigurowalnych ustawień skanowania, takich jak ustawienia indeksowania do metody formularza: post i get, post, get.

47. Podczas tworzenia zadania skanowania aplikacji webowych, administrator musi posiadać możliwość wyboru sondy skanującej zainstalowanej lokalnie lub sondy zewnętrznej hostowanej w chmurze producenta (tylko w wersji chmurowej).
48. Podczas tworzenia profilu skanowania aplikacji webowych administrator musi posiadać możliwość włączenia i wyłączenia wykonania testów „łamania” haseł typu brute force.
49. Rozwiązanie musi posiadać możliwość wyboru intensywności skanowania wydajności (wstępnie ustawiona na niską, średnią i wysoką) przez system. Umożliwia również niestandardowe ustawienia żądań na sekundę.
50. Rozwiązanie musi posiadać możliwość włączenia pełnego zestawu kategorii wykrywania podatności, a także dostosowania kategorii wykrywania podatności do skanowania, a także listy wykluczeń.
51. Rozwiązanie musi posiadać możliwość wyboru opcji skanowania wrażliwych treści, numerów kart kredytowych i zezwalania na wprowadzanie niestandardowych treści.
52. Administrator musi posiadać możliwość uruchomienia zadania skanowania aplikacji webowej jednorazowo lub zgodnie z harmonogramem.
53. Podatności wykryte podczas skanowania aplikacji webowych muszą automatycznie być umieszczane w menedżerze podatności.

SKANOWANIE AGENTOWE (WERSJA CHMUROWA)

54. Rozwiązanie musi posiadać możliwość instalacji na systemach Windows aplikacji agentowej, która będzie przysyłać do konsoli centralnej listę zainstalowanych aplikacji.
55. Systemu musi posiadać bazę podatności aplikacji zainstalowanych w systemach skanowanych przez aplikację agentową.
56. Wykryte przez aplikację agentową podatności muszą automatycznie być umieszczane w menedżerze podatności.
57. Pakiet instalacyjny aplikacji agentowej musi być udostępniony w postaci pliku .msi.
58. Aktywacja aplikacji agentowej musi wymagać podania, wygenerowanego w konsoli centralnej, tokenu.

SKANOWANIE USŁUG CHMUROWYCH (WERSJA CHMUROWA)

59. Rozwiązanie musi posiadać możliwość wykrywania i raportowania błędnej konfiguracji usług chmurowych Amazon Web Services (AWS), Microsoft Azure oraz Google Cloud.
60. Rozwiązanie musi posiadać możliwość dodawania nowych profili skanowania usług chmurowych.
61. Administrator musi posiadać możliwość uruchomienia zadania skanowania usługi chmurowej jednorazowo lub zgodnie z harmonogramem.

MONITOROWANIE SERWERÓW POCZTOWYCH I STRON INTERNETOWYCH (WERSJA CHMUROWA)

62. Rozwiązanie musi posiadać mechanizm weryfikacji listowania na czarnych listach serwerów pocztowych i stron internetowych.

ZARZĄDZANIE AKTYWAMI

63. Rozwiązanie musi posiadać możliwość wyświetlenia listy zeskanowanych zasobów: adres IP sieci i aplikacje internetowe z następującymi informacjami:
 - a. oznaczanie (lista grupowania)
 - b. nazwa zasobu
 - c. liczba wykrytych podatności w zabezpieczeniach
 - d. najwyższa wykryta podatność
 - e. krytyczność/istotność dla biznesu
 - f. informacje o systemie operacyjnym
 - g. data wprowadzenia utworzonych zasobów i ostatnio wykryty znacznik czasu.
64. 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 danym 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
 - g. aplikacja internetowa: lista przeskanowanych i wykrytych map witryn
 - h. aplikacja webowa: trend zasobu - według ważności, stanu (możliwość wyświetlania według okresu i interwału).
65. 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: aby podać kolumnę wejściową dla opisu zasobu
 - d. sieć: możliwość wybrania, czy zasób przechowuje jakiegokolwiek dane osobowe RODO
 - e. aplikacja internetowa: aby podać nazwę zasobu
 - f. aplikacja internetowa: aby podać etykietę wpływu biznesowego
 - g. aplikacja internetowa: aby zapewnić kolumnę wejściową dla opisu zasobu
 - h. aplikacja internetowa: rozwiązanie musi posiadać możliwość wybrania, czy zasób przechowuje jakiegokolwiek dane osobowe RODO
 - i. aplikacja internetowa: rozwiązanie musi posiadać możliwość zapewnienia funkcji skanowania REST API
 - j. aplikacja internetowa: może zapewnić zakres indeksowania, taki jak nazwa hosta adresu URL i podkatalog adresu URL (także w stanie jawnie określić inne adresy URL)
 - k. aplikacja webowa: możliwość podawania nagłówków i plików cookie
 - l. aplikacja internetowa: może zapewnić uwierzytelnione skanowanie, takie jak HTTP basic i HTTP form
 - m. aplikacja internetowa: zapewnienie elastyczności w utrzymywaniu listy wykluczających adresów URL, takich jak biała i czarna lista
 - n. aplikacja internetowa: rozwiązanie musi posiadać możliwość wyświetlenia listy zeskanowanych luk w zabezpieczeniach powiązanych z zasobami aplikacji internetowej.
66. Rozwiązanie musi potrafić zapewnić funkcje tworzenia i utrzymywania tagów (grup) statycznych i dynamicznych.
67. Rozwiązanie musi posiadać możliwość tworzenia ręcznego wprowadzania i importowania zasobów kategorii Network IP.

MODUŁ KAMPANII PHISHINGOWYCH I EDUKACYJNYCH (WERSJA CHMUROWA)

68. Rozwiązanie musi posiadać możliwość utworzenia kampanii phishingowych i edukacyjnych.
69. Administrator musi posiadać możliwość utworzenia własnych profili phishingowych lub importu predefiniowanych przez producenta.
70. Profile kampanii phishingowych utworzone przez producenta muszą być dostępne w językach: polskim, angielskim, niemieckim, francuskim, hiszpańskim.
71. Profil kampanii phishingowej musi zawierać szablon wiadomości email lub wiadomości email i strony internetowej.
72. Rozwiązanie musi posiadać możliwość przypisania do profilu kampanii phishingowej kategorii domen, z których wysyłane będą wiadomości.
73. Rozwiązanie musi posiadać minimum 100 dostępnych domen przydzielonych do odpowiednich kategorii.
74. Kampanie phishingowe muszą posiadać możliwość wyboru czasu rozpoczęcia kampanii oraz zdefiniowania czy wiadomości mają być wysyłane jednorazowo do wszystkich odbiorców, w grupach lub losowo w określonym zakresie czasu.
75. Platforma musi posiadać co najmniej 5 predefiniowanych szablonów kampanii:
- a. polski: wiadomości phishingowe - oszustwo związane z kontem e-mail
 - b. polski: wiadomości phishingowe i strony internetowe - oszustwa związane z kontami e-mail
 - c. polski: wiadomości phishingowe i strony internetowe - oszustwa związane z kartami kredytowymi

- d. polski: pobieranie plików - Office 365
- e. polski: phishing - Office 365

- 76. Administrator musi posiadać możliwość przypisania do kampanii phishingowej, kampanii edukacyjnej przeprowadzanej poprzez wysłanie wiadomości email i/lub strony internetowej.
- 77. Administrator musi posiadać możliwość utworzenia własnych profili edukacyjnych lub importu predefiniowanych przez producenta.
- 78. Rozwiązanie musi posiadać możliwość wyboru treści wiadomości edukacyjnej w zależności od podjętej przez odbiorcę czynności: otwarcia wiadomości, odpowiedzi na wiadomość, kliknięcia w link oraz wypełnienia formularza na stronie phishingowej.
- 79. Rozwiązanie musi posiadać możliwość stworzenia oraz wyboru treści prezentacji edukacyjnej w formie strony internetowej na której można zamieszczać treści edukacyjne w postaci tekstu, grafiki oraz wideo.
- 80. Rozwiązanie musi posiadać możliwość stworzenia oraz wyboru testu sprawdzającego wiedzę w formie strony internetowej na której można zamieszczać pytania i odpowiedzi w formie jednokrotnego i wielokrotnego wyboru.
- 81. Rozwiązanie musi posiadać możliwość anonimizacji danych odbiorców i podjętych przez nich czynności.
- 82. Rozwiązanie musi posiadać możliwość importu odbiorców wiadomości phishingowych z systemu Azure ActiveDirectory, wprowadzenia ręcznie lub importu z pliku CSV zgodnego z kodowaniem UTF-8 .

MENEDŻER PODATNOŚCI I PANEL GŁÓWNY

- 83. Platforma zarządzania podatnościami musi być w stanie zapewnić funkcje pulpitu nawigacyjnego (i konfigurowalne) z następującymi widżetami:
 - a. wyniki skanowania podatności sieci według ważności (z opcjami wykresu: słupkowy i kołowy)
 - b. wyniki skanowania podatności aplikacji internetowych według ważności (z opcjami wykresu: słupkowy i kołowy)
 - c. otwarte zgłoszenia według ważności (z opcjami wykresu: słupkowy i kołowy)
 - d. top 10 wyników skanowania sieci (dostępna opcja ustawienia celu zasobu jako wszystkich lub wybranych adresów IP/tagów)
 - e. 10 największych podatności w aplikacjach sieciowych (dostępna opcja ustawienia celu zasobu jako wszystkie lub wybrane aplikacje sieciowe/etykiety)
 - f. zgodność z OWASP (z opcjami wykresów: słupkowy i kołowy oraz dostępną opcją ustawienia dla wszystkich lub wybranych aplikacji internetowych)
 - g. ostatnie skanowania
 - h. nadchodzące skanowania
 - i. ostatnie 10 raportów
 - j. liczba podatności w zabezpieczeniach w czasie (dostępna opcja ustawienia celu zasobu jako wszystkich lub wybranych aplikacji IPS/web/tagów wraz z ustawieniem czasu, aby ustawić czas trwania i interwał)
 - k. ocena wyników kampanii phishingowych
 - l. ciągłe monitorowanie alertów (dostępna opcja ustawienia okresu na dzień/tydzień)
- 84. Platforma zarządzania podatnościami musi mieć możliwość sortowania, grupowania i priorytetyzacji podatności
 - a. możliwość tworzenia wielu zakładek w celu filtrowania następujących kryteriów:
 - b. według stanu: wszystkie, nie ignorowane/wyłączone i ignorowane/wyłączone
 - c. według typu: host i aplikacja internetowa
 - d. według statusu: nowy, aktywny, ponownie otwarty, naprawiony
 - e. według ważności: informacja, niski, średni, wysoki, krytyczny
 - f. według tagów (opcja uwzględnienia/wykluczenia tagu)
 - g. według pierwszego i ostatniego wykrycia
 - h. według kategorii: podatności w skanowaniu sieci i podatności w aplikacjach internetowych
 - i. możliwość filtrowania listy podatności według podatności lub aplikacji internetowych/hosta
 - j. możliwość tworzenia raportów bezpośrednio z menedżera podatności poprzez wybranie jednej lub więcej podatności

- k. możliwość dalszego administrowania/zarządzania listą luk w zabezpieczeniach za pomocą następujących funkcji:
- l. co ignorować: wyłącz tę podatność dla wszystkich hostów/aplikacji internetowych i ignoruj tę podatność
- m. powód ignorowania: fałszywie dodatni, ryzyko zaakceptowane, nieistotny
- n. opcja ustawienia czasu wygaśnięcia dla ignorowanych podatności
- o. możliwość tworzenia notatek do celów uwag i notatek, które pojawią się w raporcie po jego wygenerowaniu
- p. możliwość tworzenia czatu konwersacyjnego do celów współpracy między użytkownikami
- q. opcja wyświetlania następujących informacji na temat podatności:
 - i. wpływ
 - ii. rozwiązanie
 - iii. podsumowanie
 - iv. wgląd
 - v. wykrywanie
 - vi. odniesienie
 - vii. łątki
 - viii. możliwość utworzenia zgłoszenia bezpośrednio ze wskazanych luk w zabezpieczeniach
 - ix. środki zaradcze.

85. Platforma zapewnia wbudowany system ticketowy dla procesu naprawczego.

86. Możliwość dostarczania informacji o zgłoszeniach, takich jak:

- a. numerowanie ich w celu łatwego śledzenia i powiadamiania za pośrednictwem poczty elektronicznej.
- b. możliwość podawania i aktualizowania statusu zgłoszenia, takiego jak: otwarte, zamknięte lub rozwiązane
- 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 i terminu płatności
- f. możliwość tworzenia wielu zakładki do utrzymywania i zarządzania zgłoszeniami zgodnie z poniższymi zasadami:
- g. status
- h. typ zasobu
- i. kategoria usługi
- j. tagi
- k. termin płatności
- l. kategoria skanowania sieci i aplikacji internetowych
- m. istotność
- n. system operacyjny
- o. porty
- p. właściciel
- q. potrafi zapewnić proaktywną obsługę zgłoszeń opartą na zasadach.

87. Rozwiązanie musi posiadać możliwość ciągłego monitorowania oraz szybkiego i łatwego ustawienia profilu monitorowania zmian za pomocą powiadomień i alarmów.

88. W menedżerze podatności musi istnieć możliwość utworzenia własnego widoku podatności zawierającego odfiltrowane zgodnie z konfiguracją administratora danych.

89. Rozwiązanie musi posiadać możliwość zignorowania wykrytych podatności na określony czas.

SYSTEM RAPORTUJĄCY

System raportujący musi zawierać następujące typy raportów:

- 90. Skanowanie sieci.
- 91. Aplikacja sieciowa.
- 92. łątki.
- 93. Środki zaradcze.

94. Ocena phishingu e-mail.
95. Porównanie (raport typu delta).
96. Zgodność.
97. Raporty zgodności – musi być w stanie wygenerować następujący typ zgodności:
 - a. ustawa Sarbanes-Oxley
 - b. ustawa o przenośności i rozliczalności ubezpieczeń zdrowotnych
 - c. OWASP Top 10
 - d. ustawa o ochronie danych osobowych
 - e. ISO / IEC 27001
 - f. ogólne rozporządzenie o ochronie danych
 - g. bezpieczeństwo sieci i informacji
 - h. PCI DSS.
98. System powinien mieć możliwość dostarczania nowych niestandardowych raportów zgodności, które mogą być zalecane przez rząd, gdy ma to zastosowanie.
99. 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. zawartość raportu: szczegóły raportu, przegląd podatności, podsumowanie podatności, lista podatności (według podatności i hosta) z opcjami wglądu, podsumowania, wykrywania, odniesień i ograniczenia tekstu.
 - e. sposób prezentacji raportu: podatności według ważności w czasie, podatności według statusu, podatności według ważności, 5 najbardziej narażonych kategorii
 - f. filtrowanie: selektywne raportowanie podatności (pełne i niestandardowe) i wykluczenia, uwzględnione systemy operacyjne, filtry zasobów, filtry podatności.
100. Możliwość utworzenia i dostosowania szablonu raportu aplikacji internetowej.
101. Raport oparty na określonym czasie skanowania.
102. Raport oparty na wszystkich bieżących informacjach o podatnościach.
103. Zawartość raportu: szczegóły raportu, przegląd podatności, podsumowanie podatności, lista podatności (według podatności i hosta) z opcjami wglądu, podsumowania, wykrywania, odniesień i ograniczenia tekstu.
104. Filtrowanie: selektywne raportowanie podatności (pełne i niestandardowe) i wykluczenia, uwzględnione systemy operacyjne, filtry zasobów, filtry podatności.
105. Możliwość tworzenia "raportów skróconych" wysyłanych w formie podsumowania. Częstotliwość raportów można ustawić na: tygodniowe raporty skrócone i miesięczne raporty skrócone. Raporty są dostarczane kanałem e-mail.