Załącznik nr 1
do Ogłoszenia o zamówieniu

Wdrożenie systemu zarządzania podatnościami

I. Wymagania dla oferowanego oprogramowania.
II. Wymagane kompetencje.

I. Wymagania dla oferowanego oprogramowania

1. Dostarczenie licencji czasowej wraz ze wsparciem producenta, ważnej przez 12 miesięcy.
2. Oprogramowanie musi działać on-premise. Do prawidłowego funkcjonowania zarówno oprogramowania jak i jego komponentów nie jest potrzebny dostęp do sieci Internet. Instalacja kluczy licencyjnych i aktualizacja oprogramowania musi być możliwa offline, bez dostępu do sieci Internet.
3. W przypadku dostarczenia Oprogramowania jako maszyny wirtualnej musi być wspierane środowisko VMware oraz Hyper-V.
4. Jeżeli Oprogramowanie będzie instalowane na systemie operacyjnym należy dostarczyć produkt, który będzie mógł być zainstalowany na jednym z systemów operacyjnych: Red Hat Enterprise Linux 8, Red Hat Enterprise Linux 9 lub Oracle Linux 9, w wersjach 64-bit.
5. Oprogramowanie musi posiadać konsolę zarządzającą dostępną poprzez interfejs webowy.
6. Dostęp przez interfejs webowy musi być obsługiwany za pośrednictwem co najmniej następujących przeglądarek internetowych: Microsoft Edge, Google Chrome oraz Mozilla Firefox w wersjach aktualnych na dzień składania oferty.
7. Oprogramowanie musi być w architekturze skanery aktywne i pasywne plus moduł do centralnego zarządzania podatnościami i skanerami podatności.
8. Oprogramowanie musi dawać możliwość skanowania urządzeń końcowych działających na różnych systemach operacyjnych oraz znajdujących się w różnych podsieciach.
9. Agent Systemu dla stacji końcowej musi działać na następujących systemach operacyjnych: Microsoft Windows 10, Microsoft Windows 11, Windows Server 2012 R2, 2016, 2019, 2022, 2025, macOS 13,14,15 oraz Linux (RHEL/Debian/Ubuntu).
10. Elementy zarządzające i analityczne Oprogramowania nie mogą być ograniczone liczbą skanerów sieciowych w różnych podsieciach, liczbą hostów w podsieci czy liczbą możliwych do skanowania podsieci.
11. Wymagana jest możliwość wykorzystania mechanizmu proxy do komunikacji z Internetem.
12. W przypadku dostępu do Internetu Oprogramowanie musi umożliwiać aktualizację automatyczną jak również ręczną z poziomu panelu zarządzania systemem.
13. W przypadku skanowania aplikacji webowych z Internetu, Zamawiający dopuszcza możliwość skorzystania z dodatkowych narzędzi np.: dodatkowego panelu zarządzania lub dodatkowego systemu, w tym umiejscowionego w chmurze.
14. Oprogramowanie musi umożliwiać tworzenie indywidualnych kont dla każdego użytkownika/administratora systemu.
15. Dostęp do Oprogramowania możliwy jedynie po uwierzytelnieniu użytkownika w systemie.
16. Hasła dostępu muszą być przechowywane w postaci zaszyfrowanej.

17. Oprogramowanie musi zapewniać silną politykę haseł lub umożliwiać jej określenie dla użytkowników systemu.
18. Oprogramowanie musi umożliwiać konfigurowanie zakresu uprawnień w systemie z wykorzystaniem predefiniowanych ról wewnętrznych (np. dostęp tylko do raportów, administrator Oprogramowania itp.) lub poprzez możliwość przypisania określonych operacji do zdefiniowanych ról.
19. Oprogramowanie musi integrować się z Active Directory, LDAP w zakresie uwierzytelnienia oraz kontroli dostępu na bazie zdefiniowanych ról.
20. Oprogramowanie musi mieć możliwość korzystania z SAML.
21. Oprogramowanie musi mieć możliwość definiowania raportów i alertów z wykorzystaniem wszystkich danych zbieranych przez system.
22. Oprogramowanie musi mieć wbudowany panel sterowania (Dashboard) z predefiniowaną zawartością dostosowaną do potrzeb określonej roli. Dashboard powinien umożliwiać schodzenie do szczegółów z poziomu informacji zagregowanych (drill-down).
23. Oprogramowanie musi umożliwiać przechowywanie wszystkich danych pochodzących z dowolnego silnika skanującego i testującego.
24. Oprogramowanie musi umożliwiać przeglądanie tych danych w sposób przejrzysty dla użytkownika, co najmniej w postaci Top 10 podatności, Top 10 systemów zainfekowanych, możliwość filtrowania wykrytych podatności, informacje o połączeniach między systemami klienckimi a serwerami.
25. Oprogramowanie musi umożliwiać tworzenie raportów dostępnych w systemie centralnego zarządzania oraz wysyłania ich na wskazane adresy email.
26. Oprogramowanie musi zapewniać monitorowanie stanu pracy skanerów, co najmniej przez: okresową weryfikację czy skanery są uruchomione, stan pracy skanera, prezentacji informacji o podatnościach wykrytych przez skanery pasywne, prezentacji wyników skanowania otrzymanych ze skanerów aktywnych, prezentacji informacji o podatnościach w połączeniu z wynikami skanowania ze skanerów aktywnych.
27. Oprogramowanie musi zapewniać szyfrowaną komunikację między serwerem zarządzającym a agentem zainstalowanym na stacji roboczej/serwerze.
28. Oprogramowaniu musi umożliwiać tworzenie oraz uruchamianie skanów aktywnych i pasywnych.
29. Oprogramowanie musi umożliwiać harmonogramowanie (planowanie w czasie) oraz jednoczesnego uruchomienia na wybranych lub wszystkich skanerach zainstalowanych na stacjach roboczych i serwerach podłączonych do Oprogramowania centralnego zarządzania. W tym również w sytuacji, gdy stacja robocza/serwer/skaner na stacji lub serwerze nie jest uruchomiony (uruchomienie jest inicjowane przez Oprogramowanie centralnego zarządzania).
30. Oprogramowanie musi mieć możliwość wykonywania ręcznego i zaplanowanego skanowania określonych hostów lub podsieci z wykorzystaniem skanerów podatności.
31. Wszystkie dane zebrane przez zewnętrzne silniki skanujące i testujące muszą być przesyłane niezwłocznie do centralnej bazy i nie mogą być przechowywane przez skaner lokalnie. Skanery aktywne podłączone do Oprogramowania centralnego zarządzania muszą mieć możliwość wykonywania skanowania bez uwierzytelnienia oraz za pomocą uwierzytelnienia do Oprogramowania skanowanego.
32. Oprogramowanie musi zapewnić możliwość uwierzytelnienia przynajmniej za pomocą poniższych metod podczas skanowania z serwera: login i hasło, klucz ssh, Kerberos w tym integracja z Microsoft AD.

33. Skaner pasywny (agentowy) musi posiadać swój własny interfejs webowy, w którym jest prezentowany aktualny stan pracy, między innymi informacje o połączeniach między systemami klienckimi a serwerami, IP stacji roboczych/serwerów, stan połączenia z centralnym systemem zarządzania, podgląd logu pracy.
34. Skaner pasywny musi umożliwiać zdefiniowanie adresów IP stacji roboczych/serwerów/sieci, które będą podlegać monitorowaniu.
35. Skaner pasywny musi umożliwiać wysyłanie logu Oprogramowania w formacie CEF.
36. Skaner pasywny musi umożliwiać tworzenie własnych reguł służących do wykrywania określonych elementów w monitorowanym ruchu.
37. Automatyzacja procesów, powinna obejmować co najmniej: skanowanie o zaplanowanym czasie. powiadamianie i alarmowanie administratora o zdefiniowanych zdarzeniach (np. syslog, SMTP, uruchom skan, wygeneruj raport).
38. Oprogramowanie musi umożliwiać przeprowadzanie retestów luk/podatności wykrytych wcześniej w celu sprawdzenia czy zostały one poddane działaniem naprawczym.
39. Wykryte podatności powinny posiadać odnośniki do otwartych baz podatności, takich jak: MSFT, CVE, OSVDB.
40. Oprogramowanie musi umożliwiać tworzenie grup dla danych wynikowych.
41. Oprogramowanie centralnego zarządzania musi dostarczać wzorce polityk skanowania jak również umożliwiać budowanie polityk skanowania od podstaw.
42. W ramach budowy polityki skanowania Oprogramowanie musi zezwalać na wybranie podatności jakie będą sprawdzane podczas skanowania, np. w oparciu o CVSS lub CVE.
43. Musi istnieć możliwość przeszukiwania wyników co najmniej za pomocą filtrów takich jak: adres IP, severity, CVE, CVSS score i vector, dostępność exploitów, narzędzi do wykonania ataku, data opublikowania patcha dla danej podatności, port/protokół, data opublikowania podatności, data zauważenia po raz pierwszy podatności, data, kiedy ostatni raz widziana była podatność.
44. Administrator musi mieć możliwość zaakceptowania danego ryzyka oraz zmiany poziomu niebezpieczeństwa związanego z daną podatnością dla konkretnego systemu, portu, protokołu.
45. Oprogramowanie musi prezentować wyniki skanowania co najmniej za pomocą widoków: sumarycznie po IP, sumarycznie po portach, sumarycznie po CVE, Sumarycznie po protokołach, sumarycznie po systemach operacyjnych.
46. Oprogramowanie musi umożliwiać tworzenie grup systemów spełniających określone warunki.
47. Grupy systemów mogą być tworzone dynamicznie i/lub statycznie.
48. Tworzenie nowych grup systemów musi odbywać się również na podstawie wyrażeń logicznych takich jak AND, OR, NOT pomiędzy istniejącymi grupami systemów.
49. Raportowanie musi być integralną częścią Oprogramowania centralnego zarządzania.
50. Oprogramowanie musi posiadać gotowe grupy wzorców raportów udostępnionych przez producenta, które administrator może edytować.
51. Oprogramowanie musi pozwalać na budowanie raportu od podstaw.
52. Oprogramowanie musi umożliwiać generowane raportów co najmniej w formatach: PDF i CSV.
53. Oprogramowanie musi mieć możliwość generowana raportów według harmonogramu oraz na żądanie.
54. Oprogramowanie musi pozwalać na dodanie znaku wodnego podczas generowania raportu.

55. Oprogramowanie musi mieć możliwość automatycznego wysyłania raportów do wskazanych osób na maila.
56. Oprogramowanie musi mieć możliwość wyboru systemów do skanowania w oparciu o przynajmniej następujące możliwości: podanie listy adresów IP, wskazanie zakresu adresów IP, podanie listy adresów IP podsieci, tworzenie dynamicznie lub statycznie grup systemów, wskazanie nazw domenowych systemów.
57. Oprogramowanie musi posiadać gotowe wzorce widoków (ang. Dashboard) do Oprogramowania centralnego zarządzania podatnościami, które mogą być edytowane przez administratora systemu.
58. Administrator musi mieć możliwość tworzenia widoków od podstaw używając co najmniej takich elementów jak: tabela, wykres kołowy, wykres liniowy, wykres słupkowy.
59. Oprogramowanie musi posiadać wzorce zgodności z regulacjami, które dostarcza producent, co najmniej dla regulacji CIS, DISA.
60. Oprogramowanie musi umożliwiać tworzenie swoich własnych wzorców sprawdzania zgodności bez konieczności kontaktu z pomocą techniczną producenta. Producent musi udostępniać informację w jaki sposób można budować swoje własne wzorce sprawdzania zgodności ze standardami przyjętymi u Zamawiającego.
61. Oprogramowanie musi umożliwiać wykonywanie skanów audytowych/konfiguracji co najmniej dla systemów i oprogramowania: Windows, Linux, VMware, SQL (MSSQL, MySQL, PostgreSQL), Oracle.
62. Oprogramowanie musi posiadać interfejs API.
63. Oprogramowanie musi posiadać integrację z oprogramowaniem Splunk poprzez dedykowaną aplikację/dodatek producenta rozwiązania.
64. Oprogramowanie musi umożliwiać przesyłanie logów do systemu SIEM (Splunk).

II. Wymagane kompetencje

Zamawiający wymaga, aby osoba/osoby* realizująca usługę:

1. Posiada doświadczenie we wdrażaniu oferowanego systemu (w okresie ostatnich 3 lat uczestnictwo w minimum jednym wdrożeniu).
2. W zakresie kwalifikacji zawodowych posiada aktualny certyfikat wydany przez Splunk Inc.: Splunk Enterprise Certified Admin lub Splunk Enterprise Security Certified Admin lub na poziomie Architect.

* Zamawiający dopuszcza aby każda z osób spełniała co najmniej jedno z wymagań tak, aby łącznie były spełnione oba wymagania.