

Szczegółowy opis przedmiotu zamówienia

1. Opis środowiska Zamawiającego:

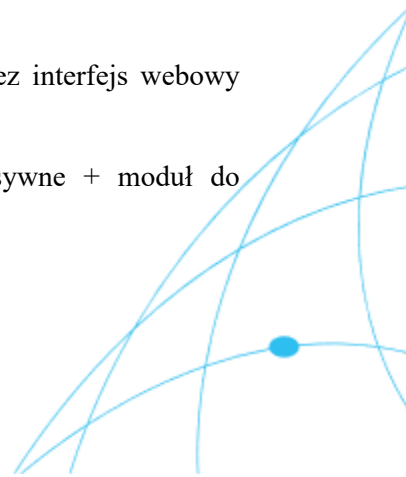
- 1) Zamawiający posiada oprogramowanie Tenable.SC wraz z licencją umożliwiającą uruchomienie 1024 szt, agentów skanera Nessus oraz nieograniczoną liczbę skanerów Nessus Professional;
- 2) posiadana przez Zamawiającego licencja oprogramowania Tenable.SC wygasa w dniu 10.09.2023 r.;
- 3) Zamawiający posiada Customer ID 940726;
- 4) oprogramowanie Tenable.SC jest obecnie zintegrowane z rozwiązaniem klasy SIEM (reguły korelacyjne) oraz Jira (raportowanie podatności);
- 5) środowisko Zamawiającego składa się z następujących stacji końcowych:
Liczba hostów o unikalnych adresach IP wymagająca skanów podatności – w tym:
 - a) stacje robocze oparte o Oprogramowanie operacyjny z rodziny MS Windows oraz Mac OS,
 - b) serwery rodziny Windows Server oraz Linux dystrybucji RHEL, Centos, Debian.

2. Przedmiot zamówienia:

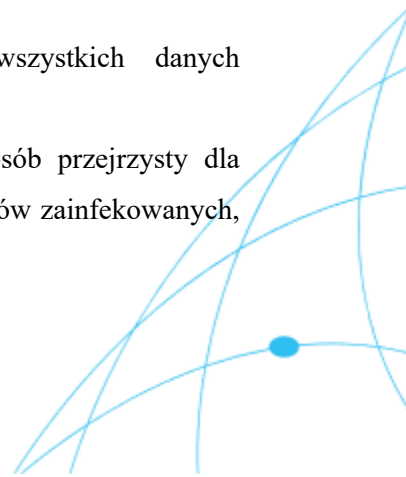
- 1) przedłużenie licencji posiadanego oprogramowania Tenable.SC dla 1024 szt. agentów lub dostawę licencji oprogramowania równoważnego dla 1000 szt. agentów, spełniającego wymagania wskazane w pkt 3 SOPZ, na okres 24/36 miesięcy w ramach zamówienia gwarantowanego;
- 2) w ramach zamówienia opcjonalnego zwiększenie liczby agentów o 50% zamówienia gwarantowanego;
- 3) zapewnieniem usługi wsparcia technicznego producenta oferowanego oprogramowania.

3. Wymagania dla oprogramowania równoważnego:

- 1) Dostarczenie niezbędnych licencji wieczystych typu virtual appliance lub software appliance;
- 2) W przypadku dostarczenia Oprogramowania jako maszyny wirtualnej musi być wspierane środowisko wykorzystywane przez Zamawiającego – VMware;
- 3) Jeżeli oprogramowanie będzie instalowane na systemie operacyjnym należy dostarczyć produkt, który będzie mógł być zainstalowany na jednym z systemów operacyjnych: Windows Server 2022 lub RHEL8/9;
- 4) Oprogramowanie musi posiadać konsolę zarządzającą dostępną poprzez interfejs webowy (http);
- 5) Oprogramowanie musi być w architekturze skanery aktywne i pasywne + moduł do centralnego zarządzania podatnościami i skanerami podatności;



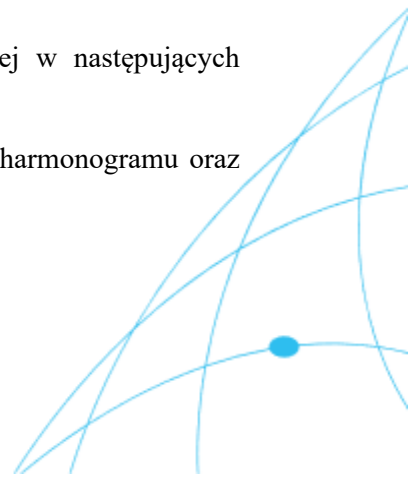
- 6) Oprogramowanie musi dawać możliwość skanowania urządzeń końcowych działających na różnych systemach operacyjnych oraz znajdujących się w różnych podsieciach;
- 7) Elementy zarządzające i analityczne Oprogramowania nie mogą być ograniczone liczbą skanerów sieciowych w różnych podsieciach, liczbą hostów w podsieci czy liczbą możliwych do skanowania podsieci;
- 8) Wymagana jest możliwość wykorzystania mechanizmu proxy do komunikacji z Internetem;
- 9) W przypadku braku dostępu do Internetu Oprogramowanie zarządzający ma mieć możliwość aktualizacji za pomocą ręcznej aktualizacji;
- 10) W przypadku dostępu do Internetu Oprogramowanie ma umożliwiać aktualizację automatyczną jak również ręczną z poziomu panelu zarządzania systemem;
- 11) W przypadku skanów aplikacji webowych z Internetu Zamawiający dopuszcza możliwość skorzystania z dodatkowych narzędzi np.: dodatkowego panelu zarządzania lub dodatkowego systemu, w tym umiejscowionego w chmurze;
- 12) Oprogramowanie musi umożliwiać tworzenie indywidualnych kont dla każdego użytkownika/administratora systemu;
- 13) Dostęp do Oprogramowania możliwy jedynie po uwierzytelnieniu użytkownika w systemie;
- 14) Hasła dostępu muszą być przechowywane w postaci zaszyfrowanej;
- 15) Oprogramowanie musi zapewniać silną politykę haseł lub umożliwiać jej określenie dla użytkowników systemu;
- 16) 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;
- 17) Oprogramowanie musi integrować się z Active Directory w zakresie uwierzytelnienia oraz kontroli dostępu na bazie zdefiniowanych ról;
- 18) Oprogramowanie musi mieć możliwość korzystania z SAML;
- 19) Oprogramowanie musi mieć możliwość definiowania raportów i alertów z wykorzystaniem wszystkich danych zbieranych przez system;
- 20) Oprogramowanie musi mieć wbudowany panel sterowania (Dashboard) z predefiniowaną zawartością dostosowaną do potrzeb określonej roli. Dashboard powinien umożliwiać schodzenie do szczegółów w poszczególnych elementach z poziomu informacji podstawowych;
- 21) Oprogramowanie musi zapewnić możliwość przechowywania wszystkich danych pochodzących z dowolnego silnika skanującego i testującego;
- 22) Oprogramowanie musi umożliwiać przeglądanie tych danych w sposób przejrzysty dla użytkownika, co najmniej w postaci Top 10 podatności, Top 10 systemów zainfekowanych,



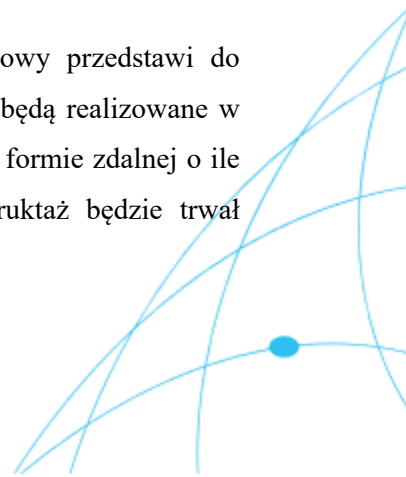
- możliwość filtrowania wykrytych podatności, informacja o połączeniach między systemami klienckimi a serwerami;
- 23) Oprogramowanie musi umożliwiać tworzenie raportów dostępnych w systemie centralnego zarządzania oraz wysyłanych na wskazane adresy email;
 - 24) Oprogramowanie musi zapewniać monitorowanie 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;
 - 25) Oprogramowanie musi zapewnić szyfrowaną komunikację między serwerem zarządzającym a agentem zainstalowanym na stacji roboczej/serwerem;
 - 26) Oprogramowaniu musi umożliwiać na tworzenie oraz uruchamianie skanów aktywnych i pasywnych;
 - 27) Oprogramowanie musi zapewniać możliwość harmonogramowania (planowania 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/-a (uruchomienie jest inicjowane przez Oprogramowanie centralnego zarządzania);
 - 28) Oprogramowanie musi mieć możliwość wykonywania ręcznego i zaplanowanego skanowania określonych hostów lub podsieci z wykorzystaniem skanerów podatności;
 - 29) 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;
 - 30) Oprogramowanie powinno zapewnić możliwość uwierzytelnienia przynajmniej za pomocą poniższych metod podczas skanowania z serwera: login i hasło, klucz ssh, integracja z kerberos, integracja z CyberArk oraz Thycotic/Delinea SecretServer;
 - 31) Skaner pasywny (agentowy) musi posiadać również 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;
 - 32) Skaner pasywny musi umożliwiać zdefiniowanie adresów IP stacji roboczych/serwerów/sieci, które będą podlegać monitorowaniu;
 - 33) Skaner pasywny musi umożliwiać wysyłanie logu Oprogramowania w formacie CEF;



- 34) Skaner pasywny musi umożliwiać tworzenie własnych reguł służących do wykrywania określonych elementów w monitorowanym ruchu;
- 35) Automatyzacja procesów, powinna obejmować co najmniej: skanowanie o zaplanowanym czasie; powiadamianie i alarmowanie administratora o zdefiniowanych zdarzeniach (np. syslog, SMTP, uruchom skan, wygeneruj raport);
- 36) Oprogramowanie musi umożliwiać przeprowadzanie retestów luk/podatności wykrytych wcześniej w celu sprawdzenia czy zostały one poddane działaniem naprawczym;
- 37) Oprogramowanie musi mieć możliwość tworzenia grup dla danych wynikowych;
- 38) Oprogramowanie centralnego zarządzania musi dostarczać wzorce polityk skanowania jak również możliwość zbudowania polityki skanowania od podstaw;
- 39) W ramach budowy polityki skanowania Oprogramowanie musi zezwalać na wybranie podatności jakie będą sprawdzane podczas skanowania, np. w oparciu o CVSS lub CVE;
- 40) 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 patch dla danej podatności, Port/Protokół, data opublikowania podatności, data zauważenia po raz pierwszy podatności, data, kiedy ostatni raz widziana była podatność;
- 41) Administrator musi mieć możliwość zaakceptowania danego ryzyka oraz zmiany poziomu niebezpieczeństwa związanego z daną podatnością dla konkretnego systemu, portu, protokołu;
- 42) 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;
- 43) Oprogramowanie musi umożliwiać tworzenie grup systemów spełniających określone warunki;
- 44) Grupy systemów mogą być tworzone dynamicznie i/lub statycznie;
- 45) Tworzenie nowych grup systemów musi odbywać się również na podstawie wyrażień logicznych takich jak AND, OR, NOT pomiędzy istniejącymi grupami systemów;
- 46) Raportowanie musi być integralną częścią Oprogramowania centralnego zarządzania;
- 47) Oprogramowanie musi posiadać gotowe grupy wzorców raportów udostępnionych przez producenta, które administrator może edytować;
- 48) Oprogramowanie musi pozwalać na budowanie raportu od podstaw;
- 49) Oprogramowanie musi umożliwiać generowanie raportów co najmniej w następujących formatach: PDF, CSV oraz opcjonalnie RTF lub docx;
- 50) Oprogramowanie musi mieć możliwość generowania raportów według harmonogramu oraz na żądanie;



- 51) Oprogramowanie musi mieć możliwość automatycznego wysyłania raportów do wskazanych osób na maila;
- 52) 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;
- 53) Oprogramowanie musi posiadać gotowe wzorce widoków (ang. Dashboard) do Oprogramowania centralnego zarządzania podatnościami, które mogą być edytowane przez administratora systemu;
- 54) Administrator musi mieć możliwość tworzenia widoków od podstaw;
- 55) Oprogramowanie musi posiadać wzorce zgodności z regulacjami, które dostarcza producent, co najmniej dla regulacji CIS, DISA;
- 56) Oprogramowanie musi umożliwiać tworzenie swoich własnych wzorców sprawdzania zgodności bez konieczności kontaktu pomocą techniczną producenta. Producent musi udostępniać informację w jaki sposób można budować swoje własne wzorce sprawdzania zgodności ze standardami przyjętymi u Zamawiającego;
- 57) Oprogramowanie musi umożliwiać wykonywanie skanów audytowych/konfiguracji co najmniej dla systemów i oprogramowania: Windows, Linux (centos i RHEL), fortigate, SQL (MSSQL, MySQL, PostgreSQL);
- 58) Oprogramowanie musi posiadać interfejs API;
- 59) Oprogramowanie musi posiadać integracje z oprogramowaniem Splunk oraz Jira poprzez dedykowaną aplikację/dodatek producenta rozwiązania;
- 60) Oprogramowanie musi umożliwiać na przesyłanie logów do SIEM – Splunk;
- 61) Wykonawca zobowiązany jest przeprowadzić instruktaż dla 2 administratorów Zamawiającego z zakresu instalacji, konfiguracji i zarządzania oprogramowaniem równoważnym, umożliwiającym pełne poznanie produktu równoważnego w terminie do 5 dni roboczych od dnia podpisania bez uwag protokołu odbioru. Zamawiający wyraża zgodę na przeprowadzenie szkolenia w siedzibie Zamawiającego lub online, bądź poprzez przekazanie voucherów;
- 62) Do realizacji usługi instruktażu Wykonawca skieruje osobę posiadającą aktualny certyfikat autoryzowany przez producenta oprogramowania, potwierdzający zaawansowaną wiedzę z Oprogramowania.
- 63) Wykonawca w terminie do 2 dni roboczych od dnia zawarcia umowy przedstawi do zatwierdzenia Zamawiającemu harmonogramy instruktaży. Instruktaże będą realizowane w dni robocze w godzinach 8:00-16:00 w siedzibie Zamawiającego lub w formie zdalnej o ile zostaną spełnione wszystkie wymagania dotyczące instruktażu. Instruktaż będzie trwał



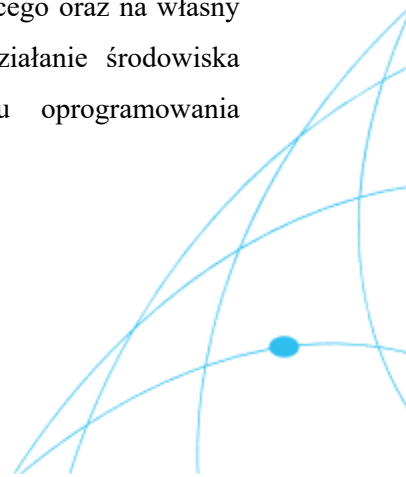
minimum 2 dni robocze (łącznie minimum 14 godzin zegarowych). Zakres tematyczny instruktażu musi obejmować poniższe obszary):

- a) architektura produktu,
- b) poruszanie się po interfejsie użytkownika,
- c) konfigurowanie skanów podatności,
- d) instalacja agenta,
- e) instalacja silnika skanującego,
- f) zdefiniowanie reguł pozwalających na wykonanie skanów podatności dla hostów w wybranej podsieci,
- g) przygotowanie raportów z wykonanych skanów,
- h) konfiguracja harmonogramu skanów okresowych,
- i) zarządzanie użytkownikami i rolami.

64) Wykonawca zobowiązany jest:

- a) zainstalować oprogramowanie równoważne w środowisku systemowo-programowym oraz dokonać poprawnej konfiguracji mechanizmów systemu typu skaner podatności (Vulnerability scanner) oraz zintegrować się z systemami/aplikacjami wykorzystywanymi w ramach działalności Zamawiającego w terminie do 3 dni roboczych od dnia podpisania umowy,
- b) dostarczyć wszelkie dodatkowe licencje - niezbędne do prawidłowego funkcjonowania oprogramowania równoważnego,
- c) w terminie 3 dni roboczych od dnia podpisania umowy przenieść historie (przeprowadzić migrację) wszystkich zrealizowanych dotąd skanów i wykrytych podatności z wykorzystywanego obecnie oprogramowania do oprogramowania równoważnego;
- d) zintegrować oprogramowanie równoważne z oprogramowaniem Splunk oraz Jira w terminie 3 dni roboczych od dnia wdrożenia oprogramowania równoważnego. W przypadku integracji z SIEM dostosować reguły korelacyjne do rozwiązania równoważnego.

65) W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu oprogramowania równoważnego;



-
- 66) Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów używanego i współpracującego z nim oprogramowania u Zamawiającego;
- 67) Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w jego nowszych wersjach;
- 68) W ramach wsparcia producenta wymagany jest:
- dostęp do aktualizacji oprogramowania,
 - dostęp do nowych wersji oprogramowania oraz poprawek,
 - dostęp do nowych sygnatur bezpieczeństwa (podatności),
 - dostęp do bazy wiedzy producenta,
 - Wsparcie producenta na okres 24/36 miesięcy.

