

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest: **rozbudowa oraz przedłużenie ważności licencji Tenable dla rozwiązania typu skaner podatności (Vulnerability scanner)** lub oprogramowanie równoważne.

1. Przedmiot zamówienia obejmuje:

- a) przedłużenie ważności dla posiadanych przez Zamawiającego licencji **Tenable** lub licencji równoważnych, spełniających wymagania wskazane w Załączniku nr 1 do OPZ, wraz z gwarancją producenta świadczoną przez **okres 24 miesięcy**:

Lp.	Nazwa licencji	Liczba licencji	Gwarancja producenta	Data wygaśnięcia gwarancji producenta
1.	Tenable.sc+ - Maintenance Annual TSCCV-M	2000 szt.	24 miesięcy	27.03.2023
2.	Standard Tenable.sc+ Console TSCCV-STNDC-M	1 szt.	24 miesięcy	27.03.2023
3.	TIO-WAS	10 szt.	24 miesięcy	27.03.2023

- b) dostawę licencji **Tenable** lub licencji równoważnych, spełniających wymagania wskazane w Załączniku nr 1 do OPZ, wraz z gwarancją producenta świadczoną przez okres 24 miesięcy:

Lp.	Nazwa licencji	Liczba licencji	Gwarancja producenta
1.	Tenable.sc+ - Maintenance Annual TSCCV-M	200 szt.	24 miesięcy
2.	TIO-WAS	15 szt.	24 miesięcy

2. Termin realizacji:

1. Dostawa zamówienia, o którym mowa w pkt 1 lit. a) i b) musi nastąpić w terminie 7 dni roboczych od zawarcia umowy. Wykonawca udostępni lub przekaze Zamawiającemu klucze licencyjne (aktywacyjne) na adres email: administrator@cez.gov.pl
2. Gwarancja producenta będzie świadczona przez okres, o którym mowa w pkt 1 lit. a) i b) od dnia podpisania Protokołu odbioru, jednakże dla licencji wskazanych w pkt 1 lit. a) nie wcześniej niż od daty wygaśnięcia aktualnej gwarancji producenta.

3. Skaner podatności Tenable wykorzystywany obecnie przez Zamawiającego:

1. Obecnie w systemie wykorzystane są następujące licencje **Tenable** wymienione w pkt. 1 lit. a).

2. Zamawiający ponadto użytkuje licencje **Tenable** wymienione poniżej:

Lp.	Nazwa licencji	Liczba licencji
1.	Tenable.sc+ - Maintenance Annual TSCCV-M	1200 szt.
2.	Tenable.sc+ - Perpetual License TSCCV-P	3200 szt.

4. Gwarancja producenta dla zakresu opisanego w pkt 1 lit. a) i b):

1. W ramach gwarancji producenta wymagany jest:
 - a) dostęp do aktualizacji oprogramowania;
 - b) dostęp do nowych wersji oprogramowania oraz poprawek;
 - c) dostęp do nowych sygnatur bezpieczeństwa;
 - d) dostęp do bazy wiedzy producenta.
2. Zamawiający będzie mógł dokonywać aktualizacji oprogramowania do najnowszej zalecanej przez producenta wersji przez okres obowiązywania umowy.

Załącznik nr 1 do OPZ

I. Zamawiający dopuszcza zaoferowanie rozwiązania równoważnego do oprogramowania Tenable:

1. W przypadku dostarczania oprogramowania równoważnego względem wyspecyfikowanego przez Zamawiającego w Opisie przedmiotu zamówienia, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane oprogramowanie spełnia wszystkie wymagania i warunki określone w Opisie przedmiotu zamówienia, w szczególności w zakresie:
 - a) warunków licencji/sublicencji w każdym aspekcie licencjonowania/sublicencjonowania, które muszą być identyczne lub rozszerzone, przy czym rozszerzony zakres musi zawierać również wszystkie elementy licencjonowania jak dla oprogramowania Tenable,
 - b) funkcjonalności równoważnej oprogramowania, która nie może być gorsza od funkcjonalności wymienionych w pkt III - „Opis wymaganych minimalnych funkcjonalności w przypadku zaoferowania oprogramowania równoważnego w stosunku do oprogramowania Tenable”,
 - c) oprogramowanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać z oprogramowaniem Tenable funkcjonującym u Zamawiającego,
 - d) oprogramowanie równoważne nie może zakłócić pracy środowiska systemowo-programowego Zamawiającego,
 - e) oprogramowanie równoważne musi w pełni współpracować z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie,

- f) oprogramowanie równoważne musi zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienność oprogramowania równoważnego z wyspecyfikowanym oprogramowaniem.
2. W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane oprogramowanie.
 3. 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.
 4. Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów używanego i współpracującego z nim oprogramowania u Zamawiającego.
 5. 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.

II. W przypadku dostawy oprogramowania równoważnego Wykonawca zobowiązany jest:

1. Przeprowadzić Instruktaż dla 4 administratorów Zamawiającego z zakresu instalacji, konfiguracji i zarządzania oprogramowaniem równoważnym, umożliwiającym pełne poznanie produktu równoważnego. Wykonawca w terminie 1 dnia roboczego od dnia zawarcia umowy przedstawi do zatwierdzenia Zamawiającemu harmonogram Instruktażu.
2. Przeprowadzić Instruktaż dla 8 operatorów Zamawiającego z zakresu użytkowania oprogramowania równoważnego, umożliwiającemu pełne poznanie produktu równoważnego.
3. Wykonawca w terminie 1 dnia roboczego od dnia zawarcia umowy przedstawi do zatwierdzenia Zamawiającemu harmonogramy Instruktaży.
4. 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 każdy (łącznie minimum 14 godzin zegarowych każdy). Zakres tematyczny instruktażu będzie zawierał się w niniejszych obszarach:
 - 4.1. Architektura produktu.
 - 4.2. Poruszanie się po interfejsie użytkownika.
 - 4.3. Konfigurowanie skanów podatności.
 - 4.4. Instalacja agenta.
 - 4.5. Instalacja silnika skanującego.

- 4.6. Zdefiniowanie reguł pozwalających na wykonanie skanów podatności dla hostów w wybranej podsieci.
- 4.7. Przygotowanie raportów z wykonanych skanów.
- 4.8. Konfiguracja harmonogramu skanów okresowych.
- 4.9. Zarządzanie użytkownikami i rolami.
5. Zainstalować oprogramowanie równoważne w środowisku systemowo-programowym oraz dokonać poprawnej konfiguracji mechanizmów systemu typu skaner podatności (Vulnerability scanner) oraz zintegrować się z systemami/aplikacjami wytwarzanymi w ramach działalności Zamawiającego w terminie do 3 dni roboczych od dnia podpisania umowy.
6. Dostarczyć wszelkie dodatkowe licencje - niezbędne do prawidłowego funkcjonowania oprogramowania równoważnego.

III. Opis wymaganych minimalnych funkcjonalności w przypadku zaferowania oprogramowania równoważnego w stosunku do oprogramowania Tenable:

1. Rozwiązania równoważne dla skanera podatności (Vulnerability scanner) (zwanego dalej „System”) wraz z niezbędnymi licencjami:
 - 1.1. Dostarczenie Systemu w modelu „on premise”, czyli zainstalowanie na infrastrukturze Zamawiającego.
2. W szczególności System równoważny dla skanera podatności obejmuje:
 - 2.1. Dostarczenie niezbędnych licencji wieczystych typu virtual appliance lub software appliance. Licencje z minimum rocznym wsparciem producenta zapewniającym aktualizacje dla Systemu.
 - 2.2. Dostarczenie najnowszej wersji Systemu na dzień składania oferty.
 - 2.3. Świadczenie usług gwarancyjnych producenta oprogramowania przez okres, o którym o którym mowa w pkt 1 lit. a) i b) od daty podpisania Protokołu odbioru.
 - 2.4. Środowisko Zamawiającego składa się z następujących stacji końcowych:

Liczba hostów o unikalnych adresach IP wymagająca skanów podatności – 3400 sztuk, w tym:

 - a) stacje robocze oparte o system operacyjny z rodziny MS Windows oraz Mac OS,
 - b) serwery rodziny Windows Server oraz Linux dystrybucji RHEL, Centos, Debian.
3. Wymagania minimalne dla Systemu typu skaner podatności:
 - 3.1. Architektura Systemu.
 - 3.1.1. W przypadku dostarczenia Systemu jako maszyny wirtualnej muszą być wspierane środowiska Hyper-V oraz Vmware.
 - 3.1.2. Jeżeli System będzie instalowany jako System na systemie operacyjnym należy dostarczyć produkt, który będzie mógł być zainstalowany na jednym z systemów operacyjnych: Windows Server 2012+, CentOS, RHEL.
 - 3.1.3. Jeżeli System będzie dostępny przez interfejs www, należy dostarczyć rozwiązanie obsługiwane za pośrednictwem popularnych przeglądarek internetowych (Chrome, MS Edge, Firefox) w aktualnych wersjach na dzień składania oferty.

- 3.1.4. Agent Systemu dla stacji końcowej powinien działać na systemach operacyjnych obsługiwanych przez Zamawiającego (Microsoft Windows 8.1, Windows 10, Microsoft Server 2012 i nowszych, macOS oraz Linux (RHEL/CentOS/Debian).
 - 3.1.5. System musi dawać możliwość skanowania urządzeń końcowych działających na różnych systemach operacyjnych oraz znajdujących się w różnych podsięciach.
 - 3.1.6. System (zarówno silnik, jak i konsola) powinien dawać możliwość wdrożenia, jako:
Aplikacja, tj. System instalowany na systemie operacyjnym skanowanego hosta – agent; maszyna wirtualna.
 - 3.1.7. System musi opcjonalnie, w określonych okolicznościach, dawać możliwość zainicjowania skanowania z poziomu: serwera (instalacja stand – alone), aplikacji dowolnego silnika skanującego (skanera), linii poleceń systemu, w którym jest zainstalowany skaner.
 - 3.1.8. System powinien obsługiwać automatyczny/zaplanowany transfer logów z konsoli w celu archiwizacji.
 - 3.1.9. Elementy zarządzające i analityczne Systemu nie mogą być ograniczone liczbą skanerów sieciowych w różnych podsięciach, liczbą hostów w podsieci czy liczbą możliwych do skanowania podsięci.
 - 3.1.10. Wymagana jest możliwość wykorzystania mechanizmu proxy do komunikacji z Internetem.
 - 3.1.11. W przypadku braku dostępu do Internetu System zarządzający ma mieć możliwość aktualizacji za pomocą ręcznej aktualizacji.
 - 3.1.12. W przypadku dostępu do Internetu System ma umożliwiać aktualizację automatyczną jak również ręczną z poziomu panelu zarządzania Systemem.
 - 3.1.13. System musi oferować w przyszłości możliwość skonfigurowania w trybie wysokiej dostępności (dostępność 24x7x365) chroniąc rozwiązanie przed awarią sprzętową, awariami pojedynczych komponentów Systemu lub błędami aplikacji.
 - 3.1.14. 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.
 - 3.1.15. W przypadku użycia w Systemie rozwiązań subskrypcyjnych Zamawiający oczekuje, aby Wykonawca zadeklarował możliwość dostarczenia licencji tymczasowej na czas przesunięcia w procesie zakupowym.
- 3.2. Zarządzanie Systemem.
- 3.2.1. System musi umożliwiać tworzenie indywidualnych kont dla każdego użytkownika/administratora Systemu.
 - 3.2.2. Dostęp do systemu możliwy jedynie po uwierzytelnieniu użytkownika w systemie.
 - 3.2.3. Hasła dostępu muszą być przechowywane w postaci zaszyfrowanej.
 - 3.2.4. System musi zapewniać silną politykę haseł lub umożliwiać jej określenie dla użytkowników Systemu.
 - 3.2.5. System musi umożliwiać konfigurowanie zakresu uprawnień w Systemie z wykorzystaniem predefiniowanych ról wewnętrznych (np. dostęp tylko do raportów, administrator systemu itp.) lub poprzez możliwość przypisania określonych operacji do zdefiniowanych ról.

- 3.2.6. System musi zapewniać segregację obowiązków poprzez umożliwianie dostępu danemu użytkownikowi tylko do wybranych zasobów.
 - 3.2.7. System powinien się integrować z Active Directory w zakresie uwierzytelnienia do Systemu oraz kontroli dostępu na bazie zdefiniowanych ról. Dopuszcza się rozwiązanie używające wewnętrznego mechanizmu uwierzytelniania do Systemu.
 - 3.2.8. System musi mieć możliwość definiowania raportów i alertów z wykorzystaniem wszystkich danych zbieranych przez system.
 - 3.2.9. System 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.
 - 3.2.10. System centralnego zarządzania musi zapewnić możliwość:
 - 3.2.10.1. przechowywania wszystkich danych pochodzących z dowolnego silnika skanującego i testującego,
 - 3.2.10.2. przeglądania 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.
 - 3.2.10.3. tworzenie raportów dostępnych w systemie centralnego zarządzania oraz wysyłanych na wskazane adresy email.
 - 3.2.10.4. monitorowania stanu pracy skanerów, co najmniej przez: okresową weryfikację czy skanery są uruchomione, stan pracy skanera,
 - 3.2.10.5. prezentacji informacji o podatnościach wykrytych przez skanery pasywne,
 - 3.2.10.6. prezentacji wyników skanowania otrzymanych ze skanerów aktywnych,
 - 3.2.10.7. prezentacji informacji o podatnościach w połączeniu z wynikami skanowania ze skanerów aktywnych.
 - 3.2.10.8. Szyfrowaną komunikację między serwerem zarządzającym a agentem zainstalowanym na stacji roboczej/serwerem.
- 3.3. Funkcjonalności Systemu.
- 3.3.1. System musi zapewniać możliwość harmonogramowania (planowania w czasie) oraz jednoczesnego uruchomienia na wybranych lub wszystkich skanerach zainstalowanych na stacjach roboczych i serwerach podłączonych do systemu centralnego zarządzania. W tym również w sytuacji, gdy stacja robocza/serwer/skaner na stacji lub serwerze nie jest uruchomiony/-a (uruchomienie jest inicjowane przez system centralnego zarządzania).
 - 3.3.2. Rozwiązanie musi zapewnić silne uwierzytelnianie tak aby bezpiecznie przesyłać poświadczenia w skanowaniu z uwierzytelnianiem.
 - 3.3.3. System musi mieć możliwość wykonywania ręcznego i zaplanowanego skanowania określonych hostów lub podsięci.
 - 3.3.4. Wszystkie dane zebrane przez zewnętrzne silniki skanujące i testujące muszą być przesyłane niezwłocznie do centralnej bazy i nie mogą być przechowywane przez skaner lokalnie.

- 3.3.5. Skanery aktywne podłączone do systemu centralnego zarządzania muszą mieć możliwość wykonywania skanowania bez uwierzytelnienia oraz za pomocą uwierzytelnienia do systemu skanowanego,
- 3.3.6. Rozwiązanie powinno zapewnić możliwość uwierzytelnienia przynajmniej za pomocą poniższych metod podczas skanowania z serwera:
 - 3.3.6.1. Hasło;
 - 3.3.6.2. Klucz SSH;
 - 3.3.6.3. Kerberos, w tym integracja z Microsoft AD oraz Azure AD opcjonalnie możliwość zapewnienia użycia logowania wieloskładnikowego (MFA).
- 3.3.7. Skaner pasywny musi posiadać również swój własny interfejs webowy, w którym prezentuje 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.
- 3.3.8. Skaner pasywny musi umożliwiać zdefiniowanie adresów IP stacji roboczych/serwerów/sieci, które będą podlegały monitorowaniu.
- 3.3.9. Skaner pasywny musi wykrywać nowo pojawiające się stacje robocze/serwery w monitorowanej sieci i informować o tym system centralnego zarządzania.
- 3.3.10. Skaner pasywny musi zapewnić monitorowanie sieci lokalnej przez 24 godziny i 7 dni w tygodniu, z minimalnym czasem pracy 95% w skali roku, co najmniej w zakresie wykrywania zagrożeń, anomalii w sieci.
- 3.3.11. Skaner pasywny musi pozwalać na import pliku typu pcap w celu jego analizy – ręczny oraz przez system centralnego zarządzania.
- 3.3.12. Skaner pasywny musi umożliwiać wysyłanie logu systemu w formacie CEF.
- 3.3.13. Skaner pasywny musi umożliwiać tworzenie własnych reguł służących do wykrywania określonych elementów w monitorowanym ruchu.
- 3.3.14. Automatyzacja procesów, powinna obejmować co najmniej:
 - 3.3.14.1. skanowanie o zaplanowanym czasie;
 - 3.3.14.2. powiadamianie i alarmowanie administratora o zdefiniowanych zdarzeniach (np. syslog, SMTP, uruchom skan, wygeneruj raport);
 - 3.3.14.3. możliwość tworzenia okien czasowych, w których skanowanie aktywne nie może rozpocząć się dla określonych przez administratora systemów;
- 3.3.15. Wszystkie testy i skany, które mogą wpłynąć na stabilność działania sprawdzanego hosta, powinny być oznaczone w jasny sposób dla administratora.
- 3.3.16. System powinien wspierać poniższe opcje konfiguracji skanowania:
 - 3.3.16.1. Attack Policy.
 - 3.3.16.2. Authentication.
 - 3.3.16.3. Crawler Restrictions.
 - 3.3.16.4. HTTP Headers Performance.
 - 3.3.16.5. Selenium Recordings.
 - 3.3.16.6. Custom URLs.
 - 3.3.16.7. Advanced Options.

Dopuszczalne jest, aby wyżej wymienione funkcjonalności realizowane były z pomocą dodatkowego panelu zarządzania lub dodatkowego systemu, w tym umiejscowionego w chmurze.

- 3.3.17. System musi umożliwiać automatyczne przeprowadzanie retestów luk/podatności wykrytych wcześniej w celu sprawdzenia czy zostały one poddane działaniem naprawczym.
- 3.3.18. Wykryte podatności powinny posiadać odnośniki do otwartych baz podatności, takich jak:
 - 3.3.18.1. Bugtraq.
 - 3.3.18.2. MSFT.
 - 3.3.18.3. CVE.
 - 3.3.18.4. BID.
 - 3.3.18.5. OSVDB ID.
- 3.3.19. System musi mieć możliwość tworzenia grup dla danych wynikowych.
- 3.3.20. System centralnego zarządzania musi dostarczać wzorce polityk skanowania jak również możliwość zbudowania polityki skanowania od podstaw.
- 3.3.21. W ramach budowy polityki skanowania system musi zezwalać na wybranie podatności jakie będą sprawdzane podczas skanowania, np. w oparciu o CVSS lub CVE.
- 3.3.22. Musi istnieć możliwość przeszukiwania wyników co najmniej za pomocą filtrów takich jak:
 - 3.3.22.1. Adres IP.
 - 3.3.22.2. Poziom niebezpieczeństwa.
 - 3.3.22.3. CVE ID.
 - 3.3.22.4. CVSS Score w wersji 2 i nowszych.
 - 3.3.22.5. CVSS Vector w wersji 2 i nowszych.
 - 3.3.22.6. Dostępny exploit.
 - 3.3.22.7. Narzędzi do wykonania ataku (musi istnieć obsługa przynajmniej dla trzech narzędzi, np. Metasploit, Core Impact, Canvas).
 - 3.3.22.8. Data opublikowania patch dla danej podatności.
 - 3.3.22.9. Port/Protokół.
 - 3.3.22.10. Data opublikowania podatności.
 - 3.3.22.11. Data zauważenia po raz pierwszy podatności dla systemu.
 - 3.3.22.12. Data, kiedy ostatni raz widziana była podatność dla systemu.
 - 3.3.22.13. Przydział do określonej grupy systemów.
 - 3.3.22.14. CCE ID.
 - 3.3.22.15. MS Bulletin ID.
- 3.3.23. System musi posiadać swój własny mechanizm przyznawania ocen dla danej podatności (np. od 0 do 10) na podstawie własnego modelu uczenia maszynowego.
- 3.3.24. Administrator musi mieć możliwość zaakceptowania danego ryzyka oraz zmiany poziomu niebezpieczeństwa związanego z daną podatnością dla konkretnego systemu, portu, protokołu.
- 3.3.25. System musi prezentować wyniki skanowania co najmniej za pomocą widoków:
 - 3.3.25.1. Sumarycznie po IP.
 - 3.3.25.2. Sumarycznie po portach.
 - 3.3.25.3. Sumarycznie po grupach systemów.
 - 3.3.25.4. Sumarycznie po CCE.
 - 3.3.25.5. Sumarycznie po CVE.
 - 3.3.25.6. Sumarycznie po MS Bulletin ID.

- 3.3.25.7. Sumarycznie po protokołach.
- 3.3.25.8. Sumarycznie po systemach operacyjnych.
- 3.3.26. System musi umożliwiać tworzenie grup systemów spełniających określone warunki. Grupy systemów mogą być tworzone dynamicznie i/lub statycznie. Tworzenie grup powinno być możliwe w oparciu o co najmniej następujące parametry:
 - 3.3.26.1. System operacyjny.
 - 3.3.26.2. MAC adres.
 - 3.3.26.3. IP adres.
 - 3.3.26.4. Porty TCP i UDP.
 - 3.3.26.5. Ilość dni od wykrycia konkretnej podatności.
 - 3.3.26.6. Czy exploit jest dostępny.
 - 3.3.26.7. Czy istnieje exploit w systemach między innymi Metasploit, Core Impact, Canvas.
- 3.3.27. Tworzenie nowych grup systemów musi odbywać się również na podstawie wyrażeń logicznych takich jak AND, OR, NOT pomiędzy istniejącymi grupami systemów.
- 3.3.28. Raportowanie musi być integralną częścią systemu centralnego zarządzania.
- 3.3.29. System musi posiadać gotowe grupy wzorców raportów udostępnionych przez producenta, które administrator może edytować.
- 3.3.30. System musi pozwalać na budowanie raportu od podstaw używając do tego co najmniej elementów takich jak: rozdziały, iteracja wyników, linie trendów, wykresy kołowe, wykresy słupkowe, tabele, macierze, sekcje tekstów.
- 3.3.31. System musi umożliwiać generowanie raportów co najmniej w następujących formatach: PDF, CSV oraz opcjonalnie RTF.
- 3.3.32. System musi pozwalać na dodanie znaku wodnego podczas generowania raportu.
- 3.3.33. System musi mieć możliwość generowania raportów według harmonogramu oraz na żądanie.
- 3.3.34. System musi mieć możliwość automatycznego wysyłania raportów do wskazanych osób na maila.
- 3.3.35. System musi mieć możliwość wyboru systemów do skanowania w oparciu o przynajmniej następujące możliwości:
 - 3.3.35.1. Podanie listy adresów IP.
 - 3.3.35.2. Wskazanie zakresu adresów IP.
 - 3.3.35.3. Podanie listy adresów IP podsieci.
 - 3.3.35.4. Tworzenie dynamicznie lub statycznie grup systemów.
 - 3.3.35.5. Wskazanie nazw domenowych systemów.
- 3.3.36. System musi posiadać gotowe wzorce widoków (ang. Dashboard) do systemu centralnego zarządzania podatnościami, które mogą być edytowane przez administratora systemu.
- 3.3.37. Administrator musi mieć możliwość tworzenia widoków od podstaw używając co najmniej takich elementów jak:
 - 3.3.37.1. Tabela.
 - 3.3.37.2. Wykres kołowy.
 - 3.3.37.3. Wykres liniowy.
 - 3.3.37.4. Wykres słupkowy.

- 3.3.37.5. Macierz (każda komórka oraz nagłówek definiowany oddzielnie).
- 3.3.38. Administrator do tworzenia widoków musi mieć możliwość używania co najmniej wymienionych filtrów:
 - 3.3.38.1. adres IP.
 - 3.3.38.2. Poziom niebezpieczeństwa.
 - 3.3.38.3. CVE ID.
 - 3.3.38.4. CVSS Score w wersji 2 i nowsze.
 - 3.3.38.5. CVSS Vector w wersji 2 i nowsze.
 - 3.3.38.6. Dostępny exploit.
 - 3.3.38.7. Narzędzie do wykonania ataku (musi istnieć obsługa przynajmniej dla trzech narzędzi, np. Metasploit, Core Impact, Canvas).
 - 3.3.38.8. Data opublikowania patch'a dla danej podatności.
 - 3.3.38.9. Port, protokół.
 - 3.3.38.10. Data opublikowania podatności.
 - 3.3.38.11. Data pierwszy raz zauważenia podatności dla systemu.
 - 3.3.38.12. Data, kiedy ostatni raz widziana była podatność dla systemu.
 - 3.3.38.13. Przydział do określonej grupy systemów.
 - 3.3.38.14. CCE ID.
 - 3.3.38.15. MS Bulletin ID.
- 3.3.39. System musi posiadać wzorce zgodności z regulacjami, które dostarcza producent, co najmniej dla regulacji CIS, DISA.
- 3.3.40. System musi umożliwiać tworzenie swoich własnych wzorców sprawdzania zgodności bez konieczności kontaktu z supportem producenta. Producent musi udostępniać informację w jaki sposób można budować swoje własne wzorca sprawdzania zgodności ze standardami przyjętymi w firmie.
- 3.3.41. System musi umożliwiać wykonywanie skanów audytowych/konfiguracji co najmniej dla systemów:
 - 3.3.41.1. Windows.
 - 3.3.41.2. Unix.
 - 3.3.41.3. Vmware.
 - 3.3.41.4. Cisco.
 - 3.3.41.5. Fortigate.
 - 3.3.41.6. Oracle.
 - 3.3.41.7. MySQL.
 - 3.3.41.8. SQL Server.
 - 3.3.41.9. PostgreSQL.
 - 3.3.41.10. Juniper.
- 3.4. Funkcjonalność kontroli aplikacji powinna być standardową częścią rozwiązania, a skanowanie powinno zawierać testy sprawdzające (co najmniej OWASP). Dopuszczalne jest, aby funkcjonalność ta realizowana była z pomocą dodatkowego panelu zarządzania lub dodatkowego systemu, w tym umiejscowionego w chmurze oraz dostępnego w modelu

subskrypcyjnym z rocznym wsparciem producenta. Zamawiający zamierza objąć skanowaniem nie mniej niż 25 FQDN.

3.5. Funkcjonalności dodatkowe Systemu.

3.5.1. System powinien integrować się systemami zarządzania aktualizacjami w celu sprawdzenia czy wynik ze skanowania pokrywa się z informacjami z tych systemów co najmniej z takimi systemami jak:

3.5.1.1. Microsoft SCCM.

3.5.1.2. Microsoft WSUS.

3.5.1.3. Red Hat Satellite Server.

3.5.2. System powinien umożliwiać ciągłe monitorowanie ruchu w sieci w celu wykrycia podejrzanych przepływów sieciowych z lub do podatnych usług, nieznanymi urządzeniami, botnetów lub serwerów Command and Control (tzw. C&C).

3.5.3. System powinien używać analizy statystycznej oraz monitorowania anomalii w zachowaniu na zewnętrznych źródłach logów w celu automatycznego wykrywania podejrzanych aktywności.

3.5.4. System powinien oferować poza wymienionymi w pkt. 4.3.39 wzorce zgodności z regulacjami takimi jak: CERT, STIG, DHS CDM, FISMA, PCI DSS, HIPAA/HITECH.

3.5.5. System powinien oferować możliwość integracji z systemami firm trzecich do zarządzania aktualizacjami.