Załącznik nr 1 do Zapytania

Opis Przedmiotu Zamówienia

1. **Przedmiot zamówienia.**
   1.1. Przedmiotem zamówienia jest **Zakup systemu typu skaner podatności.**
   1.2. Realizacja przedmiotu zamówienia polega na dostarczeniu i wdrożeniu rozwiązania typu skaner podatności (Vulnerability scanner) (zwanego dalej jako: „System") wraz z niezbędnymi licencjami oraz świadczeniu usługi gwarancji dla wdrożonego systemu. System ma być dostarczony w modelu „on premise" czyli musi być zainstalowany na infrastrukturze Zamawiającego.
   1.3. W szczególności przedmiot zamówienia obejmuje:
      1.3.1. Dostarczenie niezbędnych licencji wieczystych typu virtual appliance lub software appliance. Licencje z minimum rocznym wsparciem producenta zapewniającym aktualizacje dla Systemu.
      1.3.2. Dostarczenie najnowszej wersji Systemu na dzień składania oferty.
      1.3.3. Świadczenie usług gwarancyjnych producenta oprogramowania przez okres 12 miesięcy od daty podpisania Protokołu odbioru.
   1.4. Środowisko Zamawiającego składa się z następujących stacji końcowych:
      1.4.1. Liczba hostów o unikalnych adresach IP wymagająca skanów podatności – 1500 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.
   1.5. Zamawiający przewiduje możliwość udzielenia zamówienia opcjonalnego w zakresie objęcia Systemem dodatkowych hostów o unikalnych adresach IP w wymiarze do 80% względem wymagań zawartych łącznie w pkt 1.4.
   1.6. Termin realizacji Zamówienia podstawowego wynosi do 20 Dni roboczych od dnia podpisania Umowy.
   1.7. Termin realizacji Zamówienia opcjonalnego wynosi do 5 Dni roboczych od dnia Zlecenia opcji.

2. **Harmonogram realizacji przedmiotu zamówienia:**

Zamówienie podstawowe zostanie zrealizowane w terminie nie dłuższym niż 20 Dni roboczych, liczonym od dnia zawarcia Umowy, w podziale na niżej określone etapy:

Etap I – Opracowanie harmonogramu wdrożenia.

W ramach realizacji etapu Wykonawca:

2.1. W terminie do 3 dni roboczych od daty podpisania umowy, przygotuje i przedstawi Zamawiającemu harmonogram wdrożenia Systemu.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

2.2. Przygotuje opis niezbędnych prac w celu wdrożenia Systemu wraz ze wskazaniem podziału obowiązków pomiędzy Zamawiającego i Wykonawcę w modelu RACI.

2.3. Przedstawi listę pracowników Wykonawcy odpowiedzialnych za wykonanie poszczególnych etapów zgodnie z przedstawionym wykazem podziału obowiązków w w/w formacie RACI wraz z danymi teleadresowymi: minimalnie z numerem telefonu komórkowego oraz adresem email.

2.4. Opracuje scenariusze testowe Systemu:

2.4.1. Scenariusze testowe muszą zawierać propozycje testów wydajnościowych, funkcjonalnych i bezpieczeństwa.

2.4.2. Scenariusze testowe będą przygotowane przez Wykonawcę i wymagają zatwierdzenia przez Zamawiającego.

Etap II - Analiza przedwdrożeniowa.

W ramach realizacji etapu Wykonawca:

2.5. Wykona analizę infrastruktury informatycznej Zamawiającego, która zostanie objęta Systemem, potrzeb użytkownika i wymagań funkcjonalnych odnośnie konfiguracji Sytemu, której wynikiem będzie plan wdrożenia Systemu u Zamawiającego.

2.6. Przygotuje i przedstawi Zamawiającemu Projekt techniczny Systemu (architektura Systemu) określający:

2.6.1. Wykaz oprogramowania i licencji niezbędnych do poprawnej pracy Systemu;

2.6.2. Wymogi takie jak ilość urządzeń fizycznych/maszyn wraz z dokładnymi parametrami jak vCPU, vRAM, vHDD wirtualnych wymaganych dla wszystkich składowych Systemu.

2.7. Uzgodni z Zamawiającym polityki/reguły bezpieczeństwa Systemu oraz ich wdrożenie.

2.8. Dostarczy System i licencje niezbędne do poprawnej pracy Systemu.

Etap III – Wdrożenie, konfiguracja i testy Systemu.

W ramach realizacji etapu Wykonawca:

2.9. Wdroży w infrastrukturze Zamawiającego System zgodnie z zaakceptowanym harmonogramem, planem wdrożenia Systemu oraz Projektem technicznym Systemu z uwzględnieniem analizy przedwdrożeniowej oraz warunkami opisanymi w pkt 3 OPZ.

2.10. Wykona pełną konfigurację i parametryzację Systemu zgodnie z Projektem technicznym będącym wynikiem analizy przedwdrożeniowej .

2.11. Przeprowadzi testy akceptacyjne.

2.12. Dostarczy Dokumentację powykonawczą dla Zamawiającego.

2.13. Przeprowadzi instruktaż dla użytkowników Systemu zgodnie z warunkami opisanymi w pkt. 6.

3. Wdrożenie Systemu.

W ramach realizacji Etapu III, Wykonawca dokona wdrożenia Systemu , rozumianego jako:

3.1. Instalacja Systemu zgodna z planem wdrożenia na udostępnionym przez Zamawiającego środowisku opisanym w pkt 1.4 OPZ. Szczegóły systemowe zostaną przekazane Wykonawcy po podpisaniu umowy.

3.2. Przygotowanie konfiguracji Systemu zgodnie z projektem technicznym Systemu oraz wdrożenie polityk bezpieczeństwa odzwierciedlających obecnie posiadaną konfigurację i wiedzę o aktualnych zagrożeniach.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

3.3. Skonfigurowanie logowania zdarzeń na Systemie i umożliwienia zapisywania ich na zewnętrznym serwerze logowania udostępnionym przez Zamawiającego (możliwość zapisywania/eksportu logów w formacie Syslog/CEF/EventLog).

3.4. Przeprowadzenie testów wydajnościowych, funkcjonalnych i bezpieczeństwa zainstalowanego Systemu, zgodnie z opracowanymi w pkt 2.4 OPZ scenariuszami, z udziałem Zamawiającego. Wynikiem testów będzie raport potwierdzający spełnienie zawartych w pkt 4.3 Obligatoryjnych funkcjonalności Systemu. Raport potwierdzony zostanie przez obie strony.

3.5. Przygotowanie i dostarczenie Dokumentacji powykonawczej oraz dokumentacji użytkownika (administratora/operatora) systemu. Dokumentacja powinna zawierać architekturę rozwiązania, spis wszystkich wdrożonych polityk bezpieczeństwa, opis testów akceptacyjnych i funkcjonalnych rozwiązania, opis konfiguracji systemu (w tym nietypowe ustawienia) oraz instrukcję dla użytkownika/administratora systemu.

3.6. Za pełne wdrożenie Systemu uznaje się instalację systemu, przeprowadzenie z wynikiem pozytywnym testów akceptacyjnych, funkcjonalnych i bezpieczeństwa, integracja z systemem logowania zdarzeń Zamawiającego, dostarczenie kompletu dokumentacji, przeprowadzenie instruktażu opisanego w pkt 6, obustronne podpisanie protokołu odbioru.

4. Wymagania minimalne dla Systemu typu skaner podatności:

4.1. **Architektura Systemu.**

4.1.1. W przypadku dostarczenia Systemu jako maszyny wirtualnej muszą być wspierane środowiska Hyper-V oraz Vmware.

4.1.2. 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.

4.1.3. 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.

4.1.4. 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)).

4.1.5. System musi dawać możliwość skanowania urządzeń końcowych działających na różnych systemach operacyjnych oraz znajdujących się w różnych podsieciach.

4.1.6. System (zarówno silnik jak i konsola) powinien dawać możliwość wdrożenia, jako:

4.1.6.1. aplikacja tj. System instalowany na systemie operacyjnym skanowanego hosta – agent;

4.1.6.2. maszyna wirtualna;

4.1.7. 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.

4.1.8. System powinien obsługiwać automatyczny/zaplanowany transfer logów z konsoli w celu archiwizacji.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

4.1.9. Elementy zarządzające i analityczne Systemu nie mogą być ograniczone liczbą skanerów sieciowych w różnych podsieciach, liczbą hostów w podsieci czy liczbą możliwych do skanowania podsieci.

4.1.10. Wymagana jest możliwość wykorzystania mechanizmu proxy do komunikacji z Internetem.

4.1.11. W przypadku braku dostępu do Internetu System zarządzający ma mieć możliwość aktualizacji za pomocą ręcznej aktualizacji.

4.1.12. W przypadku dostępu do Internetu System ma umożliwiać aktualizację automatyczną jak również ręczną z poziomu panelu zarządzania Systemem.

4.1.13. 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.

4.1.14. 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.

4.1.15. W przypadku użycia w Systemie rozwiązań subskrypcyjnych Zamawiający oczekuje aby Wykonawca zadeklarował możliwość dostarczenia licencji tymczasowej na czas przesunięć w procesie zakupowym.

4.2. **Zarządzanie Systemem.**

4.2.1. System musi umożliwiać tworzenie indywidualnych kont dla każdego użytkownika/administratora Systemu.

4.2.2. Dostęp do systemu możliwy jedynie po uwierzytelnieniu użytkownika w systemie.

4.2.3. Hasła dostępu muszą być przechowywane w postaci zaszyfrowanej.

4.2.4. System musi zapewniać silną politykę haseł lub umożliwiać jej określenie dla użytkowników Systemu.

4.2.5. 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.

4.2.6. System musi zapewniać segregację obowiązków poprzez umożliwianie dostępu danemu użytkownikowi tylko do wybranych zasobów.

4.2.7. 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.

4.2.8. System musi mieć możliwość definiowania raportów i alertów z wykorzystaniem wszystkich danych zbieranych przez system.

4.2.9. System musi mieć wbudowany panel sterowania (Dashboard) z predefiniowaną zawartością dostosowaną do potrzeb określonej roli. Dashboard powinien umożliwiać schodzenie do szczegółów w poszczególnych elementów z poziomu informacji podstawowych.

4.2.10. System centralnego zarządzania musi zapewnić możliwość:

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

4.2.10.1. przechowywania wszystkich danych pochodzących z dowolnego silnika skanującego i testującego,

4.2.10.2. 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.

4.2.10.3. tworzenie raportów dostępnych w systemie centralnego zarządzania oraz wysyłanych na wskazane adresy email.

4.2.10.4. monitorowania stanu pracy skanerów, co najmniej przez: okresową weryfikację, czy skanery są uruchomione, stan pracy skanera,

4.2.10.5. prezentacji informacji o podatnościach wykrytych przez skanery pasywne,

4.2.10.6. prezentacji wyników skanowania otrzymanych ze skanerów aktywnych,

4.2.10.7. prezentacji informacji o podatnościach w połączeniu z wynikami skanowania ze skanerów aktywnych.

4.2.10.8. Szyfrowaną komunikację między serwerem zarządzającym a agentem zainstalowanym na stacji roboczej/serwerem.

4.3. **Funkcjonalności Systemu.**

4.3.1. 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).

4.3.2. Rozwiązanie musi zapewnić silne uwierzytelnianie tak aby bezpiecznie przesyłać poświadczenia w skanowaniu z uwierzytelnianiem.

4.3.3. System musi mieć możliwość wykonywania ręcznego i zaplanowanego skanowania określonych hostów lub podsieci.

4.3.4. Wszystkie dane zebrane przez zewnętrzne silniki skanujące i testujące muszą być przesyłane niezwłocznie do centralnej bazy i nie mogą być przechowywane przez skaner lokalnie.

4.3.5. Skanery aktywne podłączone do systemu centralnego zarządzania muszą mieć możliwość wykonywania skanowania bez uwierzytelnienia oraz za pomocą uwierzytelnienia do systemu skanowanego,

4.3.6. Rozwiązanie powinno zapewnić możliwość uwierzytelnienia przynajmniej za pomocą poniższych metod podczas skanowania z serwera:

4.3.6.1. Hasło

4.3.6.2. Klucz SSH

4.3.6.3. Kerberos, w tym integracja z Microsoft AD oraz Azure AD opcjonalnie możliwość zapewnienia użycia logowania wieloskładnikowego (MFA).

4.3.7. Skaner pasywny musi posiadać również swój własny interfejs webowy w którym prezentuje aktualny stan pracy, między innymi informacje o połączeniach między

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

systemami klienckimi a serwerami, IP stacji roboczych/serwerów, stan połączenia z centralnym systemem zarządzania, podgląd logu pracy.

4.3.8. Skaner pasywny musi umożliwiać zdefiniowanie adresów IP stacji roboczych/serwerów/sieci, które będą podlegać monitorowaniu.

4.3.9. Skaner pasywny musi wykrywać nowo pojawiające się stacje robocze/serwery w monitorowanej sieci i informować o tym system centralnego zarządzania.

4.3.10. 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.

4.3.11. Skaner pasywny musi pozwalać na import pliku typu pcap w celu jego analizy – ręczny oraz przez system centralnego zarządzania.

4.3.12. Skaner pasywny musi umożliwiać wysyłanie logu systemu w formacie CEF.

4.3.13. Skaner pasywny musi umożliwiać tworzenie własnych reguł służących do wykrywania określonych elementów w monitorowanym ruchu.

4.3.14. Automatyzacja procesów, powinna obejmować co najmniej:

4.3.14.1. skanowanie o zaplanowanym czasie;

4.3.14.2. powiadamianie i alarmowanie administratora o zdefiniowanych zdarzeniach (np. syslog, SMTP, uruchom skan, wygeneruj raport);

4.3.14.3. możliwość tworzenia okien czasowych, w których skanowanie aktywne nie może rozpocząć się dla określonych przez administratora systemów;

4.3.15. Wszystkie testy i skany, które mogą wpłynąć na stabilność działania sprawdzanego hosta, powinny być oznaczone w jasny sposób dla administratora.

4.3.16. System powinny wspierać poniższe opcje konfiguracji skanowania:

4.3.16.1. Attack Policy

4.3.16.2. Authentication

4.3.16.3. Crawler Restrictions

4.3.16.4. HTTP Headers Performance

4.3.16.5. Selenium Recordings

4.3.16.6. Custom URLs

4.3.16.7. Advanced Options

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

4.3.17. System musi umożliwiać automatyczne przeprowadzanie retestów luk/podatności wykrytych wcześniej w celu sprawdzenia czy zostały one poddane działaniem naprawczym.

4.3.18. Wykryte podatności powinny posiadać odnośniki do otwartych baz podatności, takich jak:

4.3.18.1. Bugtraq

4.3.18.2. MSFT

4.3.18.3. CVE

4.3.18.4. BID

4.3.18.5. OSVDB ID

4.3.19. System musi mieć możliwość tworzenia grup dla danych wynikowych.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

4.3.20. System centralnego zarządzania musi dostarczać wzorce polityk skanowania jak również możliwość zbudowania polityki skanowania od podstaw,

4.3.21. W ramach budowy polityki skanowania system musi zezwalać na wybranie podatności jakie będą sprawdzane podczas skanowania, np. w oparciu o CVSS lub CVE

4.3.22. Musi istnieć możliwość przeszukiwania wyników co najmniej za pomocą filtrów takich jak:

4.3.22.1. Adres IP,

4.3.22.2. Poziom niebezpieczeństwa,

4.3.22.3. CVE ID,

4.3.22.4. CVSS Score w wersji 2 i nowszych,

4.3.22.5. CVSS Vector w wersji 2 i nowszych,

4.3.22.6. Dostępny exploit,

4.3.22.7. narzędzi do wykonania ataku (musi istnieć obsługa przynajmniej dla trzech narzędzi, np. Metasploit, Core Impact, Canvas),

4.3.22.8. data opublikowania patch dla danej podatności,

4.3.22.9. port/protokół,

4.3.22.10. data opublikowania podatności,

4.3.22.11. data zauważenia po raz pierwszy podatności dla systemu,

4.3.22.12. data kiedy ostatni raz widziana była podatność dla systemu,

4.3.22.13. przydział do określonej grupy systemów,

4.3.22.14. CCE ID,

4.3.22.15. MS Bulletin ID,

4.3.23. System musi posiadać swój własny mechanizm przyznawania ocen dla danej podatności (np. od 0 do 10) na podstawie własnego modelu uczenia maszynowego.

4.3.24. Administrator musi mieć możliwość zaakceptowania danego ryzyka oraz zmiany poziomu niebezpieczeństwa związanego z daną podatnością dla konkretnego systemu, portu, protokołu.

4.3.25. System musi prezentować wyniki skanowania co najmniej za pomocą widoków:

4.3.25.1. sumarycznie po IP,

4.3.25.2. sumarycznie po portach,

4.3.25.3. sumarycznie po grupach systemów,

4.3.25.4. sumarycznie po CCE,

4.3.25.5. sumarycznie po CVE,

4.3.25.6. sumarycznie po MS Bulletin ID,

4.3.25.7. sumarycznie po protokołach,

4.3.25.8. sumarycznie po systemach operacyjnych,

4.3.26. 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:

4.3.26.1. system operacyjny,

4.3.26.2. MAC adres,

4.3.26.3. IP adres,

4.3.26.4. porty TCP i UDP,

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

4.3.26.5. ilość dni od wykrycia konkretnej podatności,

4.3.26.6. czy exploit jest dostępny,

4.3.26.7. czy istnieje exploit w systemach między innymi Metasploit, Core Impact, Canvas,

4.3.27. Tworzenie nowych grup systemów musi odbywać się również na podstawie wyrażeń logicznych takich jak AND, OR, NOT pomiędzy istniejącymi grupami systemów,

4.3.28. Raportowanie musi być integralną częścią systemu centralnego zarządzania,

4.3.29. System musi posiadać gotowe grupy wzorców raportów udostępnionych przez producenta, które administrator może edytować.

4.3.30. 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.

4.3.31. System musi umożliwiać generowane raportów co najmniej w następujących formatach: PDF, CSV oraz opcjonalnie RTF.

4.3.32. System musi pozwalać na dodanie znaku wodnego podczas generowania raportu,

4.3.33. System musi mieć możliwość generowana raportów według harmonogramu oraz na żądanie,

4.3.34. System musi mieć możliwość automatycznego wysyłania raportów do wskazanych osób na maila,

4.3.35. System musi mieć możliwość wyboru systemów do skanowania w oparciu o przynajmniej następujące możliwości:

4.3.35.1. podanie listy adresów IP,

4.3.35.2. wskazanie zakresu adresów IP,

4.3.35.3. podanie listy adresów IP podsieci,

4.3.35.4. tworzenie dynamicznie lub statycznie grup systemów,

4.3.35.5. wskazanie nazw domenowych systemów.

4.3.36. System musi posiadać gotowe wzorce widoków (ang. Dashboard) do systemu centralnego zarządzania podatnościami, które mogą być edytowane przez administratora systemu,

4.3.37. Administrator musi mieć możliwość tworzenia widoków od podstaw używając co najmniej takich elementów jak:

4.3.37.1. tabela,

4.3.37.2. wykres kołowy,

4.3.37.3. wykres liniowy,

4.3.37.4. wykres słupkowy,

4.3.37.5. macierz (każda komórka oraz nagłówek definiowany oddzielnie),

4.3.38. Administrator do tworzenia widoków musi mieć możliwość używania co najmniej wymienionych filtrów:

4.3.38.1. adres IP,

4.3.38.2. Poziom niebezpieczeństwa,

4.3.38.3. CVE ID,

4.3.38.4. CVSS Score w wersji 2 i nowsze,

4.3.38.5. CVSS Vector w wersji 2 i nowsze,

4.3.38.6. Dostępny exploit,

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

4.3.38.7. narzędzie do wykonania ataku (musi istnieć obsługa przynajmniej dla trzech narzędzi, np. Metasploit, Core Impact, Canvas),

4.3.38.8. data opublikowania patch'a dla danej podatności,

4.3.38.9. port, protokół,

4.3.38.10. data opublikowania podatności,

4.3.38.11. data pierwszy raz zauważenia podatności dla systemu,

4.3.38.12. data kiedy ostatni raz widziana była podatność dla systemu,

4.3.38.13. przyodział do określonej grupy systemów,

4.3.38.14. CCE ID,

4.3.38.15. MS Bulletin ID,

4.3.39. System musi posiadać wzorce zgodności z regulacjami, które dostarcza producent, co najmniej dla regulacji CIS, DISA.

4.3.40. System musi umożliwiać tworzenie swoich własnych wzorców sprawdzania zgodności bez konieczności kontaktu z suportem producenta. Producent musi udostępniać informację w jaki sposób można budować swoje własne wzorca sprawdzania zgodności ze standardami przyjętymi w firmie,

4.3.41. System musi umożliwiać wykonywanie skanów audytowych/konfiguracji co najmniej dla systemów:

4.3.41.1. Windows,

4.3.41.2. Unix,

4.3.41.3. Vmware,

4.3.41.4. Cisco,

4.3.41.5. Fortigate,

4.3.41.6. Oracle,

4.3.41.7. MySQL,

4.3.41.8. SQL Server,

4.3.41.9. PostgreSQL,

4.3.41.10. Juniper.

4.3.42. 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 10 FQDN.

4.4. **Funkcjonalności dodatkowe Systemu.**

4.4.1. 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:

4.4.1.1. Microsoft SCCM,

4.4.1.2. Microsoft WSUS,

4.4.1.3. Red Hat Satellite Server.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

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

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

4.4.4. 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.

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

5. Gwarancja

W ramach realizacji przedmiotu zamówienia, wykonawca będzie świadczył usługi gwarancyjne na zasadach wskazanych w Załączniku nr 4 do Umowy.

6. Instruktaż dla pracowników Zamawiającego

Wykonawca przeprowadzi dla nie więcej niż 6 pracowników Zamawiającego instruktaż, który przygotuje wskazanych pracowników do samodzielnego konfigurowania Systemu, operowania Systemem z poziomu administratora oraz użytkownika oraz wykorzystywania Systemu skonfigurowanego w specyficznej infrastrukturze Zamawiającego.

6.1. Lista uczestników instruktażu zostanie ustalona drogą mailową z Wykonawcą po podpisaniu umowy.

6.2. Instruktaż zostanie zorganizowany w czasie trwania wdrożenia Systemu opisanego w pkt 3.

6.3. Termin przeprowadzenia instruktażu zostanie ustalony pomiędzy Zamawiającym a Wykonawcą.

6.4. Instruktaż będzie realizowany w dni robocze w godzinach 8:00-16:00 w siedzibie Zamawiającego lub zdalnie za zgodą Zamawiającego. Instruktaż może się odbyć w postaci zdalnego spotkania o ile zostaną spełnione wszystkie wymagania instruktażu.

6.5. Instruktaż będzie trwał minimum 2 Dni Robocze (łącznie minimum 16 godzin zegarowych).

6.6. Harmonogramy zajęć zostaną ustalone drogą mailową z Zamawiającym.

6.7. Wykonawca musi posiadać autoryzację producenta Systemu w zakresie prowadzenia instruktażu z wdrożonego u Zamawiającego Systemu.

6.8. Dla uczestników instruktażu Wykonawca przygotuje środowisko testowe z zainstalowaną wersją Systemu tożsamą dla wdrożonego u Zamawiającego Systemu pozwalające na zapoznanie się, z elementami interfejsu graficznego oraz wykonanie ćwiczeń w warunkach możliwie zbliżonych do realnych. Dopuszczalne jest wykorzystanie wdrożonego u Zamawiającego Systemu na wybranych wcześniej przez Zamawiającego środowiskach do testowania.

6.9. Wykonawca zapewni dla każdego uczestnika wersję elektroniczną materiałów dydaktycznych zawierających streszczenie/omówienie wszystkich zagadnień zawartych w programie instruktażu oraz prezentacje wykorzystane podczas instruktażu;

6.10. Jeśli na potrzeby realizacji instruktażu powstaną materiały edukacyjne będące utworami w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2019. poz. 1231) będą udostępnione na wolnej licencji zapewniającej licencjobiorcy prawo do

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

dowolnego wykorzystywania utworów do celów komercyjnych i niekomercyjnych, tworzenia i rozpowszechniania kopii utworów w całości lub we fragmentach oraz wprowadzania zmian i rozpowszechniania utworów zależnych.

6.11. Zakres tematyczny instruktażu będzie zawierał się w niniejszych obszarach:

6.11.1. Architektura produktu

6.11.2. Poruszanie się po interfejsie użytkownika

6.11.3. Konfigurowanie skanów podatności

6.11.4. Instalacja agenta.

6.11.5. Instalacja silnika skanującego.

6.11.6. Zdefiniowanie reguł pozwalających na wykonanie skanów podatności dla hostów w wybranej podsieci.

6.11.7. Przygotowanie raportów z wykonanych skanów.

6.11.8. Konfiguracja harmonogramu skanów okresowych.

6.11.9. Zarządzanie użytkownikami i rolami.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706