Łukasiewicz
Instytut Technik Innowacyjnych EMAG

OPIS PRZEDMIOTU ZAMÓWIENIA

„Dostawa oprogramowania do skanów podatności webaplikacji, kontenerów, sieci i serwerów" – nr postępowania FH/ 01/ 03/ 23

Oferowany przedmiot zamówienia musi spełniać wymagania określone przez Zamawiającego, tj. posiadać parametry i funkcjonalności nie gorsze (co najmniej takie same lub lepsze) od określonych w poniższej tabeli.

Opis oprogramowania	**Oprogramowanie do skanów podatności webaplikacji, kontenerów, sieci i serwerów**
Warunki licencji	1. Licencja nie może być ograniczona ilością skanowanych adresów IP w zakresie skanowania sieci i serwerów 2. Licencja na zakres dotyczący skanowania sieci i serwerów musi umożliwiać instalację skanera w infrastrukturze klienta 3. Licencja na ma umożliwiać skanowanie co najmniej 300 webaplikacji i kontenerów oraz w ramach tej ilości instalację agentów do skanowania systemów operacyjnych na stacjach do których skaner nie ma bezpośredniego dostępu 4. Wsparcie producenta, które obejmuje aktualizacje oraz wsparcie przez okres 12 mc. aktywności subskrypcji.
Cechy oprogramowania	**Zakres dotyczący skanowania sieci i serwerów:** Przedmiotem zamówienia jest skaner podatności spełniający poniższe funkcje: - musi być zarządzany przez przeglądarkę, zabrania się używania jakiegokolwiek grubego agenta, - musi mieć opcję dostarczenia jako oprogramowanie i maszyna wirtualna. W przypadku dostarczenia jako maszyna wirtualna muszą być wspierane środowiska Hyper-V oraz Vmware. W przypadku systemu operacyjnego na którym będzie instalowany produkt jako oprogramowanie, muszą być wpierane co najmniej systemy operacyjne: Ubuntu 14.04/16.04, SUSE Enterprise 11 SP4/12, Windows Server 2008 SP2/2008 R2 SP2/2012/ 2012 R2/2016 (64 bit)/2019, Windows 7 SP1,8.1,10 (32 bit), Fedora 24/25, CentOS 7/8, Oracle Linux 6/7/8, macOS 10.10 – 10.15, - system musi mieć możliwość pracy bez dostępu do Internetu, a dostarczanie nowych reguł skanowania musi odbywać się za pomocą ręcznej aktualizacji z poziomu interfejsu, - interfejs systemu musi przedstawiać informacje o systemie takie jak użycie CPU, pamięci, ilość skanowanych systemów, ilość sesji TCP, ruch przesyłany i odbierany do/z skanera, - musi być możliwość określenia ilości jednocześnie skanowanych systemów jak również, maksymalna ilość równoczesnych sesji TCP do pojedynczego skanowanego systemu, maksymalna ilość równoczesnych sesji TCP w przypadku wykonania skanu sieci,

	- możliwość wymuszenia polityki haseł dla administratorów logujących się do systemu. - musi być dostarczony z predefiniowanymi politykami skanowania minimum polityka dotycząca wykrycia hostów w sieci, WannaCry, jak również polityka skanowania pod kontem artefaktów związanych z malwarem, - musi być możliwość skanowania systemów pod kontem zgodności z regulacjami takimi jak CIS, DISA. W przypadku zgodności z regulacjami, producent musi dostarczać gotowe wzorce polityk zgodności z CIS, DISA jak również musi być możliwość zbudowania własnej polityki sprawdzania pod kontem zgodności z przyjętymi regulacjami w firmie w oparciu o dokumentację dostarczoną przez producenta. Wzorce zgodności z regulacjami dostarczone przez producenta muszą być możliwe do edycji. Sprawdzanie systemu pod kontem zgodności z regulacjami oraz dostęp do wzorców regulacji na stronie producenta nie wymaga żadnej dodatkowej licencji, - musi być możliwość tworzenia własnej polityki skanowania w której administrator wybiera jakie podatności będą sprawdzane, - system musi umożliwiać skanowanie z uwierzytelnieniem i bez uwierzytelnienia. W przypadku skanowania z uwierzytelnieniem muszą być wspierane następujące metody: - Windows – Kerberos, LM Hash, NTLM Hash, hasło - SSH – kluczy publiczny, Kerberos, hasło, certyfikat, - SNMP3 - w przypadku skanowania systemów opartych o system linux/unix musi być możliwość podniesienia uprawnień przynajmniej za pomocą poniższych technik: .k5login, Cisco (enable), dzdo, pbrun, su, sudo, - system pozwala na tworzenie jak również używanie dostarczonych przez producenta wzorców skanowania pod kontem konfiguracji systemów bezpieczeństwa i sieciowych. Muszą być wspierane przynajmniej wymienione systemy: FireEye, SonicWall, Fortinet FortiGate, BlueCoat ProxySG, Amazon AWS, Microsoft Azure, - system zezwala na tworzenie harmonogramu skanowania podatności jak również uruchomienia na żądanie, - system musi pozwalać na porównanie wyników dwóch wykonanych skanów, - system musi umożliwiać sprawdzenie konfiguracji systemu bez dostępu do niego. Sprawdzenie ma być dokonana na podstawie pliku konfiguracyjnego. Muszą być wspierane przynajmniej systemy jak: FireEye, SonicWall ,Fortinet FortiGate, BlueCoat ProxySG, - system musi umożliwiać filtrowanie wyników przynajmniej po takich parametrach jak: CVE, CVSS , CVSS v3/v2, Czy jest dostępny exploit, hostname, kiedy była upubliczniona aktualizacja na dana podatność, port, protokół, wrażliwość w oparciu o punktację CVSS, zwartość opisu podatności, Bugtraq ID, CERT Vulnerability ID, CPE, IAVB ID, - system musi pozwalać na konfigurację wrażliwości wykrytej podatności w oparciu o punktację CVSSv2 lub CVSSv3 dla wszystkich skanów lub dla pojedynczego, - system musi być wspierany przez dodatkowy system punktowania podatności prezentowany w GUI oparty min. o uczenie maszynowe i aktualizowany codziennie. Mechanizm ten wspierany musi być

	również przez zespół ludzi producenta skanera, którzy analizują wyniki z modelu uczenia maszynowego jak również monitorują źródła takie jak min. Darknet, - system musi mieć możliwość przetrzymywać historię wykonanych skanów, - możliwość wyeksportowania wyników skanowania przynajmniej do formatów HTML, CSV, PDF, - możliwość wygenerowania przynajmniej raportu Top 10 Podatności, Wykryty system operacyjny, niewpierane oprogramowanie, Podatności na które są znane exploity, - system musi prezentować wynik skanowania wraz z rekomendacją od jakich aktualizacji zacząć, aby wyeliminować największe ryzyko przez daną aktualizację, - system musi umożliwiać zmianę wrażliwości wykrytej podatności w wyniku wykonanego skanu jak również uwzględnić zmianę w skanach, które będą wykonane w przyszłości z możliwością określenie czasu aktywności ustawienia, - aktualizacja reguł wykrywania podatności musi być wykonywana automatycznie w przypadku dostępu systemu do Internetu, - system musi umożliwiać przejście z poziomu GUI skanera na stronę dotyczącą informacji o aktualizacjach odnośnie wykrywanych podatności. **Zakres dotyczący systemu zarządzania podatnościami** System zarządzania podatnościami spełnia poniższe wymagania: - architektura systemu musi składać się z systemu centralnego zarządzania oraz skanerów podłączonych do tego systemu pochodzących od tego samego producenta co system centralnego zarządzania, - system centralnego zarządzania musi być dostarczony w modelu chmurowym, - skanery podłączone do systemu centralnego zarządzania muszą być dostępne jako oprogramowanie instalowane na systemie operacyjnym Red Hat 6/7, Fedora 25, FreeBSD 10/11,Cent OS 6/7, Windows Server 2016/2019, Windows 7/8/10, MAC OS 10.13, 10.14, 10.15 lub jako maszyna wirtualna dla środowiska Vmware lub Hyper-V, - system centralnego zarządzania musi pozwalać na podłączenie skanerów agentowych instalowanych na wybranych systemach operacyjnych. Skanery agentowe muszą mieć możliwość implementacji na systemach typu Red Hat 6/7/8, CentOS 6/7/8, Suse 11/12, Ubuntu 13.10/14.10/16.04/17.10, Fedora 25/26, Windows /7/8/10, Windows Server 2016/2019 oraz Mac OS 10.9-10.15, - zarządzanie systemem musi odbywać się za pomocą przeglądarki, nie dopuszcza się zarządzania za pomocą dodatkowo instalowanej aplikacji na komputerze administratora, - system centralnego zarządzania musi w ramach licencji zezwalać na podłączenie nieograniczonej liczby skanerów producenta systemu zarządzania, - skanery podłączone do systemu centralnego zarządzania muszą mieć możliwość wykonywania skanowania bez uwierzytelnienia oraz

	za pomocą uwierzytelnienia do systemu skanowanego, - GUI system centralnego zarządzania musi pozwalać na ściągnięcie logów ze zdalnego skanera, - system centralnego zarządzania musi prezentować informacje o użyciu licencji w formie wykresu z historią, - system centralnego zarządzania musi posiadać możliwość podłączenia się do środowisk chmurowych takie jak Amazon AWS, Microsoft Auzre, Google Cloud Platfrom, - w ramach skanowania z uwierzytelnieniem musi istnieć możliwość uwierzytelnienia przynajmniej za pomocą poniższych metod: - Hasło - Klucz SSH - Kerberos, - LM Hash - NTLM Hash - zastosowanie integracji z Liberman - zastosowanie integracji z BeyondTrust - zastosowanie integracji z LibermanThycotic Secret Server - zastosowanie integracji z Cyberark - zastosowanie integracji z Arcon, - zastosowanie integracji z Hashicorp Vault - Certyfikat - DB2 - File Transfer Protocol (FTP) - Microsoft SQL Server - MySQL Server - Oracle - Post Office Protocol (POP) - PostgreSQL - Simple Network Management Protocol (SNMP) - w przypadku niektórych metod uwierzytelnienia do systemu skanowanego musi istnieć możliwość automatycznego podniesienia uprawnień zwykłego użytkownika do uprawnień użytkownika uprzywilejowanego co najmniej dla systemów Cisco oraz systemów Linuxowych, - wykryte podatności muszą posiadać szybkie odniesienie do otwartych baz podatności, takich jak: - Bugtraq - MSFT - CVE - BID - OSVDB ID - musi być możliwość ustawienia harmonogramu automatycznego skanowania, - system musi posiadać możliwość tworzenia okien czasowych, w których skanowanie nie może rozpocząć się dla określonych przez administratora systemów, - system centralnego zarządzania musi być dostarczony jest kilkoma wzorcami polityk skanowania jak również musi istnieć możliwość zbudowania polityki skanowania od podstaw, - w ramach budowy polityki skanowania system musi zezwala na

	wybranie podatności jakie będą sprawdzane podczas skanowania, - system musi posiadać rozbudowany moduł do przeszukiwania wyników skanowania. Musi istnieć możliwość przeszukiwania wyników co najmniej za pomocą filtrów takich jak: Adres IP, Poziom niebezpieczeństwa, CVE ID, CVSS Score w wersji 2, CVSS Vector w wersji 2, CVSS Score w wersji 3, CVSS Vector w wersji 3,nazwa AWS EC2, Azure VM ID , Googl Cloud Zone, dostępny exploit, narzędzie do wykonania ataku (musi istnieć obsługa przynajmniej dla trzech narzędzi, np. Metasploit, Core Impact, Canvas), data opublikowania patch dla danej podatności, port, protokół, data opublikowania podatności, data zauważenia po raz pierwszy podatności dla systemu, data kiedy ostatni raz widziana była podatność dla systemu, przydział do określonej grupy systemów, MS Bulletin ID, - system centralnego zarzadzania musi pozwala na zapisywania filtrów przeszukiwania danych, - system musi pozwalać na eksport informacji o podatnościach w formatach, PDF, HTML, CSV, - system musi prezentować aktualizacje, które przyczyniają się do jak najszybszego obniżenia ryzyka w organizacji, - system musi posiadać swój własny mechanizm przyznawania ocen dla danej podatności od 0 do 10 na podstawie własnego modelu uczenia maszynowego oraz działu ekspertów, którzy monitorują zagrożenia w Internecie, między innymi w dark necie. - administrator systemu musi mieć możliwość zaakceptowania danego ryzyka oraz zmiany poziomu niebezpieczeństwa związanego z daną podatnością, - system musi umożliwiać tworzenie tagów, które można przypisać ręcznie lub automatycznie i używane są podczas przeszukiwania wyników sknowania, - system musi być dostarczony z gotowymi wzorcami raportów, - wybór systemów do skanowania musi być oparty o adresy IP, zakres adresów IP, podsieci adresów IP, grup systemów opartych o tagi, nazw domenowych, - producent musi dostarczyć gotowe wzorce widoków (ang. Dashboard) do systemu centralnego zarządzania podatnościami, - administrator systemu musi mieć możliwość budowania widoków od podstaw używając co najmniej takich elementów jak: tabela, wykres kołowy, wykres słupkowy, - administrator do tworzenia widoków musi mieć możliwość użycia co najmniej wymienionych filtrów: adres IP, Poziom niebezpieczeństwa, CVE ID, CVSS Score w wersji 2, CVSS Vector w wersji 2, CVSS Score w wersji 3, CVSS Vector w wersji 3, dostępny exploit, narzędzie do wykonania ataku (musi istnieć obsługa przynajmniej dla trzech narzędzi, np. Metasploit, Core Impact, Canvas), data opublikowania patch'a dla danej podatności, port, protokół, data opublikowania podatności, data pierwszy raz zauważenia podatności dla systemu, data kiedy ostatni raz widziana była podatność dla systemu, przyodział do określonej grupy systemów, Ms Bulletin ID, - rozwiązanie musi integrować się z zewnętrznymi dostawcami systemów MDM, co najmniej: AirWatch MDM, Apple Profile

	Manager, Good MDM, Mobile Iron, Microsoft Intune, Blackberry UEM, MaaS360, - system musi mieć możliwość integracji z systemami zarządzania aktualizacjami w celu sprawdzenia czy wynik ze skanowania pokrywa się z informacjami z tych systemów. System musi integrować się co najmniej z takimi systemami jak: Microsoft SCCM, Microsoft WSUS, IBM Tivoli Endpoint Manager, Red Hat Satellite Server, Red Hat Satellite 6 Server, Symantec Altiris, - system musi posiadać wzorce zgodności z regulacjami, które dostarcza producent, co najmniej dla regulacji CIS, DISA, - system musi umożliwiać tworzenie swoich własnych wzorców sprawdzania zgodności z regulacjami bez konieczności kontaktu z producentem, jak również muszą być udostępnione informacje w jaki sposób można budować swoje własne wzorca sprawdzania zgodności ze standardami przyjętymi w firmie, - musi być możliwość wykonywanie skanów audytowych/konfiguracji co najmniej dla systemów Windows, Unix, Vmware, Cisco, Fortigate, Oracle, DB2, MySQL, SQL Server, PostgreSQL, Juniper, - system musi posiadać opisane integracje min. z systemami ServiceNow, Jira, Splunk, IBM Qradar, Microsoft Azure,Google Cloud Security Command Center, Amazon Web Services. W przypadku implementacji z Jirą w środowisku lokalnym wymagane jest aby integracja była wykonana za pomocą dodatku do systemu Jira, - możliwości skryptowania / API dla systemu centralnego zarządzania, **Zakres dotyczący skanowania webaplikacji:** Skaner aplikacji webowych musi posiadać następujące funkcje: - musi być dostępny jako rozwiązanie typu cloud wraz z dostępnymi skanerami w rożnych częściach świata – minimum 9 skanerów podpiętych do systemu zarządzania umieszczonych na świecie - musi być zarządzany przez przeglądarkę webową bez konieczności instalowania systemu zarządzania na komputerze administratora, - musi być możliwość skanowania web aplikacji niedostępnych od strony Internetu, za pomocą dodatkowego silnika skanującego, który łączy się z systemem zarządzania znajdującym się w chmurze, - skaner lokalny służący do skanowania aplikacji webowych lokalnie musi być dostarczony jak maszyna wirtualna dla systemu Vmware lub Hyper-V, - musi być możliwość uwierzytelnienia do web aplikacji za pomocą cookie, użycie skryptu selenium lub login form, - system musi posiadać przynajmniej dla jednej przeglądarki internetowej dodatek pozwalający w łatwy sposób utworzyć plik selenium w celu uwierzytelnienie do aplikacji webowej, - system musi pozwalać na skonfigurowanie polityki w ramach której określone jest jakie podatności będą sprawdzane, - system musi mieć możliwość skanowania aplikacji webowej co najmniej przez 99 godzin w ramach jednego uruchomionego skanu, - musi pozwalać na skonfigurowanie jakie URL mają być poddane analizie jak również musi być opcja w której skanowane są wskazane URL oraz podstrony tych URL'i, - musi być prezentowane jakie dokładnie zapytanie http zostało

	przesłane ze skanera do analizowanej aplikacji webowej i jaka dokładnie została przesłana odpowiedź, - musi być możliwość określenia maksymalnej liczby przekierowań(redirect), - musi być możliwość ustawienia maksymalnej liczby skanowanych URL, natomiast skaner nie może mieć odgórnego limitu dla maksymalnej liczby skanowanych URL, - musi być możliwość określenia maksymalnego zagnieżdżenia analizowanej aplikacji webowej, natomiast skaner nie może mieć odgórnego limitu dla maksymalnego zagnieżdżenia, - musi być możliwość kastomizacji nagłówka http, który będzie użyty podczas wysyłania zapytań do skanowanej aplikacji webowej, - musi być możliwość ustawienia maksymalnej liczby jednoczesnych połączeń - musi być możliwość ustawienia maksymalnej liczby zapytań http na sekundę, - musi być możliwość określenia jakie URL nie będą brane pod uwagę podczas skanowania, - musi być generowana mapa aplikacji webowej z informacja jakie URL zostały znalezione podczas skanowania, - musi być rysowana linia trendu w czasie dla podatności związanych z aplikacjami webowymi, - system musi informować czy zalogowanie do analizowanej aplikacji webowej udało się czy nie, - musi być informacja o wykrytej podatności z informacją jak ją wyeliminować, - musi być informacja dla wykrytej podatności kiedy pierwszy raz dana podatność została zaobserwowana i kiedy ostatni raz dla skanowanej aplikacji webowej, - musi być informacja o punktacji CVSSv2 i CVSSv3 dla wykrytej podatności, **Zakres dotyczący skanowania kontenerów:** System do skanowania kontenerów Dockera musi zawierać: - mechanizmy sprawdzające obraz pod kontem podatności wraz z informacją o punktacji CVSS oraz poziomie ryzyka - silnik skanujący sprawdzający obrazy pod kontem malwaru, - sprawdzanie obrazów pod kontem polityk bezpieczeństwa, - możliwość podłączenia do rejestru obrazów między innymi: Docker Registry, Docker Trusted Registry, JFrog Artifactory i Amazon EC2 Container Registry, - automatyczne skanowanie obrazów w rejestrze po aktualizacji informacji o nowych zagrożeniach, - możliwość identyfikacji kontenerów uruchomionych w produkcji, które nie były testowane pod kontem podatności oraz dostarczanie informacji czy kontener był zmieniony po wdrożeniu wraz z informacją, które pakiety zostały zmienione, - możliwość integracji z systemami CI/CD minimum: Bamboo, CircleCI, Codeship, Jenkins, Solano, Shippable, Travic Ci oraz Wercker, - Restful Api z pełna dokumentacją,

	Zakres dotyczący pomiaru poziomu ryzyka w organizacji: System mierzenia cyber ryzyka w organizacji musi zawierać: - obliczanie ryzyka dla każdego systemu w organizacji w oparciu o informacje o podatnościach, prawdopodobieństwo użycia ich oraz innych wskaźników ryzyka takich jak min. krytyczność biznesowa atakowanego systemu, - obliczanie automatyczne krytyczności każdego systemu w organizacji w oparciu o parametry stosowane przez system mierzenia ryzyka oraz możliwość nadania stopnia krytyczności systemowi ręcznie w skali od 1 -10, - informacje o podatnościach pochodzące od tego samego producenta co system do obliczenia ryzyka, - wizualizację trendu efektywności programu redukcji ryzyka, - prezentację jakości dokonywanych skanów, która bierze pod uwagę minimum: częstotliwość skanowania systemów, czy skanowanie jest z uwierzytelnieniem czy nie, ilość użytych funkcji do wykrycia podatności, rekomendowane akcje w celu polepszenia jakości dokonywanych skanów w organizacji, - porównanie min. parametrów związanych z efektywnością programu obniżenia ryzyka, jakości dokonywanych skanów do innych firm z tej samej branży, - możliwość grupowania systemów w grupy pod kontem biznesowym, - obliczania cyber ryzyka w organizacji w oparciu o kontekst biznesowy, - listę rekomendowanych akcji, które zmniejszają cyber ryzyko w oparciu o decyzje biznesowe wraz z możliwością zagłębienia się w daną podatność, system w celu podjęcia bardziej efektywnej decyzji dotyczącej zmniejszenia ryzyka, - prezentację informacji na temat usuniętych podatności min. w oparciu o czas pierwszego wykrycia podatności, czas od kiedy dostępny jest patch na daną podatność,
Inne wymagania	Dopuszcza się spełnienie powyższych wymagań przez więcej niż jedno oprogramowanie, pod warunkiem że będzie dostarczone od jednego producenta.