

Opis Przedmiotu Zamówienia

1. Przedmiotem zamówienia jest: **zakup 100 szt. licencji na oprogramowanie skanujące aplikacje webowe** (rozszerzenie posiadanych licencji oprogramowania TIO-WAS Tenable Web Application Scanning lub równoważne).
2. Zamawiający posiada licencje oprogramowania TIO-WAS Tenable Web Application Scanning:
 - 2.1. Liczba posiadanych licencji: 10 szt.
 - 2.2. Licencja ważna do: **2023-03-29**.
3. Licencje na oprogramowanie skanujące aplikacje webowe, zostaną dostarczone **w terminie 10 dni roboczych** od daty zawarcia umowy.
4. Licencje na oprogramowanie zostaną udzielone od dnia podpisania Protokołu odbioru do dnia 2023-03-29, data zakończenia powinna być taka sama jak data zakończenia obecnie posiadanych licencji.
5. Oferowane licencje muszą być zakupione w autoryzowanym kanale dystrybucji producenta i posiadać pakiet usług gwarancyjnych oraz wsparcie producenta obejmujące wyspecyfikowany przedmiot zamówienia.
6. Wykonawca dostarczy dokumenty licencyjne, warunki licencjonowania oraz klucze licencyjne na adres e-mail: administrator@cez.gov.pl
7. Wymagania minimalne dla oprogramowania typu skaner podatności:
 - 7.1. Zarządzanie:**
 - 7.1.1. Oprogramowanie musi umożliwiać tworzenie indywidualnych kont dla każdego użytkownika/administratora.
 - 7.1.2. Dostęp do oprogramowania możliwy jedynie po uwierzytelnieniu użytkownika w systemie.
 - 7.1.3. Hasła dostępu muszą być przechowywane w postaci zaszyfrowanej.
 - 7.1.4. Oprogramowanie musi zapewniać silną politykę haseł lub umożliwiać jej określenie dla użytkowników.
 - 7.1.5. Oprogramowanie musi umożliwiać konfigurowanie zakresu uprawnień z wykorzystaniem predefiniowanych ról wewnętrznych (np. dostęp tylko do raportów, administrator systemu itp.) lub poprzez możliwość przypisania określonych operacji do zdefiniowanych ról.
 - 7.1.6. Oprogramowanie musi mieć możliwość definiowania raportów i alertów z wykorzystaniem wszystkich danych zbieranych przez skaner.
 - 7.1.7. 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.

7.2. Funkcjonalności:

- 7.2.1. Oprogramowanie musi zapewniać możliwość harmonogramowania (planowania w czasie).
- 7.2.2. Oprogramowanie musi zapewnić silne uwierzytelnianie tak aby bezpiecznie przesyłać poświadczenia w skanowaniu z uwierzytelnianiem.
- 7.2.3. Oprogramowanie powinno wspierać poniższe opcje konfiguracji skanowania:
 - 7.2.3.1. Attack Policy;
 - 7.2.3.2. Authentication;
 - 7.2.3.3. Crawler Restrictions;
 - 7.2.3.4. HTTP Headers Performance;
 - 7.2.3.5. Selenium Recordings;
 - 7.2.3.6. Custom URLs;
 - 7.2.3.7. Advanced Options.
- 7.2.4. Oprogramowanie musi umożliwiać automatyczne przeprowadzanie retestów luk/podatności wykrytych wcześniej w celu sprawdzenia czy zostały one poddane działaniem naprawczym.
- 7.2.5. Wykryte podatności powinny posiadać odnośniki do otwartych baz podatności, takich jak:
 - 7.2.5.1. Bugtraq;
 - 7.2.5.2. MSFT;
 - 7.2.5.3. CVE;
 - 7.2.5.4. BID;
 - 7.2.5.5. OSVDB ID.
- 7.2.6. Oprogramowanie musi mieć możliwość tworzenia grup dla danych wynikowych.
- 7.2.7. W ramach budowy polityki skanowania oprogramowanie musi zezwalać na wybranie podatności jakie będą sprawdzane podczas skanowania, np. w oparciu o CVSS lub CVE
- 7.2.8. Musi istnieć możliwość przeszukiwania wyników co najmniej za pomocą filtrów takich jak:
 - 7.2.8.1. poziom niebezpieczeństwa;
 - 7.2.8.2. CVE ID;
 - 7.2.8.3. CVSS Score w wersji 2 i nowszych;
 - 7.2.8.4. CVSS Vector w wersji 2 i nowszych;
 - 7.2.8.5. Dostępny exploit;
 - 7.2.8.6. narzędzi do wykonania ataku (musi istnieć obsługa przynajmniej dla trzech narzędzi, np. Metasploit, Core Impact, Canvas);
 - 7.2.8.7. data opublikowania patch dla danej podatności;
 - 7.2.8.8. port/protokół;
 - 7.2.8.9. data opublikowania podatności;
 - 7.2.8.10. data zauważenia po raz pierwszy podatności dla systemu;
 - 7.2.8.11. data kiedy ostatni raz widziana była podatność dla systemu;
 - 7.2.8.12. przydział do określonej grupy systemów;
 - 7.2.8.13. CCE ID;
 - 7.2.8.14. MS Bulletin ID.

- 7.2.9. Oprogramowanie musi posiadać swój własny mechanizm przyznawania ocen dla danej podatności (np. od 0 do 10) na podstawie własnego modelu uczenia maszynowego.
- 7.2.10. Oprogramowanie musi posiadać gotowe grupy wzorców raportów udostępnionych przez producenta, które administrator może edytować.
- 7.2.11. Oprogramowanie 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.
- 7.2.12. Oprogramowanie musi umożliwiać generowanie raportów co najmniej w następujących formatach: PDF, CSV.
- 7.2.13. Oprogramowanie musi mieć możliwość generowania raportów według harmonogramu oraz na żądanie.
- 7.2.14. Użytkownik do tworzenia widoków musi mieć możliwość używania co najmniej wymienionych filtrów:
 - 7.2.14.1. poziom niebezpieczeństwa,
 - 7.2.14.2. CVE ID,
 - 7.2.14.3. CVSS Score w wersji 2 i nowsze,
 - 7.2.14.4. CVSS Vector w wersji 2 i nowsze,
 - 7.2.14.5. Dostępny exploit,
 - 7.2.14.6. data opublikowania patch'a dla danej podatności,
 - 7.2.14.7. port, protokół,
 - 7.2.14.8. data opublikowania podatności,
 - 7.2.14.9. data pierwszy raz zauważenia podatności dla systemu,
 - 7.2.14.10. data kiedy ostatni raz widziana była podatność dla systemu,
 - 7.2.14.11. przydział do określonej grupy systemów,
 - 7.2.14.12. CCE ID,
 - 7.2.14.13. MS Bulletin ID.
- 7.2.15. Oprogramowanie musi posiadać wzorce zgodności z regulacjami, które dostarcza producent, co najmniej dla regulacji CIS, DISA.
- 7.2.16. Funkcjonalność kontroli aplikacji powinna zawierać testy sprawdzające (co najmniej OWASP).

8. Opis równoważności.

- 8.1. Zamawiający dopuszcza możliwość dostawy rozwiązania równoważnego względem wyspecyfikowanego przez Zamawiającego w Opisie przedmiotu zamówienia (OPZ).
- 8.2. Za rozwiązanie równoważne Zamawiający uzna oprogramowanie zapewniające bez dodatkowych nakładów finansowych bezkonfliktowe działanie posiadanego środowiska zbudowanego w oparciu o oprogramowanie wymienione w pkt. 2 oraz spełniające wszystkie funkcje oprogramowania, o którym mowa w pkt. 7
- 8.3. W przypadku dostarczenia oprogramowania równoważnego Wykonawca:
 - 8.3.1. Dostarczy oprogramowanie o funkcjonalności nie gorszej od posiadanych przez Zamawiającego.
 - 8.3.2. Zapewni kompletną, nieinwazyjną deinstalację dotychczasowego oprogramowania antywirusowego i oprogramowania antyspamowego z całej infrastruktury informatycznej (komputerów, serwerów i urządzeń mobilnych) Zamawiającego.

- 8.3.3. Zapewni kompletną, nieinwazyjną instalację i konfigurację nowego rozwiązania w infrastrukturze informatycznej Zamawiającego.
 - 8.3.4. Zapewni dodatkowe wsparcie techniczne (zdalne oraz, w razie potrzeby, bezpośrednie – realizowane w siedzibie Zamawiającego) przez Wykonawcę przez okres miesiąca od daty wdrożenia produkcyjnego rozwiązania równoważnego.
 - 8.3.5. Przeprowadzi Instruktaż dla 5 pracowników Zamawiającego z zakresu obsługi, konfiguracji i administracji całości rozwiązania równoważnego.
 - 8.3.6. Wdrożenie, Instruktaż, asysta techniczna i dodatkowe wsparcie techniczne Wykonawcy – w języku polskim w siedzibie Zamawiającego.
 - 8.3.7. Wdrożenie równoważnego oprogramowania antywirusowego i oprogramowania antyspamowego zostanie zrealizowane przez Wykonawcę nie później niż w terminie wygaśnięcia posiadanych przez Zamawiającego licencji.
- 8.4. Oprogramowanie równoważne nie może naruszać bezpieczeństwa publicznego lub istotnego interesu bezpieczeństwa państwa, mając na względzie m.in. fakt, że Zamawiający zgodnie z art. 4 pkt. 7 Ustawy o Krajowym systemie cyberbezpieczeństwa (tj. Dz. U z 2018r. poz. 1560), dalej: „Ustawa”, należy do Krajowego systemu cyberbezpieczeństwa, którego celem jest zgodnie z art. 3 Ustawy, zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym zapewnienie niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów. Tym samym, oprogramowanie musi być zgodne z celem Krajowego systemu cyberbezpieczeństwa i przepisami Ustawy oraz nie zagrażać cyberbezpieczeństwu, bezpieczeństwu publicznemu lub istotnemu interesowi bezpieczeństwa państwa.
- 8.5. Warunki licencjonowania mają umożliwiać Zamawiającemu (Licencjodawcy) objęcie dostarczonym oprogramowaniem stacji roboczych należących do podmiotów administracji publicznej, na warunkach zdefiniowanych w OPZ.
- 8.6. Dostarczana licencja oprogramowania musi pochodzić z autoryzowanego przez producenta kanału dystrybucji. Wykonawca jest zobowiązany dostarczyć Zamawiającemu dowody poświadczające autentyczność zakupionych licencji na zasadach określonych przez producenta.
- 8.7. W przypadku błędnego działania rozwiązania, po instalacji oprogramowania równoważnego, Wykonawca zobowiązany będzie na własny koszt przywrócić środowisko do stanu poprawnego funkcjonowania w terminie 1 dnia roboczego od stwierdzenia przez Zamawiającego niepoprawnego funkcjonowania, a w przypadku braku takiej możliwości do stanu pierwotnego oraz dostarczenia innego rozwiązania spełniającego wymagania OPZ w terminie do 3 dni kalendarzowych. Ponadto Wykonawca poniesie wszelkie koszty związane z poniesionymi stratami biznesowymi w związku z brakiem działania rozwiązania.