Agencja Restrukturyzacji
i Modernizacji Rolnictwa

adres korespondencyjny
Centrala ARiMR
ul. Poleczki 33, 02-822 Warszawa

Zastępca Prezesa
Jacek Paziewski

Wykonawcy

Wasze pismo znak: Data:	Nasz znak:	Data:
	ZP.248 .DPiZP.2610.15.2022.IH	26 .09.2022 r.

dotyczy: postępowania o udzielenie zamówienia publicznego w trybie podstawowym na „**Zakup i wdrożenie systemu do zarządzania podatnościami „Vulnerability Management – VM" w środowisku hybrydowym**".

Szanowni Państwo,

I. Działając na podstawie art. 135 ust. 1 i 2 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2022 poz. 1710; dalej: „ustawa") Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie przy al. Jana Pawła II nr 70, zwana w dalszej treści pisma „Zamawiającym", udziela odpowiedzi na pytania zgłoszone w przedmiotowym postępowaniu.

Pytanie nr 1

Dotyczy OPZ rozdział I.1 pkt.2 ppkt. 1b. Zamawiający wskazuje jako przedmiot zamówienia dostarczenie m.in. licencji czasowej na okres 36 miesięcy Metasploit Pro. W związku z powyższym zwracamy się z pytaniem, czy intencją Zamawiającego jest zakup konkretnego rozwiązania firmy Rapid 7, czy też Zamawiający dopuści rozwiązania równoważne?.

Odpowiedź:

Zamawiający w odpowiedzi na pytanie, działając na podstawie art. 137 ust. 1 ustawy, wprowadza następujące zmiany (**zmiany zaznaczono boldem**) w treści Specyfikacji Warunków Zamówienia (dalej „SWZ"):

ZMIANA NR 1:
Rozdział I.1 SWZ, Opis przedmiotu zamówienia, pkt 2 ppkt 1) lit. b o treści:

„b) licencji czasowej na okres 36 miesięcy (na zasadach subskrypcji) Metasploit PRO umożliwiającej wykonywanie testów penetracyjnych i aktywnego badania zabezpieczeń systemów,"

przyjmuje brzmienie:

„b) licencji czasowej na okres 36 miesięcy (na zasadach subskrypcji) Metasploit PRO umożliwiającej wykonywanie testów penetracyjnych i aktywnego badania zabezpieczeń systemów **lub rozwiązanie równoważne spełniające warunki równoważności opisane w pkt 13 Załącznika nr 1 do ppu stanowiących Załącznik nr 7 do SWZ**,"

ZMIANA NR 2:
Załącznik nr 7 do SWZ, projektowane postanowienia umowy, § 2 ust. 1 pkt 1) lit. b o treści:

„b) zapewni Zamawiającemu - na zasadach określonych w Umowie oraz ogólnych warunkach licencyjnych producenta Systemu - prawo do korzystania (na zasadach subskrypcji) z Systemu, w tym zarówno w całości jak i z poszczególnych jego elementów, dla min. 5000 assets* w tym min. 250 systemów/adresów ipv4 na adresacji publicznej w najnowszej dostępnej wersji oprogramowania oferowanego Systemu, w tym prawo do korzystania z narzędzia **typu Metasploit PRO** umożliwiającego wykonywanie testów penetracyjnych i aktywnego badania zabezpieczeń systemów, wraz z prawem do korzystania z dokumentacji producenta Systemu (techniczna, użytkownika, administratora);
Uwaga: * Za assets Zamawiający rozumie pojedynczy adres IP lub usługę na adresie IP."

przyjmuje brzmienie:

„b) zapewni Zamawiającemu - na zasadach określonych w Umowie oraz ogólnych warunkach licencyjnych producenta Systemu - prawo do korzystania (na zasadach subskrypcji) z Systemu, w tym zarówno w całości jak i z poszczególnych jego elementów, dla min. 5000 assets* w tym min. 250 systemów/adresów ipv4 na adresacji publicznej w najnowszej

dostępnej wersji oprogramowania oferowanego Systemu, w tym prawo do korzystania z narzędzia umożliwiającego wykonywanie testów penetracyjnych i aktywnego badania zabezpieczeń systemów **opisanego w Załączniku nr 1 do Umowy**, wraz z prawem do korzystania z dokumentacji producenta Systemu (techniczna, użytkownika, administratora);"

ZMIANA NR 3:
Załącznik nr 7 do SWZ, projektowane postanowienia umowy - Załącznik nr 1 do ppu Specyfikacja Systemu, pkt 12 ppkt 2) o treści:

„2) integracja z Metasploit PRO."

przyjmuje brzmienie:

„2) integracja z Metasploit PRO **lub narzędziem umożliwiającym wykonywanie testów penetracyjnych i aktywne badanie zabezpieczeń systemów zaoferowanym jako rozwiązanie równoważne spełniające warunki równoważności opisane w pkt. 13 (poniżej)"**

ZMIANA NR 4:
Załącznik nr 7 do SWZ projektowane postanowienia umowy - Załącznik nr 1 do ppu Specyfikacja Systemu, pkt 12 ppkt 4) o treści:
„4) integracja powinna umożliwiać wykonywanie skanów podatności bezpośrednio z Metasploit PRO."

przyjmuje brzmienie:

„4) integracja powinna umożliwiać wykonywanie skanów podatności bezpośrednio z Metasploit PRO **lub narzędziem umożliwiającym wykonywanie testów penetracyjnych i aktywne badanie zabezpieczeń systemów zaoferowanym jako rozwiązanie równoważne spełniające warunki równoważności opisane w pkt. 13 (poniżej)."**

ZMIANA NR 5:
Załącznik nr 7 do SWZ, projektowane postanowienia umowy - Załącznik nr 1 do ppu Specyfikacja Systemu dodaje się pkt 13 o brzmieniu:

„13. Licencja czasowa na okres 36 miesięcy (na zasadach subskrypcji) Metasploit PRO umożliwiająca wykonywanie testów penetracyjnych i aktywne badanie zabezpieczeń systemów lub rozwiązanie równoważne spełniające poniżej opisane warunki równoważności:

1) **Rozwiązanie musi umożliwiać zamknięcia cyklu ocena – korygowanie – walidacja.**
2) **Podatności znalezione w środowisku IT (systemy serwerowe, końcowe, bazy danych i sieci, ale także aplikacje webowe) przez skaner podatności mogą być od razu lub po zmianach konfiguracji poddane działaniu narzędzia do wykonywania testów penetracyjnych by ponownie sprawdzić wprowadzone poprawki (praktyczna weryfikacja skuteczności istniejących zabezpieczeń). Integracja musi umożliwiać również kontrolę najsłabszego ogniwa w łańcuchu zabezpieczeń poprzez korelację z danymi z baz exploitów (w zależności od zaproponowanego rozwiązania do testów penetracyjnych) takimi jak Metasploit, CoreImpact, Canvas, ExploitHub i filtrowanie wg prawdopodobieństwa wykorzystania podatności i jej impaktu na infrastrukturę IT.**
3) **Rozwiązanie musi umożliwiać prowadzenie wielowymiarowych, profesjonalnych testów penetracyjnych, pozwalając bezpiecznie odtworzyć próby przełamania systemów ochrony.**
4) **Minimalny zakres funkcjonalności:**

a) **Wielowymiarowe odtworzenie złożonych zagrożeń tzn. możliwość prowadzenia regularnych i powtarzalnych testów penetracyjnych z aktualizowanych baz exploitów;**
b) **Analiza What-if Attack Analysys, wykazanie i udokumentowanie stopnia ryzyka;**
c) **Zapewnienie stale aktualizowanej bibloteki exploitow;**
d) **Raportowanie obejmujące zestawienie zweryfikowanych i potwierdzonych podatności;**
e) **Przeprowadzenie ataków z wykorzystaniem zidentyfikowanych, krytycznych luk w systemach operacyjnych, urządzeniach, usługach i aplikacjach;**
f) **Cykliczne próby uzyskania dostępu do danych i manipulowanie nimi;**
g) **Weryfikacja przydatności poszczególnych zabezpieczeń w procesie rozpoznawania i blokowania ataków;**
h) **Możliwość wykorzystywania robotów, wyszukiwarek itp. do uzyskania informacji w celu ataku;**
i) **Exploity typu client-side do testowania zabezpieczeń urządzeń końcowych i oceny ich wykorzystania do ataków na zasoby organizacji;**
j) **Realizacja ataków z wykorzystaniem kradzieży uwierzytelnień:**
   i. **Próby przełamania zabezpieczeń Windowa NTLM/Kerberos;**
   ii. **Odczytywanie tożsamości nazw użytkowników, haseł, ticketów, kluczy;**
   iii. **Wykorzystania tożsamości pozyskanych w trakcie testów wielowektorowych;**
   iv. **Automatyczne lub ręczne przejmowanie kontroli nad systemami wykorzystującymi słabe uwierzytelnienie;**
   v. **Uzyskanie stałego dostępu do skompromitowanych systemów w wykorzystaniem kradzieży tożsamości.**
k) **Testy penetracyjne aplikacji Webowych/Internetowych:**

i. **Identyfikacja słabych punktów aplikacji internetowych, serwerów i związanych z nimi bazach danych, itp.;**
ii. **Test wszystkich luk w aplikacjach internetowych wymienionych w OWASP Top Ten 2019 lub nowszy;.**
iii. **Dynamiczne generowanie exploitów, które mogą skompromitować aplikacje tworzone na indywidualne zamówienie;**
iv. **Importowanie i sprawdzanie poprawności wyników pracy skanerów podatności w celu określenia priorytetów dla działań naprawczych.**
v. **Wykorzystanie najsłabiej zabezpieczonych zasobów do ataku na serwery webowe i rozwiązania back-end.**
vi. **Testowanie usług sieciowych aplikacji internetowych i mobilnych.**
l) **Testy penetracyjne urządzeń przenośnych."**

Pytanie nr 2

Dotyczy: warunku udziału w postępowaniu o którym mowa w rozdziale III.2. pkt.1 ppkt 1.1.1

Zamawiający wymaga: [...] wykazania co najmniej dwóch zamówień (umów) polegających na dostarczeniu oraz wdrożeniu oprogramowania realizującego funkcję zarządzania podatnościami klasy „Vulnerability Management" o wartości każdego z tych zamówień co najmniej 600 000, zł brutto.

Bazując na informacji pozyskanej od jednego z wiodących producentów rozwiązania w zakresie zarządzania podatnościami, żaden z jego partnerów w Polsce nie spełni warunku wykazania zamówień o wartościach oczekiwanych przez Zamawiającego.

Jako Wykonawca zrealizowaliśmy umowę na kwotę przekraczającą wartość oczekiwaną przez Zamawiającego, polegającą na dostarczeniu oraz wdrożeniu oprogramowania realizującego funkcję zarządzania podatnościami, ale nie możemy jej udokumentować ze względu na fakt, że zamawiający, na rzecz którego zamówienie było realizowane, dopuścił do udziału w postępowaniu wyłącznie oferentów, którzy posiadają dostęp do informacji niejawnych oraz nadał wszelkim dokumentom klauzulę „zastrzeżone" i nałożył na dostawcę zakaz ujawniania informacji w niej zawartych.

Oznacza to, że nie możemy jej przedstawić nawet w przypadku zastrzeżenia jej poufności. Klauzula dokumentu „zastrzeżone" oznacza, że z danym dokumentem może się zapoznać wyłącznie osoba, która została przeszkolona i uzyskała stosowny certyfikat uprawniający ją do przetwarzania dokumentu. Dodatkowo wpływ takiego dokumentu może mieć miejsce wyłącznie do organizacji, która spełnia warunki przewidziane ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. 2010 Nr 182 poz. 1228, co przy prowadzeniu postępowania w trybie elektronicznym jest de facto całkowicie niemożliwe i prawnie niedopuszczalne.

W związku z powyższym zwracamy się z pytaniem, czy Zamawiający dopuści Wykonawcę, który wykaże referencje lub inne dokumenty sporządzone przez podmiot, na rzecz którego usługi zostały wykonane, potwierdzające:

co najmniej jedno zamówienie (umowę) na dostawę oprogramowania realizującego funkcję zarządzania podatnościami klasy „Vulnerability Management" o wartości min. 400 000,00 brutto,

oraz

co najmniej jedno zamówienie (umowę) na dostawę systemu bezpieczeństwa o wartości min. 1 000 000,00 zł brutto.

Zgoda Zamawiającego na powyższe modyfikacje warunków pozwoli Zamawiającemu na rozszerzenie katalogu potencjalnych oferentów oraz nie pozbawi Zamawiającego możliwości wyboru rozwiązania, które jest liderem wśród rozwiązań zarządzania podatnościami.

Odpowiedź:

Zamawiający w odpowiedzi na pytanie, działając na podstawie art. 137 ust. 1 ustawy, wprowadza następujące zmiany (**zmiany zaznaczono boldem**) w treści SWZ:

ZMIANA NR 6:

W Rozdziale III.2 SWZ, Warunki udziału w postępowaniu, pkt 1.1 ppkt 1.1.1. SWZ o treści:

1.1. Zdolności technicznej lub zawodowej. Zamawiający uzna, że Wykonawca spełnia warunek udziału we wskazanym zakresie, jeżeli Wykonawca wykaże, że:
1.1.1. wykonał w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych: co najmniej dwa zamówienia (umowy) polegające na dostarczeniu oraz wdrożeniu oprogramowania realizującego funkcję zarządzania podatnościami klasy „Vulnerability Management – VM", o wartości każdego z tych zamówień co najmniej 600 000,00 zł brutto (słownie: sześćset tysięcy złotych 00/100).

przyjmuje brzmienie:

1.1. Zdolności technicznej lub zawodowej. Zamawiający uzna, że Wykonawca spełnia warunek udziału we wskazanym zakresie, jeżeli Wykonawca wykaże, że:
1.1.1. wykonał w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych:

1.1.1.1. co najmniej dwa zamówienia (umowy) polegające na dostarczeniu oraz wdrożeniu oprogramowania realizującego funkcję zarządzania podatnościami klasy „Vulnerability Management – VM", o wartości każdego z tych zamówień co najmniej **300 000,00 zł brutto (słownie: trzysta tysięcy złotych 00/100)**

lub

1.1.1.2. **co najmniej dwa zamówienia (umowy) polegające na dostawie oraz wdrożeniu systemu bezpieczeństwa, o wartości każdego z tych zamówień co najmniej 500 000,00 zł brutto (słownie: pięćset tysięcy złotych 00/100).**

UWAGA 1a

W celu potwierdzenia spełnienia powyższego warunku udziału Zamawiający dopuszcza wykazanie się wykonaniem dwóch zamówień (umów) w tym: jednego zamówienia w zakresie wskazanym w ppkt 1.1.1.1. oraz jednego zamówienia w zakresie wskazanym w ppkt 1.1.1.2.

Pytanie nr 3

Dotyczy Umowy par. 5 pkt 9. Zamawiający wymaga, aby Wykonawca przeprowadził certyfikowane przez producenta wdrażanego Systemu warsztaty dla administratorów. Z uwagi na fakt, iż Producent oferowanego rozwiązania nie świadczy na terenie RP usługi certyfikowanych szkoleń, zwracamy się z pytaniem, czy Zamawiający dopuści przeprowadzenie warsztatów realizowanych przez certyfikowanego inżyniera posiadającego najwyższe certyfikaty produktowe oraz partnerskie Producenta oferowanego rozwiązania?

Odpowiedź:

Zamawiający podtrzymuje zapisy SWZ.

Pytanie nr 4

Zamawiający w par 8 ust 2 projektu umowy przewiduje uprawnienie, w ramach którego ma posiadać prawo „do udostępnienia Systemu wraz z jego dokumentacją jak również do Aktualizacji ich dokumentacji spółce powołanej w celu realizacji zadań polegających na zapewnieniu rozwoju Systemu i rozwiązań teleinformatycznych służących realizacji zadań Zamawiającego".

W związku z powyższym zwracamy się z pytaniem:

1. Co Zamawiający rozumie przez sformułowanie „udostępnienie Systemu"? Czy chodzi o cesję praw i przeniesienie praw subskrypcji licencji na inny podmiot?

2. Czy w przypadku, gdy przez sformułowanie „udostępnienie Systemu" Zamawiający rozumie cesję praw i przeniesienie praw subskrypcji licencji na inny podmiot to czy Zamawiający wyrazi zgodę na modyfikację zapisu w ten sposób, aby precyzował, że nowopowstała spółka, będzie podmiotem zależnym od Zamawiającego, w którego kapitale zakładowym Zamawiający będzie posiadał co najmniej 51% udziałów uprawniających do wyboru władz w powołanej spółce?

UZASADNIENIE:

Wyjaśnienie powyższych kwestii prawnych jest niezbędne, bowiem większość producentów systemów IT ogranicza zakres warunków licencyjnych do licencji udzielonej konkretnemu podmiotowi, w ramach której wyłączony jest swobodny obrót i współdzielenie praw. Zdarza się, że producenci dopuszczają ograniczoną możliwość przeniesienia licencji lub ich współdzielenie ale wyłącznie w obrębie grupy kapitałowej tj. na spółki, w których kapitale zakładowym, konkretny zamawiający posiada udział większy niż 50%. Brak modyfikacji aktualnego brzmienia umowy może spowodować ograniczenie konkurencji bowiem może się okazać, że uprawnienie o którym mowa w par 8 ust 2 projektu umowy będzie niezgodne z warunkami licencyjnymi większości producentów oprogramowania i uniemożliwi złożenia jakiejkolwiek oferty.

Odpowiedź:

Zamawiający wyjaśnia, iż intencją wprowadzonej regulacji jest umożliwienie pracownikom spółki informatycznej utworzonej przez ARiMR (w przypadku powstania takiej spółki) wykonywanie poszczególnych czynności związanych z administrowaniem Systemem i jego użytkowaniem w imieniu i na rzecz Agencji. Dokonany podział kompetencyjny pomiędzy ARiMR a spółkę informatyczną może w szczególności prowadzić do sytuacji, w której osoby zajmujące się administrowaniem poszczególnymi systemami osadzonymi w infrastrukturze ARiMR będą pracownikami spółki. Nie można również wykluczyć w przyszłości współdzielenia nabytych przez ARiMR licencji pomiędzy Zamawiającego, a jego spółkę. Tym niemniej z punktu widzenia ukonstytuowania spółki, będzie ona podmiotem zależnym od ARiMR (Zamawiający będzie sprawował kontrolę i wywierał bezpośredni wpływ na sposób działania spółki).

Pytanie nr 5

Rozdział I Przedmiot zamówienia

I.1 Opis przedmiotu zamówienia

2.1) b) Oprogramowanie Metasploit PRO jest oprogramowaniem produkowanym i sprzedawanym tylko i wyłącznie przez firmę Rapid7, co wyklucza jakikolwiek aspekt konkurencyjności w tym postępowaniu. Wymienianie z nazwy konkretnego produktu jaki chce Zamawiający nabyć stoi w sprzeczności z trybem w jakim procedowane jest przedmiotowe postępowanie tj. przetargu nieograniczonego. Jest to bowiem postępowanie, w którym wskazano konkretny produkt konkretnego

producenta a co za tym idzie winien być to tryb w oparciu o przesłanki art. 214 ust. PZP. Wnosimy tym samym o unieważnienie postępowania albo modyfikację zapisów w sposób umożliwiający zachowanie zasady konkurencyjności w postępowaniu.

Odpowiedź:

Zgodnie z odpowiedzią na pytanie nr 1.

Pytanie nr 6.1

Rozdział III

Podstawy wykluczenia oraz warunki udziału w postępowaniu, jednolity europejski dokument zamówienia

III.1\1.1.2\dysponuje osobami, które zostaną skierowane przez Wykonawcę do realizacji zamówienia, legitymującymi się odpowiednimi kwalifikacjami zawodowymi, wykształceniem i doświadczeniem umożliwiającym realizację zamówienia na odpowiednim poziomie jakości, tj. dysponuje co najmniej 2 (dwiema) osobami, posiadającymi łącznie specjalistyczne kwalifikacje potwierdzone certyfikatami:

1.1.2.1. Advanced Vulnerability Management lub równoważnym producenta oferowanego rozwiązania

1.1.2.2. Nexpose Certified Administrator lub równoważnym producenta oferowanego rozwiązania

1.1.2.3. Metasploit PRO Certified Specialist (MPCS) lub równoważnym producenta oferowanego rozwiązania

Powyższe zapisy wskazują na certyfikację tożsamą z produktami i ścieżkami certyfikacyjnymi tylko jednego producenta - Rapid7, co w kontekście zapisów dotyczących oprogramowania Metasploit PRO oraz systemów Rapid7 Nexpose lub Rapid7 Insight VM powoduje, że zapis o równoważności jest niemożliwy do spełnienia przez parterów jakiegokolwiek innego producenta. Wnosimy tym samym o unieważnienie postępowania albo modyfikację zapisów w sposób umożliwiający zachowanie zasady konkurencyjności w postępowaniu poprzez wyspecyfikowanie zakresu równoważności dla innych producentów.

Odpowiedź:

Zamawiający w odpowiedzi na pytanie, działając na podstawie art. 137 ust. 1 ustawy, wprowadza następujące zmiany (**zmiany zaznaczono boldem**) w treści SWZ:

ZMIANA NR 7:

1.1.2. dysponuje następującymi osobami, które zostaną skierowane przez Wykonawcę do realizacji zamówienia, legitymującymi się odpowiednimi kwalifikacjami zawodowymi, wykształceniem i doświadczeniem umożliwiającymi realizację zamówienia na odpowiednim poziomie jakości, tj. dysponuje co najmniej 2 (dwiema) osobami, posiadającymi łącznie specjalistyczne kwalifikacje potwierdzone certyfikatami:

1.1.2.1. Advanced Vulnerability Management lub równoważnym producenta oferowanego rozwiązania,

1.1.2.2. Nexpose Certified Administrator lub równoważnym producenta oferowanego rozwiązania,

1.1.2.3. Metasploit Pro Certified Specialist (MPCS) lub równoważnym producenta oferowanego rozwiązania,

przy czym każda z tych osób posiada co najmniej jeden z wyżej wymienionych certyfikatów.

UWAGA 4

Przez certyfikat równoważny, o którym mowa powyżej Zamawiający rozumie certyfikat, który:

1) jest analogiczny co do zakresu z przykładowym certyfikatem wskazanym z nazwy dla danej roli, co jest rozumiane jako:

a) analogiczna dziedzina merytoryczna wynikająca z roli, której dotyczy certyfikat,

b) analogiczny stopień poziomu kompetencji,

c) analogiczny poziom doświadczenia zawodowego wymaganego do otrzymania danego certyfikatu,

2) potwierdzony jest egzaminem (dotyczy tylko tych ról, których przykładowe certyfikaty muszą być potwierdzone egzaminem).

przyjmuje brzmienie:

1.1.2. **dysponuje następującymi osobami, które zostaną skierowane przez Wykonawcę do realizacji zamówienia, legitymującymi się odpowiednimi kwalifikacjami zawodowymi, wykształceniem i doświadczeniem umożliwiającymi realizację zamówienia na odpowiednim poziomie jakości, tj. dysponuje co najmniej 2 (dwiema) osobami, posiadającymi łącznie specjalistyczne kwalifikacje potwierdzone dwoma certyfikatami na najwyższym poziomie wydawanymi przez producenta oferowanego rozwiązania, tj.:**

1.1.2.1. certyfikat obejmujący projektowanie i wdrażanie oferowanego rozwiązania, a w szczególności:

i. projektowanie i wdrażanie rozwiązania w środowisku IT,

ii. optymalizacja środowiska w zakresie skanowania w celu uzyskania optymalnej jakości i wydajności,

iii. konfiguracja bezpiecznego skanowania zasobów IT bez konieczności zarządzania danymi uwierzytelniającymi,

iv. optymalizacja wymagań dotyczących raportowania zgodności i śledzenia;

v. prioretyzacja działań naprawczych,

vi. zwiększanie efektywności przepływów pracy w aspekcie zarządzania podatnościami poprzez automatyzację,

1.1.2.2. certyfikat obejmujący wykonywanie pentestów dla oferowanego rozwiązania, a w szczególności:

i. projektowanie, uruchamianie i skalowanie oprogramowania w środowisku IT,

ii. definiowanie zakresu skanów środowisk IT,

iii. odnajdywanie i wykorzystywanie podatnych na ataki urządzeń w środowisku IT,

iv. **uzyskiwanie dostępu do środowisk IT za pomocą predefiniowanych narzędzi wykorzystujących luki,**
v. **przejmowanie kontroli nad środowiskami IT za pomocą predefiniowanych narzędzi do przechwytywania sesji,**
vi. **zbieranie i generowanie informacji i raportów z odkrytych podatności/luk w zabezpieczeniach posiadających exploity,**

- przy czym każda z tych osób posiada co najmniej jeden z wyżej wymienionych certyfikatów.

ZMIANA NR 8:
Załącznik nr 6 do SWZ, **Oświadczenia – Wykaz osób**, w pkt 1), dotychczasowa tabela o treści:

1. <u>Dwie osoby, łącznie spełniające poniższe wymagania:</u>

Wymagania Zamawiającego wskazane w Rozdziale III pkt 1.1.2. SWZ	**Wypełnia Wykonawca**					
Dwie osoby, która posiadają łącznie specjalistyczne kwalifikacje potwierdzone certyfikatami: 1. Advanced Vulnerability Management lub równoważnym producenta oferowanego rozwiązania, 2. Nexpose Certified Administrator lub równoważnym producenta oferowanego rozwiązania, 3. Metasploit Pro Certified Specialist(MPCS) lub równoważnym producenta oferowanego rozwiązania, przy czym każda z tych osób posiada co najmniej jeden z wyżej wymienionych certyfikatów. ***UWAGA:*** *Przez certyfikat równoważny, o którym mowa powyżej Zamawiający rozumie certyfikat, który:* *1) jest analogiczny co do zakresu z przykładowym certyfikatem wskazanym z nazwy dla danej roli, co jest rozumiane jako:* *a) analogiczna dziedzina merytoryczna wynikająca z roli, której dotyczy certyfikat* *b) analogiczny stopień poziomu kompetencji,* *c) analogiczny poziom doświadczenia zawodowego wymaganego do otrzymania danego certyfikatu,* *2) potwierdzony jest egzaminem (dotyczy tylko tych ról, których przykładowe certyfikaty muszą być potwierdzone egzaminem).*	1	1.1	Imię i Nazwisko			
		1.2	Posiadany certyfikat	1.2.1	Nazwa certyfikatu	
				1.2.2	Podmiot wydający certyfikat	
				1.2.3	Nr certyfikatu *[o ile dotyczy]*	
				1.2.4	Data ważności certyfikatu [DD-MM-RRRR] *[o ile dotyczy]*	
		1.3	Posiadany certyfikat	1.3.1	Nazwa certyfikatu	
				1.3.2	Podmiot wydający certyfikat	
				1.3.3	Nr certyfikatu *[o ile dotyczy]*	
				1.3.4	Data ważności certyfikatu [DD-MM-RRRR] *[o ile dotyczy]*	
		1.4	Podstawa dysponowania osobą	1.4.1	Dysponowanie bezpośrednie	
				1.4.2	Dysponowanie osobą na podstawie art. 118 ustawy – Prawo zamówień publicznych	
	2	2.1	Imię i Nazwisko			
		2.2	Posiadany certyfikat	2.2.1	Nazwa certyfikatu	
				2.2.2	Podmiot wydający certyfikat	
				2.2.3	Nr certyfikatu *[o ile dotyczy]*	
				2.2.4	Data ważności certyfikatu [DD-MM-RRRR] *[o ile dotyczy]*	
		2.3	Posiadany certyfikat	2.3.1	Nazwa certyfikatu	

				2.3.2	Podmiot wydający certyfikat	
				2.3.3	Nr certyfikatu *[o ile dotyczy]*	
				2.3.4	Data ważności certyfikatu [DD-MM-RRRR] *[o ile dotyczy]*	
		2.4	Podstawa dysponowania osobą	2.4.1	Dysponowanie bezpośrednie	
				2.4.2	Dysponowanie osobą na podstawie art. 118 ustawy – Prawo zamówień publicznych	

przyjmuje brzmienie:

1. **Dwie osoby, łącznie spełniające poniższe wymagania:**

Wymagania Zamawiającego wskazane w Rozdziale III pkt 1.1.2. SWZ	Wypełnia Wykonawca					
Dwie osoby, która posiadają łącznie specjalistyczne kwalifikacje potwierdzone dwoma certyfikatami na najwyższym poziomie wydawanymi przez producenta oferowanego rozwiązania, tj.: **1. certyfikat obejmujący projektowanie i wdrażanie oferowanego rozwiązania, a w szczególności:** i. projektowanie i wdrażanie rozwiązania w środowisku IT, ii. optymalizacja środowiska w zakresie skanowania w celu uzyskania optymalnej jakości i wydajności, iii. konfiguracja bezpiecznego skanowania zasobów IT bez konieczności zarządzania danymi uwierzytelniającymi, iv. optymalizacja wymagań dotyczących raportowania zgodności i śledzenia; v. prioretyzacja działań naprawczych, vi. zwiększanie efektywności przepływów pracy w aspekcie zarządzania podatnościami poprzez automatyzację, **2. certyfikat obejmujący wykonywanie pentestów dla oferowanego rozwiązania, a w szczególności:** i. projektowanie, uruchamianie i skalowanie oprogramowania w środowisku IT, ii. definiowanie zakresu skanów środowisk IT, iii. odnajdywanie i wykorzystywanie podatnych na ataki urządzeń w środowisku IT, iv. uzyskiwanie dostępu do środowisk IT za pomocą predefiniowanych narzędzi wykorzystujących luki, v. przejmowanie kontroli nad środowiskami IT za pomocą	1.	1.1	**Imię i Nazwisko**			
		1.2	**Posiadany certyfikat**	1.2.1	Nazwa certyfikatu i poziom certyfikatu	
				1.2.2	Podmiot wydający certyfikat	
				1.2.3	Nr certyfikatu *[o ile dotyczy]*	
				1.2.4	Data ważności certyfikatu [DD-MM-RRRR] *[o ile dotyczy]*	
				1.2.5	Obszar rozwiązań i technologii potwierdzający poziom certyfikatu	
		1.3	**Podstawa dysponowania osobą**	1.3.1	Dysponowanie bezpośrednie	
				1.3.2	Dysponowanie osobą na podstawie art. 118 ustawy – Prawo zamówień publicznych	
	2.	2.1	**Imię i Nazwisko**			
		2.2	**Posiadany certyfikat**	2.2.1	Nazwa certyfikatu i poziom certyfikatu	
				2.2.2	Podmiot wydający certyfikat	
				2.2.3	Nr certyfikatu *[o ile dotyczy]*	
				2.2.4	Data ważności certyfikatu [DD-MM-RRRR] *[o ile dotyczy]*	
				2.2.5	Obszar rozwiązań i technologii potwierdzający poziom certyfikatu	

predefiniowanych narzędzi do przechwytywania sesji, vi. zbieranie i generowanie informacji i raportów z odkrytych podatności/luk w zabezpieczeniach posiadających exploity. **- przy czym każda z tych osób posiada co najmniej jeden z wyżej wymienionych certyfikatów.**		2.3	Podstawa dysponowania osobą	2.3.1	Dysponowanie bezpośrednie	
				2.3.2	Dysponowanie osobą na podstawie art. 118 ustawy – Prawo zamówień publicznych	

Pytanie nr 6.2

Specyfikacja systemu

1.16 Zwiększenie wydajności aplikacji musi być możliwe dzięki rozbudowaniu środowiska poprzez:

a) zmianę procesora,

b) zwiększenie pamięci RAM, c) zwiększenie pojemności pamięci masowej, d) instalacji dodatkowych, nielimitowanych silników skanujących Powyższe wymagania w bezpośredni sposób zostały przeniesione z dokumentacji systemu producenta Rapid7 i tylko przez tę jedną technologię mogą być spełnione. Dokumentacja dostępna pod adresem: https://docs.rapid7.com/insightvm/using-other-tuning-options. Nie ma bowiem możliwości spełnienia tego wymagania poprzez zaoferowanie ŻADNYCH INNYCH DOSTĘPNYCH NA RYNKU ROZWIĄZAŃ konkurencyjnych. Wnosimy tym samym o unieważnienie postępowania albo modyfikację zapisów w sposób umożliwiający zachowanie zasady konkurencyjności w postępowaniu.

Odpowiedź:

Zamawiający w odpowiedzi na pytanie, działając na podstawie art. 137 ust. 1 ustawy, wprowadza następujące zmiany (**zmiany zaznaczono boldem**) w treści SWZ:

ZMIANA NR 9:

Załącznik nr 7 do SWZ, projektowane postanowienia umowy - Załącznik nr 1 do ppu Specyfikacja Systemu, pkt 1 ppkt 1.16 o treści:

„1.16. Zwiększenie wydajności aplikacji musi być możliwe dzięki rozbudowaniu środowiska poprzez:

a) zmianę procesora,
b) zwiększenie pamięci RAM,
c) zwiększenie pojemności pamięci masowej,
d) instalacji dodatkowych, nielimitowanych silników skanujących"

przyjmuje brzmienie:

„1.16 **Zamawiający wymaga aby oferowane rozwiązanie umożliwiało zwiększenie wydajności aplikacji."**

Pytanie nr 6.3

12 Pozostałe funkcjonalności: 2) Integracja z Metasploit PRO 3) wymiana informacji pomiędzy obiema aplikacjami powinna odbywać się automatycznie, bez potrzeby pobierania/ wgrywania jakichkolwiek plików przez użytkowników obu aplikacji. Powyższe zapisy wskazują na oprogramowanie jednego producenta, gdyż tylko i wyłącznie systemy (aplikacje) Rapid7 Nexpose/ Insight VM oraz Metasploit PRO są w stanie w opisany sposób wymieniać informacje w ramach integracji. Stanowi to wskazanie jedynie na oprogramowanie pochodzące od jednego producenta - Rapid7, co stanowi ograniczenie konkurencji wobec innych producentów i systemów. Nie ma bowiem możliwości spełnienia tego wymagania poprzez zaoferowanie ŻADNYCH INNYCH DOSTĘPNYCH NA RYNKU ROZWIĄZAŃ konkurencyjnych. Wnosimy tym samym o unieważnienie postępowania albo modyfikację zapisów w sposób umożliwiający zachowanie zasady konkurencyjności w postępowaniu.

Odpowiedź:

Zamawiający w odpowiedzi na pytanie, działając na podstawie art. 137 ust. 1 ustawy, wprowadza następujące zmiany (**zmiany zaznaczono boldem**) w treści SWZ Załącznik nr 7 do SWZ projektowane postanowienia umowy – Załącznik nr 1 do ppu, pkt pkt 12 ppkt 3) o treści:

ZMIANA NR 10:

„3) wymiana informacji pomiędzy obiema aplikacjami powinna odbywać się automatycznie, bez potrzeby pobierania / wgrywania jakichkolwiek plików przez użytkowników obu aplikacji."

przyjmuje brzmienie:

„3) wymiana informacji pomiędzy obiema aplikacjami powinna odbywać się automatycznie, bez potrzeby pobierania/ wgrywania jakichkolwiek plików przez użytkowników obu aplikacji **lub przez interfejs API REST do automatyzacji testów**."

II. **Działając na podstawie art. 137 ust. 1 ustawy Zamawiający, zmienia treść SWZ w niżej opisanym zakresie.**

ZMIANA NR 11:
Rozdział IX. SWZ, Sposób oraz termin składania ofert i otwarcia ofert - pkt 2 i 3 przyjmują brzmienie:

*2. Termin składania ofert upływa w dniu **14.10.2022 r.** o godzinie 11.00*
*3. Otwarcie ofert odbędzie się w dniu **14.10.2022 r.** o godzinie 12.00"*

ZMIANA NR 12
Rozdział VII SWZ, Termin związania ofertą - przyjmuje brzmienie:
*Wykonawcy pozostają związani złożoną ofertą do dnia **11.01.2023 r.** Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert."*

III. **Zamawiający informuje, że dokonane zmiany SWZ są wiążące dla Wykonawców.**

IV. **Zamawiający informuje, że zamieszcza na Platformie Zakupowej materiał pomocniczy zawierający uaktualniony Załączniki nr 6 do SWZ w wersji edytowalnej [word], zgodnie z przedstawionymi powyżej zmianami.**

ZASTĘPCA PREZESA
Jacek Paziewski