ESENDER_LOGIN:	ENOTICES
CUSTOMER_LOGIN:	IzabellaHelbing
NO_DOC_EXT:	2022-148828
SOFTWARE VERSION:	13.2.0
ORGANISATION:	ENOTICES
COUNTRY:	EU
PHONE:	/
E_MAIL:	izabella.helbing@arimr.gov.pl

LANGUAGE:	PL
CATEGORY:	ORIG
FORM:	F14
VERSION:	R2.0.9.S05
DATE_EXPECTED_PUBLICATION:	/

Sprostowanie

Ogłoszenie zmian lub dodatkowych informacji

Usługi

Podstawa prawna:
Dyrektywa 2014/24/UE

Sekcja I: Instytucja zamawiająca/podmiot zamawiający

I.1) **Nazwa i adresy**

Oficjalna nazwa: Agencja Restrukturyzacji i Modernizacji Rolnictwa
Adres pocztowy: Al. Jana Pawła II Nr 70
Miejscowość: Warszawa
Kod NUTS: PL911 Miasto Warszawa
Kod pocztowy: 00-175
Państwo: Polska
E-mail: zamowieniapubliczne@arimr.gov.pl
Tel.: +48 225950736
Faks: +48 223185411
Adresy internetowe:
Główny adres: http://www.arimr.gov.pl

Sekcja II: Przedmiot

II.1) **Wielkość lub zakres zamówienia**

II.1.1) **Nazwa:**

Zakup i wdrożenie systemu do zarządzania podatnościami „Vulnerability Management – VM” w środowisku hybrydowym
Numer referencyjny: DPiZP.2610.15.2022

II.1.2) **Główny kod CPV**

72268000 Usługi dostawy oprogramowania

II.1.3) **Rodzaj zamówienia**

Usługi

II.1.4) **Krótki opis:**

Przedmiotem zamówienia jest zakup usług wdrożenia dla Agencji Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie (al. Jana Pawła II 70, 00-175 Warszawa), zwanej dalej „Zamawiającym”, Systemu do zarządzania podatnościami „Vulnerability Management - VM” (zwanego dalej „Systemem”) w środowisku hybrydowym (on-prem i w chmurze producenta) realizowanego poprzez dostawę niezbędnych licencji czasowych (na zasadach subskrypcji), oprogramowania, pakietów suportowych zapewniających wsparcie producenta Systemu oraz świadczenie Gwarancji dla wdrożonego Systemu na zasadach określonych w projektowanych postanowieniach umowy (dalej: „ppu”), stanowiących Załącznik nr 7 do specyfikacji warunków zamówienia (dalej: „SWZ”), oraz na ogólnych warunkach licencyjnych Producenta.

Sekcja VI: Informacje uzupełniające

VI.5) **Data wysłania niniejszego ogłoszenia:**

26/09/2022

VI.6) **Numer pierwotnego ogłoszenia**

Pierwotne ogłoszenie przesłane przez eNotices:

Login TED eSender: ENOTICES
Logowanie jako klient TED eSender: IzabellaHelbing
Dane referencyjne ogłoszenia: 2022-131612
Numer ogłoszenia w Dz.Urz. UE – OJ/S: 2022/S 167-474075
Data wysłania pierwotnego ogłoszenia: 26/08/2022

Sekcja VII: Zmiany

VII.1) **Informacje do zmiany lub dodania**

VII.1.1) **Przyczyna zmiany**

Modyfikacja pierwotnej informacji podanej przez instytucję zamawiającą

VII.1.2) **Tekst, który należy poprawić w pierwotnym ogłoszeniu**

Numer sekcji: II.2.4
Miejsce, w którym znajduje się tekst do modyfikacji: ppkt 1) lit. b
Zamiast:
b) licencji czasowej na okres 36 miesięcy (na zasadach subskrypcji) Metasploit PRO umożliwiającej wykonywanie testów penetracyjnych i aktywnego badania zabezpieczeń systemów,
Powinno być:
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,
Numer sekcji: III.1.1
Miejsce, w którym znajduje się tekst do modyfikacji: rozdz. III. pkt 1.1. ppkt 1.1.1.
Zamiast:
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).
Powinno być:

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.
Numer sekcji: III.1.2
Miejsce, w którym znajduje się tekst do modyfikacji: ppkt 1.1.2.
Zamiast:
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).
Powinno być:
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.
Numer sekcji: IV.2.2
Miejsce, w którym znajduje się tekst do modyfikacji: Termin składania ofert lub wniosków o dopuszczenie do udziału
Zamiast:
Data: 30/09/2022
Czas lokalny: 11:00
Powinno być:
Data: 14/10/2022
Czas lokalny: 11:00
Numer sekcji: IV.2.6
Miejsce, w którym znajduje się tekst do modyfikacji: Minimalny okres, w którym oferent będzie związany ofertą
Zamiast:
Data: 28/12/2022
Powinno być:
Data: 11/01/2023
Numer sekcji: IV.2.7
Miejsce, w którym znajduje się tekst do modyfikacji: Warunki otwarcia ofert
Zamiast:
Data: 30/09/2022
Czas lokalny: 12:00
Powinno być:
Data: 14/10/2022
Czas lokalny: 12:00

VII.2) **Inne dodatkowe informacje:**