Agencja Restrukturyzacji
i Modernizacji Rolnictwa

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

p. o. Zastępcy Prezesa
Aneta Burghardt

Wykonawcy

Nasz znak: Data:

ZP. 4 .DPiZP.2610.6.2023.IH 14 .06.2023 r.

Sprawa: postępowanie o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego na **„Zakup usługi subskrypcji oprogramowania SOAR przez okres 36 miesięcy wraz z usługą wdrożenia i konsultacjami"**

I. Działając na podstawie art. 135 ust. 1 i 2 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2022r. poz. 1710 ze zm.; 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
Dot: Tabela 2 (rozwiązanie równoważne) punkt 7
Czy Zamawiający dopuści rozwiązanie obsługujące 500 gotowych integracji ?
Odpowiedź:
Zamawiający w odpowiedzi na pytanie, działając na podstawie art. 137 ust. 1 ustawy, wprowadza następującą zmianę w treści Specyfikacji Warunków Zamówienia (dalej: „SWZ"):

ZMIANA NR 1
W Załączniku nr 1 do projektowanych postanowień umowy (dalej: „ppu") stanowiących Załącznik nr 8 do SWZ, Tabela 2, L.p. 7 o treści:

7.	Oferowane rozwiązanie musi zapewniać zestaw co najmniej 900 gotowych integracji pozwalających na szybką, dwustronną komunikację z zewnętrznymi systemami.

przyjmuje brzmienie:

7.	Oferowane rozwiązanie musi zapewniać zestaw co najmniej 250 gotowych integracji pozwalających na szybką, dwustronną komunikację z zewnętrznymi systemami.

Pytanie nr 2
Dot: Tabela 2 (rozwiązanie równoważne) punkt 14
Czy zamawiający zrezygnuje z integracji konektorów Netwitenss EndPoint, hpsm, rtir, secureworks ? Tak postawione wymaganie może spełnić tylko jeden producent (Palo Alto)
Odpowiedź:
Zamawiający w odpowiedzi na pytanie, działając na podstawie art. 137 ust. 1 ustawy, wprowadza następującą zmianę w treści SWZ:

ZMIANA NR 2
W Załączniku nr 1 do ppu stanowiących Załącznik nr 8 do SWZ, Tabela 2, L.p. 14 o treści:

14.	Oferowane rozwiązanie musi zapewniać gotową integrację wiodących produktów i usług z zakresu bezpieczeństwa IT, w tym: 1. Microsoft Active Directory 2. Narzędzi komunikacyjnych np. serwerów pocztowych, Slack, Gsuite, MS Teams. 3. Systemów klasy SIEM i analizy logów w tym: IBM QRadar, McAfee, RSA Netwitness, Splunk. 4. Systemów ochrony stacji końcowych klasy EPP (https://www.gartner.com/it-glossary/endpoint-

	protection-platform-epp/) uwzględniających funkcje blokowania, jak również analizy i odpowiedzi w tym: Fidelis EDR, FireEye HX, McAfee, RSA Netwitness EndPoint, Symantec, Palo Alto Networks Cortex XDR, TrendMicro Deep Security, Tanium 5. Systemów bezpieczeństwa sieciowego typu firewall, NGFW, IPS/IDS 6. Repozytoriów Threat Intelligence w tym: VirusTotal, Cofense, Azure/Office365 feeds, Spamhaus, ProofPoint, Autofocus, MISP, MITRE ATT&CK, IBM X-Force oraz otwartych formatów: JSON, TXT, CSV. 7. Narzędzi typu forensics i systemów sand-box w tym: FAME, Cuckoo, FireEye, Palo Alto Networks Wildfire, Cisco Threat Grid, Volatility, Rekall. 8. Zewnętrznych baz danych w tym: PostgreSQL, MySQL, MangoDB, Microsoft SQL, Elastic 9. Systemów IT Ticketing / ITS w tym: BMC Remedy, HPSM, OTRS, RTIR, BMC, Jira, ServiceNow, Zendesk, Secureworks, Salesforce, RSA Archer. 10. Skanerem podatności Rapid7

przyjmuje brzmienie:

14.	Oferowane rozwiązanie musi zapewniać gotową integrację wiodących produktów i usług z zakresu bezpieczeństwa IT, w tym: 1. Microsoft Active Directory 2. Narzędzi komunikacyjnych np. serwerów pocztowych, Slack, Gsuite, MS Teams. 3. Systemów klasy SIEM i analizy logów w tym: IBM QRadar, McAfee, RSA Netwitness, Splunk. 4. Systemów ochrony stacji końcowych klasy EPP (https://www.gartner.com/it-glossary/endpoint-protection-platform-epp/) uwzględniających funkcje blokowania, jak również analizy i odpowiedzi w tym: Fidelis EDR, FireEye HX, McAfee, Symantec, Palo Alto Networks Cortex XDR, TrendMicro Deep Security, 5. Systemów bezpieczeństwa sieciowego typu firewall, NGFW, IPS/IDS 6. Repozytoriów Threat Intelligence w tym: VirusTotal, Cofense, Azure/Office365 feeds, Spamhaus, ProofPoint, Autofocus, MISP, MITRE ATT&CK, IBM X-Force oraz otwartych formatów: JSON, TXT, CSV. 7. Narzędzi typu forensics i systemów sand-box w tym: FAME, Cuckoo, FireEye, Palo Alto Networks Wildfire, Cisco Threat Grid, Volatility, Rekall. 8. Zewnętrznych baz danych w tym: PostgreSQL, MySQL, MangoDB, Microsoft SQL, Elastic 9. Systemów IT Ticketing / ITS - Jira, 10. Skanerem podatności - Rapid7.

Pytanie nr 3
Dot: Tabela 2 (rozwiązanie równoważne) punkt 28
Czy zamawiający dopuści rozwiązanie z trybem "debug", który dostarcza dokładne informacje o wykonaniu każdego kroku.
Odpowiedź:
Zamawiający podtrzymuje zapisy SWZ.

Pytanie nr 4
Dot:Tabela 2 (rozwiązanie równoważne) punkt 30
Czy zamawiający dopuści rozwiązanie z trybem "debug", który dostarcza dokładne informacje o wykonaniu każdego kroku.
Odpowiedź:
Zamawiający podtrzymuje zapisy SWZ.

Pytanie nr 5
Dot: Tabela 2 (rozwiązanie równoważne) punkt 53
Czy zamawiający zrezygnuje z wymagania automatycznego pozyskiwania poświadczeń CyberArk AIM, FUDO ? Tak postawione wymaganie może spełnić tylko jeden producent (Palo Alto).
Odpowiedź:
Zamawiający w odpowiedzi na pytanie, działając na podstawie art. 137 ust. 1 ustawy, wprowadza następującą zmianę w treści SWZ:

ZMIANA NR 3
W Załączniku nr 1 do ppu stanowiących Załącznik nr 8 do SWZ, Tabela 2, L.p. 53 o treści:

53.	Oferowane rozwiązanie musi pozwalać na automatyczne pozyskiwanie poświadczeń do integrowanych systemów trzecich z zewnętrznych rozwiązań do zarządzania poświadczeniami, takich jak np. CyberArk AIM, FUDO.

przyjmuje brzmienie:

53.	Oferowane rozwiązanie musi pozwalać na automatyczne pozyskiwanie poświadczeń do integrowanych systemów trzecich z zewnętrznych rozwiązań do zarządzania poświadczeniami, takich jak np. CyberArk AIM.

Pytanie nr 6
Dot: Tabela 2 (rozwiązanie równoważne) punkt 54
Czy zamawiający zrezygnuje z wymagania użycia wspólnego konta technicznego w wielu integracjach z systemami trzecimi ? Tak postawione wymaganie może spełnić tylko jeden producent (Palo Alto).
Odpowiedź:
Zamawiający w odpowiedzi na pytanie, działając na podstawie art. 137 ust. 1 ustawy, wprowadza następującą zmianę w treści SWZ:

ZMIANA NR 4
W Załączniku nr 1 do ppu stanowiących Załącznik nr 8 do SWZ, Tabela 2, L.p. 54 o treści:

54	Oferowane rozwiązanie musi pozwalać na proste wprowadzenie globalnych zestawów poświadczeń w celu ułatwienia użycia wspólnego konta technicznego w wielu integracjach z systemami trzecimi.

przyjmuje brzmienie:

54	Oferowane rozwiązanie musi pozwalać na proste wprowadzenie globalnych zestawów poświadczeń.

Pytanie nr 7
Dot: Tabela 2 (rozwiązanie równoważne) punkt 71
Czy zamawiający zrezygnuje z wymagania dostępności aplikacji w App Store i z Google Play ? Tak postawione wymaganie może spełnić tylko jeden producent (Palo Alto).
Odpowiedź:
Zamawiający podtrzymuje zapisy SWZ.

Pytanie nr 8
Dot: Tabela 2 (rozwiązanie równoważne) punkt 93 Czy zamawiający zrezygnuje z wymagania dostarczenia komponentu typu agent końcowy do uruchamiania komend lub wykonywania skryptów bezpośrednio na badanej stacji w celu pełnego wsparcia zdalnej analizy incydentu ? Tak postawione wymaganie może spełnić tylko jeden producent (Palo Alto)
Odpowiedź:
Zamawiający podtrzymuje zapisy SWZ.

Pytanie nr 9
Dot. Specyfikacja Systemu, Tabela 2, pkt 7:
Prosimy o doprecyzowanie, stosownie do art. 99 ust. 1 ustawy Pzp, jakich integracji konkretnie wymaga Zamawiający? Prosimy o wyjaśnienie i doprecyzowanie, jakie integracje są uzasadnione potrzebami Zamawiającego, gdyż liczb 900 integracji jest nieproporcjonalnie wysoka i wydaje się istotnie zawyżona w stosunku do przedmiotu wdrożenia. Żądanie tak wysokiej liczby integracji wpływa znacząco na ograniczenie konkurencyjności postępowania, wnosimy zatem o zmniejszenie liczby wymaganych integracji do 300 oraz wskazanie, jakie integracje są wymagane.
Odpowiedź:
Patrz odpowiedź Zamawiającego na pytanie nr 1. Jednocześnie Zamawiający informuje, iż przewiduje integrację z posiadanymi systemami bezpieczeństwa w infrastrukturze IT ARiMR (np. NGFW, NAC, PIM/PAM itp.).

Pytanie nr 10
Dot. Specyfikacja Systemu, Tabela 2, pkt 16:
Prosimy o doprecyzowanie, stosownie do art. 99 ust. 1 ustawy Pzp, jakich prekonfigurowanych, gotowych scenariuszy użycia konkretnie wymaga Zamawiający? Prosimy o wyjaśnienie i doprecyzowanie, jakie scenariusze są uzasadnione potrzebami Zamawiającego, gdyż liczba 300 prekonfigurowanych, gotowych scenariuszy użycia jest nieproporcjonalnie wysoka i wydaje się istotnie zawyżona w stosunku do przedmiotu wdrożenia. Żądanie tak wysokiej liczby tych scenariuszy wpływa znacząco na ograniczenie konkurencyjności postępowania, wnosimy zatem o zmniejszenie liczby wymaganych scenariuszy do 150 oraz wskazanie, jakie integracje są wymagane.
Odpowiedź:
Zamawiający w odpowiedzi na pytanie, działając na podstawie art. 137 ust. 1 ustawy, wprowadza następującą zmianę w treści SWZ:

ZMIANA NR 5

W Załączniku nr 1 do ppu stanowiących Załącznik nr 8 do SWZ, Tabela 2, L.p. 16 o treści:

16.	Oferowane rozwiązanie musi zapewniać co najmniej 300 prekonfigurowanych, gotowych scenariuszy użycia (ang. playbooks) pozwalających na ich natychmiastowe wykorzystanie do automatycznej obsługi incydentu bezpieczeństwa.

przyjmuje brzmienie:

16.	Oferowane rozwiązanie musi zapewniać co najmniej 150 prekonfigurowanych, gotowych scenariuszy użycia (ang. playbooks) pozwalających na ich natychmiastowe wykorzystanie do automatycznej obsługi incydentu bezpieczeństwa.

Jednocześnie Zamawiający wyjaśnia, iż wymaga gotowych scenariuszy użycia (ang. playbooks) pozwalających na ich natychmiastowe wykorzystanie do automatycznej obsługi incydentu bezpieczeństwa np. phisingu, malware, DoS, ransomware, web defacement.

Pytanie nr 11

Dot. Specyfikacja Systemu, Tabela 2, pkt 28:

Prosimy o doprecyzowanie opisu przedmiotu zamówienia i wyjaśnienie czy Zamawiający dopuści rozwiązanie posiadające playbook debugger, który umożliwia wykonywanie playbooków dla testowych danych, wyświetlanie dodatkowych logów na poziomie debug i zatrzymanie wykonania w wybranym miejscu, ale bez funkcji wykonania krokowego?

Uruchomienie scenariusza w trybie krokowym jest wymaganiem nieproporcjonalnym do znacznego ograniczenia czy wręcz eliminacji konkurencyjności postępowania, które powoduje. Jednocześnie, nie jest ono uzasadnione obiektywnymi potrzebami Zamawiającego, gdyż funkcjonalność może zostać zapewniona i pełnić swoją rolę bez tego wymagania, które nie ma obiektywnie istotnego znaczenia. Jego utrzymanie powoduje, że opisane kryteria równoważności jedynie pozornie dopuszczają zaoferowanie rozwiązania równoważnego.

Odpowiedź:

Zamawiający podtrzymuje zapisy SWZ.

Pytanie nr 12

Dot. Specyfikacja Systemu, Tabela 2, pkt 30:

Prosimy o doprecyzowanie opisu przedmiotu zamówienia i wyjaśnienie czy Zamawiający dopuści rozwiązanie posiadające playbook debugger, który umożliwia wykonywanie playbooków dla testowych danych, wyświetlanie dodatkowych logów na poziomie debug i zatrzymanie wykonania w wybranym miejscu, ale bez możliwości modyfikacji danych w trakcie wykonania playbooka? Ta ostatnia wymagana funkcja jest wymaganiem nieproporcjonalnym do znacznego ograniczenia czy wręcz eliminacji konkurencyjności postępowania, które powoduje. Jednocześnie, nie jest ono uzasadnione obiektywnymi potrzebami Zamawiającego, gdyż funkcjonalność może zostać zapewniona i pełnić swoją rolę bez tego wymagania, które nie ma obiektywnie istotnego znaczenia. Jego utrzymanie powoduje, że opisane kryteria równoważności jedynie pozornie dopuszczają zaoferowanie rozwiązania równoważnego.

Odpowiedź:

Zamawiający podtrzymuje zapisy SWZ.

Pytanie nr 13

Dot. Specyfikacja Systemu, Tabela 2, pkt 71:

Wnosimy o usunięcie przedmiotowego wymagania. Aktualnie, taka funkcjonalność: wgląd w stan SOC, przetwarzane incydenty, chat oraz dashboardy, nie jest w praktyce wykorzystywany i jego wymaganie nie jest uzasadnione. Taki wgląd nie jest przydatny, a na pewno nie w takim stopniu, aby uzasadniać jego wprowadzenie, które prowadzi do istotnego ograniczenia konkurencyjności postępowania. Utrzymanie tego wymagania powoduje, że opisane kryteria równoważności jedynie pozornie dopuszczają zaoferowanie rozwiązania równoważnego. Zgodnie z przepisami art. 99 ustawy Pzp, każde ze stawianych wymagań powinno znajdować uzasadnienie w obiektywnych potrzebach Zamawiającego i określona funkcjonalność nie powinna być wymagana tylko z tej przyczyny, że posiada ją produkt referencyjny. Jeśli jest ona nieprzydatna lub posiada stosunkowo małe znaczenie dla Zamawiającego, to jej wymaganie jest niedopuszczalne jako niezgodne z zasadami proporcjonalności oraz uczciwej konkurencji i równego traktowania wykonawców.

Odpowiedź:

Zamawiający podtrzymuje zapisy SWZ.

Pytanie nr 14

Dot. Specyfikacja Systemu, Tabela 2, pkt 72, 75-77:

Czy zamawiający będzie świadczył usług innym instytucjom i firmom? Prosimy o doprecyzowanie opisu przedmiotu zamówienia poprzez wskazanie, co najmniej liczby takich tenantów

Odpowiedź:

W odpowiedzi Zamawiający informuje, iż utworzył spółkę Agro Aplikacje Sp. z o.o. z siedzibą w Warszawie i adresem: ul. Poleczki 35 02-822 Warszawa („spółka") powołanej w celu realizacji zadań polegających na zapewnieniu rozwoju systemów i rozwiązań teleinformatycznych służących realizacji zadań Zamawiającego zgodnie z art. 21a ustawy z dnia 9 maja 2008 r. o Agencji Restrukturyzacji i Modernizacji Rolnictwa.

Pytanie nr 15

Dot. Specyfikacja Systemu, Tabela 2, pkt 73:

Wnosimy o rozbudowanie wymagań opisu przedmiotu zamówienia w tym zakresie i wyjaśnienie, z jakiego powodu Zamawiający wymaga zaoferowania rozwiązania w architekturze kontenerowej? Zgodnie z przepisami art. 99 ustawy Pzp, każde ze stawianych wymagań powinno znajdować uzasadnienie w obiektywnych potrzebach Zamawiającego i określona funkcjonalność nie powinna być wymagana tylko z tej przyczyny, że posiada ją produkt referencyjny. Jeśli jest ona nieprzydatna lub posiada stosunkowo małe znaczenie dla Zamawiającego, to jej wymaganie jest niedopuszczalne jako niezgodne z zasadami proporcjonalności oraz uczciwej konkurencji i równego traktowania wykonawców.

Odpowiedź:

Zamawiający podtrzymuje zapisy SWZ. Jednocześnie wyjaśnia, iż zgodnie z najlepszą wiedzą Zamawiającego nowoczesne rozwiązania na rynku opierają się na architekturze kontenerowej.

Pytanie nr 16

Dot. Specyfikacja Systemu, Tabela 2, pkt 93:

Wykonawca wskazuje, że przedmiotowe wymaganie jest typowe dla systemów XDR, a nie systemów SOAR. Czy zamawiający dopuszcza rozwiązanie, w którym komendy są wykonywane z wykorzystaniem protokołów zdalnego dostępu np. Windows Raymond management, SSH?

Takie rozwiązanie spełnia obiektywne potrzeby Zamawiającego, podczas, gdy wskazane wymaganie nie jest adekwatne do przedmiotu zamówienia ani proporcjonalne do ograniczenia konkurencyjności postępowania, do którego prowadzi.

Odpowiedź:

Zamawiający podtrzymuje zapisy SWZ.

Pytanie nr 17

Dotyczy: Załącznika nr 8 do SWZ - projektowane postanowienia umowy

Zwracamy się z pytaniem, czy Zamawiający dopuszcza możliwość modyfikacji treści ust. 7 w §10 o dodatkowy zapis: „Zamawiający oświadcza, że zapoznał z klauzulami informacyjnymi w zakresie przetwarzania danych osobowych stanowiącymi Załączniki nr ..... do Umowy osoby wyznaczone do kontaktów roboczych oraz odpowiedzialne za koordynację i realizację Umowy".

Odpowiedź:

Zamawiający podtrzymuje zapisy SWZ.

Pytanie nr 18

Dotyczy: Załącznika nr 8 do SWZ - projektowane postanowienia umowy

Zwracamy się z pytaniem, czy Zamawiający dopuszcza możliwość usunięcia ust. 8 w §10. W ust. 7 jest zobowiązanie Wykonawcy do zapoznania się z klauzulami informacyjnymi oraz poinformowanie podwykonawców i osób wyznaczonych do kontaktu o treści klauzul informacyjnych. Realizacja tych czynności jest obowiązkiem wynikającym z umowy, więc zbędne wydaje się potwierdzanie tego faktu na odrębnym oświadczeniu.

Odpowiedź:

Zamawiający podtrzymuje zapisy SWZ.

Pytanie nr 19

Dotyczy: Załącznika nr 8 do SWZ - projektowane postanowienia umowy

Zwracamy się z pytaniem, czy Zamawiający dopuszcza możliwość dodania kolejnego ustępu w §10 o następującej treści: „Jeżeli w ramach realizacji Zamówienia Zamawiający będzie powierzał Wykonawcy przetwarzanie danych osobowych w takim przypadku powierzenie będzie następowało na warunkach określonych w Umowie powierzenia przetwarzania danych osobowych stanowiącej Załącznik nr .... do Umowy".

Odpowiedź:

Zamawiający podtrzymuje zapisy SWZ.

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

ZMIANA NR 6

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

*„2. Termin składania ofert upływa w dniu **30.06.2023 r. o godzinie 11.00**.*
*3. Otwarcie ofert odbędzie się w dniu **30.06.2023 r. o godzinie 12.00**."*

ZMIANA NR 7

Rozdział VII SWZ, Termin związania ofertą - przyjmuje brzmienie:

*„Wykonawcy pozostają związani złożoną ofertą do dnia **27.09.2023 r**. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert."*

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

p.o. ZASTĘPCA PREZESA
Aneta Burobaitis

Podpis Zamawiającego