Agencja Restrukturyzacji
i Modernizacji Rolnictwa

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

Prezes
Halina Szymańska

Wykonawcy

Wasze pismo znak:	Data:	Nasz znak:	Data:
		P. 470 .DPiZP.2610.10.2022	13 .02.2023 r.

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego na „Usługę dostawy oraz wdrożenia środowiska ochrony malware (SandBOX) na potrzeby rozwiązań IT".

I. Działając na podstawie przepisu art. 135 ust. 2 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710 ze zm., dalej: „ustawa Pzp"), Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie i adresem: Al. Jana Pawła II 70, 00-175 Warszawa, zwana dalej „Zamawiającym", udziela wyjaśnień treści Specyfikacji Warunków Zamówienia (dalej: „SWZ") w niżej opisanym zakresie.

II. W wyniku wprowadzonych poniżej modyfikacji SWZ, ujętych w załączniku nr 1 do projektowanych postanowień umowy (dalej: ppu) *Specyfikacja Analizatora Plików*, zmianie uległa numeracja punktów niniejszego załącznika. Zamawiający zgodnie z odpowiedzią na pytanie nr 9 poniżej wykreślił z wymagań pkt 42 o treści „Analizator musi umożliwiać przegląd statystyki danych zebranych na poszczególnych interfejsach urządzenia". W związku z dokonaną zmianą zmianie uległa numeracja od pkt 42 w dół. W poniższych odpowiedziach Zamawiający podaje aktualną numerację po zmianie SWZ jak również numerację sprzed zmiany SWZ. Jednocześnie Zamawiający informuje, że zmieniony Załącznik nr 1 do ppu ze zmianami zaznaczonymi boldem, stanowi załącznik do niniejszego pisma.

Pytanie 1
Dotyczy: Specyfikacja Analizatora plików pkt. 45 Zamawiający wymaga aby „Analizator integrował się bezpośrednio z posiadanym przez Zamawiającego rozwiązaniem Fireeye Detection ON Demand, co najmniej w oparciu o wymianę artefaktów ataku wykrytych w skanowanych repozytoriach plików oraz musi umożliwiać przegląd generowanych alertów". W związku z powyższym zwracamy się z pytaniem:
Czy Zamawiający zaakceptuje rozwiązanie, które posiada funkcjonalność w pełni zgodną z FireEye Detection On Demand wbudowaną w proponowane rozwiązanie fizyczne bez konieczności integracji?
Odpowiedź:
Zamawiający działając na podstawie art. 137 ust. 1 ustawy dokonuje zmiany treści SWZ w niżej opisanym zakresie:

SWZ, załącznik nr 7 projektowane postanowienia umowy, załącznik nr 1 *Specyfikacja Analizatora plików*, **pkt 44)** (poprzednio pkt 45) przyjmuje brzmienie:

„44) Analizator musi integrować się bezpośrednio z posiadanym przez zamawiającego rozwiązaniem Trellix Detection as a Service, co najmniej w oparciu o wymianę artefaktów ataku wykrytych w skanowanych repozytoriach plików oraz musi umożliwiać przegląd generowanych alertów. **W przypadku zaoferowania rozwiązania posiadającego funkcjonalność w pełni zgodną z Trellix Detection as a Servicewbudowaną w proponowane rozwiązanie w celu zapewnienia analitykom wysokiego stopnia automatyzacji w aspekcie wdrażania schematów działań Zamawiający dopuszcza wykorzystanie innego narzędzia wyłącznie przez interface API (dalej: API).**"

Pytanie 2
Czy Zamawiający wymaga zapewnienia dostarczenia systemu przygotowanego do pracy w trybie wysokiej dostępności (High availability)?
Odpowiedź:
Zamawiający działając na podstawie art. 137 ust. 1 ustawy dokonuje zmiany treści SWZ w niżej opisanym zakresie:

1) SWZ, załącznik nr 7 projektowane postanowienia umowy, załącznik nr 1 *Specyfikacja Analizatora plików* dodaje się punkt (w wyniku zmienionej numeracji pkt 49) o brzmieniu:

„49) Architektura rozwiązania Analizatora plików musi pracować w trybie wysokiej dostępności (High availability)."

Jednocześnie Zamawiający informuje, iż dotychczasowy pkt 49) otrzymuje oznaczenie: pkt 48).

2) SWZ, Załącznik nr 7 – projektowane postanowienia umowy § 1 pkt 12) przyjmuje brzmienie:

„12) Sprzęt IT - dedykowane fizyczne **urządzenia (2 szt.)** pełniące funkcję analizatora plików, spełniające wymagania opisane w Załączniku nr 1 do Umowy,"

W związku z ww. zmianą, Zamawiający zamieścił na Platformie Zakupowej zmodyfikowany Załącznik nr 1 do SWZ – wzór Formularza Ofertowego.

Pytanie 3
Zgodnie z punktem 17 Specyfikacji Zamawiający wymaga by analizator miał możliwość analizy plików do 1024 MB. Czy Zamawiający dopuści rozwiązanie w którym maksymalna wielkość analizowanego pliku to 60 MB?
Odpowiedź:
Zamawiający nie zmienia zapisów SWZ.

Pytanie 4
Punkt 19 Specyfikacji mówi, że analizator musi obsługiwać natywną integrację z Microsoft SharePoint w trybie online, aby zapewnić bezpieczne udostępnianie plików. Czy Zamawiający dopuści rozwiązanie, by zamiast tej funkcjonalności natywnej integrator stworzył za pomocą API dedykowaną integrację zgodną z potrzebami klienta?
Odpowiedź:
Zamawiający działając na podstawie art. 137 ust. 1 ustawy dokonuje zmiany treści SWZ w niżej opisanym zakresie:

SWZ, załącznik nr 7 projektowane postanowienia umowy, załącznik nr 1 *Specyfikacja Analizatora plików*, pkt 19) przyjmuje brzmienie:

„19) Analizator musi obsługiwać natywną integrację z Microsoft SharePoint w trybie online **lub z wykorzystaniem API (uwierzytelnianie i autoryzacja)**, aby zapewnić bezpieczne udostępnianie plików."

Pytanie 5
Wg punktu 27 Specyfikacji, sposób działania maszyn wirtualnych musi umożliwiać wykonanie analizy zachowania obiektów PDF, Java, MS Office z użyciem kilku wersji tych aplikacji bez uruchamiania dodatkowych maszyn wirtualnych. Czy Zamawiający dopuści rozwiązanie, w którym system może detonować kod na 3 typach maszyn jednocześnie (różnie skonfigurowanych obrazów)? Pozwoli to zweryfikować stacje klienckie na trzech całkowicie różnych środowiskach.
Odpowiedź:
Zamawiający nie zmienia zapisów SWZ.

Pytanie 6
Zgodnie z punktem 33 Specyfikacji wykrywanie exploit musi się odbywać po analizie co najmniej takich formatów plików jak Java Script, zakodowany (obfuscated) Java Script, obiekty Flash, PDF, pliki graficzne, pliki multimedialne mp3/mp4, pliki MS Office, Java. Czy Zamawiający dopuści rozwiązanie, w którym analiza będzie przeprowadzana po wskazanych formatach, z wyłączeniem plików graficznych i plików multimedialnych mp3/mp4?
Odpowiedź:
Zamawiający nie zmienia zapisów SWZ.

Pytanie 7
Punkt 39 Specyfikacji zawiera informacje, że analizator musi umożliwiać tworzenie raportów ze szczegółami wykrytych alertów do formatów co najmniej JSON, CSV. Czy Zamawiający dopuści rozwiązanie, w którym zamiast wymienionych, będą generowane raporty w formacie pdf? Format pdf jest bardzo popularnym i szeroko używanym formatem.
Odpowiedź:
Zamawiający nie zmienia zapisów SWZ.

Pytanie 8
Punkt 43 Specyfikacji mówi, że analizator musi umożliwiać przegląd nowych funkcjonalności po aktualizacji oprogramowania. Czy Zamawiający dopuści rozwiązanie, w którym informacja o nowych funkcjonalnościach nie wyświetla się bezpośrednio na urządzeniu ale jest dostarczana przez producenta w dokumentacji (Release Notes)?
Odpowiedź:
Zamawiający nie zmienia zapisów SWZ.

Pytanie 9
Zgodnie z punktem 42 Analizator musi umożliwiać przegląd statystyki danych zebranych na poszczególnych interfejsach urządzenia. Czy Zamawiający dopuści rozwiązanie bez takiej funkcjonalności? Wg Wykonawcy statystyki o danych zebranych na interfejsach urządzenia nie są stosowane w przypadku rozwiązania do ochrony plików, a mają uzasadnienie wyłącznie dla rozwiązań analizujących ruch sieciowych.
Odpowiedź:
Zamawiający na podstawie art. 137 ust 1 ustawy Pzp wprowadza następujące zmiany do SWZ:

SWZ, załącznik nr 7 projektowane postanowienia umowy, załącznik nr 1 *Specyfikacja Analizatora plików,* Zamawiający wykreśla zapis o treści "42) Analizator musi umożliwiać przegląd statystyki danych zebranych na poszczególnych interfejsach urządzenia.".

W związku z wykreśleniem pkt 42) zmianie ulega dalsza numeracja tj. dotychczasowy pkt 43) otrzymuje oznaczenie 42) i tak aż do pkt 49 – dotychczasowy pkt 49) otrzymuje oznaczenie 48).

Pytanie 10
Punkt 45 określa że Analizator musi integrować się bezpośrednio z posiadanym przez zamawiającego rozwiązaniem Fireeye Detection ON Demand, co najmniej w oparciu o wymianę artefaktów ataku wykrytych w skanowanych repozytoriach plików oraz musi umożliwiać przegląd generowanych alertów. Wg Wykonawcy tylko rozwiązanie Fireeye spełnia tę funkcjonalność, co zatem jest warunkiem zupełnie ograniczającym konkurencje. W związku z tym zamawiający wnioskuje o usunięcie tego zapisu.
Odpowiedź:
Zgodnie z odpowiedzią na pytanie nr 1.

Pytanie 11
Zgodnie z wymaganiem 47 Specyfikacji analizator musi umożliwiać natywną integrację umożliwiającą skanowanie plików z Office 365 SharePoint Online storage.
Czy Zamawiający dopuści, by zamiast tej funkcjonalności natywnej integrator stworzył za pomocą API dedykowaną integrację zgodną z potrzebami klienta?
Odpowiedź:
Zamawiający działając na podstawie art. 137 ust. 1 ustawy dokonuje zmiany treści SWZ w niżej opisanym zakresie:

SWZ, załącznik nr 7 projektowane postanowienia umowy, załącznik nr 1 *Specyfikacja Analizatora plików*, **pkt 46)** (poprzednio pkt 47) przyjmuje brzmienie:

„**46)** Analizator musi umożliwiać natywną integrację umożliwiającą skanowanie plików z Office 365 SharePoint Online storage **lub z wykorzystaniem API (uwierzytelnianie i autoryzacja)**."

Pytanie 12
W punkcie 48 Specyfikacji Zamawiający zawarł wymaganie, że analizator musi umożliwiać natywną integrację umożliwiającą skanowanie plików z Microsoft OneDrive. Czy Zamawiający dopuści by zamiast tej funkcjonalności natywnej integrator stworzył za pomocą API dedykowaną integrację zgodną z potrzebami klienta?
Odpowiedź:
Zamawiający działając na podstawie art. 137 ust. 1 ustawy dokonuje zmiany treści SWZ w niżej opisanym zakresie:

SWZ, załącznik nr 7 projektowane postanowienia umowy, załącznik nr 1 *Specyfikacja Analizatora plików*, **pkt 47)** (poprzednio pkt 48) przyjmuje brzmienie:

„**47)** Analizator musi umożliwiać natywną integrację umożliwiającą skanowanie plików z Microsoft OneDrive **lub z wykorzystaniem API (uwierzytelnianie i autoryzacja)**."

Pytanie 13
Analizator musi wykonywać skanowanie udziałów plikowych: ciągłe, zaplanowane i na żądanie oraz poddawać kwarantannie złośliwe oprogramowanie odnalezione na zasobach plikowych
Pytanie: Czy dopuszczone zostanie rozwiązanie pozwalające na skanowanie w zgodnie z harmonogramem w oparciu o takie kryteria jak: minuta, godzina, dzień, tydzień?
Odpowiedź:
Zamawiający nie zmienia zapisów SWZ.

Pytanie 14
Analizator musi być w stanie przywrócić plik do jego pierwotnej lokalizacji po zwolnieniu go z kwarantanny.
Pytanie: Czy dopuszczone zostanie rozwiązanie w którym przywracaniem pliku z kwarantanny zarządza administrator samodzielnie? Założenie jest iż plik który trafił do kwarantanny jest złośliwy i tylko w wypadku false positive można go przywrócić. Oryginalny plik administrator może też pobrać i przywrócić z raportu analitycznego.
Odpowiedź:
Zamawiający nie zmienia zapisów SWZ.

Pytanie 15
Analizator musi obsługiwać natywną integrację z Microsoft SharePoint w trybie online, aby zapewnić bezpieczne udostępnianie plików.
Pytanie: Czy dopuszczone zostanie rozwiązanie pozwalające na skanowanie i ochronę nie mniej niż następujących repozytoriów plikowych: SMB v1.0, SMB v2.0, SMB v2.1, SMB v3. NFSv2, NFSv3, NFSv4, Azure File Share, AWS S3, AWS S3 BJ, AWS S3 BX, Azure Blob Storage oraz wskazanych adresów URL?
Odpowiedź:
Zamawiający nie zmienia zapisów SWZ.

Pytanie 16
Analizator musi wspierać skanowanie i ochronę dla następujących typów repozytoriów plikowych: CIFS, NFS, WebDAV, Secure WebDAV.

Pytanie: Czy dopuszczone zostanie rozwiązanie pozwalające na skanowanie i ochronę nie mniej niż następujących repozytoriów plikowych: SMB v1.0, SMB v2.0, SMB v2.1, SMB v3.0, NFSv2, NFSv3, NFSv4, Azure File Share, AWS S3, AWS S3 BJ, AWS S3 BX, Azure Blob Storage?
Odpowiedź:
Zamawiający nie zmienia zapisów SWZ.

Pytanie 17
Analizator musi mieć możliwość analizy malware w formatach co najmniej:, JAVA, PDF, MS Office documents, common multimedia contents such as JPEG, QuickTime, MP3 and ZIP/RAR/7ZIP/TNEF archives, 3gp, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm.
Pytanie: Czy za równoważne zostanie uznane rozwiązanie pozwalające na skanowanie nie mniej niż: .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .elf, .exe, .gz, .htm, html, .iqy, .iso, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx,.swf, .tar, .tgz, .upx, .rl, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z,.zip ?
Odpowiedź:
Zamawiający nie zmienia zapisów SWZ.

Pytanie 18
Analizator musi posiadać dodatkowy mechanizm wykrywania zdarzeń typu prawdopodobny malware (takich jak zaszyfrowane dokumenty MS Office, zdegradowane pliki wykonywalne Windows PE, formularze web przekazujące hasła, pliki niewykonywalne umożliwiające komunikację do niestandardowego portu). Zdarzenia te powinny być konfigurowalne jako alert lub automatyczna kwarantanna.
Pytanie: Czy dopuszczone zostanie rozwiązanie które pozwala na wykrywanie zdarzeń typu prawdopodobny malware (takich jak zaszyfrowane dokumenty MS Office, zdegradowane pliki wykonywalne Windows PE, bomby logiczne, zagnieżdżony payload, wykrywanie środowiska sandbox, skrypty, pliki niewykonywalne umożliwiające komunikację do niestandardowego portu)? Zdarzenia te powinny być konfigurowalne jako alert lub automatyczna kwarantanna.
Odpowiedź:
Zamawiający nie zmienia zapisów SWZ.

Pytanie 19
Analizator musi umożliwiać tworzenie raportów uruchamianych cyklicznie (godzinowo/dzienne/tygodniowo/miesięcznie) zawierających co najmniej wykryte zagrożenia. Raporty te muszą być dostarczane przez email.
Pytanie: Czy dopuszczone zostanie rozwiązanie dla którego raporty lokalne wykonywane są na żądanie, zaś w czasie rzeczywistym pokazywane są raporty pokazujące wykryte zagrożenia wraz z możliwością ich szczegółowej analizy lub też raporty cykliczne wykonywane są na zewnętrznym, dedykowanym rozwiązaniu pochodzącym od tego samego producenta? Separacja narzędzia analitycznego od raportującego ma pozytywny wpływ na wydajność każdego z nich. Dodatkowo rozwiązanie ma możliwość automatycznego powiadamiania email o wykrytych zagrożeniach.
Odpowiedź:
Zamawiający nie zmienia zapisów SWZ.

Pytanie 20
Analizator musi umożliwiać wysyłanie alertów o zdarzeniach poprzez protokoły RSYSLOG, SMTP, SNMP, HTTP.
Pytanie: Czy dopuszczalne jest rozwiązanie które umożliwia wysyłanie alertów poprzez syslog zamiast rsyslog?
Odpowiedź:
Zamawiający działając na podstawie art. 137 ust. 1 ustawy dokonuje zmiany treści SWZ w niżej opisanym zakresie:

SWZ, załącznik nr 7 projektowane postanowienia umowy, załącznik nr 1 *Specyfikacja Analizatora plików*, **pkt 43)** (poprzednio pkt 44) przyjmuje brzmienie:

„**43)** Analizator musi umożliwiać wysyłanie alertów o zdarzeniach poprzez protokoły **SYSLOG**, SMTP, SNMP, HTTP."

Pytanie 21
Analizator musi integrować się bezpośrednio z posiadanym przez zamawiającego rozwiązaniem Fireeye Detection ON Demand, co najmniej w oparciu o wymianę artefaktów ataku wykrytych w skanowanych repozytoriach plików oraz musi umożliwiać przegląd generowanych alertów
Pytanie: Czy dopuszczone zostanie rozwiązanie które nie integruje się z bezpośrednio z Fireeye Detection ON Demand ale samo w sobie posiada możliwość skanowania ON Demand plików oraz adresów URL?
Odpowiedź:
Zgodnie z odpowiedzią na pytanie nr 1.
Pytanie 22
Analizator musi umożliwiać natywną integrację umożliwiającą skanowanie plików z Office 365 SharePoint Online storage.
Pytanie: Czy dopuszczone zostanie rozwiązanie pozwalające na skanowanie i ochronę nie mniej niż następujących repozytoriów plikowych: SMB v1.0, SMB v2.0, SMB v2.1, SMB v3.0, NFSv2, NFSv3, NFSv4, Azure File Share, AWS S3, AWS S3 BJ, AWS S3 BX, Azure Blob Storage oraz wskazanych adresów URL?
Odpowiedź:
Zamawiający nie zmienia zapisów SWZ.

Pytanie 23
Analizator musi umożliwiać natywną integrację umożliwiającą skanowanie plików z Microsoft OneDrive.
Pytanie: Czy dopuszczone zostanie rozwiązanie pozwalające na skanowanie i ochronę nie mniej niż następujących repozytoriów plikowych: SMB v1.0, SMB v2.0, SMB v2.1, SMB v3.0, NFSv2, NFSv3, NFSv4, Azure File Share, AWS S3, AWS S3 BJ, AWS S3 BX, Azure Blob Storage oraz wskazanych adresów URL?
Odpowiedź:
Zamawiający nie zmienia zapisów SWZ.

II. Jednocześnie Zamawiający działając na podstawie art. 137 ust. 1 ustawy dokonuje zmiany treści SWZ w niżej opisanym zakresie:

ZMIANA I
Rozdział IX SWZ *Sposób oraz termin składania i otwarcia ofert, warunki zmiany albo wycofania oferty* otrzymuje brzmienie:

„IX.1. Sposób oraz termin składania ofert i otwarcia ofert pkt 2 i 3 otrzymują brzmienie:

„2. Termin składania ofert upływa w dniu **7 marca 2023 r. o godzinie 10:00.**

3. Otwarcie ofert odbędzie się w dniu **7 marca 2023 r. o godzinie 11:00."**

ZMIANA II
Rozdział VII SWZ *Termin związania ofertą* otrzymuje brzmienie:
„Wykonawcy pozostają związani złożoną ofertą do dnia **5 czerwca 2023 r**. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert."

Zamawiający informuje, że udzielone odpowiedzi oraz dokonane zmiany są wiążące dla Wykonawców.

PREZES
Halina Szymańska