Załącznik nr 1 do Zapytania

I. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja i wdrożenie Systemu typu sandbox służącemu ochronie przed atakami typu ATP (Advanced Persistent Threat), zwanego dalej „Systemem".

1. Wymagania dla Systemu.

1. System musi być dostarczony w formie:
    a. dwóch fizycznych maszyn spełniających wymagania techniczne umożliwiające realizację wymagań wydajnościowych opisanych w pkt. 1.2.
    b. oprogramowania wbudowanego w fizyczne maszyny gwarantującego stabilne i bezpieczne działanie Systemu, optymalizację wykorzystania zasobów sprzętowych, zapewniające integrację z innymi komponentami Systemu.
2. System musi zapewniać minimalną wydajność przetwarzania na poziomie 100 000 plików na godzinę, przy średniej wielkości pojedynczego pliku wynoszącej 10 MB, co odpowiada przepustowości co najmniej 1 TB danych na godzinę, przy czym przetwarzane pliki muszą obejmować różnorodne formaty, w tym m.in. dokumenty, archiwa, obrazy, pliki wykonywalne oraz inne typy danych występujące w środowisku produkcyjnym, a ich obsługa musi odbywać się w sposób ciągły, stabilny i skalowalny, bez wpływu na funkcjonalność Systemu.
3. System musi zapewniać przetwarzanie danych wyłącznie na terenie Europejskiego Obszaru Gospodarczego (EOG).
4. Wydajność Systemu oraz jego zasoby muszą zapewniać jednoczesne uruchomienie sandboxów na co najmniej 32 maszynach wirtualnych każda z działającą w środowisku posiadanym przez Zamawiającego opisanym w pkt. 5, aby zapewnić wydajność nie mniejszą niż opisaną w pkt. 1.1. Licencje dla uruchomionych maszyn wirtualnych w środowisku Zamawiającego opisanym w pkt. 5 zapewni Dostawca.
5. System musi posiadać funkcjonalność automatycznego sprawdzania dostępności oraz instalacji aktualizacji baz sygnatur zagrożeń, bez konieczności ingerencji ze strony administratora.
6. System, w zakresie wykrywania zagrożeń musi:
    a. stosować mechanizmy analizy behawioralnej wykorzystujące algorytmy sztucznej inteligencji (AI), automatycznie i samoczynnie generujące raporty z opisem podejrzanych zachowań (np. modyfikacja rejestru, nietypowe połączenia sieciowe),
    b. automatycznie pobierać pliki do analizy z systemu poczty elektronicznej posiadanej przez Zamawiającego,
    c. posiadać funkcjonalność skanowania co najmniej następujących typów plików: tar, zip, rar, 7z, tgz, cab, gz, xlam, xlsb, xltm, xlsm, xltx, xls, xlsx, pps, ppt, pptx, ppsx, doc, docx, docm, dotm, dot, dotx, pdf, exe, rtf, swf oraz zapewniać możliwość pracy autonomicznej (bez połączenia z firewall'em). Pliki archiwum zabezpieczone hasłem muszą mieć opcję wprowadzenia hasła przez administratora,
    d. posiadać funkcjonalność skanowania adresów URL zawartych w dokumentach poprzez weryfikację na blacklistach, zarówno predefiniowanych przez Producenta Systemu jak i utworzonych przez administratora Systemu oraz wykonanie próby kontrolowanej aktywacji zagrożenia w środowisku sandbox w celu przeprowadzenia analizy behawioralnej,

e. musi posiadać funkcjonalność przesyłania plików do analizy na żądanie (on-demand) przez administratorów,
f. zapewniać automatyczne przesyłanie informacji zwrotnej o każdym z przeanalizowanych plików w celu:
    i. zatrzymania zainfekowanych plików w kwarantannie,
    ii. potwierdzenia wykrycia lub braku wykrycia zagrożenia,
g. W przypadku potwierdzenia wykrycia zagrożenia informacja zwrotna powinna zawierać co najmniej następujące informacje:
    i. identyfikator pliku – unikalny identyfikator analizowanego pliku, np. nazwa i/lub hash (MD5, SHA256),
    ii. data i czas analizy – precyzyjne oznaczenie momentu, w którym dokonano analizy i wykryto zagrożenie,
    iii. typ zagrożenia – szczegółowa klasyfikacja dotycząca rodzaju wykrytego zagrożenia, np. ransomware, trojan, spyware, atak typu phishing itp.,
    iv. szczegóły techniczne – opis technicznych cech wykrytego zagrożenia, np. użyte techniki ukrywania, sygnatury, wykorzystane luki bezpieczeństwa,
    v. rekomendowane przez Producenta Systemu działania,
    vi. stan pliku po analizie – informacja, czy plik został zablokowany, poddany kwarantannie, usunięty albo dopuszczony do dalszego obiegu,
    vii. identyfikacja źródła zagrożenia – jeżeli możliwe, informacja o źródle lub pochodzeniu zagrożenia (np. adres IP, nadawca e-mail),
    viii. status aktualizacji definicji zagrożeń – data i wersja bazy sygnatur lub mechanizmów heurystycznych wykorzystanych do wykrycia.

7. System, w zakresie zarządzania, musi zapewniać co najmniej:
    a. monitoring stanu Systemu w zakresie dostępności i wydajności jego kluczowych komponentów,
    b. obsługę wszystkich funkcjonalności zarówno poprzez graficzny interfejs użytkownika (Web GUI), jak i wiersz poleceń (CLI),
    c. komunikację z panelem zarządzania Systemu z zastosowaniem szyfrowanego połączenia HTTPS,
    d. zarządzanie wieloma kontami administratorów,
    e. ustawianie różnych ról administratorów i przypisywanie im odpowiednich uprawnień dostępu do danych, funkcjonalności,
    f. zapisywanie działań administratorów zapewniając rozliczalność ich działań,
    g. monitorowanie zdarzeń w czasie rzeczywistym, m.in. poprzez statystyki wyników skanowania przedstawiane w formie widgetów,
    h. posiadać funkcjonalność automatycznego samoczynnego powiadamianie administratorów o wykrytych zagrożeniach za pomocą wiadomości e-mail.
8. System musi zapewniać lokalne logowanie zdarzeń w lokalnym repozytorium z możliwością konfiguracji i okresu retencji nie krótszy niż 30 dni oraz integrację z zewnętrznymi systemami SIEM/SOAR.
9. System, w zakresie integracji musi zapewniać integrację z systemami klasy SIEM (co najmniej takimi jak SPLUNK, Elastic) poprzez eksport informacji o zdarzeniach co najmniej w formacie CEF lub JSON,

10. System musi zapewniać integrację co najmniej z systemami klasy WAF, SIEM za pomocą dostępnych mechanizmów (np. ICAP, API REST, webhooki, konektory). W przypadku braku gotowego mechanizmu integracji Wykonawca zobowiązuje się dostosować System do wymagań Zamawiającego bez dodatkowych kosztów.
11. System musi posiadać funkcjonalność tworzenie białych i czarnych list sum kontrolnych plików.
12. Raporty generowane przez system muszą obejmować co najmniej analizę oraz charakterystykę wykrytego zagrożenia, w tym co najmniej zmiany w systemie operacyjnym, modyfikacje rejestru, operacje na procesach, wywoływane adresy URL oraz połączenia do serwerów C&C.
13. System musi umożliwiać instalację aktualizacji oprogramowania systemowego, w tym nowych wersji, poprawek bezpieczeństwa oraz firmware, wyłącznie w uprzednio uzgodnionych z Zamawiającym oknach serwisowych. W przypadku braku możliwości realizacji aktualizacji w wyznaczonym terminie, system musi zapewniać mechanizmy umożliwiające poinformowanie Zamawiającego o planowanych działaniach z odpowiednim wyprzedzeniem. System musi również umożliwiać administratorowi podjęcie decyzji o zatwierdzeniu, odrzuceniu lub odłożeniu aktualizacji w czasie, a także zapewniać możliwość pominięcia wybranych wersji oraz przeprowadzenia procedury rollback do wcześniejszej, stabilnej wersji oprogramowania w przypadku wystąpienia błędów lub nieprawidłowości po aktualizacji.
14. System musi zapewniać, że wszystkie operacje przetwarzania danych odbywają się wyłącznie na terenie Europejskiego Obszaru Gospodarczego (EOG), obejmującego kraje członkowskie Unii Europejskiej oraz Europejskie Stowarzyszenie Wolnego Handlu (EFTA), a przetwarzanie danych osobowych realizowane jest w pełnej zgodności z wymogami rozporządzenia RODO.

2. Dostawa.

1. Wykonawca jest zobowiązany do dostarczenia wszystkich elementów Systemu opisanego w pkt. 1.1 do wskazanych przez Zamawiającego w pkt. 2.2 lokalizacji w terminie nie dłuższym niż 45 dni kalendarzowych od dnia podpisania umowy.
2. Lokalizacja główna – 26-601 Radom, ul. Samorządowa 1; Lokalizacja zapasowa – 03-446 Warszawa, ul. 11 Listopada 23A.
3. Za dzień dostawy uznaje się dzień, w którym urządzenia zostaną fizycznie przekazane Zamawiającemu i potwierdzone podpisaniem protokołu odbioru obejmującego m.in. sprawdzenie kompletności dostawy, stanu technicznego oraz zgodności z zamówieniem.
4. W przypadku wystąpienia okoliczności niezależnych od Dostawcy, które mogą wpłynąć na termin realizacji dostawy (np. siła wyższa), Dostawca zobowiązany jest niezwłocznie poinformować Zamawiającego o zaistniałej sytuacji oraz przewidywanym nowym terminie dostawy.
5. Dostawca zobowiązuje się do powiadomienia Zamawiającego z co najmniej 2-dniowym wyprzedzeniem o planowanym terminie dostawy.

3. Wdrożenie.

1. Analizę aktualnych systemów do podłączania i przygotowanie projektu technicznego rozwiązania zawierającego plan i harmonogram wdrożenia oraz proponowane scenariusze testów funkcjonalnych oraz akceptacyjnych.
2. Uruchomienie Systemu w środowisku Zamawiającego.
3. Przygotowanie konfiguracji Systemu i polityk bezpieczeństwa.

4. Integrację wdrażanego Systemu z systemami WAF oraz SIEM, za pomocą mechanizmów opisanych w pkt. 9.
5. Przeprowadzenie testów funkcjonalnych i akceptacyjnych zainstalowanego Systemu zgodnie z zaakceptowanymi scenariuszami.
6. Przygotowanie powdrożeniowej dokumentacji technicznej zawierającej diagramy architektury, listę portów i protokołów wykorzystywanych przez System oraz dokumentacji użytkownika Systemu zawierającej architekturę rozwiązania, spis wszystkich wdrożonych polityk bezpieczeństwa, opis testów obciążeniowych i akceptacyjnych i rozwiązania, opis konfiguracji Systemu (w tym nietypowe ustawienia) oraz instrukcję dla użytkownika/administratora Systemu w języku polskim, w formie elektronicznej – PDF oraz w pełni edytowalnym formacie dokumentu tekstowego (.doc lub .docx)
7. Wykonawca jest zobowiązany do wdrożenia Systemu do wskazanej przez Zamawiającego lokalizacji w terminie nie dłuższym niż 30 dni kalendarzowych od dnia dostawy Systemu opisanego pkt. 1. Wykonawca w tym terminie musi wykonać wszystkie czynności wdrożeniowe, w tym instalacji, konfiguracji, testów oraz przekazania Zamawiającemu kompletnej dokumentacji powykonawczej.
8. Za pełne wdrożenie Systemu uznaje się wykonanie wszystkich czynności opisanych w pkt. 1-6.

4. Przeprowadzenie warsztaty instruktażowe.

1. Wykonawca zobowiązuje się do przeprowadzenia przeszkoleń dla maksymalnie 12 osób wskazanych przez Zamawiającego, według niżej określonych warunków.
2. Wykonawca w ramach wynagrodzenia przeprowadzi co najmniej trzydniowe warsztaty, które będą trwać łącznie co najmniej 24 godziny, jednak nie więcej niż 8 godzin jednego dnia i będą odbywały się dzień po dniu, w Dni robocze.
3. Warsztaty będą obejmowały co najmniej zagadnienia z zakresu administracji, konfiguracji oraz zarządzania Systemem, zgodnie z poniższym zakresem:
    a) architektura Systemu,
    b) komponenty fizyczne i logiczne Systemu,
    c) przepływ danych, przechowywanie danych,
    d) możliwości dalszej rozbudowy Systemu,
    e) konfiguracja przestrzeni danych,
    f) konfiguracja uprawnień i polityk dostępu do danych,
    g) dostęp do danych za pomocą różnych klientów / protokołów,
    h) monitorowanie i raportowanie Systemu,
    i) rozwiązywanie problemów związanych z Systemem,
    j) aktualizacja Oprogramowania.
4. Wykonawca przedstawi Zamawiającemu na co najmniej 10 dni przed rozpoczęciem warsztatów, do akceptacji:
    a) termin warsztatu,
    b) zakres warsztatu,
    c) agendę,
    d) kwalifikacje wykładowcy,
    e) materiały.

5. Akceptacja przez Zamawiającego warunków określonych w Rozdz. 4 pkt. 3 niniejszego OPZ stanowi warunek rozpoczęcia warsztatów i zostanie potwierdzona drogą elektroniczną przez osobę wskazaną do kontaktu ze strony Zamawiającego w Umowie.
6. Warsztaty będą prowadzone w języku polskim.
7. Wykonawca w ramach wynagrodzenia zapewni wykładowcę posiadającego kwalifikacje i wiedzę umożliwiającą przeprowadzenie warsztatów z zakresu administracji, konfiguracji oraz zarządzania zaoferowanego Systemu.
8. Każdy z uczestników warsztatów otrzyma komplet materiałów w języku polskim (w formie papierowej lub elektronicznej). Zamawiający dopuszcza przekazanie materiałów w języku angielskim pod warunkiem, że producent Systemu nie udostępnia materiałów w języku polskim.
9. Wszelkie koszty związane ze wszystkimi aspektami warsztatów ponosi Wykonawca.
10. Podczas warsztatów zachowana musi być interaktywna forma. Uczestnicy w czasie rzeczywistym muszą widzieć i słyszeć wykładowcę, móc zadawać pytania i wyjaśniać wątpliwości oraz wykonywać ćwiczenia praktyczne. Wykładowca musi udostępniać na bieżąco na ekranie materiały. Uczestnicy muszą również widzieć i słyszeć siebie wzajemnie. Wykonawca musi w tym celu zapewnić platformę dostępną dla uczestników warsztatów za pośrednictwem sieci Internet, działającą na komputerach wyposażonych w system kompatybilny ze środowiskiem Zamawiającego opisanym w pkt. 5, wyposażonych w urządzenia audio i video (słuchawki/mikrofon/kamera internetowa).
11. Wykonawca najpóźniej na 2 dni przed datą rozpoczęcia przekaże drogą mailową wszelkie dane wymagane do podłączenia się do platformy szkoleniowej (np. loginy, hasła, link dostępowy itp.) oraz instrukcję użytkowania platformy.
12. Realizacja warsztatów zostanie potwierdzona przez Zamawiającego Protokołem Odbioru, sporządzonym przez Strony zgodnie ze wzorem przekazanym przez Zamawiającego.

5. Środowisko Zamawiającego.

1. Zamawiający eksploatuje środowisko użytkowe obejmujące stacje robocze z systemem operacyjnym Windows 10/11 lub nowszym, wykorzystywane do realizacji zadań służbowych. Środowisko to stanowi platformę, na której uruchamiane są aplikacje użytkowe oraz maszyny wirtualne wykorzystywane do analiz bezpieczeństwa.
2. Zamawiający wykorzystuje pakiet biurowy Microsoft Office w wersji nie starszej niż Office 2019. Pakiet ten jest wykorzystywany do pracy z dokumentami stanowiącymi przedmiot analizy w Systemie oraz do przetwarzania danych użytkowników.
3. Informacje wskazane w punktach 1 – 2 stanowią opis środowiska Zamawiającego i mają na celu umożliwienie Wykonawcy prawidłowego przygotowania rozwiązania oraz oszacowania wymaganego poziomu wydajności Systemu. Wymagania te nie stanowią wymagania dostarczenia określonych produktów przez Wykonawcę, a jedynie opisują kontekst techniczny, w którym System będzie instalowany, konfigurowany i eksploatowany.
4. System dostarczony przez Wykonawcę musi zapewnić pełną kompatybilność działania w środowisku opisanym powyżej, w tym możliwość realizacji scenariuszy analitycznych i testowych zgodnie z wymaganiami określonymi w punkcie 1 niniejszego OPZ.