OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest rozbudowa środowiska systemu FortiSandbox VM00 i świadczenie usługi Asysty Technicznej dla Oprogramowania.

I. Rozbudowa posiadanego przez Zamawiającego środowiska systemu FortiSandbox VM00 i świadczenie usługi Asysty Technicznej obejmuje:

a) dostawę 5 sztuk zestawów licencji FortiSandbox VM00 pracujących w klastrze wysokiej dostępności – HA, wraz z gwarancją producenta oraz Usługą Asysty Techniczne świadczonymi przez okres 24 miesięcy. Zamawiający wymaga, aby każdy 5 zestawów (node) posiadał komplet licencji wymienionych w pkt. I lit. b. Zamawiający dopuszcza dostarczenie rozwiązania równoważnego, spełniającego wymagania wskazane w Załączniku nr 1 do OPZ - (zamówienie gwarantowane).

b) świadczenie Usługi Asysty Technicznej do oraz gwarancji producenta dla posiadanego przez Zamawiającego Oprogramowania FortiSandbox VM00 przez okres 24 miesięcy od daty wygaśnięcia aktualnej asysty - (zamówienie gwarantowane):

Lp.	Nazwa licencji	Liczba licencji	Data wygaśnięcia Asysty Technicznej
1.	Fortinet Sandboxing Virtual Appliance - Upgradable to max 8 VMs. Windows/Office license not included. (FSA-VM00)	1	19.10.2023
2.	Fortinet Expands FSA-VM and FSA-VM00 licensed Windows/Linux/Android VM capacity by 1. (1) Win10 license added. (FSA-VM-WIN10-1)	4	
3.	Expands FSA (Appliance/VM) licenses of Microsoft Office 2019 by 1 (FSA-UPG-OFFICE2019-1)	4	
4.	Fortinet Sandbox Threat Intelligence (Antivirus, IPS, Web Filtering, File Query, Industrial Security, SandBox Engine) plus 24x7 FortiCare. Subscribes up to 8 VMs. (FC-10-FSV00-500-02-12)	1	

c) Wsparcie Eksperckie w łącznym maksymalnym wymiarze **100 roboczogodzin** (zamówienie opcjonalne).

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309 00-184
REGON: 001377706

II. Termin realizacji

1. Dostawa zamówienia gwarantowanego, o którym mowa w pkt I lit. a musi nastąpić w terminie **10 dni roboczych** od zawarcia umowy.
2. Usługa Asysty Technicznej dla zakresu, o którym mowa w pkt I lit. a będzie świadczona przez okres 24 miesięcy od dnia podpisania protokołu odbioru dostawy, oraz przez okres 24 miesięcy od daty wygaśnięcia aktualnej asysty dla posiadanego środowiska, o którym mowa w pkt I lit. b.
3. Usługa Wsparcia Eksperckiego może być świadczona, w przypadku skorzystania z prawa opcji w okresie świadczenia Usługi Asysty Technicznej dla pkt I lit. b .

III. System sandbox wykorzystywany obecnie przez Zamawiającego:

1. Zamawiający posiada system FortiSandbox VM00 (FSAVM0TM21001326), pracujący w klastrze dwunodowym firmy Fortinet.
2. Obecnie w systemie wykorzystane są licencje wymienione w pkt. I lit. b.

IV. Gwarancja producenta dla zakresu pkt. I lit. a i b:

1. W ramach gwarancji producenta wymagany jest:
   a) dostęp do aktualizacji oprogramowania.
   b) dostęp do nowych wersji oprogramowania oraz poprawek.
   c) dostęp do nowych sygnatur bezpieczeństwa.
   d) dostęp do bazy wiedzy producenta.
2. Zamawiający wymaga, aby mógł dokonywać aktualizacji oprogramowania do najnowszej zalecanej przez producenta wersji przez okres obowiązywania umowy.

V. Wymagania dotyczące Usługi Asysty Technicznej dla zakresu pkt. I lit. a i b:

1. W ramach świadczenia Usługi Asysty Technicznej Wykonawca zobowiązany będzie do:
   1.1. Wykonywania aktualizacji Oprogramowania.
   1.2. Implementacji nowych wersji Oprogramowania oraz poprawek.
   1.3. Wsparcia Zamawiającego w rozwiązywaniu problemów z dostarczonym oprogramowaniem.
2. W ramach realizacji Usługi, Wykonawca będzie świadczył okresowe przeglądy Oprogramowania, nie rzadziej niż co 3 miesiące, polegające na:
   2.1. Przeglądzie poprawek dla eksploatowanych środowisk wykorzystujących System.
   2.2. Ocenie konieczności zastosowania poprawek rekomendowanych przez producenta oprogramowania w eksploatowanych środowiskach oraz ich wdrożenie.
   2.3. Doradztwie architektonicznym w zakresie zgodności sposobu wykorzystywania oprogramowania z najlepszymi praktykami rekomendowanymi przez dostawcę oraz zgodności z warunkami Umowy.
   2.4. Informowaniu Zamawiającego o przyczynach i sposobach rozwiązywania problemów związanych z nieprawidłowym działaniem Systemu.
   2.5. Doradztwie technicznym, przekazywaniu na bieżąco informacji o nowych funkcjonalnościach możliwych do zaimplementowania w oprogramowaniu.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309 00-184
REGON: 001377706

2.6. Założeniu zgłoszenia serwisowego w serwisie pomocy technicznej producenta, w przypadku wad i błędów oprogramowania, przekazanie zgłoszenia serwisowego do producenta oprogramowania oraz prowadzenie zgłoszenia w imieniu Zamawiającego.

2.7. Wsparciu w konfiguracji i optymalizacji Systemu.

VI. Wsparcie Eksperckie (zamówienie opcjonalne)

1. W ramach realizacji Usługi, Wykonawca zapewni Wsparcie Eksperckie.

1.1. W łącznym maksymalnym wymiarze 100 roboczogodzin.

1.2. Obejmujące swoim zakresem:

- wsparcie w pielęgnacji środowiska i jego dokumentowanie.
- przeglądy środowiska obejmujące weryfikację poprawności instalacji, konfiguracji i działania systemów.
- konsultacje i doradztwo w zakresie eksploatacji środowiska oraz jego bezpieczeństwa.
- konsultacje w ramach rozwoju środowiska pod kątem obejmowania funkcjonalnością przez środowisko nowych systemów Zamawiającego.
- konsultacje implementacji nowych, nietypowych oraz dostosowywania już istniejących metod optymalizacji systemów Zamawiającego w zakresie funkcjonalności oferowanej przez środowisko.
- inne prace wg. potrzeb Zamawiającego (w uzgodnieniu z Wykonawcą).

1.3. Wykonawca zapewni minimum jednego Konsultanta technicznego w zakresie Oprogramowania. Konsultant ten musi posiadać:

- Minimum 2 lata doświadczenia zawodowego w zakresie konfigurowania oprogramowania FortiSandbox lub równoważnego.
- Minimum 2 lata doświadczenia zawodowego w zakresie administrowania oprogramowaniem FortiSandbox lub równoważnym.

1.4. Prace w ramach Wsparcia Eksperckiego będą zlecane Wykonawcy z co najmniej 14 dniowym wyprzedzeniem.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309 00-184
REGON: 001377706

Załącznik nr 1 do OPZ

Opis wymagań dla oprogramowania równoważnego do FortiSandbox

Zamawiający posiada licencje na oprogramowanie FortiSandbox oraz zintegrowane systemy informatyczne, które korzystają z rozwiązania firmy Fortinet.

Zamawiający wymaga, żeby dostarczone oprogramowanie integrowało się z posiadanymi urządzaniami takimi jak: FortiAnalyzer (przesyłanie logów i generowanie raportów oraz alarmów), FortiWeb (skanowanie plików i blokada złośliwego plików w czasie rzeczywistym), FortiGate (skanowanie antywirusowe, blokada złośliwych plików i URL w czasie rzeczywistym) oraz FortiMail (skanowanie plików i URL w czasie rzeczywistym przed dostarczeniem korespondencji).
Zamawiający **nie wyraża zgody** na wymianę posiadanego oprogramowania na inne w ramach realizacji niniejszego zamówienia.

Jeżeli Zamawiający określił w Opisie przedmiotu zamówienia wymagania z użyciem nazw własnych produktów lub marek producentów, w szczególności w obszarze specyfikacji przedmiotu zamówienia, to należy traktować wskazane produkty jako rozwiązania wzorcowe. W każdym takim przypadku Zamawiający oczekuje dostarczenia produktów wzorcowych lub równoważnych, spełniających poniższe warunki równoważności.

I. Zamawiający dopuszcza zaoferowanie produktów równoważnych do oprogramowania FortiSandbox

1. W przypadku dostarczania oprogramowania, równoważnego względem wyspecyfikowanego przez Zamawiającego w Opisie Przedmiotu Zamówienia, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane oprogramowanie spełnia wszystkie wymagania i warunki określone w Istotnych Warunkach Zamówienia, w szczególności w zakresie:
   a) warunków licencji / sublicencji w każdym aspekcie licencjonowania / sublicencjonowania, które muszą być identyczne lub rozszerzone, przy czym rozszerzony zakres musi zawierać również wszystkie elementy licencjonowania jak dla oprogramowania FortiSandbox.
   b) funkcjonalności równoważnej oprogramowania, która nie może być gorsza od funkcjonalności wymienionych w pkt III - „Opis wymaganych minimalnych funkcjonalności w przypadku zaoferowania oprogramowania równoważnego”.
   c) oprogramowanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać z oprogramowaniem FortiSandbox funkcjonującym u Zamawiającego.
   d) oprogramowanie równoważne nie może zakłócić pracy środowiska systemowo-programowego Zamawiającego.
   e) oprogramowanie równoważne musi w pełni współpracować z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie.
   f) oprogramowanie równoważne musi zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienność oprogramowania równoważnego z wyspecyfikowanym oprogramowaniem.
2. W przypadku zaoferowania przez Wykonawcę oprogramowania Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane oprogramowanie.
3. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309 00-184
REGON: 001377706

Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu oprogramowania równoważnego.

4. Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów używanego i współpracującego z nim oprogramowania u Zamawiającego.
5. Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w jego nowszych wersjach.

II. W przypadku dostawy oprogramowania równoważnego Wykonawca zobowiązany jest:

1. Przeprowadzić Instruktaż dla 4 administratorów Zamawiającego z zakresu instalacji, konfiguracji i zarządzania oprogramowaniem równoważnym, umożliwiającym pełne poznanie produktu równoważnego. Wykonawca w terminie 1 Dnia Roboczego od dnia zawarcia Umowy przedstawi do zatwierdzenia Zamawiającemu harmonogram Instruktażu.
2. Przeprowadzić Instruktaż dla 8 operatorów Zamawiającego z zakresu użytkowania oprogramowania równoważnego, umożliwiającego pełne poznanie produktu równoważnego.
3. Wykonawca w terminie 1 Dnia Roboczego od dnia zawarcia Umowy przedstawi do zatwierdzenia Zamawiającemu harmonogramy Instruktaży.
4. Instruktaże będą realizowane w Dni Robocze w godzinach 8:00-16:00 w siedzibie Zamawiającego lub w formie zdalnej o ile zostaną spełnione wszystkie wymagania dotyczące Instruktażu. Instruktaże będzie trwał minimum 2 Dni Robocze każdy (łącznie minimum 14 godzin zegarowych każdy).
5. Zainstalować oprogramowanie równoważne w środowisku systemowo-programowym oraz dokonać poprawnej konfiguracji mechanizmów systemu sandbox służącego ochrony przed atakami typu APT (Advanced Persistent Threat), działającego w klastrze dwunodowym z sandbox'em firmy Fortinet oraz zintegrować się z systemami/aplikacjami wytwarzanymi w zamach działalności Zamawiającego w terminie do **10 dni roboczych** od dnia podpisania Umowy.
6. Dostarczyć wszelkich dodatkowych licencji - niezbędnych do prawidłowego funkcjonowania oprogramowania równoważnego.

III. Opis wymaganych minimalnych funkcjonalności w przypadku zaoferowania oprogramowania równoważnego w stosunku do oprogramowania FortiSandbox

1. System typu sandbox służącemu ochronie przed atakami typu APT (Advanced Persistent Threat) będącego rozszerzeniem funkcjonalności używanego przez Zamawiającego systemu Secure Mail Gateway FortiMail. Wymagania dla Systemu:
    a) System powinien zostać dostarczony w formie usługi typu cloud uruchomionej w środowisku producenta.
    b) Dostarczony System musi obejmować wszelkie licencje niezbędne do wdrożenia produkcyjnego oraz uzyskania wsparcia producenta.
    c) System musi zapewniać przetwarzanie danych do niego wysyłanych na terenie EOG (Europejskiego Obszaru Gospodarczego).

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309 00-184
REGON: 001377706

d) System powinien umożliwiać dostęp do dedykowanego dla Zamawiającego zasobu pozwalającego na uruchomieniu minimum 10 maszyn wirtualnych.
e) Wpierane systemy operacyjne maszyn wirtualnych: Windows 10, macOS, Android, iOS.
f) System musi zapewniać mechanizm automatycznego sprawdzania nowych wersji oraz automatycznej aktualizacji.
g) System powinien zapewniać monitoring stanu maszyn wirtualnych.
h) Obsługa Systemu powinno być możliwa w pełnym zakresie za pomocą graficznego interfejsu użytkownika (WebGUI) oraz wiersza poleceń (CLI).
i) Komunikacja z panelem zarządzania powinna wykorzystywać szyfrowanie połączenie – https.
j) System powinien zapewniać wsparcie dla wielu kont administratorów, minimum dwóch.
k) System powinien zapewniać rozliczalność działań administratorów.
l) Moduł analizy zagrożeń powinien wykorzystywać m.in. mechanizmy analizy behawiorystycznej opartej o algorytmy sztucznej inteligencji (AI).
m) System powinien mieć wbudowany mechanizm automatycznej aktualizacji baz zagrożeń.
n) System powinien automatycznie pobierać do analizy pliki z systemu FortiMail.
o) System powinien umożliwiać przesyłanie informacji zwrotnej o analizowanym pliku do urządzenia FortiMail umożliwiającej zatrzymanie zainfekowanej przesyłki w kwarantannie oraz do urządzeń FortiGate informacji umożliwiającej aktualizację polityk bezpieczeństwa.
p) Logowanie zdarzeń powinno być wykonane lokalnie oraz do systemów zewnętrznych.
q) Powinna być zapewniona integracja z systemami klasy SIEM.
r) System w zakresie logowania powinien umożliwiać komunikację szyfrowaną.
s) Wymagane obsługiwane formaty skanowanych plików:
t) Archiwa: tar, gz, bz2, cab, rar, zip, arj, 7z, ace, tgz
u) Pliki wykonywalne: exe, msi, bat, dll
v) Pliki: PDF, MS Office, htm/html, lnk
w) Adobe Flash
x) Java Archive: jar
y) Skrypty: js, vbs, cmd
z) System powinien posiadać mechanizm tworzenia białych i czarnych list sum kontrolnych plików.
aa) System powinien posiadać mechanizm skanowania adresów URL zawartych w dokumentach.
bb) Monitorowanie zdarzeń w Systemie powinno odbywać się w czasie rzeczywistym, np. statystyki wyników skanowania i być przedstawiane w formie widgetów.
cc) Szczegółowa informacja o zdarzeniu powinna zawierać nazwę zagrożenia, źródło ataku i cel oraz czas wykrycia.
dd) Raporty generowane z poziomu Systemu powinny dotyczyć analizy złośliwego pliku i zawierać charakterystykę ataku – np. modyfikowane pliki w systemie operacyjnym, modyfikacje rejestru, operacje związane z procesami, wywoływane adresy URL, połączenia do serwerów C&C.
ee) System powinien umożliwiać informowanie przy pomocy e-maila o wykryciu zagrożenia.
ff) System powinien umożliwiać przesyłanie plików do analizy poprzez administratora (on-demand).

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309 00-184
REGON: 001377706