**190525**

## Opis Przedmiotu Zamówienia

## Świadczenie usługi Asysty Technicznej do oprogramowania Sandbox (FortiSandbox VM00) i Secure Mail Gateway (FortiMail VM04)

**1. Przedmiot zamówienia obejmuje:**

1.1. Przedłużenie do dnia 2028-11-30 świadczenia Usługi Asysty Technicznej do Oprogramowania FortiSandbox VM00 służącego do kompleksowego zabezpieczenia plików i URL w infrastrukturze IT Zamawiającego, w ramach systemu FortiSandbox VM00, w trybie on-premise, w szczególności:

1.1.1. Fortinet Sandbox Threat Intelligence (Antivirus, IPS, Web Filtering, File Query, Industrial Security, SandBox Engine) plus 24x7 FortiCare. Subscribes up to 8 VMs.

1.2. Przedłużenie do dnia 2028-11-30 świadczenia Usługi Asysty Technicznej do Oprogramowania FortiMail służącego do kompleksowego zabezpieczenia poczty elektronicznej w infrastrukturze IT Zamawiającego, w ramach systemu Secure Mail Gateway, w trybie on-premise, w szczególności:

1.2.1. F24x7 FortiCare and FortiGuard Enterprise ATP Bundle Contract.

1.2.2. Office365 API Intergration Service.

1.3. Zamawiający posiada licencje oraz Asystę Techniczną na Oprogramowanie zgodnie tabelą nr 1

Tabela nr 1.

| NR | Numer seryjny | Nazwa licencji | Data wygaśnięcia Asysty Technicznej |
|---|---|---|---|
| 1. | FortiSandbox VM00<br>s/n: FSAVM0TM21001326 | Fortinet Sandbox Threat Intelligence (Antivirus, IPS, Web Filtering, File Query, Industrial Security, SandBox Engine) plus 24x7 FortiCare. Subscribes up to 8 VMs.<br><br>FC-10-FSV00-500-02-12 | 2025-10-19 |
| 2. | FortiSandbox VM00<br>s/n: FSAVM0TM24001027 | Fortinet Sandbox Threat Intelligence (Antivirus, IPS, Web Filtering, File Query, Industrial Security, SandBox Engine) plus 24x7 FortiCare. Subscribes up to 8 VMs.<br><br>FC-10-FSV00-500-02-12 | 2026-03-01 |
| 3. | FortiSandbox VM00<br>s/n: FSAVM0TM24001038 | Fortinet Sandbox Threat Intelligence (Antivirus, IPS, Web Filtering, File Query, Industrial Security, SandBox Engine) plus 24x7 FortiCare. Subscribes up to 8 VMs. | 2026-03-04 |



Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

| | | | |
|---|---|---|---|
| | | FC-10-FSV00-500-02-12 | |
| 4. | FortiSandbox VM00<br>s/n: FSAVM0TM24001039 | Fortinet Sandbox Threat Intelligence (Antivirus, IPS, Web Filtering, File Query, Industrial Security, SandBox Engine) plus 24x7 FortiCare. Subscribes up to 8 VMs.<br><br>FC-10-FSV00-500-02-12 | 2026-03-04 |
| 5. | FortiSandbox VM00<br>s/n: FSAVM0TM24001040 | Fortinet Sandbox Threat Intelligence (Antivirus, IPS, Web Filtering, File Query, Industrial Security, SandBox Engine) plus 24x7 FortiCare. Subscribes up to 8 VMs.<br><br>FC-10-FSV00-500-02-12 | 2026-03-04 |
| 6. | FortiSandbox VM00<br>s/n: FSAVM0TM24001041 | Fortinet Sandbox Threat Intelligence (Antivirus, IPS, Web Filtering, File Query, Industrial Security, SandBox Engine) plus 24x7 FortiCare. Subscribes up to 8 VMs.<br><br>FC-10-FSV00-500-02-12 | 2026-03-04 |
| 7. | FortiMail VM04<br>s/n: FEVM040000210256 | F24x7 FortiCare and FortiGuard Enterprise ATP Bundle Contract<br><br>FC-10-0VM04-643-02-12<br>Office365 API Intergration Service<br><br>10-0VM04-409-02-21 | 2025-11-21 |

**2. Termin realizacji:**

2.1. Wykonawca dostarczy dokumenty potwierdzające przedłużenie świadczenia Usług Asysty Technicznej, o których mowa w ust. 1, w ciągu 10 dni od dnia podpisania Umowy.

**3. Wymagania dotyczące Usługi Asysty Technicznej**

3.1. W ramach świadczenia Usługi Asysty Technicznej wymagana jest:
- 3.1.1. Aktualizacja Oprogramowania.
- 3.1.2. Dostęp do nowych wersji oprogramowania oraz poprawek.
- 3.1.3. Dostęp do nowych sygnatur bezpieczeństwa.
- 3.1.4. Wsparcie w rozwiązywaniu problemów z dostarczonym oprogramowaniem.
- 3.1.5. Dostęp do bazy wiedzy producenta.

3.2. W ramach realizacji usług, Wykonawca zobowiązany będzie do:
- 3.2.1. Doradztwa architektonicznego w zakresie zgodności sposobu wykorzystywania oprogramowania z najlepszymi praktykami rekomendowanymi przez dostawcę oraz zgodności z warunkami Umowy.



Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

3.2.2. Informowania Zamawiającego o przyczynach i sposobach rozwiązywania problemów związanych z nieprawidłowym działaniem Systemu.

3.2.3. Doradztwa technicznego, przekazywania na bieżąco informacji o nowych funkcjonalnościach możliwych do zaimplementowania w oprogramowaniu.

3.2.4. 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.

3.2.5. Wsparciu w konfiguracji i optymalizacji Systemu.

**4. Opis równoważności:**

4.1. Zamawiający dopuszcza rozwiązanie równoważne, przy następujących założeniach:

4.1.1. Zamawiający przez „rozwiązanie równoważne" rozumie oprogramowanie zapewniające bez dodatkowych nakładów finansowych bezkonfliktowe działanie posiadanego środowiska zbudowanego w oparciu o licencje wymienione w pkt. 1.1 – 1.2. wraz z Usługą Asysty Technicznej dla tych licencji na okres opisany w pkt. 1.

4.1.2. Zamawiający wymaga, żeby dostarczone rozwiązanie równoważne 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), FortiMail (skanowanie plików i URL w czasie rzeczywistym przed dostarczeniem korespondencji) oraz FortiSandbox (Zamawiający posiada systemy, które wykorzystują API do przesyłania plików).

4.1.3. Dodatkowo w przypadku błędnego działania środowiska po instalacji oprogramowania równoważnego Wykonawca zobowiązany będzie na własny koszt przywrócić środowisko do stanu poprawnego funkcjonowania w przeciągu 24h od stwierdzenia przez Zamawiającego niepoprawnego funkcjonowania, a w przypadku braku takiej możliwości do stanu pierwotnego oraz dostarczenia innego rozwiązania spełniającego wymagania OPZ w terminie do 3 dni kalendarzowych.



Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

**Opis wymagań dla oprogramowania równoważnego do Sandbox (FortiSandbox VM00)**

1) Zamawiający posiada licencje na oprogramowanie FortiSandbox oraz zintegrowane systemy informatyczne, które korzystają z rozwiązania firmy Fortinet.
2) 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 złośliwych 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).
3) 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 dostarczenia 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 Opisie przedmiotu 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



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

spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u 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. Każdy Instruktaż będzie trwał minimum 2 Dni Robocze (łącznie minimum 14 godzin zegarowych).
5. Zainstalować oprogramowanie równoważne w środowisku systemowo-programowym oraz dokonać poprawnej konfiguracji mechanizmów systemu sandbox służącego do ochrony przed atakami typu APT (Advanced Persistent Threat) oraz zintegrować się z systemami/aplikacjami wytwarzanymi w ramach 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 służący ochronie przed atakami typu APT (Advanced Persistent Threat) będący 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.



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

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).
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 i 11, 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 powinna być możliwa w pełnym zakresie za pomocą graficznego interfejsu użytkownika (WebGUI) oraz wiersza poleceń (CLI).
i) Komunikacja z panelem zarządzania powinna wykorzystywać szyfrowane połączenie – https.
j) System powinien zapewniać wsparcie dla minimum dwóch kont administratorów.
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 Secure Mail Gateway.
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.



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

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
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

**Opis wymagań dla oprogramowania równoważnego do Secure Mail Gateway (FortiMail VM04)**

1) Zamawiający posiada licencje na oprogramowanie FortiMail VM04 oraz zintegrowane systemy informatyczne, które korzystają z rozwiązania firmy Fortinet.
2) Zamawiający wymaga, żeby dostarczone oprogramowanie integrowało się z posiadanymi urządzaniami takimi jak: FortiAnalyzer (przesyłanie logów i generowanie raportów oraz alarmów), FortiSandbox (wysyłanie plików i URL w celu weryfikowania zawartości i bezpieczeństwa odbieranej zawartości z sieci Internet).
3) 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 FortiMail**

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 Opisie przedmiotu 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 FortiMail.
   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 nie może zakłócić pracy środowiska systemowo-programowego Zamawiającego.
   d) oprogramowanie równoważne musi w pełni współpracować z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie.
   e) 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 Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona



Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

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. <u>W przypadku dostawy oprogramowania równoważnego Wykonawca zobowiązany jest:</u>**

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. Każdy Instruktaż będzie trwał minimum 2 Dni Robocze (łącznie minimum 14 godzin zegarowych).
5. Zainstalować oprogramowanie równoważne w środowisku systemowo-programowym oraz dokonać poprawnej konfiguracji mechanizmów systemu Secure Mail Gateway służącego do ochrony poczty oraz zintegrować się z systemami wykorzystywanymi w ramach działalności Zamawiającego w terminie do **10 dni roboczych** od dnia podpisania Umowy.
6. Dostarczyć wszelkich dodatkowych licencji - niezbędnych do prawidłowego funkcjonowania oprogramowania równoważnego.

**III. <u>Opis wymaganych minimalnych funkcjonalności w przypadku zaoferowania oprogramowania równoważnego w stosunku do oprogramowania FortiMail</u>**

1. Integracja z systemami Zamawiającego, w tym zakresie dostarczony system ochrony poczty musi zapewniać:
    a. Integrację z rozwiązaniami typu FortiGate (komponent Fortinet), w zakresie logowania oraz budowy topologii sieci FortiOS.
    b. Integrację z rozwiązaniem FortiSandbox (komponent Fortinet) w celu dynamicznego skanowania plików i URL (sprawdzanie pod kątem bezpieczeństwa plików i URL).
    c. integrację z systemem FortiAnalyzer (komponent Fortinet) w zakresie dostarczania danych, które będą potem rejestrowane, kolekcjonowane, monitorowane, analizowane i



Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

przetwarzane pod względem bezpieczeństwa. Zamawiający wymaga utworzenie minimum 3 raportów bezpieczeństwa z przesyłanych logów.

2. Funkcje logowania i raportowania, w tym zakresie dostarczony system ochrony poczty musi zapewniać:
    a. Logowanie do zewnętrznego serwera SYSLOG;
    b. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku;
    c. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
    d. Możliwość podglądu logów w czasie rzeczywistym;
    e. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych;
    f. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora system;
    g. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.
3. Ogólne funkcje systemu ochrony poczty, dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:
    a. Wsparcie dla co najmniej 100 domen pocztowych,
    b. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all),
    c. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP,
    d. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości),
    e. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej,
    f. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów,
    g. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP,
    h. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania wiadomości z kwarantanny przez użytkownika,
    i. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail oraz POP3,
    j. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki,
    k. Backup poczty realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI,
    l. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu,
    m. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników,
    n. Zapobieganie przed wyciekiem informacji poufnej DLP (Data Leak Preention).
4. Kontrola antywirusowa, w tym zakresie dostarczony system ochrony poczty musi zapewniać:
    a. Skanowanie antywirusowe wiadomości SMTP,
    b. Kwarantannę dla zainfekowanych plików,
    c. Skanowanie załączników skompresowanych,
    d. Definiowanie komunikatów powiadomień w języku polskim,
    e. Blokowanie załączników w oparciu o typ pliku,
    f. Możliwość zdefiniowania nie mniej niż [50] polityk kontroli antywirusowej,



Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

g. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.

5. Kontrola antyspamowa, system musi zapewniać poniższe funkcje i metody filtrowania spamu:
   a. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta,
   b. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania,
   c. Szczegółowa kontrola nagłówka wiadomości,
   d. Analiza Heurystyczna,
   e. Współpraca z zewnętrznymi serwerami RBL, SURBL,
   f. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub poszczególnych chronionych domen,
   g. Możliwość dostrajania filtrów Bayes'a przez poszczególnych użytkowników,
   h. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF,
   i. Kontrola w oparciu o Greylisting oraz SPF,
   j. Filtrowanie treści wiadomości i załączników,
   k. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości,
   l. Możliwość zdefiniowania nie mniej niż [50] polityk kontroli antyspamowej,
   m. System musi realizować skanowanie antyspamowe z wydajnością min. 54 tyś wiadomości/godzinę,
   n. Ochrona typu outbrake,
   o. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking),
   p. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości.
6. Ochrona przed atakami na usługę poczty, system musi zapewniać poniższe funkcje i metody filtrowania:
   a. Ochrona przed atakami na adres odbiorcy,
   b. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu,
   c. Kontrola Reverse DNS (ochrona przed Anty-Spoofing),
   d. Weryfikacja poprawności adresu e-mail nadawcy.
7. Funkcje pracy w trybie wysokiej dostępności (HA), system ochrony poczty musi zapewniać poniższe funkcje:
   a. Konfigurację HA w każdym z trybów: gateway, transparent,
   b. Tryb A-P [Active-Passive] z synchronizacją polityk i wiadomości, gdzie klaster występuje pod jednym adresem IP,
   c. Tryb synchronizacji konfiguracji dla scenariuszy, gdy każde z urządzeń występuje pod innym adresem IP,
   d. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu,
   e. Monitorowanie stanu pracy klastra.



Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

8. Aktualizacje sygnatur, dostęp do bazy spamu, w tym zakresie dostarczony system ochrony poczty musi zapewniać:
    a. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym,
    b. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.
9. Zarządzanie, system ochrony poczty musi zapewniać poniższe funkcje:
    a. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH,
    b. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.



Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706