(288500)

Opis Przedmiotu Zamówienia

1. **Zakup licencji do posiadanego oprogramowania Sandbox (FortiSandbox VM00) i Secure Mail Gateway (FortiMail VM04) wraz z gwarancją/wsparciem technicznym oraz zakup licencji Slotów i pakietu oprogramowania Windows 11 z Office 2024 do FortiSandbox VM00 (WIN11O24) lub rozwiązania równoważnego. Przedmiot zamówienia obejmuje:**

1.1. Zakup licencji Fortinet Sandbox Threat Intelligence do Oprogramowania FortiSandbox VM00 wraz z gwarancją/wsparciem technicznym **do dnia 2029-11-30.** Przedmiotem zamówienia jest przedłużenie następujących elementów dla wszystkich egzemplarzy FortiSandbox VM00 (zgodnie z Tabelą nr 1.):

1.1.1. Licencji Fortinet Sandbox Threat Intelligence zawierającej moduły: Firmware & General Updates, Enhanced Support, Telephone Support, Advanced Malware Protection, FortiGuard IPS Service, SandBox Engine, FortiGuard URL, DNS & Video Filtering Service, File Query, FortiGuard OT Security Service.

1.1.2. Nowy okres ważności licencji wraz z gwarancją/wsparciem technicznym musi:

1.1.2.1. rozpoczynać się bezpośrednio po zakończeniu bieżącego okresu (bez jakiejkolwiek przerwy w pokryciu).

1.2. Zakup licencji FortiGuard Enterprise ATP Bundle do Oprogramowania FortiMail służącego do kompleksowego zabezpieczenia poczty elektronicznej w infrastrukturze IT Zamawiającego wraz z gwarancją/wsparciem technicznym **do dnia 2029-11-30**. Przedmiotem zamówienia jest przedłużenie następujących elementów dla FortiMail VM04 (zgodnie z Tabelą nr 1):

1.2.1. Licencji 24x7 FortiCare and FortiGuard Enterprise ATP Bundle Contract zawierającej moduły: Firmware & General Updates, Enhanced Support, Telephone Support, Advanced Malware Protection, URI Click Protection, AntiSpam, FortiGuard Virus Outbreak Protection Service, FortiSandbox Cloud, Content Disarm & Reconstruction.

1.2.2. Nowy okres ważności licencji wraz z gwarancją i wsparciem technicznym musi:

1.2.2.1. rozpoczynać się bezpośrednio po zakończeniu bieżącego okresu (bez jakiejkolwiek przerwy w pokryciu).

1.3. Zakup i aktywacja licencji **32 dodatkowych slotów** (VM clone count) dla systemów FortiSandbox VM00. Zamawiający posiada obecnie po 4 sloty na każdy z 8 egzemplarzy FortiSandbox VM00 (Tabela nr 1.). W ramach zamówienia Wykonawca jest zobowiązany dostarczyć i aktywować dodatkowe 4 sloty na każdym z 8 systemów, tak aby każdy system FortiSandbox VM00 dysponował ostatecznie 8 slotami (łącznie 32 dodatkowe sloty). Sloty są opisane przez producenta jako: „Expands FortiSandbox capacity by 1 VM clone count on Local (including Custom) and Cloud. On VM, allows up to 200 VMs. Offered as subscription service for new and existing Sandboxing VMs” (kod produktu: FC1-10-FSV00-1035-02-12). Dodatkowe sloty stanowią licencje terminowe i muszą być aktywne do dnia **2029-11-30**.

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

1.4. Zakup **32 kompletów licencji** wieczystych pakietu oprogramowania Windows 11 i Office 2024 (WIN11O24) przeznaczonych do pracy w środowisku FortiSandbox VM00. Zamawiający posiada 8 egzemplarzy oprogramowania FortiSandbox VM00 (Tabela nr 1.), przy czym na każdym z nich zostaną uruchomione 4 kompletne instancje licencyjne WIN11O24.
Dostarczone licencje Windows 11 oraz Office 2024 muszą uprawniać Zamawiającego do legalnego użycia w 32 instancjach lub środowiskach detonacyjnych FortiSandbox VM00. Licencje muszą umożliwiać aktywację, ewidencję, odtworzenie oraz reinstalację środowisk VM w przypadku awarii, migracji, przebudowy lub ponownego przygotowania środowisk detonacyjnych. Wykonawca ponosi odpowiedzialność za dostarczenie licencji zgodnych z przeznaczeniem wskazanym w OPZ. Dowodem spełnienia wymagania będzie dokument licencyjny, certyfikat, potwierdzenie producenta lub dystrybutora, klucz aktywacyjny albo inny dokument jednoznacznie potwierdzający liczbę, zakres, legalność i możliwość użycia licencji w środowisku FortiSandbox VM00.

1.5. Zamawiający posiada licencje wraz z gwarancją/wsparciem technicznym na Oprogramowanie zgodnie tabelą nr 1.

Tabela nr 1.

NR	Numer seryjny	Nazwa licencji	Data wygaśnięcia licencji/gwarancji /wsparcia technicznego
1	2	3	4
1.	FortiSandbox VM00 s/n: **********1326	Fortinet Sandbox Threat Intelligence (Firmware & General Updates, Enhanced Support, Telephone Support, Advanced Malware Protection, FortiGuard IPS Service, SandBox Engine, FortiGuard URL, DNS & Video Filtering Service, File Query, FortiGuard OT Security Service) plus 24x7 FortiCare. Subscribes up to 8 VMs. FC-10-FSV00-500-02-12	2026-11-30
2.	FortiSandbox VM00 s/n: **********1027	Fortinet Sandbox Threat Intelligence (Firmware & General Updates, Enhanced Support, Telephone Support, Advanced Malware Protection, FortiGuard IPS Service, SandBox Engine, FortiGuard URL, DNS & Video	2026-11-30

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

		Filtering Service, File Query, FortiGuard OT Security Service) plus 24x7 FortiCare. Subscribes up to 8 VMs. FC-10-FSV00-500-02-12	
3.	FortiSandbox VM00 s/n: **********1038	Fortinet Sandbox Threat Intelligence (Firmware & General Updates, Enhanced Support, Telephone Support, Advanced Malware Protection, FortiGuard IPS Service, SandBox Engine, FortiGuard URL, DNS & Video Filtering Service, File Query, FortiGuard OT Security Service) plus 24x7 FortiCare. Subscribes up to 8 VMs. FC-10-FSV00-500-02-12	2026-11-30
4.	FortiSandbox VM00 s/n: **********1039	Fortinet Sandbox Threat Intelligence (Firmware & General Updates, Enhanced Support, Telephone Support, Advanced Malware Protection, FortiGuard IPS Service, SandBox Engine, FortiGuard URL, DNS & Video Filtering Service, File Query, FortiGuard OT Security Service) plus 24x7 FortiCare. Subscribes up to 8 VMs. FC-10-FSV00-500-02-12	2026-11-30
5.	FortiSandbox VM00 s/n: **********1040	Fortinet Sandbox Threat Intelligence (Firmware & General Updates, Enhanced Support, Telephone Support, Advanced Malware Protection, FortiGuard IPS Service, SandBox Engine, FortiGuard URL, DNS & Video Filtering Service, File Query, FortiGuard OT Security Service)	2026-11-30

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

		plus 24x7 FortiCare. Subscribes up to 8 VMs. FC-10-FSV00-500-02-12	
6.	FortiSandbox VM00 s/n: **********1041	Fortinet Sandbox Threat Intelligence (Firmware & General Updates, Enhanced Support, Telephone Support, Advanced Malware Protection, FortiGuard IPS Service, SandBox Engine, FortiGuard URL, DNS & Video Filtering Service, File Query, FortiGuard OT Security Service) plus 24x7 FortiCare. Subscribes up to 8 VMs. FC-10-FSV00-500-02-12	2026-11-30
7.	FortiSandbox VM00 s/n: **********2576	Fortinet Sandbox Threat Intelligence (Firmware & General Updates, Enhanced Support, Telephone Support, Advanced Malware Protection, FortiGuard IPS Service, SandBox Engine, FortiGuard URL, DNS & Video Filtering Service, File Query, FortiGuard OT Security Service) plus 24x7 FortiCare. Subscribes up to 8 VMs. FC-10-FSV00-500-02-12	2026-11-18
8.	FortiSandbox VM00 s/n: **********2577	Fortinet Sandbox Threat Intelligence (Firmware & General Updates, Enhanced Support, Telephone Support, Advanced Malware Protection, FortiGuard IPS Service, SandBox Engine, FortiGuard URL, DNS & Video Filtering Service, File Query, FortiGuard OT Security Service) plus 24x7 FortiCare. Subscribes up to 8 VMs.	2026-11-18

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	
9.	FortiMail VM04 s/n: **********0256	F24x7 FortiCare and FortiGuard Enterprise ATP Bundle Contract (Firmware & General Updates, Enhanced Support, Telephone Support, Advanced Malware Protection, URI Click Protection, AntiSpam, FortiGuard Virus Outbreak Protection Service, FortiSandbox Cloud, Content Disarm & Reconstruction) FC-10-0VM04-643-02-12	2026-11-30

1.6. Wsparcie FortiSandbox i FortiMail musi być aktywne przez wymagany okres, bez przerwy względem obecnego okresu wsparcia, co zostanie potwierdzone dokumentem producenta, dystrybutora albo statusem w portalu producenta. Dodatkowe sloty FortiSandbox muszą zostać aktywowane na właściwych instancjach, z potwierdzeniem liczby slotów przed i po aktywacji. Licencje Windows 11 i Office 2024 muszą być legalne, aktywowalne, możliwe do użycia w środowisku FortiSandbox VM00 i możliwe do udokumentowania przy odbiorze. Gwarancja/wsparcie techniczne muszą być realizowane zgodnie z SLA, obejmować eskalację do producenta dla zgłoszeń wymagających takiej eskalacji, przekazywanie numerów zgłoszeń, RCA dla P1/P2 oraz zamykanie zgłoszeń wyłącznie po akceptacji Zamawiającego. Rozwiązanie równoważne, jeżeli zostanie zaoferowane, musi spełnić mierzalne kryteria równoważności, zaliczyć POC i nie powodować dodatkowych kosztów po stronie Zamawiającego.

1.7. Zamówienie nie jest zakupem nowego, oderwanego od środowiska systemu bezpieczeństwa, lecz kontynuacją wsparcia, utrzymania i rozbudowy istniejącego ekosystemu bezpieczeństwa Zamawiającego. Zamawiający dopuszcza rozwiązania równoważne wyłącznie w zakresie, w jakim wykonawca jest w stanie wykazać, że rozwiązanie równoważne zapewni co najmniej ten sam poziom funkcjonalności, bezpieczeństwa, kompatybilności, integracji, wsparcia producenta, ciągłości działania i rozliczalności odbiorowej, bez dodatkowych kosztów i bez pogorszenia poziomu ochrony środowiska Zamawiającego. Wymogi równoważności mają charakter mierzalny i podlegają ocenie na etapie badania ofert oraz odbioru.

2. Termin realizacji:

2.1. Termin realizacji zamówienia wynosi 14 dni od dnia zawarcia Umowy. Wykonawca jest zobowiązany dostarczyć Zamawiającemu dokumenty potwierdzające realizację ust. 1.1–1.4 (dostarczenie licencji).

2.2. Jako dokumenty potwierdzające Zamawiający akceptuje wyłącznie następujące rodzaje dokumentów:

2.2.1. oficjalny certyfikat lub potwierdzenie producenta o przedłużeniu/aktywacji licencji,

2.2.2. potwierdzenie dystrybutora lub autoryzowanego partnera Fortinet,

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

2.2.3. aktualny status licencji w portalu producenta,

2.2.4. jednoznaczne przypisanie licencji do konkretnych numerów seryjnych lub identyfikatorów instancji FortiSandbox VM00 oraz FortiMail.

2.3. W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany jest przekazać Zamawiającemu, poprzez podpięcie do istniejącego konta Zamawiającego na portalu producenta Oprogramowania lub na adres e-mail: licencje@cez.gov.pl dane i dokumenty umożliwiające korzystanie z Oprogramowania w pełnym zakresie funkcjonalnym.

Wszystkie dokumenty muszą być w formie elektronicznej, w języku polskim lub angielskim. Wykonawca ponosi pełną odpowiedzialność za autentyczność, kompletność i zgodność dostarczonych dokumentów z wymaganiami Zamawiającego.

3. Gwarancja/wsparcie techniczne

3.1. W ramach świadczenia gwarancji/wsparcia technicznego:

3.1.1. Wykonawca zapewni Zamawiającemu dostęp do aktualizacji, nowych wersji i poprawek producenta dla oprogramowania objętego Umową oraz na zgłoszenie Zamawiającego, zapewni wsparcie przy planowaniu i wykonaniu aktualizacji. Wsparcie obejmuje co najmniej ocenę wpływu aktualizacji na środowisko Zamawiającego, rekomendację sposobu wdrożenia, uzgodnienie okna serwisowego, przygotowanie planu zmiany, przygotowanie planu wycofania, udział w pracach aktualizacyjnych oraz przekazanie informacji podsumowującej wykonane czynności. Wykonawca nie wykonuje zmian w środowisku produkcyjnym bez uprzedniej akceptacji Zamawiającego.

3.1.2. Wsparcie w rozwiązywaniu problemów z dostarczonym oprogramowaniem. Wykonawca zapewnia Zamawiającemu profesjonalne wsparcie techniczne w rozwiązywaniu wszelkich problemów z dostarczonym oprogramowaniem zgodnie z poniższą tabelą SLA:

Tabela nr 2.

Priorytet	Definicja	Czas reakcji	Eskalacja do producenta	Wymagany rezultat	Dokument zamknięcia
P1 – Krytyczny	Całkowity brak możliwości korzystania z Systemu lub kluczowych funkcji, uniemożliwiający prowadzenie podstawowej działalności Zamawiającego	2 godziny robocze	niezwłocznie (max 4 godziny)	usunięcie usterki lub skuteczne obejście	potwierdzenie Zamawiającego + Raport RCA
P2 – Wysoki	Poważne ograniczenie kluczowych funkcji Systemu, powodujące istotny wpływ na działalność operacyjną	4 godziny robocze	w ciągu 8 godzin roboczych	usunięcie usterki lub skuteczne obejście	potwierdzenie Zamawiającego + Raport RCA
P3 – Średni	Częściowe ograniczenie funkcjonalności Systemu, nie powodujące znaczącego wpływu na działalność	24 godzin roboczych	w ciągu 48 godzin roboczych	usunięcie usterki lub skuteczne obejście	potwierdzenie Zamawiającego
P4 – Niski	Drobne usterki, błędy kosmetyczne lub pytania eksploatacyjne nie wpływające istotnie na działanie Systemu	72 godziny robocze	na żądanie Zamawiającego	usunięcie usterki lub udzielenie	potwierdzenie Zamawiającego

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

				odpowiedzi	

3.1.3. Dodatkowe postanowienia:

3.1.3.1. Czas reakcji liczy się od momentu prawidłowego zgłoszenia incydentu przez Zamawiającego.

3.1.3.2. Wszystkie czasy reakcji oraz rozwiązywania incydentów (SLA) podane w niniejszym OPZ są liczone wyłącznie w godzinach roboczych Zamawiającego, tj. od poniedziałku do piątku w godzinach 8:00–16:00. Poza godzinami roboczymi (w tym w weekendy i dni ustawowo wolne od pracy) zgłoszenia, w tym incydenty o priorytecie P1, są obsługiwane bezpośrednio przez producenta (Fortinet) w ramach umowy FortiCare 24×7. Wykonawca nie ma obowiązku monitorowania, eskalowania ani reagowania na zgłoszenia poza godzinami roboczymi Zamawiającego.

3.1.3.3. Zamknięcie zgłoszenia może nastąpić wyłącznie za zgodą Zamawiającego.

3.1.3.4. Wykonawca jest zobowiązany do aktywnego prowadzenia zgłoszenia w imieniu Zamawiającego, w tym eskalacji do najwyższego poziomu wsparcia u producenta.

Wykonawca ponosi pełną odpowiedzialność za dotrzymanie parametrów SLA określonych powyżej.

3.1.4. Dostęp do bazy wiedzy producenta jest uprawnieniem wynikającym z aktywnego wsparcia producenta i nie stanowi odrębnego elementu odbioru. Wykonawca jest zobowiązany zapewnić aktywność wsparcia producenta w zakresie umożliwiającym Zamawiającemu korzystanie z dokumentacji, informacji technicznych i materiałów producenta zgodnie z zasadami producenta.

3.2. W ramach realizacji gwarancji/wsparcia technicznego, 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. Doradztwo architektoniczne i techniczne jest realizowane na podstawie zgłoszeń Zamawiającego, w ramach limitu godzin określonego w OPZ, z zastrzeżeniem obowiązków dotyczących zgłoszeń P1 i P2. Wynikiem doradztwa jest udokumentowany produkt końcowy w postaci: konsultacji technicznej zarejestrowanej w systemie zgłoszeniowym, pisemnej rekomendacji technicznej, notatki z konsultacji, planu zmiany, analizy ryzyka, rekomendacji konfiguracyjnej, stanowiska technicznego lub potwierdzenia zgodności proponowanego działania z dokumentacją lub dobrymi praktykami producenta. Każdy rezultat doradztwa musi zostać formalnie udokumentowany w systemie zgłoszeniowym, korespondencji lub w odrębnym dokumencie i przekazany Zamawiającemu.

3.2.2. Informowania Zamawiającego o przyczynach i sposobach rozwiązywania problemów związanych z nieprawidłowym działaniem Systemu. Wykonawca jest zobowiązany do niezwłocznego informowania Zamawiającego o zdiagnozowanych przyczynach wystąpienia problemów oraz proponowanych sposobach ich rozwiązania. W przypadku incydentów zakwalifikowanych jako priorytet P1 lub P2 Wykonawca jest zobowiązany do przygotowania i przekazania Zamawiającemu, nie później niż w ciągu 7 dni roboczych od zamknięcia

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

zgłoszenia, szczegółowego Raportu Analizy Przyczyny Incydentu (RCA) lub Raportu Podsumowującego Incydent, zawierającego co najmniej:

3.2.2.1. opis zdarzenia i jego chronologię,

3.2.2.2. wpływ incydentu na funkcjonowanie Systemu i procesy Zamawiającego,

3.2.2.3. zidentyfikowaną przyczynę pierwotną (root cause) lub hipotezę przyczyny,

3.2.2.4. podjęte działania diagnostyczne i naprawcze,

3.2.2.5. zastosowane obejście czasowe (workaround),

3.2.2.6. rekomendowane trwałe rozwiązanie problemu,

3.2.2.7. informacje o eskalacji zgłoszenia do producenta (w tym numer zgłoszenia),

3.2.2.8. datę zamknięcia incydentu.

Raport przekazywany jest w formie pisemnej (PDF) w języku polskim. Wykonawca ponosi pełną odpowiedzialność za rzetelność, kompletność i terminowość przygotowania raportu.

3.2.3. W ramach gwarancji/wsparcia technicznego Wykonawca jest zobowiązany do wsparcia w zakresie eksploatacji, konfiguracji, bezpieczeństwa i rozwoju Systemu. Wsparcie realizowane jest wyłącznie na podstawie zgłoszeń Zamawiającego rejestrowanych w systemie ticketowym. Na zgłoszenia w ramach doradztwa technicznego mają zastosowanie czasy reakcji i rozwiązywania określone w tabeli SLA dla priorytetów P3 i P4. Rezultatem każdego zgłoszenia jest udokumentowane w systemie zgłoszeniowym wsparcie w postaci konsultacji technicznej, rekomendacji konfiguracyjnej, notatki lub stanowiska technicznego.

3.2.4. W przypadku wystąpienia wad, błędów lub usterek oprogramowania Wykonawca jest zobowiązany do:

3.2.4.1. założenia zgłoszenia serwisowego w systemie pomocy technicznej producenta,

3.2.4.2. przekazania Zamawiającemu (CeZ) numeru zgłoszenia (Ticket ID),

3.2.4.3. aktywnego prowadzenia zgłoszenia w imieniu Zamawiającego oraz regularnego informowania Zamawiającego o aktualnym statusie, minimum raz na 72 godziny lub niezwłocznie na każde żądanie Zamawiającego,

3.2.4.4. przekazywania Zamawiającemu na bieżąco całej korespondencji, załączników oraz innych dokumentów otrzymanych od producenta,

3.2.4.5. zamknięcia zgłoszenia serwisowego wyłącznie za pisemną zgodą Zamawiającego i po potwierdzeniu przez Zamawiającego, że usterka została skutecznie usunięta.

Wykonawca ponosi pełną odpowiedzialność za terminowość, prawidłowość i skuteczność obsługi zgłoszeń u producenta.

3.2.5. Wykonawca zapewni wsparcie w zakresie konfiguracji oraz optymalizacji Systemu. Wszystkie zmiany konfiguracyjne, optymalizacyjne oraz inne modyfikacje wprowadzane w środowisku produkcyjnym mogą być realizowane wyłącznie zgodnie z procedurą zarządzania zmianami obowiązującą u Zamawiającego i wymagają:

3.2.5.1. akceptacji CeZ/Zamawiającego przed rozpoczęciem prac,

3.2.5.2. przygotowania i zatwierdzenia Planu Zmiany,

3.2.5.3. przygotowania Planu Wycofania (rollback),

3.2.5.4. uzgodnienia okna serwisowego.

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

Wykonawca ponosi pełną odpowiedzialność za prawidłowe przeprowadzenie zmian oraz wszelkie skutki wynikające z ich realizacji lub nieprawidłowego funkcjonowania Systemu po zmianie.

4. Opis równoważności:

4.1. Zamawiający dopuszcza rozwiązanie równoważne wyłącznie jako rozwiązanie realnie zdolne do zastąpienia wskazanego rozwiązania referencyjnego bez pogorszenia bezpieczeństwa, ciągłości działania, kompatybilności, funkcjonalności, integracji, obsługi incydentów i wsparcia producenta. Wykonawca oferujący rozwiązanie równoważne musi wykazać spełnienie kryteriów równoważności na etapie oferty poprzez tabelę zgodności, opis architektury, opis integracji z systemami Zamawiającego, BOM/licence matrix, dokumentację producenta potwierdzającą wymagane integracje, opis migracji, plan rollbacku, wykaz kosztów ujętych w cenie oraz oświadczenie, że wdrożenie rozwiązania równoważnego nie spowoduje po stronie Zamawiającego żadnych dodatkowych kosztów licencyjnych, integracyjnych, sprzętowych, szkoleniowych ani utrzymaniowych.

4.1.1. Zamawiający przez „rozwiązanie równoważne" rozumie oprogramowanie, które łącznie:

4.1.1.1. w pełni spełnia wszystkie wymagania określone w Załączniku nr 1 (dla sandbox) do OPZ oraz/lub Załączniku nr 2 do OPZ (dla secure mail gateway),

4.1.1.2. zapewnia bezkonfliktowe działanie w istniejącym środowisku Zamawiającego zbudowanym w oparciu o licencje wymienione w pkt. 1.1–1.4,

4.1.1.3. jest dostarczane wraz z gwarancją/wsparciem technicznym na okres i warunkach określonych w pkt. 1,

4.1.1.4. nie powoduje po stronie Zamawiającego żadnych dodatkowych nakładów finansowych.

W celu wykazania równoważności Wykonawca zobowiązany jest dołączyć do oferty:

4.1.1.5. wypełnioną szczegółową Tabelę Zgodności z wymaganiami zawartymi w Załącznikach nr 1 i/lub nr 2 do OPZ, podpisaną przez Wykonawcę, wraz z następującymi dokumentami niezbędnymi do oceny równoważności: szczegółowy opis architektury proponowanego rozwiązania równoważnego, opis sposobu integracji z istniejącą infrastrukturą Zamawiającego (w tym FortiMail i FortiSandbox), Bill of Materials (BOM) oraz macierz licencji (licence matrix), dokumentację producenta oferowanego rozwiązania potwierdzającą integrację i kompatybilność, szczegółowy plan migracji, plan rollbacku (cofnięcia migracji), pisemne oświadczenie Wykonawcy, że wdrożenie i eksploatacja rozwiązania równoważnego nie będzie generować po stronie Zamawiającego żadnych dodatkowych kosztów. Dokumenty te stanowią integralną część oferty i podlegają ocenie pod względem spełnienia wymagań równoważnośc.

Zamawiający dokona oceny równoważności na etapie badania ofert wyłącznie na podstawie powyższych dokumentów. Brak wymaganych środków dowodowych lub niespełnienie któregokolwiek z powyższych warunków stanowi podstawę do odrzucenia oferty jako niezgodnej z SIWZ.

4.1.2. Zamawiający wymaga, żeby dostarczone rozwiązanie równoważne integrowało się z posiadanymi urządzaniami takimi jak: FortiAnalyzer (przesyłanie logów i generowanie

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

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. W przypadku oferowania oprogramowania równoważnego Wykonawca jest zobowiązany do:

4.1.3.1. przeprowadzenia na własny koszt testów przedprodukcyjnych / Proof of Concept (POC) w środowisku testowym Zamawiającego w celu weryfikacji funkcjonalności, wydajności, kompatybilności i stabilności oferowanego rozwiązania, w zakresie uzgodnionym z Zamawiającym. POC rozwiązania równoważnego obejmuje co najmniej test integracji z FortiMail, test integracji z FortiAnalyzer, test integracji z FortiGate i FortiWeb, test przekazywania plików i adresów URL do analizy, test zwrotnego przekazania werdyktu do systemu pocztowego, test logowania i raportowania, test wydajności, test awarii, test rollbacku oraz test braku negatywnego wpływu na istniejące środowisko Zamawiającego. Kryterium zaliczenia POC jest potwierdzenie, że rozwiązanie równoważne spełnia wszystkie wymagania OPZ, działa bezkonfliktowo z istniejącym środowiskiem, nie powoduje dodatkowych kosztów po stronie Zamawiającego i nie obniża poziomu bezpieczeństwa ani ciągłości działania,

4.1.3.2. przedstawienia do akceptacji Zamawiającego szczegółowego Planu Migracji oraz Planu Rollbacku,

4.1.3.3. uzgodnienia z Zamawiającym okien serwisowych na przeprowadzenie migracji oraz wszelkich prac naprawczych i wdrożeniowych,

4.1.3.4. ponoszenia pełnej odpowiedzialności za wszelkie przestoje (downtime), zakłócenia w działaniu środowiska oraz inne negatywne skutki powstałe w związku z wdrożeniem lub funkcjonowaniem rozwiązania równoważnego,

4.1.3.5. przywrócenia na własny koszt środowiska do stanu pełnej funkcjonalności w ciągu 24 godzin od zgłoszenia nieprawidłowości przez Zamawiającego. W przypadku niemożności usunięcia usterki w powyższym terminie, niezwłocznego przywrócenia środowiska do stanu sprzed wdrożenia (rollback),

4.1.3.6. Zamawiający zastrzega sobie prawo do odmowy odbioru rozwiązania równoważnego w przypadku niezaliczenia testów POC, braku akceptacji planów migracji/rollbacku lub niespełnienia wymagań określonych w SIWZ.

4.1.3.7. Wdrożenie i eksploatacja rozwiązania równoważnego nie może generować po stronie Zamawiającego żadnych dodatkowych kosztów, w szczególności kosztów: licencyjnych, integracyjnych, migracyjnych, sprzętowych, szkoleniowych, utrzymaniowych, serwisowych, testowych, oraz kosztów przywrócenia środowiska do stanu pierwotnego. Wszelkie koszty związane z wdrożeniem, migracją, integracją i eksploatacją rozwiązania równoważnego muszą być w pełni uwzględnione w cenie ofertowej i nie mogą obciążać Zamawiającego w żadnym zakresie ani na żadnym etapie realizacji zamówienia.

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. <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 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. Wykonawca jest zobowiązany dostarczyć wraz z ofertą pełny BOM licencyjny / Licence Matrix, obejmujący wszystkie licencje, subskrypcje, moduły oraz inne składniki licencyjne niezbędne do prawidłowego, kompletnego i nieograniczonego funkcjonowania oferowanego oprogramowania przez cały okres gwarancji/wsparcia technicznego.

W cenie oferty muszą być uwzględnione wszystkie wymagane licencje i opłaty licencyjne. Wykonawca gwarantuje, że po odbiorze przedmiotu zamówienia Zamawiający nie poniesie żadnych dodatkowych kosztów licencyjnych, nie wystąpią braki licencyjne ani ukryte zależności producenta nieujęte w ofercie.

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

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 on-prem uruchomionej w środowisku Zamawiającego.
    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

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

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
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. 279 tys. Wiadomości na godzinę. Zgodnie z tabelą producenta, obecne rozwiązanie FortiMail VM04 posiada ww. wydajność. Parametr będzie weryfikowany na podstawie specyfikacji dostarczonego rozwiązania (deklaracji producenta).
   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,

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

d. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu,
e. Monitorowanie stanu pracy klastra.

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