(164106)

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa i wdrożenie systemu ochrony typu DNS (Domain Name System).

Spis treści

I. Definicje

1) „**System ochrony DNS”/„System**” – oprogramowanie służące do zarządzania i ochrony DNS, czyli System Nazw Domenowych (Domain Name System), spełniający wszystkie wymagania określone w OPZ, Umowie oraz Dokumentacji.
2) „**Administrator Systemu**” – wyznaczony pracownik Zamawiającego posiadający dostęp do każdego modułu Systemu (funkcji, widoków, pól lub wydzielonych grup/podzbiorów danych) z najwyższymi uprawnieniami, wraz z możliwością nadawania uprawnień użytkownikom oraz parametryzacji funkcji rozliczalności użytkowników oraz obsługujący System w zakresie instalacji oprogramowania i konfiguracji sprzętu komputerowego.
3) „**Awaria**” - Zatrzymanie Systemu lub brak możliwości korzystania z kluczowych funkcjonalności Systemu. Awaria może wynikać zarówno z błędnego lub wadliwego, niezgodnego z dokumentacją działania Systemu jak i wad Systemu objętych gwarancją, w tym z powodu awarii sprzętu.
4) „**Błąd**” – nieprawidłowe działanie Systemu niezależnie od przyczyny nieprawidłowości, spowodowane w szczególności Awarią lub Usterką.

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

5) „**Czas Naprawy (rozwiązania)**” – Czas liczony od momentu reakcji na zgłoszenie do momentu rozwiązania zgłoszenia (usunięcia Błędu).
6) „**Czas Reakcji**” – czas między zgłoszeniem przez Zamawiającego Błędu, a potwierdzeniem przyjęcia zgłoszenia Awarii lub Usterki przez Wykonawcę oraz wskazaniem dalszych kroków postępowania.
7) „**Dni Robocze**” – należy rozumieć dni od poniedziałku do piątku w godzinach 8-17, z wyjątkiem dni ustawowo wolnych od pracy oraz dni wolnych u Zamawiającego.
8) „**Dokumentacja**” – wszelka dokumentacja dotycząca Systemu lub jakichkolwiek innych prac Wykonawcy, która jest dostarczana lub zapisywana w Repozytorium kodów źródłowych Zamawiającego, lub powstanie w ramach realizacji Umowy, w szczególności szczegółowy opis Systemu wraz ze schematami, procedurami i politykami.
9) „**Etap**” – wyodrębnione w rozdziale II, pkt 1, ppkt 2) OPZ poszczególne części realizacyjne Wdrożenia.
10) „**Gwarancja**” – usługa świadczona przez Wykonawcę od zakończenia Okresu Stabilizacji obejmująca usuwanie lub/i naprawę wszystkich Błędów, a także dokonywanie niezbędnych modyfikacji Systemu w celu dostosowania do aktualnie obowiązującego prawa. W ramach Gwarancji możliwe będzie również dokonywanie zmian w Systemie mających na celu poprawę jego funkcjonalności.
11) „**Infrastruktura” -** infrastruktura informatyczna Zamawiającego, w szczególności infrastruktura sprzętowa, teleinformatyczna i oprogramowanie komputerowe, niezbędna do realizacji Wdrożenia i poprawnego funkcjonowania Systemu, w szczególności zachowania gwarantowanych parametrów wydajnościowych Systemu.
12) **„Instruktaż stanowiskowy”/„Instruktaż” –** instruktaż prowadzony w formie warsztatów z zakresu obsługi Systemu lub/i modułów, zgodnie z planem warsztatów i opisem w rozdziale III, pkt 2, ppkt 2.5.
13) **„Konsultant”** – przedstawiciel Wykonawcy, który realizuje zlecenia w ramach Usług Rozwoju.
14) „**Obejście**” – Przywrócenie funkcjonalności Systemu poprzez zastosowanie rozwiązania zastępczego do czasu usunięcia Awarii lub Usterki w sposób i w terminie uzgodnionym z Zamawiającym.
15) **„Odbiór Wdrożenia”** - odbiór realizowany po zakończeniu Etapu VII stwierdzający zakończenie wdrożenia Systemu w Protokole Odbioru Systemu podpisanym przez przedstawicieli Stron i wnioskującym o rozliczenie finansowe.
16) „**Oferta**” – oferta złożona przez Wykonawcę i wybrana przez Zamawiającego w postępowaniu o udzielenie przedmiotowego zamówienia publicznego.
17) **„Okres Stabilizacji”** – 15 dniowy okres rozpoczynający się od dnia Uruchomienia Produkcyjnego.
18) „**Oprogramowanie”** – Oprogramowanie licencjonowane lub sublicencjonowane przez Producenta wraz z aktualizacjami wykonanymi w tym Oprogramowaniu, dostarczone Zamawiającemu przez Wykonawcę w związku z realizacją Umowy oraz Dokumentacja takiego oprogramowania.
19) **„OPZ”** – Opis Przedmiotu Zamówienia stanowiący Załącznik nr 1 do 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

20) **”Personel Wykonawcy”** – osoby oddelegowane do realizacji Umowy przez Wykonawcę, zatrudnione na podstawie umowy o pracę lub umowy cywilnoprawne, w tym przedstawiciel wskazany w Umowie.
21) **”Plan Realizacji Projektu” -** to zbiorczy dokument, którego używa się jako przewodnika w realizacji projektu jak również w jego kontrolowaniu. To znaczy, że plan projektu jest formalnym i zarazem zatwierdzonym dokumentem, którego używa się do zarządzania oraz nadzoru wykonywanego projektu.
22) **„Produkt”** - określone świadczenie Wykonawcy opisane Umową lub Projektem Systemu jako Produkt.
23) „**Projekt**” – powiązane ze sobą działania mające na celu realizację Przedmiotu Umowy.
24) **”Projekt Systemu”-** dokument opisujący sposób spełnienia wymagań funkcjonalnych i niefunkcjonalnych przez System.
25) **”Repozytorium kodu”** – cyfrowe miejsce przechowywania kodu źródłowego aplikacji przez Zamawiającego.
26) **“RODO”** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
27) „**Uruchomienie Produkcyjne**” – uruchomienie Systemu realizującego wszystkie wymagane i opisane w OPZ funkcje. Po Uruchomieniu Produkcyjnym następuje rozpoczęcie pracy w Systemie przez Zamawiającego.
28) **„Usługi Rozwoju”** – opisane Umową usługi mające na celu zapewnienie modyfikacji i rozbudowy Systemu, które świadczone będą na podstawie zleceń.
29) **„Usterka” -** Ograniczona możliwość realizowania mniej ważnych funkcji, które nie są kluczowe dla normalnego funkcjonowania Systemu. Usterką jest również podatność bezpieczeństwa wykryta w Systemie.
30) „**Użytkownik**” – pracownik Zamawiającego mający dostęp do modułów (funkcji, widoków, pól lub wydzielonych grup danych) Systemu w zakresie niezbędnym do wykonywania obowiązków służbowych.
31) **„Wdrożenie”** – opisane Umową oraz załącznikami do Umowy wszystkie czynności do Uruchomienia Produkcyjnego.
32) „**Zgłoszenie**” - Poinformowanie Wykonawcy przez przedstawiciela Zamawiającego za pomocą wiadomości e-mail, strony internetowej lub systemu do zgłoszeń udostępnionego przez Wykonawcę na potrzeby realizacji Umowy o zaistniałym wydarzeniu powodującym konieczność podjęcia przez niego interwencji serwisowej. Zgłoszenie może dotyczyć Awarii lub Usterki.

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

II. Wymagania ogólne

1. Przedmiot zamówienia

1) Przedmiotem zamówienia jest dostawa i wdrożenie rozwiązania typu DNS (Domain Name System) - zamówienie podstawowe, obejmujące:
- dostawę Systemu wraz z niezbędnymi licencjami na okres 36 miesięcy z dostępem do danych o zagrożeniach bezpieczeństwa teleinformatycznego,
- Usługi Rozwoju w maksymalnym wymiarze 150 roboczogodzin,
- wdrożenie i przeprowadzenie Instruktażu,
- świadczenie usługi Gwarancji przez okres 36 miesięcy od daty zakończenia wdrożenia.

2) Zamawiający zakłada podzielenie procesu Wdrożenia, czyli uruchomienia i integracji Systemu z infrastrukturą Zamawiającego na następujące Etapy:
- Etap I – Analiza wdrożeniowa;
- Etap II – Dostawa Licencji i Oprogramowania;
- Etap III – Przygotowanie i Konfiguracja Środowiska Produkcyjnego;
- Etap IV – Testy akceptacyjne Systemu;
- Etap V – Instruktaż stanowiskowy;
- Etap VI – Uruchomienie Produkcyjne Systemu;
- Etap VII - Okres Stabilizacji.

3) Odbiorowi będą podlegać poszczególne Etapy Wdrożenia, w skład których wchodzą dostarczane Produkty. Szczegółowy opis Produktów przedstawiono w rozdziale III, pkt 2, dostarczenie oraz odbiór bez uwag przez Zamawiającego będzie stanowił podstawę do zakończenia prac w ramach danego Etapu.

4) Zamawiający przewiduje również możliwość udzielenia zamówienia opcjonalnego w zakresie:
- świadczenia Usługi Rozwoju w maksymalnym wymiarze 300 roboczogodzin, na zasadach opisanych w rozdziale III, pkt 4, ppkt 4.1.,
- dostawy wraz z wdrożeniem licencji na External Serwer DNS, w liczbie 2 szt., opisanej w rozdziale III, pkt 4, ppkt 4.2.

5) Usługi Rozwoju będą zlecane przez Zamawiającego zgodnie z następującą procedurą:
   a) Zamawiający przekaże Wykonawcy zlecenie realizacji Usług Rozwoju, w którym określi:
      i) zakres prac,
      ii) oczekiwany termin wykonania Usług Rozwoju.
   b) Wykonawca w terminie do 5 Dni Roboczych od otrzymania zlecenia Zamawiającego wystosuje do Zamawiającego odpowiedź zawierającą:
      i) wskazanie liczby roboczogodzin koniecznych do wykonania zleconych Usług Rozwoju,
      ii) wskazanie osób, które po stronie Wykonawcy będą odpowiedzialne za realizację Usług Rozwoju,
      iii) potwierdzenie terminu realizacji zleconych prac lub propozycję nowego terminu realizacji zlecenia.
   c) Zamawiający po otrzymaniu odpowiedzi Wykonawcy może:
      i) potwierdzić zlecenie Usług Rozwoju zgodnie z treścią zlecenia i odpowiedzi Wykonawcy, albo
      ii) zrezygnować z realizacji danych Usług Rozwoju albo

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) zaprosić Wykonawcę do negocjacji celem ustalenia zakresu, pracochłonności i terminu realizacji Usług Rozwoju.

d) Zlecenia realizacji Usług Rozwoju mogą być składane przez Zamawiającego pisemnie lub elektronicznie. Potwierdzenie zlecenia prac rozwojowych lub rezygnacja z ich wykonania wymaga formy pisemnej lub elektronicznej na adres upoważnionego przedstawiciela Wykonawcy wskazanego w Umowie.

1) Zamawiający może zlecać realizację Usług Rozwoju w siedzibie Zamawiającego lub w innym miejscu zaakceptowanym przez Zamawiającego.
2) W godziny pracy Konsultantów nie będzie wliczony czas dojazdu Konsultanta do siedziby Zamawiającego.
3) Wykonawca jest zobowiązany do prowadzenia pełnej i szczegółowej ewidencji wykorzystanych godzin pracy Konsultantów zawierającej, co najmniej:
   a) numer kolejny zgłoszenia w danym okresie rozliczeniowym;
   b) dane osoby zgłaszającej ze strony Zamawiającego;
   c) data zgłoszenia;
   d) imię i nazwisko Konsultanta;
   e) imię i nazwisko osoby, do której przyjechał Konsultant (jeśli dotyczy);
   f) opis udzielonej konsultacji (modyfikacji, warsztatów);
   g) nazwa modułu, którego dotyczy konsultacja lub modyfikacja;
   h) funkcjonalność, której dotyczy konsultacja lub modyfikacja;
   i) data i godzina rozpoczęcia i zakończenia konsultacji lub modyfikacji.

2. Zakres zamówienia

1) Zadaniem Systemu ma być realizowanie obsługi zapytań DNS w infrastrukturze Zamawiającego, informowanie o zdarzeniach mogących świadczyć o potencjalnym ryzyku złamania polis bezpieczeństwa oraz blokowanie działań mogących świadczyć o zaistnieniu potencjalnego incydentu bezpieczeństwa.
2) Szczegółowy zakres wymagań funkcjonalnych i technicznych został opisany w dalszej części tego dokumentu.
3) Oprócz wykonania Wdrożenia w zakresie merytorycznym wymaga się od Wykonawcy, aby w szczególności:
   a) pełnił aktywną i wiodącą rolę w realizacji całego przedmiotu zamówienia,
   b) przygotował i dostarczył uzgodnione z Zamawiającym, w ramach realizacji Etapu I Analiza Wdrożeniowa, dokumenty zawierające: opis zasad, które będą przestrzegane w ramach realizacji przedmiotu zamówienia, uszczegółowiony harmonogram prowadzenia prac, analizę wdrożeniową - wchodzące w skład Dokumentacji,
   c) opracował dokument „Projekt Systemu”, zawierający w szczególności elementy opisane w rozdziale III, pkt 2, ppkt 2.1.3.1,
   d) zainstalował niezbędne oprogramowanie dla Środowiska Produkcyjnego,
   e) dostarczył sparametryzowany gotowy do testów System,
   f) opracował i dostarczył scenariusze i przypadki testowe zgodnie z wymaganiami określonymi w rozdziale III, pkt 2, ppkt 2.4.2,

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) wspierał Zamawiającego w okresie testów akceptacyjnych, które zostaną przeprowadzone zgodnie z wymaganiami określonymi w rozdziale III, pkt 2, ppkt 2.4,
h) przygotował i przeprowadził Instruktaż stanowiskowy zgodnie z wymaganiami zawartymi w rozdziale III, pkt 2, ppkt 2.5,
i) przeprowadził instalacje i uruchomienie produkcyjne Systemu potwierdzone przez strony poprzez dokonanie odbioru Wdrożenia zgodnie z Umową,
j) opracował i dostarczył Dokumentację, powstałą w ramach realizacji przedmiotu zamówienia,
k) zapewnił świadczenie Gwarancji,
l) zapewnił świadczenie Usług Rozwoju.

3. Termin, miejsce i personel realizujący zamówienie

3.1. Harmonogram realizacji

Przedmiot zamówienia zostanie zrealizowany w terminie nie dłuższym niż 90 dni kalendarzowych, liczonym od dnia zawarcia Umowy, w podziale na niżej określone etapy:

Szczegółowy Harmonogram realizacji zamówienia zostanie opracowany na Etapie I - Analiza wdrożeniowa, z uwzględnieniem następujących priorytetów Zamawiającego:

1) Zakończenie Etapu I Analiza wdrożeniowa nastąpi nie później niż 14 dni kalendarzowych od dnia zawarcia Umowy przez Strony.
2) Zakończenie Etapu II Dostawa Licencji i Oprogramowania nastąpi nie później niż 14 dni kalendarzowych od zawarcia Umowy przez Strony.
3) Zakończenie Etapu III Przygotowanie i Konfiguracja Środowiska Produkcyjnego nastąpią nie później niż 45 dni kalendarzowych od zawarcia Umowy przez Strony.
4) Zakończenie Etapu IV - Testy akceptacyjne Systemu nastąpi nie później niż 7 dni kalendarzowych od zakończenia Etapu III Przygotowanie i Konfiguracja Środowiska Produkcyjnego.
5) Zakończenie Etapu V - Instruktaż stanowiskowy nastąpi w terminie dogodnym dla Zamawiającego, jednak nie później niż zakończenie etapu VII Okres Stabilizacji.
6) Zakończenie Etapu VI Weryfikacja i uruchomienie Produkcyjne Systemu nastąpią nie później niż 75 dni kalendarzowych od dnia zawarcia Umowy przez Strony.
7) Zakończenie Etapu VII Okres Stabilizacji nastąpi nie później niż 15 dni kalendarzowych od zakończenia Etapu VI Uruchomienie Produkcyjne Systemu.
8) Usługi Rozwoju mogą być zlecone Wykonawcy do końca okresu świadczenia usługi Gwarancji.

3.2. Miejsce realizacji Projektu

1) Zamówienie będzie realizowane w siedzibie Zamawiającego, zdalnie lub innym miejscu zaakceptowanym przez Zamawiającego.
2) Usługi Rozwoju realizowane będą zdalnie lub w miejscu określonym w zleceniu. W przypadku gdy zlecenie nie określa miejsca jego realizacji, będzie ono realizowane w siedzibie 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

3) Zamawiający zapewni przedstawicielom Wykonawcy dostęp do pomieszczeń Zamawiającego, w których będą realizowane zadania związane z wykonaniem Umowy.
4) Wykonawca jest zobowiązany do zachowania procedur i regulaminów obowiązujących u Zamawiającego.

3.3. Personel Wykonawcy

1) W celu zapewnienia prawidłowej realizacji Umowy Zamawiający wymaga od Wykonawcy zapewnienia osób pełniących role o kwalifikacjach co najmniej opisanych w Tabeli poniżej:

Nazwa pełnionej roli	Kwalifikacje	Minimalna Liczba osób
Analityk bezpieczeństwa	1. Minimum 3 lata doświadczenia we wdrażaniu systemów do zarządzania bezpieczeństwem IT; 2. Certyfikat inżynierski producenta w zakresie oferowanego systemu wydany przez producenta rozwiązania co najmniej 12 miesięcy przed terminem wyznaczonym na składanie ofert.	1
Inżynier odpowiedzialny za wdrożenie systemu	1. Minimum 3 lata doświadczenia we wdrażaniu systemów do zarządzania bezpieczeństwem IT; 2. Udział w minimum 3 wdrożeniach systemu bezpieczeństwa DNS, w charakterze inżyniera, w zakresie oferowanego systemu; Certyfikat inżynierski producenta oferowanego rozwiązania (inżyniera / administratora / wdrożeniowca / architekta) - wydany przez producenta rozwiązania co najmniej 12 miesięcy przed terminem wyznaczonym na składanie ofert lub Certyfikat w zakresie bezpieczeństwa informacji, np.: CompTIA Security+, CISSP – Certified Information Systems Security Professional.	1

2) Użyte powyżej nazwy własne są nazwami metodyk prowadzenia projektów, technologii lub oprogramowania używanego przez Zamawiającego w istniejących systemach informatycznych.
3) Zamawiający dopuszcza posiadanie równoważnych certyfikatów innych niż wskazane przez Zamawiającego. Przez certyfikat równoważny Zamawiający rozumie certyfikat, który jest analogiczny co do zakresu z przykładowymi certyfikatami wskazanymi z nazwy dla danej roli, co jest rozumiane jako:

   a) analogiczna dziedzina merytoryczna wynikająca z roli, której dotyczy certyfikat,
   b) analogiczny stopień poziomu kompetencji,
   c) analogiczny poziom doświadczenia zawodowego wymaganego do otrzymania danego certyfikatu,
   d) potwierdzony jest egzaminem (dotyczy tylko tych ról, których przykładowe certyfikaty

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

muszą być potwierdzone).

4) Certyfikat równoważny nie może być wystawiony przez Wykonawcę lub podmiot zależny od Wykonawcy.
5) Personel Wykonawcy przypisany do ról, dla których wymagane jest posiadanie wskazanych przez Zamawiającego certyfikatów będzie posiadał przedmiotowe certyfikaty przez cały okres realizacji Umowy.

III. Założenia realizacyjne

1. Wymagania ogólne

1) Produkty i usługi dostarczone w ramach realizacji przedmiotu zamówienia przed podpisaniem protokołu odbioru będą poddane przez Zamawiającego procedurze akceptacji. Do akceptacji przedmiotu zamówienia niezbędne jest dostarczenie wszystkich dokumentów oraz spełnienie warunków akceptacji przedmiotu zamówienia. Dokumenty wytworzone przez Wykonawcę i przedstawiane do odbioru powinny być wersjonowane i dostarczone w postaci elektronicznej nieedytowalnej. W przypadku dokumentów dostarczanych w postaci papierowej, każdy dokument powinien być podpisany przez przedstawiciela Wykonawcy.
2) Na żądanie Zamawiającego Wykonawca przedstawi sposób przygotowania dokumentów przedłożonych do akceptacji oraz sugerowane metody ich weryfikacji. W przypadku, gdy dokument nie będzie czytelny dla Zamawiającego Wykonawca przyjmie uwagi i poprawi dokument zgodnie z jego wytycznymi.
3) Zamawiający wymaga realizacji zamówienia bezpośrednio przez Personel wymieniony w rozdziale II, pkt 3, ppkt .3.3.
4) W przypadku stwierdzenia przez Zamawiającego, że Wykonawca oddelegował do realizacji przedmiotu Umowy Personel, którego kwalifikacje nie są zgodne z wymaganiami Zamawiającego, lub z powodu nienależytej realizacji Umowy lub nieprzestrzegania zasad współżycia społecznego, Zamawiający zgłasza taki fakt Wykonawcy mailowo lub pisemnie. Wykonawca niezwłocznie dokonuje zmiany Personelu realizującego przedmiot Umowy. Zgłoszenie potrzeby zmiany lub zmiana Personelu Wykonawcy nie będzie podstawą do zmian harmonogramu.
5) Wykonawca jest zobowiązany na wraz z postępem prac tworzyć i aktualizować Dokumentację Systemu tak, aby aktualna jej wersja była dostępna dla Zamawiającego.

2. Wdrożenie

2.1. Etap I – Analiza Wdrożeniowa

1) Etap I obejmuje przeprowadzenie spotkań analitycznych z Zamawiającym; opracowanie i dostarczenie analizy wdrożeniowej w ramach której nastąpi:
   a) Analiza infrastruktury informatycznej Zamawiającego, która zostanie objęta Systemem oraz potrzeb Użytkownika i wymagań funkcjonalnych odnośnie do konfiguracji Sytemu, której wynikiem będzie plan wdrożenia Systemu u 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

b) Przedstawienie docelowej architektury Systemu, w postaci Projektu Systemu, uwzględniającej:
   - Informacje i wymagania przekazane przez Zamawiającego.
   - Obecną architekturę Zamawiającego, obejmującą trzy ośrodki przetwarzania danych ulokowane na terenie Warszawy.
   - Uwzględnienie wysokiej dostępności High Availability (HA).
   - Uwzględnienie usług bezpieczeństwa świadczonych w ramach SaaS.
   - Uwzględnienie konieczności gromadzenia danych przez okres trwania umowy.
   - System musi być „zwirtualizowany" tzw. virtual appliance i współpracować z posiadanymi licencjami VMware Hypervisor Enterprise.

c) Przygotowanie wykazu oprogramowania i licencji niezbędnych do poprawnej pracy Systemu.

d) Przygotowanie specyfikacji technicznej określającej wymogi takie jak:
   - Opisanie wymagań: vCPU, vRAM, HDD dla poszczególnych składowych Systemu ulokowanych w fizycznych i wirtualnych ośrodkach przetwarzania danych.
   - Ilość maszyn wirtualnych wymaganych dla wszystkich składowych Systemu.
   - Wymagane parametry łącza pomiędzy składowymi Systemu.
   - Wymagane połączenia sieciowe pomiędzy wszystkimi składowymi Systemu. W przypadku, gdy System komunikuje się z zasobami zewnętrznymi np. bazy reputacyjne, należy wskazać wszystkie wymagane połączenia z dokładnością do portu, protokołu oraz strony inicjującej połączenie.

e) Przedstawienie przez Wykonawcę proponowanego katalogu polityk bezpieczeństwa oraz uzgodnienie docelowej listy co najmniej 10 polityk, we współpracy z Zamawiającym.

f) Przedstawienie przez Wykonawcę proponowanego katalogu raportów oraz uzgodnienie docelowej listy, obejmującej co najmniej 5 raportów, we współpracy z Zamawiającym.

g) Przedstawienie przez Wykonawcę proponowanych scenariuszy testowych Systemu, wymagających zatwierdzenia przez Zamawiającego:
   - Scenariusze testowe muszą zawierać propozycje testów wydajnościowych, funkcjonalnych i bezpieczeństwa.
   - Scenariusze testowe muszą obejmować przypadki testowe potwierdzające poprawność integracji Systemu z systemami wskazanymi w analizie przedwdrożeniowej.

2) W ramach Etapu I zostanie opracowany i dostarczony Projekt Systemu, Plan Realizacji Projektu oraz zasady przeprowadzenia Uruchomienia Produkcyjnego, w którym zostaną ustalone zasady obowiązujące podczas Wdrożenia Systemu oraz zostanie uszczegółowiony harmonogram prowadzenia prac zgodnie z wymaganiami dotyczącymi Zamawiającego, określonymi poniżej.

3) Zamawiający wymaga, aby w ramach realizacji Etapu I Wykonawca dostarczył Zamawiającemu dokumenty zawierające co najmniej:
   a) Propozycję sposobu realizacji przedmiotu zamówienia obejmującą:
      i) słownik terminów i pojęć używanych w Planie Realizacji Projektu,
      ii) zakres projektu,
      iii) notacje i metodyki używane w dokumentach i projekcie,

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

iv) narzędzia, które będą wykorzystywane do wspomagania prowadzenia projektu,

v) skład zespołu projektowego przeznaczonego do realizacji wdrożenia z opisem ról projektowych.

b) Harmonogram realizacji poszczególnych Etapów Wdrożenia i całości Umowy uwzględniający priorytety Zamawiającego

c) Plan Instruktaży stanowiskowych zawierający planowaną liczbę dni Instruktaży dla Administratorów Systemu.

d) Listę zasobów niezbędnych do realizacji poszczególnych Etapów i całej Umowy w zaproponowanym harmonogramie, w szczególności: sprzęt, urządzenia, pomieszczenia, łącze internetowe.

e) Listę pracowników Wykonawcy odpowiedzialnych za wykonanie poszczególnych Etapów i całej Umowy, w formacie RACI, zawierającą dane teleadresowe osób biorących udział w wykonaniu Umowy ze strony Wykonawcy.

f) Sposoby komunikacji osób zaangażowanych w wykonanie Umowy po stronie Wykonawcy.

g) Inne dane i informacje, które Wykonawca uzna za niezbędne do poprawnego wykonania Umowy.

4) Zamawiający wymaga, aby przedstawiony harmonogram nie przekraczał ostatecznych terminów realizacji projektu. Tworząc harmonogram Wykonawca powinien uwzględnić czas odbioru każdego Etapu przez Zamawiającego wraz z prawem Zamawiającego do zgłaszania uwag lub zastrzeżeń zgodnie z postanowieniami Umowy, co Wykonawca powinien uwzględnić przy realizacji przedmiotu zamówienia oraz ewentualne ryzyko nieodebrania Etapu. Ostatni dzień odbioru Etapu nie może wypadać w inny dzień niż Dzień Roboczy. W wypadku takiej sytuacji Zamawiający będzie uznawał za datę odbioru Etapu najbliższy Dzień Roboczy po zaproponowanej dacie odbioru. Analogiczna sytuacja dotyczy odbiorów poszczególnych części Etapów.
5) Zamawiający wymaga, żeby z punktu widzenia zapewnienia ciągłości działania systemów Zamawiającego, prace wdrożeniowe prowadzone na środowisku produkcyjnym odbywały się w sposób skoordynowany
6) Przedmiotem akceptacji Etapu I będzie dostarczony przez Wykonawcę zestaw dokumentów, który zostanie oceniony pod względem kompletności, poprawności oraz szczegółowości.

2.1.1. Wymagania w zakresie metodyki projektowej

Zamawiający wymaga:

1) Prowadzenia Projektu wyłącznie w języku polskim. Wszystkie Produkty Projektu będą sporządzane w języku polskim i zostaną dostarczone Zamawiającemu w formie wydrukowanej oraz elektronicznej w postaci edytowalnych dokumentów lub zbiorów danych wykorzystujących formaty używane w oprogramowaniu Microsoft Office.
2) Akceptacji najważniejszych Produktów Projektu. Zamawiający nie dopuszcza uruchomienia prac związanych z konfiguracją i modyfikacją Systemu bez uprzedniej akceptacji Projektu Systemu i dokonania jego odbioru. Harmonogram Projektu musi uwzględniać czas niezbędny

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

dla dokonania przeglądu jakości i akceptacji Produktów Projektu dostarczanych przez Wykonawcę. Dla Produktów typu „dokument" termin wynosi co najmniej 10 Dni Roboczych, dla Produktów typu Instruktaż stanowiskowy co najmniej 5 Dni Roboczych. W przypadku testów akceptacyjnych Systemu, Wykonawca powinien uwzględnić czas niezbędny na wykonanie testów potwierdzających naprawę błędów oraz testów regresji.

3) Zamawiający wymaga, aby przedstawiona przez Wykonawcę metodyka zapewniła dostarczenie wszystkich Produktów Projektu.

2.1.2. Lista Produktów Projektu

Lp.	Produkt	Forma Produktu
1)	Projekt Systemu	Dokument
2)	Plan testów akceptacyjnych Systemu	Dokument
3)	Scenariusze i przypadki testowe dla testów akceptacyjnych Systemu	Dokument
4)	Materiały do przeprowadzenia Instruktażu	Dokument
5)	Dostawa Licencji i Oprogramowania	Dokument i Oprogramowanie
6)	Dokumentacja wdrożeniowa	Dokument
7)	Katalog polityk bezpieczeństwa i raportów	Dokument

2.1.3. Definicje produktów Projektu

2.1.3.1. Projekt Systemu

1) Dokument opisujący sposób spełnienia wymagań funkcjonalnych i niefunkcjonalnych przez System. Dokument powinien zawierać co najmniej:
   a) opis stanu zastanego, opisującego funkcjonujące w Centrum procesy objęte wymaganymi przez Zamawiającego funkcjonalnościami Systemu,
   b) aktualizacja opisu realizacji procesów w Systemie z zapewnieniem spójności pomiędzy poszczególnymi obszarami merytorycznymi (wskazanie czy krok jest realizowany w Systemie czy poza Systemem, dla kroków realizowanych w Systemie: krótki opis kroku, komórka odpowiedzialna, ścieżka realizacji w Systemie, efekt kroku, dokumenty wejściowe i wyjściowe). Wykonawca przygotuje mapy docelowych procesów biznesowych Zamawiającego objętych Systemem, wraz z modelem procesów oraz z opisem przejścia od procesów „jakie są" do procesów docelowych, które po optymalizacji zapewnią równomierne rozłożenie obciążenia Infrastruktury Zamawiającego,
   c) opis sposobu odwzorowania struktury organizacyjnej Zamawiającego w Systemie,
   d) szczegółowy opis danych podstawowych i transakcyjnych,

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

e) opis architektury Systemu, w tym specyfikacja wymaganej architektury sprzętowej i sieciowej,
f) opis koncepcji integracji Systemu z innymi aplikacjami używanymi przez Zamawiającego (zakres i przepływ danych, odwzorowanie (mapowanie) danych pomiędzy Systemem a integrowanymi systemami, sposób i forma przekazywania danych, częstotliwość i sposób uruchamiania, wolumen danych, monitorowanie poprawności działania narzędzia integracyjnego, postępowanie w przypadku Błędów, postępowanie awaryjne, kompletne założenia techniczne niezbędne realizacji integracji),
g) plan Okresu Stabilizacji,
h) plan wsparcia w okresie Usług Gwarancji,
i) plan zarządzania konfiguracją oprogramowania,
j) opracowanie technicznych założeń do archiwizacji obiektów biznesowych w Systemie na użytek docelowych procedur archiwizacji,
k) opis standardowych i dedykowanych formularzy, zestawień i raportów (cel i opis działania, odbiorca biznesowy, częstotliwość uruchamiania, parametry selekcji, układ graficzny z uwzględnieniem kryteriów sortowania i sumowania, rozwiązanie alternatywne, specyfikacja funkcjonalna wraz z kompletnymi założeniami technicznymi niezbędnymi do jej realizacji),
l) opis koncepcji nadawania uprawnień Użytkownikom Systemu (wykaz ról z opisem dostępnych funkcji i danych oraz opis relacji pomiędzy rolami),
m) opis koncepcji administracyjnego monitorowania całego środowiska Systemu, w tym: umożliwiającego zapobieganiu Błędom, lokalizacji Błędów, monitorowania wydajności środowiska,
n) założenia do administrowania Systemem w trakcie eksploatacji wraz z wyszczególnieniem działań eksploatacyjnych niewymagających zgody Wykonawcy.

2) Projekt Systemu może składać się z kilku dokumentów, przy czym muszą one łącznie pokrywać cały w/w. zakres.

2.1.3.2. Dokumentacja wdrożeniowa

Dokumentacja wdrożeniowa obejmuje co najmniej:

1) Ogólny opis Systemu.
2) Wykaz całościowy oprogramowania oraz licencji wykorzystywanych w ramach wdrożonego Systemu – w tym systemy operacyjne, bazy danych, serwery aplikacyjne, kolektory danych itp.
3) Architektura logiczna Systemu – graficzna prezentacja Systemu i jego połączeń wraz z opisem.
4) Przepływ danych w Systemie (koncepcja obiegu informacji w Systemie pomiędzy poszczególnymi komponentami, warstwami Systemu).
5) Szczegółową konfigurację poszczególnych elementów Systemu (serwery zarządzające, serwery baz danych, systemy operacyjne, serwery aplikacyjne, serwery www – zrzuty ekranów, pliki konfiguracyjne, opisy konfiguracji, opisy uruchomionych usług, opisy poszczególnych funkcji Systemu).

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

6) Systemy zależne np. agenci na innych serwerach, dodatkowe oprogramowanie na innych stacjach roboczych i serwerach współpracujące z Systemem, opis integracji z innymi usługami.
7) Specyfikacja i konfiguracja serwerów wirtualnych.
8) Architektura sieciowa Systemu – opis połączeń sieciowych pomiędzy poszczególnymi elementami, adresacja IP, umiejscowienie elementów Systemu w poszczególnych strefach – DMZ, LAN, Internet.
9) Szczegółowy opis portów komunikacyjnych.
10) Rodzaje kont systemowych i ich uprawnienia (określenie standardowych profili uprawnień, sposobu zarządzania Użytkownikami oraz uprawnieniami w Systemie).
11) Role administracyjne.
12) Ustawienia polityki haseł.
13) Opis integracji z usługą katalogową Active Directory.
14) Opis integracji z systemami klasy SIEM, systemem kolekcji logów.
15) Opis integracji z systemem poczty elektronicznej.
16) Opis integracji z systemami monitoringu infrastruktury.
17) Opis rozwiązań w zakresie logowania zdarzeń (wskazanie rodzajów oraz lokalizacji dzienników w Systemie, opis logowanych zdarzeń, w przypadku niestandardowych logów opis ich struktury).
18) Ochrona dzienników (opis sposobu zabezpieczenia zapisów w logach przed ich utratą oraz nieuprawnioną zmianą, informacja o czasie przechowywania logów, możliwości przekazania logów do systemów zewnętrznych).
19) Procedury wykonywania krytycznych operacji w Systemie - aktualizacja, odtworzenie Systemu.
20) Procedury eksploatacyjne dla administratorów Systemu opisujące szczegółowo funkcjonalności, interfejs, zarządzanie kontami Użytkowników, mechanizmy wykorzystywania funkcjonalności wraz z przykładami budowania reguł, polityk, raportów. Procedura odtwarzania Systemu (opisanie procedury backupu i odtworzenia całego systemu i jego poszczególnych elementów, określenie czasu potrzebnego na odtworzenie całego systemu oraz jego poszczególnych elementów, opis procedur przywracania Systemu do pełnej funkcjonalności po awarii). Procedura instalacji Systemu (opis wszystkich kroków instalacji i konfiguracji Systemu w postaci zrzutów ekranu z opisami).

2.1.3.3. Katalog polityk bezpieczeństwa i raportów

Zestawienie zawierające polityki bezpieczeństwa oraz wdrożone raporty wraz z dokładnym opisem funkcjonalnym, w każdej pozycji zawierającym odnośniki do instrukcji ich budowania.

2.1.3.4. Pozostałe Produkty

1) Plan testów akceptacyjnych Systemu.
2) Scenariusze i przypadki testowe dla testów akceptacyjnych Systemu.
3) Materiały do przeprowadzenia Instruktażu.
4) Dostawa Licencji i Oprogramowania.

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. Etap II – Dostawa Licencji i Oprogramowania

1) Etap polegający na dostarczeniu Oprogramowania niezbędnego do realizacji Przedmiotu Umowy oraz wszelkich wymaganych licencji na to oprogramowanie oraz zapewnienia ciągłego i prawidłowego funkcjonowania Systemu zgodnie z wymaganiami dotyczącymi dostarczanego oprogramowania.
2) Przedmiotem akceptacji Etapu II będzie:
   a) dostawa Oprogramowania niezbędnego do realizacji Przedmiotu Umowy oraz wszelkich wymaganych licencji na to oprogramowanie;

2.2.1. Dostawa Oprogramowania

1) Wszelkie Oprogramowanie opisane w niniejszym dokumencie będzie dostarczone przez Wykonawcę w ostatecznej wersji wraz z niezbędnymi licencjami i nośnikami (np. pamięć USB) lub umieszczone w Repozytorium kodu Zamawiającego, lub udostępnione w portalu internetowym producenta.
2) Zamawiający wymaga dostarczenia rozwiązania wraz licencjami umożliwiającymi użytkowanie Systemu przez okres 36 miesięcy, bez konieczności ponoszenia dodatkowych kosztów nieprzewidzianych w niniejszym OPZ oraz Umowie.
3) Wymagane jest dostarczenie oprogramowania, realizujące co najmniej wymagania funkcjonalne określone w Ofercie.
4) Wykonawca gwarantuje dostarczenie dokumentacji użytkowej, systemowej, instalacyjnej, w tym dokumentacji interfejsów i rozszerzeń zgodnej ze stanem faktycznym. Kody źródłowe wszystkich rozszerzeń dostosowujących System muszą być dostępne dla Zamawiającego. Zamawiający musi mieć prawo używania ww. rozszerzeń i ich modyfikacji Oprogramowania nawet po zakończeniu umowy wsparcia z Wykonawcą.

2.2.2. Dostawa Licencji

1) Wymagane jest dostarczenie wszelkich niezbędnych licencji pozwalających na korzystanie z funkcjonalności Systemu co najmniej określonych w niniejszym OPZ, Umowie i Ofercie Wykonawcy.
2) Jeżeli do poprawnej pracy Systemu spełniającej wymagania Zamawiającego niezbędne jest dostarczenie oprogramowania firm zewnętrznych, Wykonawca musi dostarczyć to oprogramowanie wraz z licencjami (w niezbędnej odpowiedniej ilości do instalowanych stacji) oraz nośnikami.
3) Licencje zostaną udzielone na zasadach wskazanych w Umowie.
4) Uprawnienia licencyjne pozwolą Zamawiającemu na integrowanie Systemu z innymi systemami w zakresie przekazywania komunikatów i danych (dwukierunkowo).
5) Uprawnienia licencyjne pozwolą Zamawiającemu na samodzielne rozszerzanie funkcjonalności oprogramowania, w tym definiowanie i modyfikowanie raportów, z zastrzeżeniem braku wprowadzania modyfikacji w Oprogramowaniu, kodzie źródłowym aplikacji i strukturze bazy danych.
6) Oferowane licencje nie mogą być ogłoszone przez producenta jako end-of-support w momencie wdrażania Systemu.

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

7) Wykonawca zobowiązany jest przedstawić Umowę Licencji Systemu zgodną z wymaganiami Zamawiającego, przedstawionymi w Umowie. Zamawiający nie wyklucza jednak zaakceptowania Umowy Licencji przedstawionej przez Licencjodawcę.

2.3. Etap III Przygotowanie i Konfiguracja Środowiska Produkcyjnego

Etap III obejmuje przygotowanie Systemu do uruchomienia produkcyjnego, zgodnie z wymaganiami dotyczącymi Instalowania Środowiska Produkcyjnego oraz dostarczenia Dokumentacji zgodnie z wymaganymi określonymi poniżej:

1) Środowisko Produkcyjne zainstaluje i skonfiguruje Wykonawca pod nadzorem przedstawiciela Zamawiającego.
2) Założenie w Systemie kont docelowych oraz przypisanie im wymaganych uprawnień i parametrów.
3) Odebranie instalacji wersji produkcyjnej przez Administratorów nastąpi poprzez podpisanie Protokołu Odbioru Częściowego potwierdzającego poprawny przebieg procesu instalacji Systemu na podstawie zaakceptowanych przez Zamawiającego co najmniej:
   a) Raportów z działania podstawowych funkcjonalności Systemu,
   b) Raportów z testów wydajnościowych/przeciążeniowych,
   c) Raportów z testów bezpieczeństwa.

2.4. Etap IV – Testy akceptacyjne Systemu

Etap obejmujący przeprowadzenie testów akceptacyjnych zgodnie z przygotowanym planem testów w oparciu o dokument zawierający scenariusze testowe zgodnie z wymaganiami określonymi poniżej:

2.4.1. Plan testów akceptacyjnych Systemu

Dokument opisujący następujące aspekty związane z testami akceptacyjnymi:

1) zakres testów (w szczególności: testy integracyjne, testy uprawnień, testy wydajnościowe, testy funkcjonalne, testy bezpieczeństwa), określenie wymaganego stopnia pokrycia wymagań wobec Systemu przez testy,
2) warunki rozpoczęcia testów,
3) warunki zakończenia testów,
4) harmonogram testów, z uwzględnieniem cykli testowych,
5) sposób klasyfikacji błędów,
6) sposób prezentacji wyników testów.

2.4.2. Scenariusze i przypadki testowe dla testów akceptacyjnych Systemu

1) Dokument zawierający zestaw scenariuszy i przypadków testowych dla testów akceptacyjnych Systemu pokrywających zakres testów zdefiniowany w planie testów.
2) Opis każdego przypadku testowego powinien obejmować:
   a) opis wykonywanego testu,
   b) opis kroków wykonywanych w ramach testu wraz z instrukcją wykonania (szczegółowy opis czynności wykonywanych w Systemie, wraz ze ścieżką realizacji w Systemie),
   c) oczekiwany rezultat przypadku testowego,

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) sytuacji wariantowych podlegających weryfikacji.

3) Scenariusze testowe powinny być tak skonstruowane, aby przypadki testowe wykonywane w ramach scenariuszy umożliwiały przetestowanie procesów Zamawiającego realizowanych w Systemie.

2.4.3. System po testach akceptacyjnych

Przedmiotem odbioru Etapu IV przez Zamawiającego będzie (zgodnie ze zdefiniowanymi kryteriami akceptacji) docelowe rozwiązanie biznesowe w postaci przygotowanego do użytkowania Systemu wraz z dokumentacją przeprowadzenia testów. System po testach akceptacyjnych powinien być pozbawiony błędów wykrytych w trakcie testów, przy czym Zamawiający może dopuścić występowanie Błędów, co powinno zostać potwierdzone pozytywnym wynikiem powtórnie wykonanych przypadków testowych, które wcześniej zakończyły się błędem. Ponadto w ramach odbioru Wykonawca zobowiązany jest dostarczyć zestaw dokumentów przewidzianych w Etapie IV, który zostanie oceniony pod względem kompletności, poprawności oraz szczegółowości.

2.5. Etap V - Instruktaż stanowiskowy

1) Etap, w ramach którego zostanie przeprowadzony Instruktaż stanowiskowy dla Administratorów Systemu, wykonany na środowisku testowym przygotowanym przez Wykonawcę, zgodnie z przygotowanym planem warsztatów w oparciu o dostarczone materiały do przeprowadzenia Instruktaży. Instruktaż stanowiskowy będzie spełniał wymagania określone poniżej.
2) Przedmiotem akceptacji Etapu V będzie:
   a) dostarczanie przez Wykonawcę materiałów do przeprowadzenia Instruktaży stanowiskowych dla Administratorów Systemu w Etapie V, które zostaną ocenione pod względem kompletności, poprawności oraz szczegółowości.
   b) przeprowadzenie instruktażu stanowiskowego dla Administratorów Systemu, zgodnie z opisanymi założeniami

2.5.1. Instruktaż stanowiskowy

1) Wykonawca przeprowadzi Instruktaż stanowiskowy dla minimum 6 osób wskazanych przez Zamawiającego. Instruktaż będzie trwał minimum 5 Dni Roboczych.
2) W warsztatach mogą uczestniczyć dodatkowe 4 osoby wskazane przez Zamawiającego.
3) Instruktaż stanowiskowy dla Administratorów Systemu będzie przeprowadzony jako zajęcia teoretyczne i praktyczne. Wykonawca określi liczbę dni oraz zakres instruktaży niezbędnych do pozyskania wiedzy niezbędnej do administrowania Systemem. Wymagana jest akceptacja zakresu oraz liczby dni zaproponowanych przez Wykonawcę instruktaży przez upoważnionego przedstawiciela Zamawiającego.. Instruktaż dla Administratorów będzie obejmować wszelkie możliwe zagadnienia przydatne w codziennej pracy, a w szczególności:
   a) szczegółowe omówienie budowy reguł bezpieczeństwa, polityk monitorowania,
   b) analizę reguł bezpieczeństwa i polityk monitorowania wbudowanych w System oraz zdefiniowanych przez Użytkownika,

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

c) ćwiczenia praktyczne z budowania reguł bezpieczeństwa, polityk monitorowania, tworzenia raportów, dashboardów, definiowania alarmów, dodawania różnych źródeł danych,
d) zarządzanie konfiguracją i bezpieczeństwem w Systemie,
e) proces aktualizacji Systemu,
f) proces tworzenia kopii bezpieczeństwa i archiwizacji danych w Systemie oraz ich przywracania po awarii,
g) omówienie architektury Systemu i procesu przetwarzania danych w Systemie,
h) omówienie instalacji, aktualizacji Systemu oraz przywracania w przypadku awarii,
i) omówienie procedur eksploatacyjnych.

4) Zamawiający dopuszcza przeprowadzenie Instruktażu online lub w siedzibie Zamawiającego i decyzję przekaże Wykonawcy na etapie realizacji zamówienia, z uwzględnieniem sytuacji epidemiologicznej. Na potrzeby Instruktażu Zamawiający zapewni sale, stacje robocze oraz pozostałą infrastrukturę (rzutnik, sieć, itp.).

2.5.2. Plan przeprowadzenia Instruktażu stanowiskowego

Dokument opisujący następujące aspekty związane z Instruktażem stanowiskowym:

1) zakres Instruktażu (w szczególności: zajęcia praktyczne dla Administratorów).
2) szczegółowe określenie tematów Instruktażu,
3) Harmonogram.

2.5.3. Materiały do przeprowadzenia Instruktażu stanowiskowego

W ramach Etapu V – Instruktaż stanowiskowy dla Administratorów Systemu, wymagane jest dostarczenie następującej, zaakceptowanej przez Zamawiającego Dokumentacji:

1) Materiały do przeprowadzenia Instruktaży stanowiskowych dla Administratorów Systemu zawierające dokładne, szczegółowe instrukcje, pozwalające Zamawiającemu, samodzielnie zainstalować i skonfigurować System na wszystkich stanowiskach pracy i serwerach oraz skonfigurować wszelkie, niezbędne do pracy Systemu urządzenia komunikacyjne (np. przełączniki sieciowe, punkty dostępowe, routery, interfejsy sieciowe).
   a) wszystkie parametry konfiguracyjne Systemu,
   b) wszystkie parametry konfiguracyjne instancji i bazy danych,
   c) opis procedury archiwizowania danych zawartych w Systemie,
   d) opis procedury odtwarzania danych z urządzenia,
   e) opis wszystkich niezbędnych czynności związanych z poprawną administracją i zarządzaniem modułem/Systemem (np. ustawianie parametrów konfiguracyjnych, nadawanie uprawnień, dodawanie licencji użytkowych).
2) Materiały (instrukcje, video) niezbędne do pracy w Systemie dla Użytkowników.
3) Wszystkie ww. materiały do przeprowadzenia instruktaży stanowiskowych muszą zostać przygotowane w języku polskim.

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

2.6. Etap VI – Weryfikacja i Uruchomienie Produkcyjne Systemu

1) Etap VI traktowany będzie jako ostatnie sprawdzenie poprawności funkcjonowania Systemu oraz przeprowadzenie Uruchomienia Produkcyjnego Systemu zgodnie z opisem zawartym poniżej:
   a) W czasie Weryfikacji System musi działać poprawnie, spełniając wszystkie wymagania funkcjonalne jak i pozafunkcjonalne.
   b) Za niepoprawną pracę Systemu uważać się będzie wystąpienie Błędu w czasie trwania Weryfikacji Systemu.
   c) W przypadku niepomyślnego wyniku Weryfikacji Systemu Wykonawca dokona stosownych poprawek Systemu i aktualizacji Dokumentacji
   d) W przypadku dokonania poprawek Systemu przez Wykonawcę w następstwie stwierdzonych Błędów, Zamawiający może przeprowadzić testowanie i odbiór dla każdego z powiązanych ze sobą modułów w celu zweryfikowania ich integracji.
   e) W okresie trwania Weryfikacji Systemu Zamawiający wymaga wsparcia przez Personel Wykonawcy w postaci osobistej obecności specjalistów w siedzibie Zamawiającego lub za pomocą telekonferencji.
   f) Wykonawca nie może dokonywać w czasie Weryfikacji Systemu żadnych poprawek lub zmian konfiguracyjnych w Systemie bez zgody upoważnionego przedstawiciela Zamawiającego.
   g) Zasady przeprowadzenia Uruchomienia Produkcyjnego zostaną określone na Etapie I - Analiza wdrożeniowa.

2) Przedmiotem akceptacji Etapu VI będzie
   a) spełnienie wszystkich warunków opisanych w Etapie VI przez System,
   b) dostarczanie przez Wykonawcę ostatecznej wersji Dokumentacji, która zostanie oceniona pod względem kompletności, poprawności oraz szczegółowości, a także gwarancji należytego wykonania całości przedmiotu zamówienia.

2.7. Etap VII – Okres Stabilizacji

1) Okres Stabilizacji będzie trwać od dnia Uruchomienia Produkcyjnego w Okresie Stabilizacji Wykonawca będzie wspierać pracowników Zamawiającego w zakresie użytkowania Systemu.
2) W Okresie Stabilizacji Wykonawca zapewni nieograniczone czasowo usługi polegające na asyście i bieżącym wsparciu Administratorów Systemu w godzinach zdefiniowanych dla Dnia Roboczego. Pomoc będzie realizowana poprzez bezpośrednie konsultacje telefoniczne, konsultacje mailowe, telekonferencje nie później niż w następnym Dniu Roboczym po zgłoszeniu oraz konsultacje osobiste Personelu Wykonawcy, we wskazanym przez Zamawiającego terminie, nie później jednak niż w terminie 3 Dni Roboczych od zgłoszenia. Zgłoszenia konsultacji osobistych będą dokonywane przez upoważnionych przedstawicieli Zamawiającego. Wykonawca rozpocznie świadczenie usług wchodzących w zakres Okresu Stabilizacji nie później niż w następnym dniu po Uruchomieniu Produkcyjnym Systemu.

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) Ponadto w Okresie Stabilizacji Wykonawca zapewni funkcjonowanie Systemu poprzez świadczenie usług przewidzianych dla Usług Gwarancji, z tym, że w przypadku wystąpienia Błędu Czas Reakcji i Czas Naprawy będzie analogiczny jak dla Usterki.
4) W przypadku ujawnienia w trakcie Okresu Stabilizacji faktu, że System nie realizuje funkcji określonych w Umowie lub w Załącznikach do Umowy i Projekcie Systemu, Wykonawca dokona niezbędnych modyfikacji skutkujących poprawną pracą wraz z przeprowadzeniem ponownego testowania i odbioru dla każdego z powiązanych ze sobą modułów w celu zweryfikowania ich integracji w terminie nie dłuższym niż 7 Dni Roboczych od dnia zgłoszenia mu tego faktu.
5) W terminie 3 Dni Roboczych od zakończenia każdego miesiąca kalendarzowego Okresu Stabilizacji, Wykonawca przekazywać będzie Zamawiającemu raport ze zrealizowanych konsultacji oraz napraw Błędów.

3. Usługi Gwarancji

Dostarczone produkty muszą być objęte co najmniej 36 miesięcznym serwisem gwarancyjnym świadczonym bezpośrednio przez producenta w reżimie 24 godziny na dobę, 7 dni w tygodniu, gwarantowanym czasem reakcji na następny dzień roboczy uprawniającym do:

1) wsparcie telefoniczne i online w języku polskim i/lub angielskim w zakresie rozwiązywania problemów oraz dostęp do poprawek i nowych wersji oprogramowania (upgrade).
2) Usuwania błędów i wgrywania poprawek.
3) Aktualizacji systemu i poszczególnych jego komponentów do najnowszych wersji zalecanych przez producenta.
4) Okresowe przeglądy Systemu.

3.1. Stała telefoniczna pomoc dla Administratorów

1) Dla celów realizacji usługi Wykonawca wyznaczy dedykowaną dla Zamawiającego linię telefoniczną. W pilnych przypadkach, w razie braku możliwości skomunikowania się z Wykonawcą drogą telefoniczną, Zamawiający ma możliwość zgłoszenia potrzeby konsultacji drogą mailową, na adres e-mail udostępniony w dniu podpisania Umowy. Wówczas Wykonawca ma obowiązek skomunikowania się z nadawcą wiadomości najpóźniej w ciągu jednej godziny zegarowej od wysłania wiadomości. Zamawiający deklaruje gotowość oczekiwania na reakcję Wykonawcy w Dni Robocze.
2) Wykonawca powiadomi pisemnie lub elektronicznie na adres e-mail Zamawiającego o udostępnionym numerze telefonicznym oraz adresie e-mail przed podpisaniem Umowy. Wykonawca będzie każdorazowo powiadamiał pisemnie lub elektronicznie Zamawiającego o zmianie numeru telefonicznego i/lub adresu e-mail, najpóźniej na 14 dni przed zmianą.
3) Wykonawca jest zobowiązany do prowadzenia pełnej i szczegółowej ewidencji konsultacji telefonicznych, zawierającej co najmniej:
    a) numer kolejny konsultacji telefonicznej w danym okresie rozliczeniowym;
    b) datę i godzinę rozpoczęcia konsultacji;
    c) nazwę modułu, którego dotyczy problem;
    d) imię i nazwisko osoby zgłaszającej problem;

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

e) opis zgłoszonego problemu;
f) imię i nazwisko osoby udzielającej konsultacji;
g) opis rozwiązania;
h) datę i godzinę ostatecznego zakończenia rozwiązywania problemu i przekazywania Zamawiającemu wersji elektronicznej ewidencji konsultacji telefonicznych w pierwszym Dniu Roboczym miesiąca kalendarzowego, następującego po zakończeniu miesiąca, którego dotyczy ewidencja konsultacji.

3.2. Usuwanie Błędów Systemu

1) Wykonawca jest zobowiązany do dotrzymania poniżej przedstawionych parametrów czasowych w przypadku problemów dotyczących funkcjonowania Systemu w okresie Gwarancji:

L.p.	Kategoria zgłoszenia	Czas Reakcji	Czas Naprawy	Czas zaproponowania Obejścia	Maksymalny dozwolony czas funkcjonowania Obejścia
1.	Awaria	do 1 godziny	niezwłocznie (do 6 godzin)	do 2 godzin	5 Dni roboczych
2.	Usterka	do 2 godzin roboczych	do 5 Dni roboczych	do 8 godzin roboczych	21 Dni roboczych

Zastosowanie obejścia oznacza tymczasowe rozwiązanie w związku z wystąpieniem Błędu, które może być realizowane poprzez zmianę parametrów Systemu, rekomendację modyfikacji procesu przetwarzania danych. Wykonanie Obejścia w Czasie Naprawy powoduje dwukrotne przedłużenie Czasu Naprawy pierwotnie zgłoszonego Błędu. Zastosowanie Obejścia nie zwalnia Wykonawcy od obowiązku usunięcia Błędu poprzez dostarczenie poprawki, pakietu poprawek lub aktualizacji Systemu wraz ze zaktualizowaną Dokumentacją.

2) Wykonawca jest zobowiązany do prowadzenia pełnej i szczegółowej ewidencji zgłoszonych Błędów zawierającej co najmniej:
a) numer kolejny zgłoszenia w danym okresie rozliczeniowym;
b) datę wpisu;
c) datę wpływu do Wykonawcy pisemnego lub elektronicznego lub telefonicznego zgłoszenia;
d) numer zgłoszenia;
e) kategorię problemu;
f) datę zgłoszenia;
g) treść merytoryczną zgłoszenia;
h) datę rozwiązania zgłoszenia;
i) opis sposobu rozwiązania zgłoszenia;
j) ewentualne uwagi;

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

k) wskazanie Dokumentacji Systemu zaktualizowanej w związku z naprawą i przekazywania Zamawiającemu wersji elektronicznej ewidencji zgłoszonych Błędów w pierwszym Dniu Roboczym miesiąca kalendarzowego, następującego po zakończeniu miesiąca, którego dotyczy ewidencja zgłoszonych Błędów.

3) Zamawiający może zgłaszać Błędy w działaniu Systemu na specjalnie do tego celu udostępnionym portalu Wykonawcy albo za pomocą poczty elektronicznej na formularzu zgłoszenia opracowanym przez Wykonawcę i zaakceptowanym przez Zamawiającego albo telefonicznie. Zgłoszenie telefoniczne musi być potwierdzone w formie pisemnej lub pocztą elektroniczną przez osobę zgłaszającą Błąd po stronie Zamawiającego.
4) Przyjęcie Zgłoszenia przez Wykonawcę musi być potwierdzone w formie pisemnej lub elektronicznej (pocztą elektroniczną) nie później niż w terminie 1 dnia roboczego.
5) Zgłoszenia Usterek będą obsługiwane przez Wykonawcę w Dni Robocze.
6) W przypadku kontaktu serwisowego poprzez formularz elektroniczny udostępniony przez Wykonawcę za pomocą dedykowanego portalu zgłoszeniowego za ,,Zgłoszenie Błędu" oraz potwierdzenie naprawy można będzie uznać wpis potwierdzający poprawność wykonanych zmian, dokonany przez Zamawiającego na dedykowanym portalu zgłoszeniowym. Zamawiający otrzyma potwierdzenie poza systemem Wykonawcy, że jego zgłoszenie zostało przyjęte wraz z datą, godziną rejestracji oraz treścią tego zgłoszenia. Portal zgłoszeniowy Wykonawcy musi powiadamiać Zamawiającego o usunięciu Błędu.
7) Czas rozwiązania Zgłoszenia (naprawy Błędu) nie obowiązuje w przypadku błędu Oprogramowania lub innych problemów potwierdzonych analizą producenta, które musi rozwiązać sam producent.
8) Wykonawca po naprawie Błędu sprawdzi jej skuteczność i uzyska potwierdzenie od Zamawiającego.
9) Za moment rozwiązania zgłoszenia (naprawy Błędu) uznaje się datę przywrócenia pełnej wydajności i funkcjonalności Systemu.
10) W przypadku Błędu za moment rozwiązania Zgłoszenia (naprawy Błędu) uznaje się także przywrócenie funkcjonalności Systemu poprzez zastosowanie rozwiązania zastępczego (obejścia) do czasu usunięcia Błędu w terminie uzgodnionym z Zamawiającym, ale nie dłużej niż w terminie wskazanym w Tabeli powyżej.
11) Zamawiający dopuszcza możliwość przedłużenia Czasu Naprawy Błędu przez Wykonawcę na mocy dwustronnego porozumienia, o ile usunięcie Błędu w terminach określonych powyżej jest niemożliwe z przyczyn niezależnych od Wykonawcy.
12) Wykonawca zobowiązuje się do świadczenia Usług Gwarancji w sposób zapobiegający utracie danych Zamawiającego, w tym także tych, do których będzie miał dostęp w trakcie wykonywania usług. W przypadku gdy wykonanie danej czynności przez Wykonawcę lub przez Zamawiającego w oparciu o rekomendację Wykonawcy wiąże się z ryzykiem utraty danych, Wykonawca zobowiązany jest poinformować o tym Zamawiającego przed przystąpieniem do wykonania takiej czynności lub z chwilą przekazania takiej rekomendacji Zamawiającemu.

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

3.3. Aktualizacja Systemu

1) Realizacja usługi będzie polegała na aktualizowaniu Systemu przez Wykonawcę w związku z wprowadzeniem przez Producenta aktualizacji lub nowej wersji Systemu (w ramach licencji objętych Przedmiotem zamówienia).
2) W przypadku wprowadzenia zmian w Systemie przez Wykonawcę na wniosek Zamawiającego, Wykonawca zobowiązany jest do powiązania tych zmian z tymi funkcjonalnościami Systemu, na które ta zmiana ma wpływ.
3) Prace, o których mowa powyżej będą realizowane przez Wykonawcę w terminie 7 dni liczonych od dnia ich zgłoszenia Wykonawcy przez Zamawiającego.
4) Wykonawca zobowiązany jest w terminie 30 dni od każdej aktualizacji powodującej zmianę konfiguracji Systemu przedstawić Zamawiającemu oświadczenie, że System spełnia wymagania dotyczące bezpieczeństwa, tj. zachowania poufności, integralności, dostępności, rozliczalności, niezaprzeczalności, przetwarzania informacji przetwarzanych danych.
5) Wykonawca jest zobowiązany do prowadzenia pełnej i szczegółowej ewidencji przeprowadzonych aktualizacji (zmiany w Dokumentacji mogą być dostarczane w postaci suplementu w wersji elektronicznej z zastrzeżeniem, że w przypadku wdrożenia kolejnej wersji oprogramowania zmiany te zostaną zamieszczone w kompletnej Dokumentacji) zawierającej co najmniej:
   a) numer kolejny/nr wersji;
   b) oznaczenie, czy jest to aktualizacja Systemu wynikająca ze zamiany przepisów prawa;
   c) nazwa modułu, którego dotyczy aktualizacja;
   d) wskazanie Dokumentacji Systemu zaktualizowanej w związku z aktualizacją;
   e) imiona i nazwiska osób ze strony Wykonawcy, z którymi można się kontaktować w celu omówienia szczegółów związanych z wprowadzoną aktualizacją.
6) Zakres Aktualizacji powinien zapewnić osiągnięcie pełnych funkcjonalności dostępnych we wszystkich obszarach Systemu, a w szczególności umożliwiać współpracę z innymi modułami oraz innymi systemami.

3.4. Okresowe przeglądy Systemu

W ramach realizacji usług Gwarancji, Wykonawca będzie świadczył okresowe przeglądy Systemu, nie rzadziej niż co 3 miesiące, polegające na:

1) Przeglądzie poprawek dla eksploatowanych środowisk wykorzystujących System.
2) Ocenie konieczności zastosowania poprawek rekomendowanych przez producenta oprogramowania w eksploatowanych środowiskach oraz ich wdrożenie.
3) Doradztwie architektonicznym w zakresie zgodności sposobu wykorzystywania Oprogramowania z najlepszymi praktykami rekomendowanymi przez dostawcę oraz zgodności z warunkami Umowy.
4) Informowaniu Zamawiającego o przyczynach i sposobach rozwiązywania problemów związanych z nieprawidłowym działaniem Systemu.
5) Doradztwie technicznym, przekazywaniu na bieżąco informacji o nowych funkcjonalnościach możliwych do zaimplementowania w Systemie.

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

6) Założeniu zgłoszenia serwisowego w serwisie pomocy technicznej producenta, w przypadku wad i błędów Oprogramowania składającego się na System, przekazanie zgłoszenia serwisowego do producenta oprogramowania oraz prowadzenie zgłoszenia w imieniu Zamawiającego.
7) Wsparciu w konfiguracji i optymalizacji Systemu.
8) Wsparciu w zakresie integracji kolejnych serwerów bazodanowych do Systemu.
9) Instruktażu uwzględniającym nowe funkcjonalności po aktualizacji Systemu, aktualizacja dokumentacji technicznej Systemu.

3.5. Wsparcie producenta Oprogramowania

W ramach realizacji umowy, Wykonawca zapewni wsparcie producenta Oprogramowania, rozumiane jako:

1) Wsparcie świadczone w trybie: 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku, bez ograniczenia liczby zgłoszeń;
2) Prawo do aktualizacji oprogramowania do najnowszej wersji wszelkich poprawek, w tym związanych z bezpieczeństwem;
3) Dostęp do portalu pomocy technicznej producenta oprogramowania przez 24 godziny na dobę w celu:
   a) przeglądania i składania informacji o problemach dotyczących przedmiotu zamówienia;
   b) informacji o nowych produktach;
   c) dostępu do bazy wiedzy do oprogramowania będącego przedmiotem zamówienia;
   d) informacji o dostępnych poprawkach do oprogramowania.
4) Wysyłanie zgłoszeń serwisowych do producenta oprogramowania z poziomu portalu Użytkownika, służącego również do zarządzania kluczami licencyjnymi oraz potwierdzenia poziomu posiadanego wsparcia u producenta przez Zamawiającego w ramach niniejszego zamówienia.

4. Zakres opcjonalny

Zamawiający przewiduje możliwość udzielenia zamówienia opcjonalnego w zakresie:

4.1. Zlecenia Usług Rozwoju

1) W ramach Usług Rozwoju Zamawiający ma prawo zlecać Wykonawcy prace rozwojowe obejmujące wizyty Konsultanta oraz prace programistyczne w okresie Gwarancji w celu realizacji ewentualnych dodatkowych prac dostosowujących System do potrzeb Użytkowników, wykonywania drobnych zmian, konfiguracji Systemu oraz dodatkowych Instruktaży.
2) Łączna liczba godzin przeznaczona na prace w ramach Usługi Rozwoju nie może przekroczyć 300 roboczogodzin.

4.2. Dostawy Licencji na External DNS

1) W terminie 60 dni kalendarzowych od dnia podpisania Umowy Zamawiający ma prawo zlecić zakup i wdrożenie licencji, o których mowa w pkt. 10.1.3 Serwer DNS External Załącznika nr 1

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

do OPZ „Wymagania funkcjonalne i jakościowe Systemu ochrony DNS", w liczbie 2 szt. W przypadku podjęcia tej decyzji w terminie 10 dni kalendarzowych Wykonawca ma obowiązek uwzględnić ten element w ramach Analizy wdrożeniowej oraz objąć wdrożeniem.

Zamówienie opcjonalne nie stanowi zobowiązania Zamawiającego do jego udzielenia, jak również nie stanowi podstawy do dochodzenia przez Wykonawcę roszczeń odszkodowawczych z tytułu niezłożenia tego zamówienia.

IV. Wymagania szczegółowe w zakresie Systemu

1. Wymagania funkcjonalne oraz jakościowe

Szczegółowy zakres obszarów funkcjonalnych objętych zakresem wdrożenia Systemu zawarty został w **Załączniku nr 1 do OPZ – Wymagania funkcjonalne i jakościowe Systemu ochrony DNS.**

2. Wymagania pozafunkcjonalne

2.1. Bezpieczeństwo

2.1.1. Wymagania ogólne

1) Oferowane rozwiązanie musi być jednolite (tj. pochodzić od jednego producenta) i kompleksowe z elastyczną możliwością skalowania w kontekście potencjalnej rozbudowy tj. rozszerzenia zakresu obejmującego chroniony obszar oraz objęcia ochroną kolejnych Użytkowników.
2) Zamawiający wymaga, aby zarządzanie całością Systemu i usługi bezpiecznego DNS, możliwe było z wykorzystaniem jednej konsoli zarządzającej.
3) Wykonawca musi zagwarantować bezpieczeństwo danych znajdujących się w Systemie. W Projekcie Systemu opracowanym przez Wykonawcę musi znajdować się dokładny opis proponowanych rozwiązań w zakresie bezpieczeństwa Systemu oraz projekt konfiguracji infrastruktury Systemu i sposób jej zabezpieczenia.
4) System musi spełniać wymogi krajowych i unijnych przepisów prawa dotyczących bezpieczeństwa informacji, w szczególności z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
5) System musi wykorzystywać szyfrowanie przy komunikacji pomiędzy wszystkimi komponentami. Szyfrowanie musi być zrealizowane w oparciu o rozwiązania zapewniające poziom bezpieczeństwa co najmniej równy temu jaki zapewniają protokoły SSL/TLS lub VPN.
6) Minimalnym akceptowalnym algorytmem asymetrycznym jest RSA 2048.
7) Minimalnym akceptowalnym algorytmem symetrycznym jest AES 128.
8) Minimalnym akceptowalnym standardem funkcji skrótu jest SHA-2.
9) System musi być zgodny ze standardem bezpieczeństwa aplikacji OWASP ASVS poziom 2 (aktualne wydanie), co Wykonawca potwierdzi przedstawiając raport z testów bezpieczeństwa przeprowadzony przez niezależną od Wykonawcy firmę zajmującą się usługami bezpieczeństwa. Raport musi zawierać listę kontrolną stworzoną na bazie OWASP ASVS.

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

10) System musi w odpowiedni sposób weryfikować błędy tak, aby Użytkownikowi nie była prezentowana informacja o Błędzie, zawierająca szczegóły techniczne wystąpienia tego Błędu, ujawniające zastosowane oprogramowanie i jego konfigurację. Powinien być generowany standardowy, niezmienny komunikat o Błędzie.
11) System nie może udostępniać poprzez aplikację/usługę plików/katalogów związanych z konfiguracją czy administrowaniem daną usługą.
12) System musi w odpowiedni sposób weryfikować zawartość pól/formularzy aplikacji pod kątem wprowadzanych znaków (zastosowanej walidacji oraz kontroli poprawności składni zapytań), w celu zabezpieczenia przed atakami typu SQL Injection, Cross Site Scripting itd.
13) W przypadku technologii WEB, konfiguracja serwera webowego musi wymuszać ustawienie parametru httpOnly w cookies wysyłanych do Użytkownika.
14) System powinien mieć możliwość ograniczenia korzystania tylko do jednej sesji jednocześnie dla danego Użytkownika, chyba że używanie jednocześnie kilku lub więcej sesji dla danego pojedynczego Użytkownika jest niezbędne w celu wykonania przypisanych mu zadań.
15) System musi blokować jednoczesny dostęp do modyfikacji tych samych danych przez dwóch lub więcej Użytkowników w celu zabezpieczenia przed ewentualnym nadpisaniem.
16) System musi posiadać wbudowany mechanizm zakończenia sesji po zamknięciu przeglądarki lub aplikacji (w celu uniemożliwienia powrotu do sesji poprzez naciśnięcie przycisku „wstecz" bez ponownego logowania).
17) System musi posiadać mechanizm powodujący zakończenie lub zablokowanie sesji w przypadku nieaktywności Użytkownika przekraczającej 15 minut (parametr konfigurowalny). W przypadku sesji Administratora, zamykanie lub blokowanie sesji musi następować po 3 minutach nieaktywności (parametr konfigurowalny).
18) Wykonawca jest zobowiązany w ramach Gwarancji, aby wszystkie elementy Systemu, system operacyjny, system baz danych, jak i aplikacje posiadały zainstalowane aktualne, stabilne dostępne poprawki bezpieczeństwa.
19) W przypadku wykorzystywania komponentów innych dostawców, System może wykorzystywać wyłącznie komponenty, które posiadają wsparcie producenta danego komponentu np. systemów operacyjnych, bibliotek programowych itd. Wykorzystanie takich komponentów musi być w pełni udokumentowane, aby było można je objąć monitorowaniem pod względem znanych podatności.
20) System musi być zbudowany z modułów/obszarów, tak aby była możliwość rozdzielenia jego składowych pomiędzy różne strefy VLAN jak DMZ, baza danych, aplikacja.
21) System musi mieć zsynchronizowany czas w oparciu o konfigurowalny wzorzec czasu Centrum E-Zdrowia – serwer NTP.

2.1.2. Logowanie zdarzeń

1) System musi tworzyć i utrzymywać log Systemu, rejestrujący historię logowania do Systemu wszystkich Użytkowników oraz wykonane przez nich czynności odczytu (w tym wydruku), wprowadzania, modyfikacji i usuwania danych. Zakres danych, które powinny podlegać takiemu audytowi/logowaniu zostanie określony na etapie analizy przedwdrożeniowej. Ze względu na szczególny charakter przetwarzanych danych tj. "danych wrażliwych"

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

w rozumieniu RODO, muszą zostać spełnione wszystkie wymagania wynikające z przedmiotowego rozporządzenia, jak i innych aktów wykonawczych.

2) W przypadku każdej (zarówno udanej, jak i nieudanej) próby uwierzytelnienia i wylogowania z Systemu, musi on rejestrować następujące informacje: czas wykonania próby uwierzytelnienia z dokładnością do 1 sekundy, wprowadzony identyfikator Użytkownika, adres IP komputera, z którego wykonano próbę uwierzytelniania, rezultat procedury uwierzytelniania oraz autoryzacji (przyznanie lub odmowa dostępu z informacją o przyczynie odrzucenia).
3) System musi posiadać log aktywności dla Użytkowników z uprawnieniami administracyjnymi rejestrując każdą akcję wykonaną przez Administratora.
4) System musi zapewniać bezpieczny mechanizm przechowywania logów Błędów Systemu.
5) System musi zapewniać bezpieczny mechanizm przechowywania logów audytowych (w oddzielnym środowisku i niedostępny do modyfikacji).
6) System powinien umożliwiać audyt systemowy – udokumentowanie historii czynności związanych z zasobami i dostępów do zasobów, tj. monitorowanie nieautoryzowanego dostępu. Włączona klasa ochrony C2 [TCSEC] (śledzenie dostępu, identyfikacja Użytkownika, kontrola dystrybucji uprawnień).
7) Dane związane z rozliczalnością (logi Systemu) powinny być przechowywane w innej bazie danych niż dane wykorzystywane w poszczególnych modułach Systemu. Zamawiający dopuszcza możliwość przechowywania danych niezbędnych do rozliczalności w tej samej fizycznej bazie danych pod warunkiem, że będzie istniała możliwość archiwizowania danych związanych z rozliczalnością w oddzielnej bazie danych po upływie ustalonego okresu np.: miesiąca. W skład informacji na temat działania Użytkownika musi wchodzić minimum: nazwa Użytkownika (login); data i godzina zdarzenia (YYYY-MM-DD HH:MM:SS); nazwa stacji i adres IP z którego nastąpiło logowanie; opis wykonywanej czynności; formularze, na których dokonano czynności.
8) System musi zapewniać możliwość eksportu danych, o których mowa w poprzednim punkcie, w formatach zgodnych z Rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r**.** w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 773).
9) System musi zapewniać współpracę poprzez interfejsy z systemami klasy SIEM w zakresie wysyłania logów.

2.2. Wydajność i skalowalność Systemu

1) Jednym z podstawowych wymagań jest skalowalność rozumiana jako możliwość efektywnej pracy przy zwiększeniu liczby i wielkości przetwarzanych zgłoszeń, oraz liczby jednocześnie pracujących Użytkowników.
2) W zależności od rodzaju Systemu i sposobu jego skonfigurowania skalowalność powinna być realizowana w każdej z warstw Systemu w zależności od tego, jaki element Systemu jest najbardziej obciążony. System powinien być skalowalny zarówno w warstwie prezentacji, warstwie aplikacyjnej i warstwie bazodanowej. Skalowalność polega na możliwości dodania zasobów sprzętowych (serwer, RAM, powierzchnia dyskowa) w każdej z warstw Systemu.

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

Zwiększanie wydajności (skalowanie) powinno być możliwe bez modyfikacji logiki Systemu. Skalowalność nie może polegać na wymianie zasobów sprzętowych na bardziej wydajne, ale na możliwości wykorzystania dodawanych zasobów.

2.3. Niezawodność i dostępność

1) System musi działać w trybie ciągłym. Aktualizacje i inne czynności techniczne, w tym czynności pielęgnacyjne (np. kopie zapasowe), które wpływają na ciągłość pracy, muszą być wykonywane poza godzinami pracy Zamawiającego (od 18:00 do 7:00 dnia następnego).
2) System musi działać z dostępnością (rozumianą jako czas działania usług Systemu bez Błędów w stosunku do całości czasu w danym okresie, z wyłączeniem uzgodnionych przerw serwisowych oraz niedostępności Infrastruktury będącej w utrzymaniu Zamawiającego) wynoszącą minimum 98,00% w skali miesiąca.

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

Wymagania funkcjonalne i jakościowe Systemu ochrony DNS

1. **Wymagania Ogólne**

1.1 Usługa Bezpieczny DNS (dalej zwana Usługą) musi udostępniać funkcjonalność rekursywnego rozwiązywania zapytań DNS dla domen internetowych

1.2 Usługa musi przyjmować zapytania DNS:

1.2.1 Kierowane bezpośrednio na jej publiczny internetowy adres IP z możliwością ograniczenia zakresu akceptowalnych adresów źródłowych zapytań;

1.2.2 Kierowane bezpośrednio na dedykowany adres URL przy pomocy protokołu DNS-over-HTTPS;

1.2.3 Kierowane pośrednio poprzez wirtualny serwer DNS forwarding proxy możliwy do zaimplementowania w sieci wew. Zamawiającego jako maszyna wirtualna uruchamiana na platformach Vmware oraz Microsoft Hyper-V:

1.2.3.1 Proxy musi dodawać do zapytań DNS informację o wewnętrznym prywatnym adresie IP hosta oraz adresie IP hosta;

1.2.3.2 Proxy musi przesyłać zapytania DNS do Usługi w sposób zaszyfrowany poprzez protokół DNS-over-TLS lub DNS-over-HTTPS;

1.2.4 Poprzez oprogramowanie Agenta DNS (wymaganie nieobowiązkowe, dodatkowo punktowane) dostarczone wraz z usługą i uruchomione na stanowiskach roboczych pracowników Zamawiającego:

1.2.4.1 Agent musi wspierać systemy operacyjne MS Windows 10, 11 oraz MacOS w wersjach Sonoma, Ventura, Monterey i BigSur, Linux Ubuntu 22, RedHat 8, Android 11 +, iPhone IOS 14+, iPad IOS 14+, i nowsze;

1.2.4.2 Agent musi dodawać do zapytań DNS informacje o nazwie stanowiska roboczego, adresie MAC stanowiska roboczego, nazwę zalogowanego Użytkownika i wersję systemu operacyjnego;

1.2.4.3 Agent musi przesyłać zapytania DNS do usługi bezpieczny DNS w sposób zaszyfrowany poprzez protokół DNS-over-TLS lub DNS-over-HTTPS;

1.2.4.4 Agent musi wspierać możliwość instalacji w środowisku Microsoft Active Directory przy wykorzystaniu mechanizmu GPO oraz w środowisku Apple z wykorzystaniem Apple Remote Desktop, a w przypadku urządzeń Android/iPhone/iPad przy pomocy systemu klasy Mobile Device Management, jak i bez takiego systemu;

1.2.4.5 Agent DNS na stacjach roboczych:

1.2.4.5.1 Zakres wdrożenia dotyczący Agenta DNS ma zastosowanie jedynie w sytuacji, gdy System ma możliwość objęcia ochroną stacji roboczych poprzez zainstalowanie Agenta DNS.

1.2.4.5.2 Jeżeli dostarczane rozwiązanie posiada funkcjonalność ochrony stacji roboczych,

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

z wykorzystaniem Agenta DNS, to w trakcie Etapu I Analiza wdrożeniowa Wykonawca ma obowiązek wykonania analizy, uwzględniającej konieczność objęcia ochroną stacji roboczych z wykorzystaniem Agenta DNS.

1.2.4.5.3 W ramach ochrony przewiduje się wykorzystanie licencji na potrzeby zabezpieczenia 600 stacji roboczych.

1.2.4.5.4 W ramach wdrożenia wymaga się instalacji nie mniej niż 30 Agentów DNS na stacjach roboczych.

2. Polityka bezpieczeństwa

2.1 System musi mieć możliwość podejmowania działań w odniesieniu do zapytań i odpowiedzi DNS na podstawie zdefiniowanych przez Zamawiającego polityk bezpieczeństwa;

2.2 Możliwie działania powinny obejmować:

2.2.1 Zezwolenie na zapytanie,

2.2.2 Blokowanie zapytania przy pomocy odpowiedzi NXDomain (brak takiej domeny),

2.2.3 Przekierowanie:

2.2.3.1 Odpowiedzi ze zdefiniowanym przez Zamawiającego adresem IP,

2.2.3.2 Odpowiedź ze zdefiniowanym przez Zamawiającego adresem CNAME

2.2.3.3 Każda z tych akcji musi mieć możliwość odnotowania jej podjęcia w logach lub nieodnotowywania,

2.2.3.4 Przekierowanie powinno być również możliwe do strony internetowej udostępnionej przez dostawcę z możliwością jej personalizacji przez Zamawiającego;

2.3 System musi podjąć działania w oparciu o nazwę domeny w zapytaniu, nazwę domeny występującej jako CNAME dla nazwy zapytania i na podstawie adresu IP w odpowiedzi. Działanie na podstawie nazw domen powinno funkcjonować dla dowolnego typu zapytania – system nie może pozwolić na ominięcie blokowania domeny przez wysłanie określonych typów zapytań ja SOA, MX lub NS;

2.4 System musi umożliwiać Zamawiającemu zdefiniowanie własnej listy domen / adresów IP, na podstawie których ma podejmować reakcję, a także musi dostarczać listę domen i adresów IP w postaci listy zagrożeń określonych dalej. W przypadku list własnych Zamawiającego, System musi mieć możliwość zdefiniowania poziomu zagrożenia i pewności informacji oddzielnie dla każdej listy. System musi umożliwiać tworzenie i edycję własnych list manualnie z portalu klienta, automatycznie poprzez import z pliku CSV (zawierającego listę domen oraz pole z opisem każdej z domen) oraz poprzez interfejs API, aby umożliwiać łatwy import zewnętrznych danych o zagrożeniach. System musi umożliwiać utworzenie min. 50 list własnych, o łącznej pojemności min. 400.000 rekordów;

2.5 Usługa musi mieć możliwość zdefiniowania listy domen wewnętrznych Zamawiającego, czyli takich dla których DNS lub oprogramowanie Agenta nie będzie przesyłać zapytań DNS do Usługi, ale zamiast tego prześle je do określonego wewnętrznego serwera DNS Zamawiającego;

3. Kody pomijania blokady

3.1 System musi umożliwiać obejście blokowania domeny/IP przy pomocy specjalnych kodów dostarczanych wybranym Użytkownikom;

3.2 Usługa musi umożliwiać wpisanie kodu na specjalnej stronie udostępnionej w ramach Usługi, na którą następuje przekierowanie zgodnie z konfiguracją polityki bezpieczeństwa;

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

3.3 Kody muszą mieć możliwość przypisania kategorii zagrożeń lub kategorii treści, których obejście umożliwiają;

4. DNSSEC

4.1 Usługa musi wspierać walidację DNSSEC;

5. Listy zagrożeń

5.1 Usługa musi zapewnić dostęp do danych o zagrożeniach cyberbezpieczeństwa przez okres co najmniej 3 lat;

5.2 Dane o zagrożeniach dostarczone przez dostawcę muszą zawierać:

5.2.1 Lista domen internetowych związanych z atakami mailware, ransomware, APT, exploit kitami, złośliwymi serwerami DNS, domenami sinkhole;

5.2.2 Listę złośliwych oraz skompromitowanych adresów IP;

5.2.3 Listę domen, których złośliwość nie została jeszcze potwierdzona, ale są wysoce podejrzane i z dużym prawdopodobieństwem w przyszłości zostaną użyte do działalności przestępczej i w związku z tym dostawca danych o zagrożeniach zaleca blokowanie tych domen;

5.2.4 Listę domen, których złośliwość nie została jeszcze potwierdzona, ale są podejrzane i istnieje prawdopodobieństwo, że w przyszłości zostaną użyte do działalności przestępczej i w związku z tym dostawca danych o zagrożeniach zaleca blokowanie tych domen w większości przypadków;

5.2.5 Listę domen, których złośliwość nie została jeszcze potwierdzona, ale są w niewielkim stopniu podejrzane i potencjalnie mogą zostać użyte w przyszłości do działalności przestępczej i w związku z tym dostawca danych o zagrożeniach zaleca co najmniej logowanie zapytań do tych domen, a dla środowisk bardziej wrażliwych blokowanie tych domen;

5.2.6 Listę domen oferujących publiczne usługi DNS-over-HTTPS;

5.2.7 Listę domen zarejestrowanych i uaktywnionych w ciągu ostatnich 7 dni;

5.2.8 Listę nowo obserwowanych domen internetowych, tj. takich o które po raz pierwszy zapytano w Internecie w ciągu ostatnich 3 dni. Dane muszą pochodzić z systemu co najmniej 400 sensorów Passive DNS rozlokowanych na całym świecie. System Passive DNS musi zbierać dane od min. 10 lat.

5.3 Dane z pkt. 5.2.1-7 powinny pochodzić z działu znajdowania zagrożeń usługodawcy oferowanego w tym postępowaniu rozwiązania;

5.4 Listy zagrożeń muszą posiadać dane o zagrożeniach celujących w Polskę. Zamawiający zastrzega sobie możliwość dokonania weryfikacji tego faktu na podstawie listy CERT.PL (https://hole.cert.pl/domains/v2/domains.json) – co najmniej 70% domen z listy CERT.PL z ostatnich 14 dni musi znajdować się na listach z pkt. Błąd! Nie można odnaleźć źródła odwołania.-5;

5.5 Wszystkie powyższe listy zagrożeń muszą być możliwe do wykorzystania w konfiguracji polityki bezpieczeństwa Usługi.

5.6 Dane o zagrożeniach muszą również zawierać domeny lookalike, tj. domeny, których nazwa wygląda podobnie do najpopularniejszych domen w Internecie (np. Gooogle.com, g00gle.com itp.) i posiadają inne cechy typowe dla domen złośliwych. Zamawiający musi mieć możliwość zdefiniowania co najmniej 20 dowolnych domen, dla których algorytm dostawcy danych będzie regularnie wyszukiwał domen podobnych

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

do nich, a znalezione domeny lookalike będzie automatycznie dodawał do list z pkt. Błąd! Nie można odnaleźć źródła odwołania.-5

5.7 Usługa musi zawierać informacje o kategorii treści dla domen i musi być w stanie na nią reagować, musi zapewniać możliwość podejmowania działań co najmniej w przypadku domen hostujących pornografię, hazard, sieci społecznościowe, anonimizatory, reklamy.

5.8 Dane o zagrożeniach pochodzące od usługodawcy muszą być dostępne za pośrednictwem interfejsu API w formatach CSV, JSON, CEF, XML, STIX do użytku w innych systemach bezpieczeństwa, takich jak SIEM, SOAR, firewall lub SWG.

5.9 Należy dostarczyć licencje, które gwarantują dostęp do danych o zagrożeniach dla instytucji liczącej 600 pracowników. Dostęp do danych nie może być ograniczony ze względu na liczbę serwerów DNS lub innych systemów bezpieczeństwa korzystających z tych danych.

6. Wykrywanie zagrożeń na bazie analizy zapytań DNS

6.1 Usługa musi posiadać funkcję wykrywania i blokowania tunelowania DNS za pomocą silnika analitycznego opartego na uczeniu maszynowym i umożliwiającego wykrywania nieznanych wzorców tunelowania i eksfiltracji danych przez DNS. System nie może działać wyłącznie w oparciu o sygnatury dla ruchu DNS znanych narzędzi tunelujących.

System musi analizować co najmniej 6 atrybutów każdego zapytania DNS, które musza obejmować:

6.1.1 Entropię znaków;

6.1.2 Popularność występowania w językach naturalnych n-gramów z nazwy DNS;

6.1.3 Rozmiar zapytania;

6.1.4 Częstotliwość zapytań DNS;

6.1.5 Różnorodność adresów IP w odpowiedziach;

6.1.6 Różnorodność systemów ASN do których te adresy IP należą;

6.2 Usługa musi wykrywać tunelowanie DNS niezależnie od kategorii treści domeny użytej w zapytaniach DNS;

6.3 Usługa musi posiadać funkcję analizy odpowiedzi i wykrywania infiltracji przez DNS, w szczególności musi wykrywać technikę wykorzystywaną przez złośliwe oprogramowanie Powersouce / DNS Messenger, to znaczy musi blokować próby przesyłania danych zakodowanych w odpowiedziach DNS w ramach rekordów TXT;

6.4 Usługa musi mieć funkcję wykrywania w ruchu DNS Zamawiającego odpytań o domeny, o które nigdy wcześniej nie było zapytań DNS wychodzących z sieci Zamawiającego, a których nie ma jeszcze na listach świeżych domen i ich blokowania w czasie nie przekraczającym 5 minut, na okres 48 godzin

7. Wymagania dot. portalu dla klientów

7.1 W ramach portalu dla klientów dostawca musi zapewnić możliwość analizy reputacji domen, adresów IP, adresów URL. Narzędzie analityczne musi bezpośrednio wyświetlać informacje o domenie / adresie IP co najmniej z bazy danych o zagrożeniach opisanej w pkt. Błąd! Nie można odnaleźć źródła odwołania., z usługi pasywnego DNS, whois, rankingu popularności domen.

7.2 W ramach Usługi Zamawiający musi mieć możliwość wykonania co najmniej 2 000 zapytań dotyczących domeny / adresu IP w ramach zapewnianego dostępu rocznie.

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

Dostęp do narzędzia analizy będzie możliwy za pośrednictwem przeglądarki internetowej, a także poprzez interfejs API z danymi udostępnionymi w formacie JSON (do ich wykorzystania np. w narzędziach klasy SIEM).

8. Wymagania dot. portalu Usługi

8.1 Portal Usługi musi zapewniać funkcje raportowania. Raporty powinny zawierać:

8.1.1 Raporty aktywności pokazujące zapytania DNS wysyłane do Usługi;

8.1.2 Raporty bezpieczeństwa pokazujące zapytania DNS, dla których Usługa podjęła akcje zgodnie z polityką bezpieczeństwa;

8.1.3 Raporty bezpieczeństwa muszą posiadać możliwość filtrowania w oparciu o:

8.1.3.1 Źródło zapytania;

8.1.3.2 Adres oryginalnego źródła zapytania;

8.1.3.3 Adres MAC oryginalnego źródła zapytania;

8.1.3.4 Domena w zapytaniu;

8.1.3.5 Rodzaj w zapytaniu;

8.1.3.6 Odpowiedź;

8.1.3.7 Klasa zagrożenia (np. Malware);

8.1.3.8 Rodzaj zagrożenia (np. Malware C2);

8.1.3.9 Poziom zagrożenia;

8.1.3.10 Poziom zaufania do danych;

8.1.3.11 Nazwa użytkownika;

8.1.3.12 Podjęta akcja;

8.1.3.13 Lista zagrożeń;

8.1.3.14 Polityka bezpieczeństwa

8.1.3.15 Musi być również możliwość filtrowania w oparciu o kombinację powyższych atrybutów;

8.1.4 Raporty muszą mieć możliwość grupowania zdarzeń per Użytkownik, źródło zapytań (serwery DNS, Agent, sieć IP), oryginalne źródło zapytania (prywatny adres IP z sieci LAN lub nazwa komputera z oprogramowaniem Agenta);

8.1.5 Dla każdego zapytania DNS w raporcie bezpieczeństwa Usługa musi pobierać i wyświetlać informację o kliencie DNS przechowywaną w bazie adresacji IP. Pobierane informacje muszą uwzględniać prywatny adres IP, adres MAC oraz nazwę urządzenia inicjującego zapytanie DNS, DHCP fingerprint systemu operacyjnego oraz nazwę Użytkownika.

9. Wymagania pozostałe

9.1 Usługa musi mieć funkcjonalność przesyłania wszystkich zapytań DNS i zdarzeń bezpieczeństwa w postaci komunikatów syslog do systemu SIEM znajdującego się w sieci Zamawiającego. Dane te muszą być przesyłane w formacie syslog, CEF, LEEF i Splunk CIM;

9.2 Dostęp do portalu klienta musi opierać się na określonych prawach dostępu, takich jak dostęp tylko do odczytu lub dostęp administracyjny. Zmiany w konfiguracji usługi DNS muszą być rejestrowane w dzienniku dostępnym dla Zamawiającego. Dostęp do portalu musi mieć możliwość ograniczenia adresów IP z jakich może się do niego łączyć określona grupa administratorów;

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

9.3 Usługa musi być świadczona na bazie licencji obejmującej również wsparcie Usługodawcy i ważnej co najmniej przez okres 3 lat;

10. Architektura Systemu

10.1 System musi składać się z poniższych komponentów obsługiwanych przez wirtualne maszyny VMware:

10.1.1 Serwer DNS Internal – szt. 2

10.1.1.1 Funkcjonalność serwera:

10.1.1.1.1 Obsługa minimum 55 000 zapytań DNS na sekundę.

10.1.1.1.2 Pojemność bazy systemu DNS/IP na minimum 400000 rekordów;

10.1.1.1.3 Serwer musi dostarczać na bieżąco informacje o przyznawaniu adresów IP i urządzeniach, którym dany adres został przypisany (adres MAC, czas i data przyznania adresu, IP);

10.1.1.1.4 Serwer musi dostarczać usługę zarządzania adresami IP – IPAM (IP Address Management);

10.1.1.1.5 Serwer musi zarządzać adresami IPv4 i IPv6 pozwalając na graficzną (mapy sieci) oraz obiektową metodę zarządzania adresacją;

10.1.1.1.6 Serwer musi pozwalać na integrację z usługami VMware vCenter oraz OpenStack; w celu wykonywania procesu odnajdowania maszyn wirtualnych pracujących na infrastrukturze VMware/OpenStack oraz tworzenia rekordów DNS dla tych maszyn;

10.1.1.1.7 W przypadku kasowania maszyny wirtualnej system musi automatycznie usuwać powiązany rekord DNS;

10.1.1.1.8 System musi mieć posiadać możliwość generowania raportów z historii przydziałów adresów IP i rekord DNS dla maszyn wirtualnych do wykorzystania w audytach bezpieczeństwa;

10.1.1.1.9 Serwer musi posiadać mechanizmy kontroli wprowadzania danych (poprawność adresów IP, masek itp.);

10.1.1.1.10 Serwer musi umożliwiać dodawanie opisów i atrybutów dla obiektów sieci, adresów IP, domen. Atrybuty te muszą umożliwiać definicję typu i rozmiar danego atrybutu. Musi być możliwość stosowania słowników atrybutów z wymuszenie lub proponowaniem danego typu atrybutu dla danego typu obiektu. Serwer musi umożliwiać dziedziczenie atrybutów w ramach struktury sieci i podsieci;

10.1.1.1.11 Serwer musi mieć możliwość rozbudowy o mechanizm skanowania sieci i hostów/adresów IP (ang. network discovery). Mechanizm ten musi działać w trybie na żądanie oraz musi pozwalać na planowane powtarzalne rozpoznawania w przyszłości;

10.1.1.1.12 Serwer musi posiadać mechanizmy typu „znajdź 10 nieużywanych adresów z sieci X" oraz „znajdź 10 nieużywanych podsieci rozmiaru np. /24 w podsieci np. a.b.c.d/16". Funkcja musi być dostępna dla IPv4 i IPv6;

10.1.1.1.13 Serwer musi umożliwiać import danych w formacie CSV bezpośrednio z GUI i posiadać szczegółową dokumentację formatu danych importowanych;

10.1.1.1.14 Producent rozwiązania musi udostępniać bezpłatnie narzędzie do importu danych

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

z innych systemów DNS: Bind oraz Microsoft;

10.1.1.1.15 Serwer musi umożliwiać rozbudowę w przyszłości o zarządzanie usługami DNS na wielu serwerach Microsoft Windows bez potrzeby instalowania oprogramowania po stronie serwerów MS Windows; Wymagane jest wsparcie dla:

- Microsoft Windows 2012 Standard i DataCenter Initial Release 64 bits
- Microsoft Windows 2016 Standard i DataCenter Initial Release 64 bits
- Microsoft Windows 2019 Standard i DataCenter Initial Release 64 bits
- Microsoft Windows 2022 Standard i DataCenter Initial Release 64 bits

10.1.1.1.16 Serwer musi wspierać integrację co najmniej z systemami bezpieczeństwa SIEM, Cisco ISE, Tenable Security Center, Rapid7, Qualys, FireEye NX, McAfee OpenDXL oraz posiadać otwarty interfejs Rest API do komunikacji z innymi systemami;

10.1.1.1.17 Serwer musi dostarczać usługi rozwiązywania nazw domenowych przy użyciu protokołu DNS (Domain Name System);

10.1.1.1.18 Obsługa minimum 80 000 zapytań DNS na sekundę;

10.1.1.1.19 Serwer musi być zgodny z wymogami dokumentów RFC 1034, 1035, 1995, 1996, 2136, 2317, 2671, 2782, 3596 (RFC, tj. Request for Comments http://www.ietf.org/rfc.html);

10.1.1.1.20 Serwer musi realizować funkcje automatycznej aktualizacji serwisów DNS, zgodne z dokumentem RFC 2136;

10.1.1.1.21 Serwer musi posiadać wbudowany mechanizm powiadamiania o zmianach stref, zgodne z dokumentem RFC 1996;

10.1.1.1.22 Serwer musi wspierać protokoły DNS w wersji IPv4 i IPv6;

10.1.1.1.23 Serwer musi wspierać usługę DNS Anycast dla IPv4 i IPv6 (za pomocą protokołów BGP i OSPF);

10.1.1.1.24 Serwer musi wspierać usługę DNSSEC z automatycznym aktualizowaniem podpisów przy zmianach dokonywanych w strefach DNS;

10.1.1.1.25 Serwer musi wspierać rozbudowę o usługę DNS dla usług Active Directory;

10.1.1.1.26 Serwer musi wspierać usługę DDNS;

10.1.1.1.27 Serwer musi wspierać bezpieczną aktualizację rekordów DNS tzw. Secure Update, ze wsparciem dla protokołu GSS-TSIG;

10.1.1.1.28 Serwer musi wspierać obsługę MultiMaster DNS;

10.1.1.1.29 Serwer musi obsługiwać mechanizm IDN (Internationalized Domain Names) – (w tym polskie znaki) i posiadać wbudowany konwerter tzw. Punycode;

10.1.1.1.30 Serwer musi mieć funkcjonalność DNS Firewall opartą o polityki bezpieczeństwa realizowane na bazie stref Response Policy Zone (RPZ);

10.1.1.1.31 Serwer musi być przystosowane do obsługi stref RPZ o łącznym rozmiarze nie mniejszym niż 20 mln rekordów;

10.1.1.1.32 Serwer musi posiadać funkcjonalność wykrywania i blokowania tunelowania w DNS (DNS tunneling) za pomocą silnika analitycznego bazującego na uczeniu maszynowym i pozwalającego na wykrycie nieznanych jeszcze wzorców tunelowania i wycieku danych przez protokół DNS. W tym celu urządzenie dla nazw FQDN w zapytaniach DNS (w tym dla zapytań o rekordy A) musi co najmniej:

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

- wyliczać entropię znaków;
- sprawdzać popularność występowania w językach naturalnych wszystkich 2- i 3-znaków;
- obliczać współczynnik liczby samogłosek do wszystkich znaków w nazwie;
- obliczać współczynnik liczby cyfr do wszystkich znaków w nazwie;
- analizować rozmiar zapytania;
- analizować częstotliwość;

10.1.1.2 Zarządzanie i konfiguracja:

10.1.1.2.1 Serwer musi działać pod kontrolą systemu operacyjnego, przeznaczonego do realizacji funkcjonalności określonych w OPZ. Nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia;

10.1.1.2.2 Zarządzanie Systemem musi odbywać się z jednego miejsca (IP) za pomocą jednolitego systemu graficznego;

10.1.1.2.3 Serwer musi posiadać mechanizm Workflow do zarządzania procesem potwierdzania i akceptacji zmian;

10.1.1.2.4 Zarządzanie systemem musi się odbywać przez przeglądarkę WWW bez potrzeby instalacji specjalnego oprogramowania typu agent, klient itp.;

10.1.1.2.5 Serwer musi dostarczać mechanizm REST API do kontroli systemu, wykonywania i automatyzacji zadań wykonywanych za pomocą GUI. Musi być dostarczona pełna dokumentacja systemu API z przykładami zastosowania itp.;

10.1.1.2.6 Serwer musi pracować jako platforma dystrybucji plików za pomocą protokołów TFTP, FTP, HTTP, oraz oferować usługi synchronizacji czasu za pomocą protokołu NTP (Network Time Protocol);

10.1.1.2.7 Serwer musi posiadać funkcję budowy Systemu rozproszonego, która pozwoli na zbudowanie systemu rozproszonego z synchronizacją danych poprzez sieć IP z centralnym zarządzaniem całym systemem;

10.1.1.2.8 Serwer musi dostarczać informacje o wszystkich zmianach wprowadzanych przez administratorów (kto, kiedy, co zostało zmienione);

10.1.1.2.9 Serwer musi mieć możliwość wysyłania tych informacji do centralnego repozytorium za pomocą mechanizmu Syslog (TCP i UDP);

10.1.1.2.10 Serwer musi umożliwiać nadawanie administratorom praw opartych o grupy i role, co pozwala na ograniczenie ich dostępu do wymaganych zasobów. Granulacja uprawnień powinna umożliwiać konfigurowanie uprawnień dla pojedynczych obiektów typu sieć, strefa DNS, rekord DNS;

10.1.1.2.11 Serwer musi wpierać uwierzytelnianie Iżytkowników poprzez: lokalną bazę Użytkowników, protokół RADIUS, protokół TACACS+, SAML, LDAP, Microsoft Active Directory oraz sprzętowy moduł bezpieczeństwa (HSM): Entrust i Thales;

10.1.1.2.12 Serwer musi posiadać wbudowaną bazę danych. Baza danych nie może wymagać żadnych czynności administracyjnych związanych z jej konfiguracją i utrzymaniem;

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

10.1.1.2.13 Serwer musi mieć możliwość monitorowania parametrów urządzeń przy użyciu protokołu SNMP (Simple Network Management Protocol);

10.1.1.2.14 Dostęp do konsoli administracyjnej urządzeń Systemu powinien być możliwy poprzez:

- Interfejs zdalny dostępny poprzez protokół SSH, wsparcie dla wersji SSHv2;
- Interfejs znakowy – dostępny poprzez port szeregowy, zabezpieczony hasłem dostępu, które jest powiązane z Użytkownikiem;

10.1.1.2.15 Serwer musi umożliwiać wykonywanie planowanych kopii bezpieczeństwa do zewnętrznego serwera w celu uproszczenia procedur odzyskiwania w razie awarii (TFTP, FTP, SCP);

10.1.2 Serwer DNS Cache – szt. 2

10.1.2.1 Funkcjonalność urządzenia:

10.1.2.1.1 Obsługa minimum 55 000 zapytań DNS na sekundę.

10.1.2.1.2 Pojemność bazy systemu DNS/IP na minimum 400 000 rekordów;

10.1.2.1.3 Serwer musi dostarczać na bieżąco informacje o przyznawaniu adresów IP i urządzeniach, którym dany adres został przypisany (adres MAC, czas i data przyznania adresu, IP);

10.1.2.1.4 Serwer musi dostarczać usługę zarządzania adresami IP – IPAM (IP Address Management);

10.1.2.1.5 Serwer musi zarządzać adresami IPv4 i IPv6 pozwalając na graficzną (mapy sieci) oraz obiektową metodę zarządzania adresacją;

10.1.2.1.6 Serwer musi pozwalać na integrację z usługami VMware vCenter oraz OpenStack, w celu wykonywania procesu odnajdowania maszyn wirtualnych pracujących na infrastrukturze VMware/OpenStack oraz tworzenia rekordów DNS dla tych maszyn;

10.1.2.1.7 W przypadku kasowania maszyny wirtualnej system musi automatycznie usuwać powiązany rekord DNS;

10.1.2.1.8 System musi mieć posiadać możliwość generowania raportów z historii przydziałów adresów IP i rekord DNS dla maszyn wirtualnych do wykorzystania w audytach bezpieczeństwa;

10.1.2.1.9 Serwer musi posiadać mechanizmy kontroli wprowadzania danych (poprawność adresów IP, masek itp.);

10.1.2.1.10 Serwer musi umożliwiać dodawanie opisów i atrybutów dla obiektów sieci, adresów IP, domen. Atrybuty te muszą umożliwiać definicję typu i rozmiar danego atrybutu. Musi być możliwość stosowania słowników atrybutów z wymuszenie lub proponowaniem danego typu atrybutu dla danego typu obiektu. Urządzenie musi umożliwiać dziedziczenie atrybutów w ramach struktury sieci i podsieci;

10.1.2.1.11 Serwer musi mieć możliwość rozbudowy o mechanizm skanowania sieci i hostów/adresów IP (ang. network discovery). Mechanizm ten musi działać w trybie na żądanie oraz musi pozwalać na planowane powtarzalne rozpoznawania w przyszłości;

10.1.2.1.12 Serwer musi posiadać mechanizmy typu „znajdź 10 nieużywanych adresów

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

z sieci X" oraz „znajdź 10 nieużywanych podsieci rozmiaru np. /24 w podsieci np. a.b.c.d/16". Funkcja musi być dostępna dla IPv4 i IPv6;

10.1.2.1.13 Serwer musi umożliwiać import danych w formacie CSV bezpośrednio z GUI i posiadać szczegółową dokumentację formatu danych importowanych;

10.1.2.1.14 Producent rozwiązania musi udostępniać bezpłatnie narzędzie do importu danych
z innych systemów DNS: Bind oraz Microsoft;

10.1.2.1.15 Serwer musi umożliwiać rozbudowę w przyszłości o zarządzanie usługami DNS na wielu serwerach Microsoft Windows bez potrzeby instalowania oprogramowania po stronie serwerów MS Windows; Wymagane jest wsparcie dla:
- Microsoft Windows 2012 Standard i DataCenter Initial Release 64 bits;
- Microsoft Windows 2016 Standard i DataCenter Initial Release 64 bits;
- Microsoft Windows 2019 Standard i DataCenter Initial Release 64 bits;
- Microsoft Windows 2022 Standard i DataCenter Initial Release 64 bits;

10.1.2.1.16 Serwer musi wspierać integrację co najmniej z systemami bezpieczeństwa SIEM, Cisco ISE, Tenable Security Center, Rapid7, Qualys, FireEye NX, McAfee OpenDXL oraz posiadać otwarty interfejs Rest API do komunikacji z innymi systemami;

10.1.2.1.17 Serwer musi dostarczać usługi rozwiązywania nazw domenowych przy użyciu protokołu DNS (Domain Name System);

10.1.2.1.18 Obsługa minimum 70 000 zapytań DNS na sekundę;

10.1.2.1.19 Serwer musi być zgodny z wymogami dokumentów RFC 1034, 1035, 1995, 1996, 2136, 2317, 2671, 2782, 3596 (RFC, tj. Request for Comments http://www.ietf.org/rfc.html);

10.1.2.1.20 Serwer musi realizować funkcje automatycznej aktualizacji serwisów DNS, zgodne z dokumentem RFC 2136;

10.1.2.1.21 Serwer musi posiadać wbudowany mechanizm powiadamiania o zmianach stref, zgodne z dokumentem RFC 1996;

10.1.2.1.22 Serwer musi wspierać protokoły DNS w wersji IPv4 i IPv6;

10.1.2.1.23 Serwer musi wspierać usługę DNS Anycast dla IPv4 i IPv6 (za pomocą protokołów BGP i OSPF);

10.1.2.1.24 Serwer musi wspierać usługę DNSSEC z automatycznym aktualizowaniem podpisów przy zmianach dokonywanych w strefach DNS;

10.1.2.1.25 Serwer musi wspierać rozbudowę o usługę DNS dla usług Active Directory;

10.1.2.1.26 Serwer musi wspierać usługę DDNS;

10.1.2.1.27 Serwer musi wspierać bezpieczną aktualizację rekordów DNS tzw. Secure Update, ze wsparciem dla protokołu GSS-TSIG;

10.1.2.1.28 Serwer musi wspierać obsługę MultiMaster DNS;

10.1.2.1.29 Serwer musi obsługiwać mechanizm IDN (Internationalized Domain Names) – (w tym polskie znaki) i posiadać wbudowany konwerter tzw. Punycode;

10.1.2.1.30 Serwer musi mieć funkcjonalność DNS Firewall opartą o polityki bezpieczeństwa realizowane na bazie stref Response Policy Zone (RPZ);

10.1.2.1.31 Serwer musi posiadać funkcjonalność wykrywania i blokowania tunelowania

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

w DNS (DNS tunneling) za pomocą silnika analitycznego bazującego na uczeniu maszynowym i pozwalającego na wykrycie nieznanych jeszcze wzorców tunelowania
i wycieku danych przez protokół DNS. W tym celu urządzenie dla nazw FQDN
w zapytaniach DNS (w tym dla zapytań o rekordy A) musi co najmniej:
- wyliczać entropię znaków;
- sprawdzać popularność występowania w językach naturalnych wszystkich 2- i 3-znaków;
- obliczać współczynnik liczby samogłosek do wszystkich znaków w nazwie;
- obliczać współczynnik liczby cyfr do wszystkich znaków w nazwie;
- analizować rozmiar zapytania;
- analizować częstotliwość;

10.1.2.2 Zarządzanie i konfiguracja:

10.1.2.2.1 Serwer musi działać pod kontrolą systemu operacyjnego, przeznaczonego do realizacji funkcjonalności określonych w OPZ. Nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia;

10.1.2.2.2 Zarządzanie Systemem musi odbywać się z jednego miejsca (IP) za pomocą jednolitego systemu graficznego;

10.1.2.2.3 Serwer musi posiadać mechanizm Workflow do zarządzania procesem potwierdzania i akceptacji zmian;

10.1.2.2.4 Zarządzanie systemem musi się odbywać przez przeglądarkę WWW bez potrzeby instalacji specjalnego oprogramowania typu agent, klient itp.;

10.1.2.2.5 Serwer musi dostarczać mechanizm REST API do kontroli systemu, wykonywania
i automatyzacji zadań wykonywanych za pomocą GUI. Musi być dostarczona pełna dokumentacja systemu API z przykładami zastosowania itp.;

10.1.2.2.6 Serwer musi pracować jako platforma dystrybucji plików za pomocą protokołów TFTP, FTP, HTTP, oraz oferować usługi synchronizacji czasu za pomocą protokołu NTP (Network Time Protocol);

10.1.2.2.7 Serwer musi posiadać funkcję budowy Systemu rozproszonego, która pozwoli na zbudowanie systemu rozproszonego z synchronizacją danych poprzez sieć IP
z centralnym zarządzaniem całym systemem;

10.1.2.2.8 Serwer musi dostarczać informacje o wszystkich zmianach wprowadzanych przez administratorów (kto, kiedy, co zostało zmienione);

10.1.2.2.9 Serwer musi mieć możliwość wysyłania tych informacji do centralnego repozytorium za pomocą mechanizmu Syslog (TCP i UDP);

10.1.2.2.10 Serwer musi umożliwiać nadawanie administratorom praw opartych o grupy i role, co pozwala na ograniczenie ich dostępu do wymaganych zasobów.
Granulacja uprawnień powinna umożliwiać konfigurowanie uprawnień
dla pojedynczych obiektów typu sieć, strefa DNS, rekord DNS;

10.1.2.2.11 Serwer musi wpierać uwierzytelnianie Użytkowników poprzez: lokalną bazę Użytkowników, protokół RADIUS, protokół TACACS+, SAML, LDAP, Microsoft Active Directory oraz sprzętowy moduł bezpieczeństwa (HSM): Entrust i Thales;

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

10.1.2.2.12 Serwer musi posiadać wbudowaną bazę danych. Baza danych nie może wymagać żadnych czynności administracyjnych związanych z jej konfiguracją i utrzymaniem;

10.1.2.2.13 Serwer musi mieć możliwość monitorowania parametrów urządzeń przy użyciu protokołu SNMP (Simple Network Management Protocol);

10.1.2.2.14 Dostęp do konsoli administracyjnej urządzeń Systemu powinien być możliwy poprzez:

- Interfejs zdalny dostępny poprzez protokół SSH, wsparcie dla wersji SSHv2;
- Interfejs znakowy – dostępny poprzez port szeregowy, zabezpieczony hasłem dostępu, które jest powiązane z Użytkownikiem;

10.1.2.2.15 Serwer musi umożliwiać wykonywanie planowanych kopii bezpieczeństwa do zewnętrznego serwera w celu uproszczenia procedur odzyskiwania w razie awarii (TFTP, FTP, SCP);

10.1.3 Serwer DNS External – szt. 2

10.1.3.1 Funkcjonalność urządzenia:

10.1.3.1.1 Obsługa minimum 30 000 zapytań DNS na sekundę.

10.1.3.1.2 Pojemność bazy na minimum 100 000 rekordów

10.1.3.1.3 Serwer musi dostarczać usługi rozwiązywania nazw domenowych przy użyciu protokołu DNS (Domain Name System);

10.1.3.1.4 Serwer musi być zgodne z wymogami dokumentów RFC 1034, 1035, 1995, 1996, 2136, 2317, 2671, 2782, 3596 (RFC, tj. Request for Comments http://www.ietf.org/rfc.html);

10.1.3.1.5 Serwer musi realizować funkcje automatycznej aktualizacji serwisów DNS, zgodne z dokumentem RFC 2136;

10.1.3.1.6 Serwer musi posiadać wbudowany mechanizm powiadamiania o zmianach stref, zgodne z dokumentem RFC 1996;

10.1.3.1.7 Serwer musi wspierać protokoły DNS w wersji IPv4 i IPv6;

10.1.3.1.8 Serwer musi wspierać usługę DNS Anycast dla IPv4 i IPv6 (za pomocą protokołów BGP i OSPF);

10.1.3.1.9 Serwer musi wspierać usługę DNSSEC z automatycznym aktualizowaniem podpisów przy zmianach dokonywanych w strefach DNS;

10.1.3.1.10 Serwer musi wspierać rozbudowę o usługę DNS dla usług Active Directory;

10.1.3.1.11 Serwer musi wspierać usługę DDNS;

10.1.3.1.12 Serwer musi wspierać bezpieczną aktualizację rekordów DNS tzw. Secure Update;

10.1.3.1.13 Serwer musi wspierać obsługę MultiMaster DNS;

10.1.3.1.14 Serwer musi obsługiwać mechanizm IDN (Internationalized Domain Names) – (w tym polskie znaki) i posiadać wbudowany konwerter tzw. Punycode;

10.1.3.1.15 Dla rekordów DNS w strefach urządzenie musi logować czas utworzenia danego rekordu, czas ostatniego zapytania o ten rekord oraz umożliwiać automatyczne wykrywanie i zaznaczanie rekordów, dla których nie było zapytań od określonego czasu a które były utworzone dawniej niż zadany okres.

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

10.1.3.1.16 Serwer musi mieć wbudowaną ochronę przed atakami związanymi z protokołami DNS, BGP, OSPF, NTP. Ochrona musi być zrealizowana w oparciu o zestaw reguł ochrony dostarczanych przez producenta;

10.1.3.1.17 Musi być możliwość automatycznego pobierania i uaktywniania nowych reguł ochrony od producenta systemu bez interwencji administratora systemu.

10.1.3.1.18 Serwer musi również umożliwiać tworzenie własnych reguł ochrony pozwalających
na blokowanie lub limitowanie określonego ruchu.

10.1.3.1.19 Zestaw reguł ochrony musi obejmować ochronę co najmniej przed atakami:

- Wykorzystującymi odbicie/wzmocnienie przy pomocy DNS;
- Wykorzystującymi podatności w oprogramowaniu DNS;
- Typu cache-poisoning;
- Typu NXDOMAIN;
- Typu Phantom Domain;
- Wykorzystującymi anomalie w protokole DNS;
- Typu TCP/UDP/ICMP flood;

10.1.3.1.20 Serwer musi wykrywać ataki typu DNS Hijacking polegające
na nieautoryzowanym przekierowaniu domen Zamawiającego na inne serwery DNS;

10.1.3.1.21 Serwer w ramach obsługiwanych stref DNS musi mieć możliwość udzielania odpowiedzi w zależności od następujących parametrów: lokalizacja geograficzna klienta DNS, podsieć IP klienta DNS, atrybuty zdefiniowane przez Zamawiającego pobierane z bazy adresacji IP, dostępność usługi świadczonej przez serwer docelowy (z możliwością weryfikowania dostępności na bazie próbek http/SNMP/icmp/tcp);

10.1.3.2 Zarządzanie i konfiguracja:

10.1.3.2.1 Serwer musi umożliwiać zarządzanie z poziomu Centralnego Zarządzania systemem bezpieczeństwa DNS;

10.1.3.2.2 Dostęp do konsoli administracyjnej Systemu powinien być możliwy poprzez:

- Interfejs zdalny dostępny poprzez protokół SSH, wsparcie dla wersji SSHv2;

10.1.4 Serwer Management – szt. 2

10.1.4.1 Funkcjonalność urządzenia:

10.1.4.1.1 Pojemność bazy na minimum 400 000 rekordów;

10.1.4.1.2 Możliwość pełnienia funkcji zarządzania dla 20 urządzeń podsystemów usługowych;

10.1.4.1.3 Możliwość obsługi do 20 administratorów systemu jednocześnie;

10.1.4.1.4 Serwer musi dostarczać na bieżąco informacje o przyznawaniu adresów IP
i urządzeniach, którym dany adres został przypisany (adres MAC, czas i data przyznania adresu, IP);

10.1.4.1.5 Serwer musi dostarczać usługę zarządzania adresami IP – IPAM (IP Address Management);

10.1.4.1.6 Serwer musi zarządzać adresami IPv4 i IPv6 pozwalając na graficzną (mapy sieci) oraz obiektową metodę zarządzania adresacją; Serwer musi pozwalać
na integrację z usługami VMware vCenter oraz OpenStack,

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

w celu wykonywania procesu odnajdowania maszyn wirtualnych pracujących na infrastrukturze VMware/OpenStack oraz tworzenia rekordów DNS dla tych maszyn;

10.1.4.1.7 W przypadku kasowania maszyny wirtualnej system musi automatycznie usuwać powiązany rekord DNS;

10.1.4.1.8 System musi mieć posiadać możliwość generowania raportów z historii przydziałów adresów IP i rekord DNS dla maszyn wirtualnych do wykorzystania w audytach bezpieczeństwa;

10.1.4.1.9 Serwer musi posiadać mechanizmy kontroli wprowadzania danych (poprawność adresów IP, masek itp.);

10.1.4.1.10 Serwer musi umożliwiać dodawanie opisów i atrybutów dla obiektów sieci, adresów IP, domen. Atrybuty te muszą umożliwiać definicję typu i rozmiar danego atrybutu. Musi być możliwość stosowania słowników atrybutów z wymuszenie lub proponowaniem danego typu atrybutu dla danego typu obiektu. Urządzenie musi umożliwiać dziedziczenie atrybutów w ramach struktury sieci i podsieci;

10.1.4.1.11 Serwer musi mieć możliwość rozbudowy o mechanizm skanowania sieci i hostów/adresów IP (ang. network discovery). Mechanizm ten musi działać w trybie na żądanie oraz musi pozwalać na planowane powtarzalne rozpoznawania w przyszłości;

10.1.4.1.12 Serwer musi posiadać mechanizmy typu „znajdź 10 nieużywanych adresów z sieci X" oraz „znajdź 10 nieużywanych podsieci rozmiaru np. /24 w podsieci np. a.b.c.d/16". Funkcja musi być dostępna dla IPv4 i IPv6;

10.1.4.1.13 Serwer musi umożliwiać import danych w formacie CSV bezpośrednio z GUI i posiadać szczegółową dokumentację formatu danych importowanych;

10.1.4.1.14 Producent rozwiązania musi udostępniać bezpłatnie narzędzie do importu danych z innych systemów DNS: Bind oraz Microsoft;

10.1.4.1.15 Serwer musi umożliwiać rozbudowę w przyszłości o zarządzanie usługami DNS na wielu serwerach Microsoft Windows bez potrzeby instalowania oprogramowania po stronie serwerów MS Windows; Wymagane jest wsparcie dla:

- Microsoft Windows 2012 Standard i DataCenter Initial Release 64 bits;
- Microsoft Windows 2016 Standard i DataCenter Initial Release 64 bits;
- Microsoft Windows 2019 Standard i DataCenter Initial Release 64 bits;
- Microsoft Windows 2022 Standard i DataCenter Initial Release 64 bits;

10.1.4.1.16 Serwer musi wspierać integrację co najmniej z systemami bezpieczeństwa SIEM, Cisco ISE, Tenable Security Center, Rapid7, Qualys, FireEye NX, McAfee OpenDXL oraz posiadać otwarty interfejs Rest API do komunikacji z innymi systemami;

10.1.4.1.17 Serwer musi dostarczać usługi rozwiązywania nazw domenowych przy użyciu protokołu DNS (Domain Name System);

10.1.4.1.18 Serwer musi być zgodne z wymogami dokumentów RFC 1034, 1035, 1995, 1996, 2136, 2317, 2671, 2782, 3596 (RFC, tj. Request for Comments http://www.ietf.org/rfc.html);

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

10.1.4.1.19 Serwer musi realizować funkcje automatycznej aktualizacji serwisów DNS, zgodne z dokumentem RFC 2136;
10.1.4.1.20 Serwer musi posiadać wbudowany mechanizm powiadamiania o zmianach stref, zgodne z dokumentem RFC 1996;
10.1.4.1.21 Serwer musi wspierać protokoły DNS w wersji IPv4 i IPv6;
10.1.4.1.22 Serwer musi wspierać usługę DNS Anycast dla IPv4 i IPv6 (za pomocą protokołów BGP i OSPF);
10.1.4.1.23 Serwer musi wspierać usługę DNSSEC z automatycznym aktualizowaniem podpisów przy zmianach dokonywanych w strefach DNS;
10.1.4.1.24 Serwer musi wspierać rozbudowę o usługę DNS dla usług Active Directory;
10.1.4.1.25 Serwer musi wspierać usługę DDNS;
10.1.4.1.26 Serwer musi wspierać bezpieczną aktualizację rekordów DNS tzw. Secure Update, ze wsparciem dla protokołu GSS-TSIG;
10.1.4.1.27 Serwer musi wspierać obsługę MultiMaster DNS;
10.1.4.1.28 Serwer musi obsługiwać mechanizm IDN (Internationalized Domain Names) – (w tym polskie znaki) i posiadać wbudowany konwerter tzw. Punycode;
10.1.4.1.29 Serwer musi mieć funkcjonalność DNS Firewall opartą o polityki bezpieczeństwa realizowane na bazie stref Response Policy Zone (RPZ);
10.1.4.1.30 Serwer musi być przystosowane do obsługi stref RPZ o łącznym rozmiarze nie mniejszym niż 6 mln rekordów;
10.1.4.1.31 Serwer musi posiadać funkcjonalność wykrywania i blokowania tunelowania w DNS (DNS tunneling) za pomocą silnika analitycznego bazującego na uczeniu maszynowym i pozwalającego na wykrycie nieznanych jeszcze wzorców tunelowania i wycieku danych przez protokół DNS. W tym celu serwer dla nazw FQDN w zapytaniach DNS (w tym dla zapytań o rekordy A) musi co najmniej:
- wyliczać entropię znaków;
- sprawdzać popularność występowania w językach naturalnych wszystkich 2- i 3-znaków;
- obliczać współczynnik liczby samogłosek do wszystkich znaków w nazwie;
- obliczać współczynnik liczby cyfr do wszystkich znaków w nazwie;
- analizować rozmiar zapytania;
- analizować częstotliwość;
10.1.4.2 Zarządzanie i konfiguracja:
10.1.4.2.1 Serwer musi działać pod kontrolą systemu operacyjnego, przeznaczonego do realizacji funkcjonalności określonych w OPZ. Nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia;
10.1.4.2.2 Zarządzanie Systemem musi odbywać się z jednego miejsca (IP) za pomocą jednolitego systemu graficznego;
10.1.4.2.3 Serwer musi posiadać mechanizm Workflow do zarządzania procesem potwierdzania i akceptacji zmian;
10.1.4.2.4 Zarządzanie systemem musi się odbywać przez przeglądarkę WWW bez potrzeby instalacji specjalnego oprogramowania typu agent, klient itp.;

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

10.1.4.2.5 Serwer musi dostarczać mechanizm REST API do kontroli systemu, wykonywania
i automatyzacji zadań wykonywanych za pomocą GUI. Musi być dostarczona pełna dokumentacja systemu API z przykładami zastosowania itp.;
10.1.4.2.6 Serwer musi pracować jako platforma dystrybucji plików za pomocą protokołów TFTP, FTP, HTTP, oraz oferować usługi synchronizacji czasu za pomocą protokołu NTP (Network Time Protocol);
10.1.4.2.7 Serwer musi posiadać funkcję budowy Systemu rozproszonego, która pozwoli na zbudowanie systemu rozproszonego z synchronizacją danych poprzez sieć IP
z centralnym zarządzaniem całym systemem;
10.1.4.2.8 Serwer musi dostarczać informacje o wszystkich zmianach wprowadzanych przez administratorów (kto, kiedy, co zostało zmienione);
10.1.4.2.9 Serwer musi mieć możliwość wysyłania tych informacji do centralnego repozytorium za pomocą mechanizmu Syslog (TCP i UDP);
10.1.4.2.10 Serwer musi umożliwiać nadawanie administratorom praw opartych o grupy i role, co pozwala na ograniczenie ich dostępu do wymaganych zasobów.
Granulacja uprawnień powinna umożliwiać konfigurowanie uprawnień
dla pojedynczych obiektów typu sieć, strefa DNS, rekord DNS;
10.1.4.2.11 Serwer musi wpierać uwierzytelnianie Użytkowników poprzez: lokalną bazę Użytkowników, protokół RADIUS, protokół TACACS+, SAML, LDAP, Microsoft Active Directory oraz sprzętowy moduł bezpieczeństwa (HSM): Entrust i Thales;
10.1.4.2.12 Serwer musi posiadać wbudowaną bazę danych. Baza danych nie może wymagać żadnych czynności administracyjnych związanych z jej konfiguracją
i utrzymaniem;
10.1.4.2.13 Serwer musi mieć możliwość monitorowania parametrów urządzeń przy użyciu protokołu SNMP (Simple Network Management Protocol);
10.1.4.2.14 Dostęp do konsoli administracyjnej urządzeń Systemu powinien być możliwy poprzez:
10.1.4.2.15 Interfejs zdalny dostępny poprzez protokół SSH, wsparcie dla wersji SSHv2;
10.1.4.2.16 Serwer musi umożliwiać wykonywanie planowanych kopii bezpieczeństwa do zewnętrznego serwera w celu uproszczenia procedur odzyskiwania w razie awarii (TFTP, FTP, SCP);
10.1.5 Serwer Raportujący – szt. 1
10.1.5.1 Funkcjonalność urządzenia:
10.1.5.1.1 System musi realizować usługi raportowania dla systemu IPAM, DNS;
10.1.5.1.2 System musi posiadać odpowiednie uprawnienia dla Użytkowników związane z dostępem do funkcji raportowania
10.1.5.1.3 Wymagane jest generowanie minimum raportów:
10.1.5.1.3.1 Ochrona na bazie DNS:
10.1.5.1.3.1.1 Raport aktywności w ramach ukrytych w DNS tuneli komunikacyjnych;
10.1.5.1.3.1.2 Główne adresy IP powiązane z aktywnością malware oraz tunelami DNS;
10.1.5.1.3.1.3 Główne zdarzenia bezpieczeństwa z DNS firewalla;

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

10.1.5.1.3.1.4 Szkodliwa aktywność per adres IP;
10.1.5.1.4 Wydajność DNS:
10.1.5.1.4.1 Szybkość aktualizacji DDNS
10.1.5.1.4.2 Najczęściej żądane nazwy domen DNS;
10.1.5.1.4.3 Trend odpowiedzi DNS;
10.1.5.1.4.4 Trend trafień w bufor DNS (Cache Hit Ratio);
10.1.5.1.4.5 Ilość zapytań DNS wg typu zapytań;
10.1.5.1.4.6 Trend czasu odpowiedzi na zapytania DNS;
10.1.5.1.4.7 Adresy IP będące źródłem największej ilości zapytań DNS;
10.1.5.1.4.8 Ilość zapytań DNS dziennie w podziale na poszczególne serwery DNS;
10.1.5.1.4.9 Największe obciążenie godzinowe wg liczby zapytań DNS dla poszczególnych serwerów;
10.1.5.1.4.10 Liczba zapytań DNS per serwer DNS;
10.1.5.1.4.11 Raport odpowiedzi NXDOMAIN / NOERROR;
10.1.5.1.4.12 Raport błędów SERVFAIL
10.1.5.1.5 Raporty użycia bazy adresów IPAMv4:
10.1.5.1.5.1 Raport użycia adresów sieciowych IPv4;
10.1.5.1.5.2 Trend użycia adresów sieciowych IPv4;
10.1.5.1.5.3 Raport podsieci o największej liczbie wykorzystanych adresów IPv4
10.1.5.1.6 Obciążenia systemu:
10.1.5.1.6.1 Trend wykorzystania procesora;
10.1.5.1.6.2 Trend wykorzystania pamięci RAM;
10.1.5.1.6.3 Ilość ruchu sieciowego per serwer
10.1.5.1.7 Możliwość definiowania własnych raportów oraz kopiowania raportów w systemie.
10.1.5.2 Zarządzanie i konfiguracja:
10.1.5.2.1 Serwer musi umożliwiać zarządzanie z poziomu Centralnego Zarządzania systemem bezpieczeństwa DNS;
10.1.5.2.2 Dostęp do konsoli administracyjnej urządzeń Systemu powinien być możliwy poprzez:
- Interfejs zdalny dostępny poprzez protokół SSH, wsparcie dla wersji SSHv2;
- Interfejs znakowy – dostępny poprzez port szeregowy, zabezpieczony hasłem dostępu, które jest powiązane z Użytkownikiem.

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