Załącznik nr 1 do Zapytania

2021-27494

Opis Przedmiotu Zamówienia

1. Przedmiot zamówienia.

1.1. Przedmiotem zamówienia jest **Zakup systemu zarządzania dostępem do sieci NAC.**

1.2. Realizacja przedmiotu zamówienia polega na dostarczeniu i wdrożeniu rozwiązania typu NAC (Network Access Control) (zwanego dalej Systemem) wraz oprogramowaniem, niezbędnymi licencjami oraz świadczeniu usługi gwarancji dla wdrożonego systemu. System ma być dostarczony w modelu „on premise" czyli musi być zainstalowany na infrastrukturze Zamawiającego.

1.3. W szczególności przedmiot zamówienia obejmuje:

1.3.1. Dostarczenie niezbędnych licencji wieczystych typu virtual appliance lub software appliance.

1.3.2. Dostarczenie najnowszej wersji Systemu.

1.3.3. Świadczenie usług gwarancyjnych producenta oprogramowania przez okres nie krótszy niż 12 miesięcy i nie dłuższy niż 24 miesiące od daty podpisania Protokołu odbioru.

1.4. Systemem zostanie objęte środowisko Zamawiającego składające się z:

1.4.1. **WARIANT I**

1.4.1.1. 600 stacji końcowych monitorowanych agentowo.

1.4.1.2. 300 urządzeń typu BYOD (Bring Your Own Device)

1.4.1.3. 1100 jednoczesnych unikatowych operacji uwierzytelniania do sieci Zamawiającego.

1.4.1.4. Sumarycznie 1500 monitorowanych hostów

1.4.1.5. Zamawiający przewiduje możliwość udzielenia zamówienia opcjonalnego w zakresie objęcia Systemem dodatkowych 100 urządzeń końcowych oraz zwiększenia o 100 liczby jednoczesnych unikatowych uwierzytelnień względem wymagań zawartych łącznie w pkt 1.4.1.1 - 1.4.1.4.

1.4.2. **WARIANT II**

1.4.2.1. 600 stacji końcowych monitorowanych agentowo.

1.4.2.2. 300 urządzeń typu BYOD (Bring Your Own Device)

1.4.2.3. 1500 jednoczesnych unikatowych operacji uwierzytelniania do sieci Zamawiającego.

1.4.2.4. Sumarycznie 3500 monitorowanych hostów

1.4.2.5. Zamawiający przewiduje możliwość udzielenia zamówienia opcjonalnego w zakresie objęcia Systemem dodatkowych 300 urządzeń końcowych oraz zwiększenia o 300 liczby jednoczesnych unikatowych uwierzytelnień względem wymagań zawartych łącznie w pkt 1.4.2.1 - 1.4.2.4.

2. Harmonogram realizacji przedmiotu zamówienia:

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

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

NIP: 5251575309
REGON: 001377706

Przedmiot zamówienia zostanie zrealizowany w terminie nie dłuższym niż 30 Dni roboczych, liczonym od dnia zawarcia Umowy, w podziale na niżej określone etapy:

Etap I – Opracowanie harmonogramu wdrożenia.

W ramach realizacji etapu Wykonawca:

2.1. W terminie do 10 dni od daty podpisania umowy, przygotuje i przedstawi Zamawiającemu harmonogram wdrożenia Systemu.

2.2. Przygotuje opis niezbędnych prac w celu wdrożenia Systemu wraz ze wskazaniem podziału obowiązków pomiędzy Zamawiającego i Wykonawcę w modelu RACI.

2.3. Przedstawi listę pracowników Wykonawcy odpowiedzialnych za wykonanie poszczególnych etapów zgodnie z przedstawionym wykazem podziału obowiązków w w/w formacie RACI wraz z danymi teleadresowymi minimalnie numer telefonu komórkowego, adres email.

2.4. Opracuje scenariusze testowe Systemu:

2.4.1. Scenariusze testowe muszą zawierać propozycje testów wydajnościowych, funkcjonalnych i bezpieczeństwa.

2.4.2. Scenariusze testowe będą przygotowane przez Wykonawcę i wymagają zatwierdzenia przez Zamawiającego.

Etap II - Analiza przedwdrożeniowa.

W ramach realizacji etapu Wykonawca:

2.5. Wykona analizę infrastruktury informatycznej Zamawiającego, która zostanie objęta Systemem, potrzeb użytkownika i wymagań funkcjonalnych odnośnie konfiguracji Sytemu, której wynikiem będzie plan wdrożenia Systemu u Zamawiającego.

2.6. Przygotuje i przedstawi Zamawiającemu Projekt techniczny Systemu (architektura Systemu) określający:

2.6.1. Wykaz oprogramowania i licencji niezbędnych do poprawnej pracy Systemu;

2.6.2. Wymogi takie jak ilość urządzeń fizycznych/maszyn wraz z dokładnymi parametrami jak vCPU, vRAM, vHDD wirtualnych wymaganych dla wszystkich składowych Systemu.

2.7. Uzgodni z Zamawiającym polityki/reguły bezpieczeństwa Systemu oraz ich wdrożenie.

2.8. Dostarczy oprogramowanie i licencje niezbędne do poprawnej pracy Systemu.

Etap III – Wdrożenie, konfiguracja i testy Systemu.

W ramach realizacji etapu Wykonawca:

2.9. Wdroży w infrastrukturze Zamawiającego System zgodnie z zaakceptowanym harmonogramem, planem wdrożenia Systemu oraz Projektem technicznym Systemu z uwzględnieniem analizy przedwdrożeniowej oraz warunkami opisanymi w pkt 3 OPZ.

2.10. Wykona pełną konfigurację i parametryzację Systemu zgodnie z Projektem technicznym będącym wynikiem analizy przedwdrożeniowej.

2.11. Przeprowadzi testy akceptacyjne.

2.12. Dostarczy Dokumentację powykonawczą dla Zamawiającego.

2.13. Przeprowadzi instruktaż dla użytkowników Systemu zgodnie z warunkami opisanymi w pkt. 6.

3. Wdrożenie Systemu.

W ramach realizacji Etapu III, Wykonawca dokona wdrożenia Systemu , rozumianego jako:

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

3.1. Instalacja Systemu zgodna z planem wdrożenia na udostępnionym przez Zamawiającego środowisku opisanym w pkt 1.4 OPZ. Szczegóły systemowe zostaną przekazane Wykonawcy po podpisaniu umowy.

3.2. Przygotowanie konfiguracji Systemu zgodnie z projektem technicznym Systemu oraz wdrożenie polityk bezpieczeństwa odzwierciedlających obecnie posiadaną konfigurację i wiedzę o aktualnych zagrożeniach.

3.3. Skonfigurowanie logowania zdarzeń na Systemie i umożliwienia zapisywania ich na zewnętrznym serwerze logowania udostępnionym przez Zamawiającego (możliwość zapisywania/eksportu logów w formacie Syslog/CEF/EventLog).

3.4. Przeprowadzenie testów wydajnościowych, funkcjonalnych i bezpieczeństwa zainstalowanego Systemu, zgodnie z opracowanymi w pkt 2.4 OPZ scenariuszami, z udziałem Zamawiającego. Wynikiem testów będzie raport potwierdzający spełnienie zawartych w pkt 4.3 Obligatoryjnych funkcjonalności Systemu. Raport potwierdzony zostanie przez obie strony.

3.5. Przygotowanie i dostarczenie Dokumentacji powykonawczej oraz dokumentacji użytkownika (administratora/operatora) systemu. Dokumentacja powinna zawierać architekturę rozwiązania, spis wszystkich wdrożonych polityk bezpieczeństwa, opis testów akceptacyjnych i funkcjonalnych rozwiązania, opis konfiguracji systemu (w tym nietypowe ustawienia) oraz instrukcję dla użytkownika/administratora systemu.

3.6. Za pełne wdrożenie Systemu uznaje się instalację systemu, przeprowadzenie z wynikiem pozytywnym testów akceptacyjnych, funkcjonalnych i bezpieczeństwa, integracja z systemem logowania zdarzeń Zamawiającego, dostarczenie kompletu dokumentacji, przeprowadzenie instruktażu opisanego w pkt 6, obustronne podpisanie protokołu odbioru.

4. Wymagania minimalne dla Systemu NAC:

4.1. **Architektura Systemu.**

4.1.1. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor).

4.1.2. W przypadku dostarczenia Systemu jako maszyny wirtualnej muszą być wspierane środowiska Hyper-V oraz Vmware.

4.1.3. System musi wspierać możliwość pracy w konfiguracji HA (High Availability) z trybem Active-Passive lub Active-Active w celu zwiększenia niezawodności.

4.1.4. Jeżeli System będzie instalowany jako oprogramowanie na systemie operacyjnym należy dostarczyć produkt, który będzie mógł być zainstalowany na jednym z systemów operacyjnych: Windows Server 2012+, CentOS, RHEL.

4.1.5. System musi być w pełni zarządzalny z jednej konsoli przez interfejs www, należy dostarczyć rozwiązanie obsługiwane za pośrednictwem popularnych przeglądarek internetowych (Chrome, MS Edge, Firefox) w aktualnych wersji na dzień składania oferty.

4.1.6. Konsola zarządzania musi być wykonana w HTML5 oraz nie może wymagać dodatkowych wtyczek.

4.1.7. Konsola zarządzania musi umożliwiać dostęp szyfrowany z pomoc protokołu SSL, w wersji co najmniej TLS 1.2.

4.1.8. Agent Systemu dla stacji końcowej powinien działać na systemach operacyjnych obsługiwanych przez Zamawiającego (Microsoft Windows 8.1, Windows 10, Microsoft Server 2012 i nowszych, macOS oraz Linux (RHEL/CentOS/Debian)).

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

4.1.9. System powinien chronić zarządzane punkty końcowe działające w systemach połączonych, systemach rozproszonych i niezależnych środowiskach.

4.1.10. Wszystkie komponenty Systemu na stacji monitorowanej powinny mieć możliwość automatycznego wdrażania i konfiguracji w oparciu o predefiniowane reguły zarządzania.

4.1.11. System powinien obsługiwać automatyczny/zaplanowany transfer logów z agentów w celu archiwizacji.

4.1.12. Elementy zarządzające i analityczne Systemu muszą być skalowane w celu obsługi co najmniej 10 000 jednoczesnych unikatowych autoryzacji do sieci w ciągu doby.

4.1.13. Praca Systemu musi pozwalać na działanie bez dostępu do Internetu.

4.1.14. Wymagana jest możliwość wykorzystania mechanizmy proxy do komunikacji z Internetem.

4.1.15. W przypadku braku dostępu do Internetu System zarządzający ma mieć możliwość aktualizacji za pomocą ręcznej aktualizacji.

4.1.16. W przypadku dostępu do Internetu System ma umożliwiać aktualizację automatyczną jak również ręczną z poziomu panelu zarządzania Systemem.

4.1.17. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych urządzeń w sieci.

4.1.18. Licencja na jednoczesne unikatowe uwierzytelniania ma być zwalniana po rozłączeniu urządzenia końcowego.

4.2. **Zarządzanie Systemem.**

4.2.1. System musi umożliwiać tworzenie indywidualnych kont dla każdego użytkownika/administratora Systemu.

4.2.2. System musi zapewniać silną politykę haseł lub umożliwiać jej określenie dla użytkowników Systemu.

4.2.3. System musi umożliwiać konfigurowanie zakresu uprawnień w Systemie z wykorzystaniem predefiniowanych ról wewnętrznych (np. dostęp tylko do raportów, administrator systemu, analityk itp.).

4.2.4. System powinien się integrować z usługą Microsoft Active Directory w zakresie uwierzytelnienia do Systemu oraz kontroli dostępu na bazie zdefiniowanych ról. Dopuszcza się rozwiązanie używające wewnętrznego mechanizmu uwierzytelniania do Systemu.

4.2.5. System musi mieć możliwość definiowania raportów i alertów z wykorzystaniem wszystkich danych zbieranych przez system.

4.2.6. System musi mieć wbudowany panel sterowania (Dashboard) z predefiniowaną zawartością dostosowaną do potrzeb określonej roli co najmniej analityka, kierownika zespołu, dyrektora bezpieczeństwa. Dashboard powinien umożliwiać schodzenie do szczegółu poszczególnych elementów od poziomu informacji podstawowych.

4.2.7. Konsola zarządzania systemu musi być dostępna co najmniej w angielskiej wersji językowej.

4.3. **Obligatoryjne funkcjonalności Systemu.**

4.3.1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników oraz urządzeń końcowych.

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

4.3.2. System musi umożliwiać automatyczne wykrywanie, rejestrowanie, analizowanie oraz reagowanie w zakresie parametrów i zdarzeń definiowanych przez producenta lub skonfigurowanych i wybranych przez użytkownika w celu oceny działania systemu monitorowanego, wsparcia zarządzania ryzykiem oraz umożliwienia działań związanych z informatyką śledczą i analizą po włamaniową.

4.3.3. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, , WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC.

4.3.4. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z minimum systemów zewnętrznych:

4.3.4.1. Microsoft Active Directory

4.3.4.2. Radius

4.3.4.3. LDAP

4.3.5. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, konfiguracji VPN, wysłania konfiguracji dostępowych poprzez email.

4.3.6. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.

4.3.7. System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników.

4.3.8. System musi posiadać możliwość identyfikacji urządzeń końcowych z wykorzystaniem MUD (Manufacturer Usage Description) zgodnie ze standardem IETF i RFC 8520.

4.3.9. System musi posiadać mechanizm podglądu, tworzenia map graficznych umiejscowienia urządzeń sieciowych, końcowych, gniazdek internetowych z możliwością podziału logicznego na budynki, pokoje oraz węzły sieciowe.

4.3.10. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, adresadres MAC, nazwa urządzenia końcowego HOSTNAME, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony VLAN z przydzielonym adresem IP.

4.3.11. System musi zapewniać scentralizowane zarządzanie z pomocą panelu zarządzania urządzeniami sieciowymi. Zarządzanie musi dopuszczać możliwość zarządzania agentowo jak i bez-agentowo.

4.3.12. System musi umożliwiać monitorowanie urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.

4.3.13. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu oraz konfiguracji ustawień portu z zakresu:

4.3.13.1. VLAN

4.3.13.2. Autoryzacja

4.3.13.3. Status

4.3.13.4. Opis

4.3.14. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.

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

4.3.15. System musi zapewniać funkcjonalność wizualizacji konfiguracji podsieci IP oraz przypisania jej do jednostek.

4.3.16. System musi wspierać funkcjonalność włączania i wyłączania podsieci IP, adresów IP bez konieczności usuwania ich z systemu.

4.3.17. System musi umożliwiać śledzenie atrybutów urządzeń zainstalowanych w sieci, takich jak numer seryjny, etykieta zasobu, wersja zainstalowanego oprogramowania (firmware).

4.3.18. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.

4.3.19. System musi posiadać mechanizm automatyzacji wg harmonogramu z możliwością symulacji działania, min:

4.3.19.1. Włączenie wskazanych portów urządzeń sieciowych.

4.3.19.2. Wyłączenie wskazanych portów urządzeń sieciowych.

4.3.19.3. Wykonania komend na wskazanych urządzeń sieciowych.

4.3.19.4. Dodanie znalezionych urządzeń sieciowych w skazanych podsieciach z możliwością sklonowania konfiguracji z podanego urządzenia sieciowego wg podanych parametrów jak: parametry dostępowe SNMP w wersji 1, 2c, 3, producenta, modelu urządzenia.

4.3.20. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP.

4.3.21. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa konfiguracji lokalnie lub na udziałach zewnętrznych.

4.3.22. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).

4.3.23. Captive Portal musi umożliwiać obsługę instalacji agentów, dystrybucji certyfikatów użytkowników oraz generowania autokonfiguratorów sieci.

4.3.24. System musi posiadać mechanizm zarządzania uprawnieniami użytkowników, którzy będą mogli rejestrować swoje urządzenia, pobierać certyfikaty, agenty oraz uruchamiać autokonfiguratorów sieci.

4.3.25. Captive Portal musi się automatycznie dostosować wyświetlanym formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.

4.3.26. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.

4.3.27. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP)..

4.3.28. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.

4.3.29. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.

4.3.30. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.

4.3.31. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.

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

4.3.32. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim lub dając możliwość zdefiniowania treści z polskim kodowaniem znaków, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).

4.3.33. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.

4.3.34. Captive Portal powinien umożliwiać podgląd ostatnich 10 logowań do sieci.

4.3.35. Captive Portal powinien umożliwiać zmianę konfiguracji numeru portów HTTP i HTTPS.

4.3.36. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.

4.3.37. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.

4.3.38. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.

4.3.39. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego, co najmniej:

4.3.39.1. Cisco

4.3.39.2. Fortinet

4.3.39.3. ESET

4.3.39.4. RSA

4.3.40. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.

4.3.41. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z IETF RFC 5176.

4.3.42. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.

4.3.43. System musi obsługiwać metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej:

4.3.43.1. DHCP Fingerprinting

4.3.43.2. DHCP SPAN

4.3.43.3. SNMP

4.3.43.4. Vendor OUI

4.3.43.5. TCP

4.3.43.6. Active Directory

4.3.43.7. CDP/LLDP

4.3.43.8. HTTP/S

4.3.43.9. DNS

4.3.43.10. Radius

4.3.43.11. WMI

4.3.44. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa 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

4.3.44.1. Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności
4.3.44.2. Czy włączony jest firewall
4.3.44.3. Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur
4.3.44.4. Czy jest włączone szyfrowanie dysku systemowego
4.3.44.5. Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory
4.3.44.6. Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora
4.3.44.7. Czy w systemie są uruchomione procesy wskazane przez administratora
4.3.44.8. Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności
4.3.44.9. Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:
4.3.44.9.1. Wartości klucza rejestru.
4.3.44.9.2. Typu wartości: Number, String, Version.

4.3.45. System musi posiadać obsługę realizowaną przez dedykowanego agenta przełączanie VLANów na określonych portach urządzeń sieciowych.

4.3.46. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.

4.3.47. System musi współpracować z serwerem tokenów.

4.3.48. System musi posiadać mechanizm auto konfiguracji sieci (auto konfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej:

4.3.48.1. Microsoft Windows
4.3.48.2. Mac OS

4.3.49. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).

4.3.50. System musi umożliwiać wsparcie dla systemów typu HOT-SPOT oraz serwisami umożliwiającym oferowanie materiałów promocyjnych.

4.3.51. System musi posiadać wbudowany skaner sieciowy umożliwiający co najmniej weryfikacje otwartych portów urządzenia końcowego oraz zainstalowany system operacyjny.

4.3.52. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

4.3.53. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.

4.3.54. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:

4.3.54.1. MAC
4.3.54.2. PAP/ASCII
4.3.54.3. CHAP
4.3.54.4. SNMP
4.3.54.5. 802.1X
4.3.54.6. wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), 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

4.3.55. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.

4.3.56. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.

4.3.57. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows 8 i 8.1, Windows 10, Apple Mac OS X Supplicant, , RHEL Supplicant).

4.3.58. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:

4.3.58.1. Tożsamość/Urządzenie końcowe,

4.3.58.2. Grupa tożsamości/urządzeń końcowych,

4.3.58.3. Parametry urządzeń końcowych, min: system operacyjny, wersja,

4.3.58.4. Atrybuty Active Directory,

4.3.58.5. Jednostka organizacyjna tożsamości/urządzeń końcowych,

4.3.58.6. Urządzenia sieciowe sieci przewodowej, bezprzewodowej,

4.3.58.7. Grupy urządzeń sieciowych,

4.3.58.8. Porty urządzeń sieciowych,

4.3.58.9. Grupy portów urządzeń sieciowych,

4.3.58.10. Jednostka organizacyjna portów,

4.3.58.11. Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),

4.3.58.12. Data, czas ważności polityki,

4.3.58.13. Wewnętrzny Captive Portal,

4.3.58.14. Metoda autoryzacji.

4.3.59. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów:

4.3.59.1. Cisco Networks

4.3.59.2. Aruba Networks

4.3.59.3. Hewlett Packard Enterprise

4.3.59.4. Juniper Networks

4.3.60. System musi wspierać funkcjonalność IP-to-ID Mapping, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.

4.3.61. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.

4.3.62. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.

4.3.63. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.

4.3.64. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.

4.3.65. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.

4.3.66. System musi umożliwiać automatyczną konfigurację parametrów dostępowych do serwerów VPN z poziomu tożsamości.

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

4.3.67. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.

4.3.68. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.

4.3.69. System musi pozwalać na weryfikację zalogowanego urządzenia końcowego IoT (Internet of Things) minimum za pomocą mechanizmów SNMP, DHCP, NMAP, Agenta oraz wywołania akcji: powiadomienie administratorów i/lub zablokowanie i rozłączenie sesji.

4.3.70. System musi umożliwiać automatyczną generację certyfikatów z poziomu tożsamości i urządzeń końcowych.

4.3.71. System musi posiadać funkcjonalność testowania poprawności polityk z poziomu interfejsu graficznego dla wybranych tożsamości bądź urządzeń końcowych wraz z informacją zwrotną, za pomocą, której polityki zostanie przydzielony dostęp do sieci.

4.3.72. System musi wspierać funkcjonalność różnych typu autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.

4.3.73. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników. System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

4.3.74. Obsługa serwerów certyfikatów CA

4.3.74.1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.

4.3.74.2. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:

4.3.74.2.1. możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych;

4.3.74.2.2. możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych;

4.3.74.2.3. możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol);

4.3.74.2.4. usługę OCSP (Online Certificate Status Protocol).

4.3.75. Obsługa serwerów VPN

4.3.75.1. System musi posiadać funkcję zintegrowanego serwera VPN oraz zapewniać współpracę z zintegrowanym oraz zewnętrznym serwerem CA,

4.3.75.2. System musi umożliwiać wystawianie konfiguracji klienckich, certyfikatów dla serwerów VPN.

4.3.75.3. System musi logować wszelkie próby autoryzacji do serwerów VPN.

4.3.75.4. System musi zapewniać przynajmniej następujące funkcjonalności serwera VPN:

4.3.75.4.1. Logowanie do zasobów firmy,

4.3.75.4.2. Obsługę OTP,

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

4.3.75.4.3. Przypisanie ustalonego adresu IP.

4.3.76. Obsługa serwerów DHCP

4.3.76.1. System musi posiadać funkcję zintegrowanego serwera DHCP.

4.3.76.2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.

4.3.76.3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:

4.3.76.3.1. Uruchamianie usługi dla wybranych podsieci,

4.3.76.3.2. Przypisanie ustalonego adresu IP dla adresu MAC.

4.3.76.3.3. Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,

4.3.76.3.4. Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,

4.3.76.3.5. Możliwość określania braku dostępu dla wybranych adresów MAC,

4.3.76.3.6. Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,

4.3.76.3.7. Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,

4.3.76.3.8. Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,

4.3.76.3.9. Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,

4.3.76.3.10. Dokonywanie zmian bez konieczności wyłączania usług.

4.3.77. Obsługa serwerów TACACS+

4.3.77.1. System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych:

4.3.77.1.1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.

4.3.77.1.2. System musi umożliwiać tworzenia haseł administratorom.

4.3.77.1.3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów

4.3.77.1.4. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.

4.3.77.1.5. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.

4.3.77.1.6. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.

4.3.77.1.7. System musi wspierać logowanie administratorów za pomocą tokenów OTP.

4.3.78. Raportowanie i monitoring

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

4.3.78.1. Monitoring autoryzacji:

4.3.78.1.1. Top 10 uwierzytelnień pomyślnych (zaakceptowanych autoryzacji),

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

4.3.78.1.2. Top 10 autoryzacji odrzuconych,
4.3.78.1.3. Top 10 urządzeń sieciowych z największą liczbą autoryzacji,
4.3.78.1.4. Top 10 urządzeń sieciowych z największą liczbą autoryzacji odrzuconych,
4.3.78.1.5. Top 10 SSID z największą liczbą autoryzacji,
4.3.78.1.6. Top 10 SSID z największą liczbą autoryzacji odrzuconych,
4.3.78.1.7. Autoryzacje zaakceptowane w ciągu ostatnich 30 dni,
4.3.78.1.8. Autoryzacje odrzucone w ciągu ostatnich 30 dni,
4.3.78.1.9. Obciążenie serwera autoryzacji,
4.3.78.1.10. Ostatnie 100 zdarzeń autoryzacji,
4.3.78.1.11. Top 10 unikalnych urządzeń końcowych wg. tożsamości.

4.3.78.2. Monitoring dla zdarzeń systemowych:
4.3.78.2.1. Ostatnie 100 zdarzeń systemowych,
4.3.78.2.2. Top 10 zdarzenia typu error z Sysloga,
4.3.78.2.3. Top 10 zdarzenia typu TopSeverity z Sysloga,
4.3.78.2.4. Obciążenie serwera Syslog.

4.3.78.3. Monitoring dla zdarzeń DHCP:
4.3.78.3.1. Wykorzystanie podsieci statyczne i dynamiczne,
4.3.78.3.2. Ilość używanych adresów DHCP,
4.3.78.3.3. Ostatnie 100 zdarzeń DHCP,
4.3.78.3.4. Procentowe wykorzystanie serwera DHCP,
4.3.78.3.5. Top 10 DHCP z największą liczbą przyznanych adresów,
4.3.78.3.6. Top 10 DHCP z największą liczbą kolizji IP,
4.3.78.3.7. Top 10 DHCP z największą liczbą odrzuconych IP,
4.3.78.3.8. Top 10 DHCP z wykorzystaną pulą IP,
4.3.78.3.9. Obciążenie serwera DHCP.

4.3.78.4. Monitoring dla tożsamości:
4.3.78.4.1. Podział tożsamości ze względu na typ konta,
4.3.78.4.2. Podział tożsamości ze względu na tożsamości aktywne i nieaktywne,
4.3.78.4.3. Podział tożsamości ze względu na serwer autoryzacji,
4.3.78.4.4. Podział tożsamości ze względu na konta, które straciły ważność,
4.3.78.4.5. Wykorzystanie kont gościnnych z dostępem czasowym.

4.3.78.5. Monitoring dla urządzeń końcowych:
4.3.78.5.1. Podział urządzeń ze względu na ich status,
4.3.78.5.2. Podział urządzeń ze względu na ich typ,
4.3.78.5.3. Podział urządzeń ze względu na serwer autoryzacji,
4.3.78.5.4. Podział urządzeń ze względu na urządzenia aktywne i nieaktywne.

4.3.78.6. Monitoring dla urządzeń sieciowych:
4.3.78.6.1. Podział urządzeń ze względu na urządzenia aktywne i nieaktywne.
4.3.78.6.2. Podział urządzeń ze względu na ich typ.

4.3.78.7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP,

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

autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.

4.3.78.8. Raport ze zdarzeń logowania z informacją o nadam adresie IP.

4.3.78.9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.

4.3.78.10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.

4.3.78.11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.

4.3.78.12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.

4.3.78.13. System musi wspierać mechanizm graficznego podglądu wykrytych nie-zgodności vlanów w urządzeniach sieciowych działających w środowisku.

4.3.78.14. System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.

4.3.78.15. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.

4.3.78.16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.

4.3.78.17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wy-słanego tokenu przez bramkę SMS.

4.3.78.18. Raport zdarzeń Microsoft Active Directory, minimum:

4.3.78.18.1. Logowania, wylogowania z system w tym błędne logowania.

4.3.78.18.2. Logowania do sieci 802.1X.

4.3.79. Alertowanie

4.3.79.1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:

4.3.79.1.1. wiadomości e-mail,

4.3.79.1.2. Syslog,

4.3.79.1.3. notyfikacji systemowych.

4.3.79.2. Alarmy mogą być generowane w sytuacjach, min:

4.3.79.2.1. Ilości obsługiwanych transakcji RADIUS,

4.3.79.2.2. Opóźnienie obsługi transkacji RADIUS,

4.3.79.2.3. Statusu krytycznego modułów.

4.3.79.3. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:

4.3.79.3.1. badanie łączności IP za pomocą ping, traceroute,

4.3.79.3.2. tcpdump protokołów RADIUS, TACACS+,

4.3.79.3.3. wyszukiwanie zdarzeń RADIUS z uwzględnieniem: nazwy użytkownika, adresu MAC, statusu uwierzytelnienia (udana lub nieudana), powodu, jeżeli uwierzytelnienie nieudane, zakresu czasowego, co do dnia, godziny i minuty.

4.3.79.3.4. wykonanie zdalnego polecenia na urządzeniu sieciowym.

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. Gwarancja

W ramach realizacji przedmiotu zamówienia, wykonawca będzie świadczył usługi gwarancyjne na określonych poniżej zasadach.

5.1. Zapisy ogólne

5.1.1. Wykonawca udziela Zamawiającemu Gwarancji na:

5.1.1.1. wdrożony System,

5.1.1.2. Oprogramowanie.

5.1.2. Wykonawca oświadcza, że Oprogramowanie przez niego dostarczone objęte jest gwarancją producenta.

5.1.3. Wykonawca udziela gwarancji na elementy wymienione w pkt 1.1-1.3 która obowiązuje przez okres nie krótszy niż 12 miesięcy i nie dłuższy niż 24 miesiące od daty podpisania Protokołu odbioru, wskazanego w Umowie.

5.1.4. Wykonawca zobowiązany jest w okresie realizacji Umowy do usuwania Błędów elementów wymienionych w pkt 1.1-1.3 na zasadach opisanych w niniejszym załączniku.

5.1.5. Zakres świadczeń w ramach Gwarancji obejmuje:

5.1.5.1. usuwanie Błędów elementów wymienionych w pkt 1.1-1.3 zgodnie z Czasami Reakcji, Czasami Naprawy, Czas Propozycji Rozwiązania i dla poszczególnych kategorii Błędów,

5.1.5.2. dostarczanie nowych wersji Oprogramowania,

5.1.5.3. aktualizację Dokumentacji w przypadku wprowadzania zmian w Systemie lub Oprogramowaniu w wyniku naprawy Błędu, w terminie 5 Dni roboczych od dnia naprawy

5.1.6. Wykonawca zobowiązuje się do świadczenia usług w ramach Gwarancji w sposób zapobiegający utracie jakichkolwiek danych przetwarzanych z wykorzystaniem Systemu.

5.1.7. W ramach świadczenia przez Wykonawcę usług w ramach Gwarancji, Wykonawca zobowiązany jest do umożliwienia osobom wskazanym przez Zamawiającego obserwacji prac Wykonawcy.

5.1.8. W przypadku wykrycia przez Zamawiającego Błędu, Zamawiający dokona kwalifikacji zgłoszenia (Błąd Krytyczny / Błąd Zwykły / Błąd Systemu) według własnego uznania na podstawie zdefiniowanych kryteriów. Zgłoszenie zawierać będzie posiadane przez Zamawiającego informacje na temat nieprawidłowego działania Systemu istotne w ocenie Zamawiającego dla zdiagnozowania i usunięcia nieprawidłowości w działaniu Systemu.

5.1.9. Formalne potwierdzenie Zgłoszenia stanowi przesłanie przez Zamawiającego do Wykonawcy informacji o wystąpieniu Błędu i opisie jego symptomów.

5.1.10. Wykonawca zobowiązuje się rejestrować zgłaszane Błędy wykorzystując rozwiązania umożliwiające raportowanie Zgłoszeń - w tym Czas Reakcji, Czas Propozycji Rozwiązania oraz Czas Naprawy.

5.1.11. Wykonawca będzie przyjmował Zgłoszenia przez cały czas, tj. w systemie 8:00-16:00 Dni robocze.

5.1.12. Wykonawca będzie przyjmował Zgłoszenia przekazywane w jeden z następujących sposobów:

5.1.12.1. za pomocą aplikacji serwisowej (interfejsu serwisowego);

5.1.12.2. przez przesłanie Zgłoszenia pocztą elektroniczną na adres: ……@.....;

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

5.1.13. W razie otrzymania przez Wykonawcę Zgłoszenia lub w razie uzyskania przez Wykonawcę wiedzy o wystąpieniu Błędu z innego źródła niż Zgłoszenie, Wykonawca zobowiązany będzie do podjęcia działań zmierzających do usunięcia Błędu.

5.1.14. Jeżeli Zamawiający nie wie o istnieniu Błędu, Wykonawca poinformuje w ciągu 24 godzin, Zamawiającego o jej wystąpieniu.

5.1.15. Jeżeli Wada została wykryta przez Wykonawcę, Wykonawca nada jej odpowiednią wstępną kategorię (Błąd Krytyczny / Błąd Zwykły / Błąd Systemu). W ciągu 2 godzin od powiadomienia przez Wykonawcę Zamawiający ma prawo zmienić kategorię Błędu.

5.1.16. Ostatecznie o klasyfikacji kategorii Błędu (Błąd Krytyczny / Błąd Zwykły / Błąd Systemu) decyduje Zamawiający.

5.1.17. Wykonawca zobowiązany jest do potwierdzenia przyjęcia Zgłoszenia odpowiednim wpisem we własnej aplikacji serwisowej (dotyczy to również Zgłoszeń składanych pocztą elektroniczną) oraz o nadaniu indywidualnego identyfikatora zgłoszenia. Chwila potwierdzenia przyjęcia Zgłoszenia nie ma wpływu na Czas Reakcji, Czas Propozycji Rozwiązania, Czas Naprawy. Wykonawca jest zobowiązany do udostępnienia Zamawiającemu własnej aplikacji serwisowej w zakresie przeglądania Zgłoszeń związanych z realizacją Umowy.

5.1.18. Jeżeli Wykonawca stwierdzi, iż nieprawidłowe działanie Systemu, którego dotyczy Zgłoszenie nie jest spowodowane Błędem, za który odpowiedzialny jest Wykonawca, wówczas Wykonawca zobowiązany jest:

5.1.18.1. wskazać przyczynę nieprawidłowego działania poprzez wskazanie elementu, który ją powoduje,

5.1.18.2. udzielić wsparcia Zamawiającemu lub innej osobie trzeciej wskazanej przez Zamawiającego usuwającej przyczyny Zgłoszenia, w tym udzielić takiej osobie wszelkich informacji o Systemie lub Oprogramowaniu potrzebnych do przywrócenia pełnej funkcjonalności.

5.1.19. Po przeprowadzeniu Naprawy, Wykonawca zgłosi ją do odbioru poprzez przekazanie informacji :

5.1.19.1. za pomocą aplikacji serwisowej (interfejsu serwisowego);

5.1.19.2. przez przesłanie pocztą elektroniczną na adres: ……@.....;

5.1.20. Po weryfikacji dokonania Naprawy, przedstawiciel Zamawiającego niezwłocznie potwierdzi w systemie lub drogą elektroniczną skuteczność lub nieskuteczność Naprawy. Data i godzina rejestracji w systemie lub wysłania maila przez przedstawiciela Zamawiającego jest datą i godziną wykonania usługi Naprawy.

5.1.21. W przypadku stwierdzenia dokonania skutecznej Naprawy Wykonawca zamyka Zgłoszenie i potwierdza jego wykonanie poprzez „zamknięcie” zgłoszenia w aplikacji serwisowej.

5.1.22. Naprawa, co do której Wykonawca poinformował o jej wykonaniu, a która została odrzucona przez przedstawiciela Zamawiającego ze względu na fakt, iż testy przeprowadzone przez Zamawiającego wykazują, że Błąd nadal występuje, trwa do czasu jej skutecznego wykonania.

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

5.1.23. Wykonawca zobowiązany jest do prowadzenia ewidencji otwartych i zamkniętych Zgłoszeń, obejmującej w szczególności opis stanu realizacji danej Naprawy. Powyższe dane dostępne są cały czas dla Zamawiającego za pośrednictwem aplikacji serwisowej.

5.1.24. Wraz z dokonaniem Naprawy Wykonawca zobowiązany jest opracować i przekazać Zamawiającemu odpowiednie Dokumenty, o ile zachodzi taka potrzeba.

5.1.25. Jeżeli Wykonawca nie dokona Naprawy Błędu w określonym terminie to Zamawiający może:

5.1.25.1. zawiadamiając uprzednio Wykonawcę usunąć Błąd we własnym zakresie lub powierzyć jej usunięcie innym podmiotom trzecim na ryzyko i koszt Wykonawcy, co nie spowoduje utraty przysługujących Zamawiającemu uprawnień z tytułu Gwarancji– przy czym koszty poniesione przez Zamawiającego przy usunięciu Błędu mogą być potrącone z wynagrodzenia przysługującego Wykonawcy lub z zabezpieczenia należytego wykonania przedmiotu Umowy, na co Wykonawca wyraża zgodę;

5.1.25.2. obciążyć Wykonawcę karą umowną.

5.1.26. Jeżeli w trakcie realizacji zobowiązań z tytułu Gwarancji dojdzie do wprowadzenia zmian w Dokumentach, wówczas do przejścia autorskich praw majątkowych do zmienionych Dokumentów stosuje się odpowiednio postanowienia Umowy, w zakresie Dokumentów będących wynikiem zmian. W zakresie Oprogramowania lub jego dokumentacji, ich producent z chwilą wykonania zobowiązań z tytułu gwarancji udziela licencji na zasadach określonych w Umowie.

5.1.27. W uzasadnionych przypadkach Strony mogą podjąć decyzję o wydłużeniu Czasu Naprawy.

5.2. Warunki Gwarancji dla Oprogramowania

5.2.1. Gwarancją objęta jest całość dostarczonego Oprogramowania.

5.2.2. Wykonawca zapewni elektroniczny dostęp do informacji na temat dostarczonego Oprogramowania oraz biuletynów technicznych, poprawek, aktualizacji, nowych wersji Oprogramowania.

5.2.3. W przypadku Oprogramowania:

5.2.3.1. Wykonawca zapewnia Zamawiającemu dostarczanie aktualizacji, nowych wersji oraz zmian w Oprogramowania/ opracowanych przez producentów w okresie gwarancji. Wykonawca zapewnia, że dostarczane aktualizacje, nowe wersje lub zmiany są produktami wykonanymi przez producenta, a tym samym nie naruszają praw własności intelektualnej oraz że Wykonawca posiada prawo do ich dostarczania osobom trzecim na zasadach określonych w niniejszym załączniku oraz Umowie.

5.2.3.2. Aktualizację Oprogramowania , w szczególności dostarczania i instalacji nowych wersji Oprogramowania systemowego i Oprogramowania, dostarczania i instalacji wersji podwyższonych, wydań uzupełniających oraz poprawek programistycznych, bez dodatkowych opłat licencyjnych;

5.2.3.3. informuje o najlepszych praktykach i zasadach postępowania.

6. Instruktaż dla pracowników Zamawiającego

Wykonawca przeprowadzi instruktaż dla nie więcej niż 10 pracowników Zamawiającego, który przygotuje wskazanych pracowników do samodzielnego konfigurowania Systemu, operowania Systemem z poziomu

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

administratora oraz użytkownika oraz wykorzystywania Systemu skonfigurowanego w specyficznej infrastrukturze Zamawiającego, w szczególności do samodzielnej konfiguracji Systemu.

6.1. Warsztaty szkoleniowe zostaną przeprowadzone [w języku polskim] przez osoby będące trenerami producenta lub Wykonawcy oraz posiadające kwalifikacje i umiejętności potwierdzone certyfikatem producenta oferowanego Systemu.

6.2. Lista uczestników instruktażu zostanie ustalona drogą mailową z Wykonawcą po podpisaniu umowy.

6.3. Instruktaż zostanie zorganizowany w czasie trwania wdrożenia Systemu opisanego w pkt 3.

6.4. Termin przeprowadzenia instruktażu zostanie ustalony pomiędzy Zamawiającym a Wykonawcą.

6.5. Instruktaż będzie realizowany w dni robocze w godzinach 8:00-16:00 w siedzibie Zamawiającego lub zdalnie za zgodą Zamawiającego. Instruktaż może się odbyć w postaci zdalnego spotkania o ile zostaną spełnione wszystkie wymagania instruktażu.

6.6. Instruktaż będzie trwał minimum 4 Dni Robocze (łącznie minimum 32 godzin zegarowych).

6.7. Harmonogramy zajęć zostaną ustalone drogą mailową z Zamawiającym.

6.8. Wykonawca musi posiadać autoryzację producenta Systemu w zakresie prowadzenia instruktażu z wdrożonego u Zamawiającego Systemu.

6.9. Dla uczestników instruktażu Wykonawca przygotuje środowisko testowe z zainstalowaną wersją Systemu tożsamą dla wdrożonego u Zamawiającego Systemu pozwalające na zapoznanie się, z elementami interfejsu graficznego oraz wykonanie ćwiczeń w warunkach możliwie zbliżonych do realnych.

6.10. Wykonawca zapewni dla każdego uczestnika wersję elektroniczną materiałów dydaktycznych zawierających streszczenie/omówienie wszystkich zagadnień zawartych w programie instruktażu oraz prezentacje wykorzystane podczas instruktażu.

6.11. Jeśli na potrzeby realizacji instruktażu powstaną materiały edukacyjne będące utworami w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2019. poz. 1231) będą udostępnione na wolnej licencji zapewniającej licencjobiorcy prawo do dowolnego wykorzystywania utworów do celów komercyjnych i niekomercyjnych, tworzenia i rozpowszechniania kopii utworów w całości lub we fragmentach oraz wprowadzania zmian i rozpowszechniania utworów zależnych.

6.12. Zakres tematyczny instruktażu będzie zawierał się w niniejszych obszarach:

6.12.1. Architektura produktu

6.12.2. Poruszanie się po interfejsie użytkownika

6.12.3. Planowanie wdrożenia systemu wraz z architekturą systemu

6.12.4. Instalacja konsoli zarządzania i agentów na stacjach końcowych

6.12.5. Konfiguracja reguł filtrujących/analizujących dla dedykowanego systemu końcowego.

6.12.6. Wykonanie przykładowych scenariuszy:

6.12.6.1. Konfigurowanie nowych polityk dostępu.

6.12.6.2. Konfigurowanie nowych polityk weryfikacji zgodności stacji końcowych.

6.12.6.3. Konfigurację wysyłania logów do systemu klasy SIEM.

6.12.7. Monitorowanie działania systemu.

6.12.8. Automatyzacja zadań w tym definiowanie alertów w odpowiedzi na wykryte zdarzenia.

6.12.9. Manualne uruchamianie zadań.

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

6.12.10. Analiza i raportowanie wyników.

6.12.11. Konfiguracja zadań/reakcji na zdarzenia.

6.12.12. Zarządzanie użytkownikami i rolami.

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