OPIS PRZEDMIOTU ZAMÓWIENIA

Rozbudowa systemu bezpieczeństwa kont uprzywilejowanych PAM

1. Przedmiot zamówienia obejmuje rozbudowę systemu bezpieczeństwa kont uprzywilejowanych PAM, rozumianą jako :

   1.1. Dostawa 265 licencji wskazanych w pkt 1.3 w modelu subskrypcyjnym na okres **24 lub 36 miesięcy** od dnia podpisania przez Zamawiającego protokołu odbioru tych licencji, jednak nie wcześniej niż od dnia 15.12.2024, wraz ze wsparciem producenta/Wykonawcy – (zamówienie gwarantowane);

   1.2. Dostawa maksymalnie 155 licencji wskazanych pkt 1.3 w modelu subskrypcyjnym na okres **24 lub 36 miesięcy** od dnia podpisania przez Zamawiającego protokołu odbioru tych licencji, wraz ze wsparciem producenta/Wykonawcy - (zamówienie opcjonalne);

   1.3. Zamawiający posiada środowisko systemu bezpieczeństwa kont uprzywilejowanych (PAM), na które składają się następujące licencje:

Lp.	Nazwa licencji	Liczba licencji
1.	Privileged User Subscription PRIV-STANDARD-USER-SUBS	320

   1.4. Zamawiający dopuszcza dostarczenie rozwiązania równoważnego spełniającego wymagania wskazane do Załączniku nr 1 do OPZ.

2. **Termin realizacji:**

   2.1. Dostawa zamówienia gwarantowanego, o którym mowa w pkt 1.1 musi nastąpić w terminie do 10 dni roboczych od zawarcia umowy.

   2.2. Dostawa zamówienia opcjonalnego, o którym mowa w pkt 1.2 musi nastąpić w terminie do 10 dni roboczych od dnia doręczenia Wykonawcy Zlecenia Opcji. Zamawiający może poinformować Wykonawcę o skorzystaniu z prawa opcji w terminie 12 miesięcy od dnia zawarcia Umowy.

3. **Wsparcie producenta/Wykonawcy:**

   3.1. W ramach wsparcia producenta/Wykonawcy wymagany jest:

   3.1.1. Dostęp do aktualizacji oprogramowania;

   3.1.2. Dostęp do nowych wersji oprogramowania oraz poprawek;

   3.1.3. Dostęp do nowych sygnatur bezpieczeństwa;

   3.1.4. Dostęp do bazy wiedzy producenta;

   3.1.5. Wsparcie w implementacji krytycznych poprawek systemu zalecanych przez producenta;

   3.1.6. Wsparcie w aktualizacji systemu do nowych wersji zalecanych przez producenta,

   3.1.7. Cykliczne, nie częściej niż raz na kwartał, przeglądy kwartalne systemu,

   3.1.8. Cykliczne, nie częściej niż dwa razy w roku, testy Disaster Recovery,

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

3.1.9. Cykliczne, nie częściej niż dwa razy w roku, opracowanie dodatkowych procedur i instrukcji oraz ich aktualizacja,

3.1.10. Przyjmowanie i obsługa zgłoszeń problemów w trybie 24/7, przyjmowanie zgłoszeń oraz wsparcie w obsłudze problemów wymagających rozwiązania przez producenta. Czas reakcji Wykonawcy na zgłoszenie to 30 min.

3.1.11. Wskazywanie rozwiązania zastępczego, pozwalającego na zachowanie podstawowej funkcjonalności systemu do czasu przekazania rozwiązania przez producenta.

3.1.12. Przeprowadzenie instruktażu stanowiskowego z dostarczonego oprogramowania obejmującego swoim zakresem:

3.1.12.1. architekturę i przepływy systemu,

3.1.12.2. skuteczne zarządzanie hasłami (weryfikacja, zmiana i uzgadnianie),

3.1.12.3. korzystanie i konfiguracja funkcji automatycznego wykrywania kont i narzędzia do weryfikacji haseł,

3.1.12.4. konfigurowanie izolacji i monitorowania sesji PSM,

3.1.12.5. monitorowanie sesji, przegląd nagranych sesji,

3.1.12.6. omówienie modułu PTA do monitorowania aktywności kont uprzywilejowanych,

3.1.12.7. omówienie komponentu PSMP,

3.1.12.8. konfiguracja polityk,

3.1.12.9. tworzenie raportów na temat działań systemowych i użytkowników,

3.1.12.10. monitorowanie środowiska PAM,

3.1.12.11. wykonywanie typowych zadań administracyjnych,

3.1.12.12. identyfikacja i rozwiązywanie problemów,

3.1.12.13. działania proaktywne,

3.1.12.14. instruktaż będzie przeprowadzony dla 1 grupy dla maksymalnie 10 pracowników Zamawiającego,

3.1.12.15. instruktaż może odbyć się trybie stacjonarnym w Warszawie lub w trybie zdalnym,

3.1.12.16. czas trwania instruktażu to od 4 do 5 dni.

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

Załącznik nr 1 do OPZ

I. Zamawiający dopuszcza zaoferowanie rozwiązania równoważnego do posiadanego przez Zamawiającego oprogramowania PAM:

1. W przypadku dostarczania oprogramowania równoważnego względem wyspecyfikowanego przez Zamawiającego w Opisie przedmiotu zamówienia, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane oprogramowanie spełnia wszystkie wymagania i warunki określone w Opisie przedmiotu zamówienia, w szczególności w zakresie:
   a) warunków licencji/sublicencji w każdym aspekcie licencjonowania/sublicencjonowania, które muszą być identyczne lub rozszerzone, przy czym rozszerzony zakres musi zawierać również wszystkie elementy licencjonowania jak dla posiadanego przez Zamawiającego oprogramowania,
   b) funkcjonalności równoważnej oprogramowania, która nie może być gorsza od funkcjonalności wymienionych w pkt III - „Opis wymaganych minimalnych funkcjonalności w przypadku zaoferowania oprogramowania równoważnego w stosunku do posiadanego oprogramowania**”**
   c) oprogramowanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać z oprogramowaniem PAM funkcjonującym u Zamawiającego,
   d) oprogramowanie równoważne nie może zakłócić pracy środowiska systemowo-programowego Zamawiającego,
   e) oprogramowanie równoważne musi w pełni współpracować z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie,
   f) oprogramowanie równoważne musi zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienność oprogramowania równoważnego z wyspecyfikowanym oprogramowaniem.
2. W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane oprogramowanie.
3. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu oprogramowania równoważnego.
4. Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów używanego i współpracującego z nim oprogramowania u Zamawiającego.
5. Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie

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

oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w Jego nowszych wersjach.

II. W przypadku dostawy oprogramowania równoważnego Wykonawca zobowiązany jest:

1. Przeprowadzić Instruktaż dla 10 administratorów Zamawiającego z zakresu instalacji, konfiguracji i zarządzania oprogramowaniem równoważnym, umożliwiającym pełne poznanie produktu równoważnego. Wykonawca w terminie 1 Dnia Roboczego od dnia zawarcia Umowy przedstawi do zatwierdzenia Zamawiającemu harmonogram Instruktażu.
2. Przeprowadzić Instruktaż dla operatorów Zamawiającego z zakresu użytkowania oprogramowania równoważnego, umożliwiającego pełne poznanie produktu równoważnego.
3. Wykonawca w terminie 1 Dnia Roboczego od dnia zawarcia Umowy przedstawi do zatwierdzenia Zamawiającemu harmonogramy Instruktaży.
4. Instruktaże będą realizowane w Dni Robocze w godzinach 8:00-16:00 w siedzibie Zamawiającego lub w formie zdalnej o ile zostaną spełnione wszystkie wymagania dotyczące Instruktażu. Instruktaż będzie trwał minimum 2 dni robocze każdy (łącznie minimum 14 godzin zegarowych każdy).
5. Zainstalować oprogramowanie równoważne w środowisku systemowo-programowym oraz dokonać poprawnej konfiguracji mechanizmów systemu typu PAM oraz zintegrować się z systemami/aplikacjami wytwarzanymi w ramach działalności Zamawiającego w terminie do 3 dni roboczych od dnia podpisania Umowy.
6. Dostarczyć wszelkie dodatkowe licencje - niezbędne do prawidłowego funkcjonowania oprogramowania równoważnego.

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

1. Licencje subskrypcyjne powinny realizować co najmniej wszystkie funkcjonalności posiadanych przez CeZ licencji PAM wymienionych w ust. 1 przedmiotu zamówienia.
2. Licencje subskrypcyjne muszą realizować dla minimum liczby posiadanych przez CeZ licencji PAM wymienionych w ust. 1 przedmiotu zamówienia jednoczesnych użytkowników:
   2.1. Wieloskładnikowe uwierzytelnienie oraz zabezpieczenie dostępu do kluczowych aplikacji poprzez portal Single Sign-On,
   2.2. Funkcję bezpiecznego, uprzywilejowanego dostępu zdalnego dla pracowników firm zewnętrznych, bez konieczności instalacji rozwiązań klasy VPN (site-2-site lub client-site) po stronie sieci lub stacji roboczej firmy zewnętrznej.
3. System musi posiadać budowę modularną i możliwość rozbudowy w ramach oferowanych licencji subskrypcyjnych z funkcjonalnościami o kolejne komponenty, odpowiedzialne za nie mniej niż:
   3.1. Wieloskładnikowe uwierzytelnienie użytkowników oraz zabezpieczenie dostępu do kluczowych aplikacji Web (wewnętrznych oraz chmurowych) poprzez moduł Single Sign-On.
   3.2. Ochronę dostępu zdalnego dla pracowników i zewnętrznych dostawców.
   3.3. Agentowe ograniczanie uprawnień użytkowników na stacjach Windows / MAC oraz serwerach Windows poprzez usuwanie kont lokalnych administratorów i podnoszenie uprawnień w kontekście konkretnych obiektów (skryptów, aplikacji, instalacji, dll i innych) dla konkretnych

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

użytkowników, kontrolę aplikacyjną oraz blokowanie wycieku poświadczeń (np. haseł) z repozytoriów systemu operacyjnego Windows oraz aplikacji (np. przeglądarek internetowych, pamięci LSASS, SAM i innych).

3.4. Ochronę kont uprzywilejowanych w środowiskach DevOps.

3.5. Ochronę kont uprzywilejowanych zaszytych w kodzie statycznych aplikacji i skryptów.

3.6. Automatyczną klasyfikację ryzyka związanego ze zbyt obszernymi uprawnieniami w środowiskach chmurowych.

3.7. Agentowe ograniczanie dostępu do zbioru poleceń w połączeniach terminalowych do serwerów Linux/Unix (definiowanie centralnej polityki białych/czarnych list wykonywanych poleceń, podnoszenia uprawnień poprzez sudo, rozliczania użytkowników z wykonanych zadań).

3.8. Moduł umożliwiający przechowywanie poświadczeń użytkownika biznesowego w centralnym repozytorium. Poświadczenia zapisane w repozytorium muszą być dostępne dla użytkownika w ramach platformy SSO. Po uwierzytelnieniu w SSO system musi umożliwiać wykorzystanie pluginu w przeglądarce użytkownika na potrzeby automatyzacji procesu zestawiania sesji web (pobranie poświadczeń z repozytorium i auto uzupełnienie ich w ramach sesji web). Plugin musi również posiadać funkcję generatora haseł.

3.9. Moduł rozszerzający funkcję SSO o nie mniej niż nagrywanie aktywności użytkownika w sesjach web, realizowane poprzez zrzuty ekranu wykonywane na poziomie przeglądarki użytkownika inicjowane przez minimum kliknięcia myszą przez użytkownika w sesji web, wykorzystanie przycisku Tab oraz Enter. Oprócz zrzutów ekranu systemu musi również zapisywać metadane powiązane z akcjami wykonanymi przez użytkownika.

4. System musi umożliwiać integrację z mechanizmami wykorzystywanymi do uwierzytelniania użytkowników, minimum hasła, LDAP, Windows NTLM, klucze SSH, Smart card, PKI, RADIUS, SAML, wieloskładnikowe uwierzytelnianie, RSA SecurID, Oracle SSO, Amazon Cognito Authentication, OpenID Connect (OIDC).
5. System musi posiadać skorelowaną ze sobą oficjalną metodykę implementacji, udostępnianą przez producenta systemu na stronie internetowej producenta. Metodyka ta musi zawierać minimum opis kroków, które należy wykonać w celu należytego i kompleksowego zaimplementowania rozwiązania typu PAS, umożliwiającego minimum ochronę dostępów uprzywilejowanych, wdrożenie polityki minimalnych uprawnień na stacjach roboczych i serwerach oraz ochronę kont uprzywilejowanych i danych uwierzytelniających wykorzystywanych przez aplikacje na potrzeby dostępu do innych systemów docelowych (włącznie z ochroną aplikacji wdrożonych w oparciu o metodykę DevOps). Metodyka poprzez analizę ryzyka musi umożliwiać pomoc w klasyfikacji kluczowych typów kont uprzywilejowanych oraz przypisanie ich do kolejnych etapów planowanej implementacji rozwiązania PAS. Metodyka musi być dostępna na oficjalnej stronie producenta na dzień składania ofert, link do oficjalnej strony producenta zawierającej opis metodyki należy dołączyć do oferty.

IV. Zamawiający wymaga wieloskładnikowego uwierzytelnienia oraz zabezpieczenia dostępu do kluczowych aplikacji poprzez portal Single Sign-On

1. System musi realizować funkcję:Wieloskładnikowego adaptacyjnego uwierzytelnienia.

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

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

NIP: 5251575309
REGON: 001377706

1.2. Zabezpieczenia dostępu zarówno do wewnętrznych jak i zewnętrznych (SaaS) aplikacji poprzez wykorzystanie zabezpieczonego portalu SSO.
1.3. Zarządzania cyklem życia tożsamości (ang. lifecycle management, wymagający dodatkowej licencji czasowej)

2. Wymagana jest możliwość obsługi minimum następujących składników uwierzytelniających MFA: hasło, sms, email, oauth, aplikacja mobilna, phone call, pytanie bezpieczeństwa, Qrcode generowany w ramach procesu uwierzytelnienia do interfejsu Systemu, umożliwiający uwierzytelnienie użytkownika przy użyciu aplikacji mobilnej uprzednio zarejestrowanej w systemie.
3. System musi wspierać kontekstowe uwierzytelnianie bazujące na minimum następujących warunkach: adres IP, dzień tygodnia, data, zakres dat, zakres czasu, adaptacyjnie poprzez automatyczną analizę zachowań użytkowników (profilowanie urządzenia, adresu IP, śledzenia zagrożeń poprzez funkcję "Threat Intelligence")
4. Moduł MFA poprzez protokół Radius musi umożliwiać integrację z popularnymi koncentratorami VPN jak minimum Cisco Systems, Palo Alto Networks, Pulse Secure, Fortinet.
5. System musi być dostarczony jako usługa zewnętrzna (SaaS) wraz z modułem umożliwiającym integrację ze środowiskiem usług katalogowych AD/LDAP oraz uruchomienie serwera Radius dla klientów sieciowych Zamawiającego.
6. System musi realizować usługę SSO dla aplikacji chmurowych oraz wewnętrznych, realizując w sposób scentralizowany bezpieczne uwierzytelnienie przy wykorzystaniu metod opisanych w punktach 2.1.2. Musi istnieć możliwość integracji z własnymi aplikacjami poprzez nie mniej niż następujące integracje:
    - plugin do przeglądarki,
    - NTLM,
    - Basic auth,
    - Klient Oauth2,
    - Serwer Oauth2,
    - OpenID Connect,
    - Saml,
    - WS-Fed,
    - Użytkownik - hasło
7. System musi posiadać gotowe integracje SSO z nie mniej niż następującymi aplikacjami: Adobe Sign, Amazon Web Services, Box, Dropbox, NetSuite, Office 365, Salesforce, ServiceNow, Slack, Webex, Zendesk.
8. Dla użytkowników zewnętrznych którzy chcą skorzystać z aplikacji web w centrum danych Zamawiającego System musi posiadać funkcję (dostępną w ramach dodatkowej licencji czasowej) nawiązania bezpiecznego połączenia bez konieczności zestawiania dodatkowych tuneli VPN pomiędzy stacją roboczą a centrum danych (realizować funkcję reverse proxy).
9. Poprzez dodatkowe rozszerzenie licencyjne system musi realizować funkcję MFA wymuszane na chronionych serwerach Windows przy połączeniu uprzywilejowanym realizowanym w oparciu o moduł proxy. W ramach realizacji połączenia uprzywilejowanego moduł proxy musi auto uzupełnić poświadczenia i umożliwić użytkownikowi wpisanie kolejnego składnika MFA. Sesja

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

musi być zestawiana w oparciu o koncepcję izolacji. System musi umożliwiać wymuszenie weryfikacji trzeciego składnika MFA na poziomie aplikacji mobilnej (minimum możliwe do zastosowania: PIN oraz uwierzytelnianie biometryczne).

V. Wymagana ochrona dostępu zdalnego

1. Rozwiązanie musi realizować funkcję bezpiecznego, uprzywilejowanego dostępu zdalnego dla pracowników firm zewnętrznych (zwanego dalej Dostępem Zewnętrznym), bez konieczności instalacji rozwiązań klasy VPN (site-2-site lub client-site) po stronie sieci lub stacji roboczej firmy zewnętrznej.
2. Rozwiązanie nie może wymagać instalowania dodatkowego oprogramowania po stronie stacji roboczej użytkownika zewnętrznego poza przeglądarką internetową (wsparcie dla nie mniej niż przeglądarki Chrome, Internet Explorer, Edge, Firefox).
3. Proponowane rozwiązanie musi posiadać architekturę pozwalającą na zestawienie połączenia szyfrowanego pomiędzy stacją roboczą zewnętrznego dostawcy a siecią Zamawiającego bez konieczności otwierania ruchu przychodzącego do sieci Zamawiającego. W celu realizacji niniejszego punktu Rozwiązanie musi posiadać w swojej architekturze aplikację klasy SaaS (wymagane jest oferowanie przez Dostawcę aplikacji SaaS w rejonie Unii Europejskiej), do której z jednej strony zestawiany będzie ruch firm zewnętrznych, z drugiej zestawiane będzie bezpieczne połączenie z sieci Zamawiającego. Oprócz zwiększenia poziomu bezpieczeństwa Dostępu Zewnętrznego aplikacja musi realizować funkcję nadawania dostępu dla firm zewnętrznych, dzięki czemu Zamawiający będzie w stanie w trybie natychmiastowym (ang. Just-in-Time Provisioning) generować, akceptować i automatycznie wysyłać na podany podczas rejestracji adres e-mail wiadomości z zaproszeniem do zestawienia Dostępu Zewnętrznego. Aplikacja powinna umożliwiać zarządzanie utworzonymi użytkownikami (tworzenie nowych zaproszeń, nadawanie uprawnień, wyłączanie kont). Dostęp do aplikacji musi być możliwy poprzez wykorzystanie uwierzytelnienia biometrycznego, bez konieczności podawania danych dostępowych użytkownika (jak jego nazwa czy hasło).
4. Rozwiązanie musi obsługiwać uniwersalne uwierzytelnienie biometryczne (bez konieczności wpisywania przed zestawieniem połączenia danych dostępowych, jak użytkownik - hasło) realizowane przy użyciu stosowanych powszechnie urządzeń klasy smartphone.
5. Rozwiązanie musi posiadać wsparcie dla następujących platform mobilnych: IOS od wersji 10, Android od wersji 6.0. Dane biometryczne wykorzystywane do uwierzytelnienia składowane muszą być wyłącznie w modułach Secure Enclave / Trusted Execution Environment.
6. Oprócz realizacji funkcji uwierzytelnienia biometrycznego aplikacja mobilna Rozwiązania musi posiadać funkcję potwierdzenia tożsamości dla kluczowych operacji realizowanych przez aplikację SaaS, np. nadawanie uprawnień administracyjnych innym użytkownikom.
7. W celu obsłużenia całości ruchu uprzywilejowanego do sieci Zamawiającego przez przeglądarkę internetową. Rozwiązanie musi posiadać wsparcie tunelowania sesji graficznych RDP przy użyciu HTML5 oraz protokołu SDP.
8. Rozwiązanie musi wspierać transfer plików w trakcie trwania sesji graficznej
9. Rozwiązanie musi posiadać interfejs REST API do automatyzacji procesu zarządzania użytkownikami.

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. Rozwiązanie musi wspierać konfigurację dla wielu instytucji, zarówno od strony Zamawiającego jak i zewnętrznych dostawców (Zamawiający może zarządzać dostępami wielu dostawców, dostawca potrzebuje wyłącznie jednej aplikacji na urządzeniu mobilnym by dostawać się do wielu Klientów, jeśli korzystają z tego samego rozwiązania)
11. Aplikacja mobilna Rozwiązania musi posiadać funkcję zapraszania innych użytkowników. Proces ten musi umożliwiać automatyczne założenie tożsamości użytkownika zewnętrznego w systemie PAS.

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

VI. Wdrożenie i wsparcie Wykonawcy

1. Analiza wymagań, analiza środowiska, opracowanie koncepcji systemu i projektu przedwdrożeniowego:
   1.1. Przeprowadzenie warsztatu technologicznego.
   1.2. Przeprowadzenie analizy potrzeb Zamawiającego.
   1.3. Przeprowadzenie analizy środowiska Zamawiającego.
   1.4. Opracowanie architektury systemu.
   1.5. Przygotowanie dokumentacji.
2. Przygotowanie środowiska pod system, instalacja komponentów PAS, konfiguracja bazowa i integracja z systemami współdziałającymi
   2.1. Przygotowanie lub modyfikacja posiadanego przez Zamawiającego środowiska,
   2.2. Instalacja komponentów system,
   2.3. Integracja systemu z systemami współdziałającymi (AD, FreeIPA, syslog, SIEM, SMTP),
   2.4. Opracowanie docelowej listy zasobów, które będą wprowadzane do systemu,
3. Konfiguracja kont, wciąganie zasobów do systemu
   3.1. Opracowanie struktury logicznej.
   3.2. Przygotowanie przez Zamawiającego listy kont i haseł.
   3.3. Przedstawienie listy wymaganych dostępów pomiędzy komponentami systemu a systemami docelowymi, które ma obejmować rozwiązanie.
   3.4. Przeprowadzenie konfiguracji na systemie PAS w zakresie wciągania kont do systemu.
   3.5. Przeprowadzenie konfiguracji na systemie PAS w zakresie zarządzania hasłami do kont objętych systemem.
   3.6. Przeprowadzenie konfiguracji na systemie w zakresie nagrywania sesji dla w/w kont.
   3.7. Konfiguracja MFA i SSO na potrzeby logowania do systemu.
   3.8. Konfiguracja modułu zdalnego dostępu dla wskazanych administratorów.
   3.9. Konfiguracja systemu wykrywania anomalii w sesjach uprzywilejowanych dla 5 przykładowych definicji incydentów.
4. Dokumentacja powykonawcza i procedury administracyjne i utrzymaniowe:
   4.1. Wspólne opracowanie i przygotowanie scenariuszy testów akceptacyjnych.
   4.2. Przeprowadzenie testów.
   4.3. Opracowanie planów i procedur odtworzenia systemu w przypadku częściowej lub całkowitej awarii systemu.
   4.4. Wspólne wykonanie testów dla procedur odtworzeniowych na systemie.
   4.5. Opracowanie dokumentacji powykonawczej dla wdrożonego system.
   4.6. Opracowanie procedur administracyjnych i utrzymaniowych dla wypracowanego standardu konfiguracji kont i ich utrzymania w systemie.
   4.7. Opracowanie dokumentacji i procedur realizacji zdalnego dostępu użytkowników.
5. Instruktaż z zakresu obsługi i utrzymania systemu:
   5.1. Opracowanie scenariuszy warsztatowych wg wymagań Zamawiającego.
   5.2. Przygotowanie środowiska i systemów (zasobów) do realizacji.
   5.3. Przeprowadzenie instruktażu autorskiego z administratorami. Przykładowy zakres instruktażu:

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

5.3.1. Ogólny opis architektury, scenariusze instalacji i wdrożenia,
5.3.2. Konfigurowanie i administracja,
5.3.3. Monitorowanie,
5.3.4. Zarządzanie uprawnieniami,
5.3.5. Diagnostyka problemów.

6. Instruktaż z zakresu obsługi systemu dla użytkowników
6.1. Opracowanie scenariuszy warsztatowych wg wymagań Zamawiającego,
6.2. Przygotowanie środowiska i systemów (zasobów) do realizacji warsztatu,
6.3. Przeprowadzenie instruktażu autorskiego z użytkownikami wewnętrznymi oraz zewnętrznymi. Przykładowy zakres instruktażu:
6.3.1. Wprowadzenie do koncepcji systemu,
6.3.2. Dostęp do systemu,
6.3.3. Omówienie interfejsu użytkownika,
6.3.4. Praktyczne wykorzystanie systemu PAM do realizacji dostępu do zasobów chronionych,
6.3.5. Rozwiązywanie problemów
6.3.6. Przygotowanie nagrania (w formie pliku avi) z instruktaży dla użytkowników wewnętrznych i zewnętrznych na potrzeby późniejszego wykorzystania przez Zamawiającego

7. Wsparcie zamawiającego
7.1. Konsultacje w zakresie czynności, związanych z eksploatacją w liczbie roboczogodzin niezbędnej do uruchomienia funkcjonalności oprogramowania. W ramach konsultacji możliwe jest zlecanie m.in takich prac jak.:
7.1.1. implementacja krytycznych poprawek systemu zalecanych przez producenta
7.1.2. aktualizacja systemu do nowych wersji zalecanych przez producenta,
7.1.3. cykliczne, nie częściej niż raz na kwartał, przeglądy kwartalne systemu,
7.1.4. cykliczne, nie częściej niż dwa razy w roku, testy Disaster Recovery,
7.1.5. cykliczne, nie częściej niż dwa razy w roku, opracowanie dodatkowych procedur i instrukcji oraz ich aktualizacja,
7.2. Przyjmowanie i obsługa zgłoszeń problemów: 24 godziny na dobę, 7 dni w tygodniu przyjmowanie zgłoszeń problemów oraz zgłaszanie problemów wymagających rozwiązania przez producenta, w ramach wykupionego przez Klienta wsparcia producenta. Czas reakcji Wykonawcy na zgłoszenie to 30 min,
7.3. Wskazywanie rozwiązania zastępczego, pozwalającego na zachowanie podstawowej funkcjonalności systemu do czasu przekazania rozwiązania przez producenta.

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