Załącznik nr 1 do Zapytania

38066

OPIS PRZEDMIOTU ZAMÓWIENIA

Migracja licencji systemu bezpieczeństwa kont uprzywilejowanych (PAM) posiadanych przez Centrum e-Zdrowia (CeZ) oraz zakup 24 miesięcznego wsparcia.

1. Przedmiotem Zamówienia jest:

1.1. Migracja licencji systemu bezpieczeństwa CyberArk kont uprzywilejowanych (PAM) posiadanych przez Centrum e-Zdrowia do licencji subskrypcyjnych CyberArk lub rozwiązanie równoważne [1] na okres 24 miesięcy wraz z wsparciem producenta.

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

Nazwa Licencji	**Ilość**
EPVUser - Enterprise Password Vault End User EPV User	265
AIMAccount - Application Account	100
CPM - Central Policy Manager	5
PVWA - Password Vault Web Access	5
PSMHTML5Gateway - Privileged Session Manager HTML5 Gateway	10
PSM - Privileged Session Manager	5
AppProvider - Application Password Provider	10
OPMProvider - On-demand Privileges Manager Provider	2
PSMPADBridge - Privileged Session Manager SSH Proxy AdBridge	5
PSMPServer - Privileged Session Manager SSH Proxy	5
DR_Fallback - DR Fallback user type	2
ENE - Event Notification engine user	1
PTA - Privileged Threat Analytics	10
Telemetry - Telemetry Tool Application User	5
Idadaptive - CyberArk SaaS Integration User Type for Idaptive application	3
DiscoveryApp - Discovery Mangement Service Application User	20
xRayAdminApp - An Application User for CyberArk xRay Software	3
PSMWeb - A PSM for Web Dedicated User Type Used for Managing Privileged Session	100
EPM User - An EPM Integration User	5
DAP Service - An Application User For CyberArk AAM Backend Service	20
PSMForServers - PSM For Servers Count	99999

1.3. Licencje subskrypcyjne powinny być w liczbie nie mniejszej niż 265 oraz realizować co najmniej wszystkie funkcjonalności posiadanych przez CeZ licencji PAM wymienionych w pkt. 1.2.

[1] Przez rozwiązanie równoważne Zamawiający rozumie dostawę subskrypcji oprogramowania o funkcjonalnościach opisanych poniżej

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

1.4. Dodatkowo licencje subskrypcyjne muszą realizować dla minimum 265 jednoczesnych użytkowników:
   1.4.1. wieloskładnikowe uwierzytelnienie oraz zabezpieczenie dostępu do kluczowych aplikacji poprzez portal Single Sign-On,
   1.4.2. 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.
1.5. System musi posiadać budowę modularną i możliwość rozbudowy w ramach oferowanych licencji subskrypcyjnych z funkcjonalnościami o kolejne komponenty, odpowiedzialne za nie mniej niż:
   1.5.1. wieloskładnikowe uwierzytelnienie użytkowników oraz zabezpieczenie dostępu do kluczowych aplikacji Web (wewnętrznych oraz chmurowych) poprzez moduł Single Sign-On
   1.5.2. ochronę dostępu zdalnego dla pracowników i zewnętrznych dostawców
   1.5.3. 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 użytkowników, kontrolę aplikacyjną oraz blokowanie wycieku poświadczeń (np. haseł) z repozytoriów systemu operacyjnego Windows oraz aplikacji (np. przeglądarek internetowych, pamięci LSASS, SAM i innych)
   1.5.4. ochronę kont uprzywilejowanych w środowiskach DevOps
   1.5.5. ochronę kont uprzywilejowanych zaszytych w kodzie statycznych aplikacji i skryptów
   1.5.6. automatyczną klasyfikację ryzyka związanego ze zbyt obszernymi uprawnieniami w środowiskach chmurowych
   1.5.7. 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)
   1.5.8. moduł umożliwiający przechowywanie poświadczeń użytkownika biznesowego w centralnym repozytorium opisanym w punkcie 1.39. 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,
   1.5.9. 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
1.6. 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),
1.7. System musi posiadać skorelowaną ze sobą oficjalną metodykę implementacji, udostępnianą przez producenta systemu na stronie internetowej producenta. Metodyka ta musi zawierać

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

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.

2. **W ramach migracji Zamawiający wymaga wieloskładnikowego uwierzytelnienia oraz zabezpieczenia dostępu do kluczowych aplikacji poprzez portal Single Sign-On**

2.1.1. System musi realizować funkcję:

2.1.1.1. wieloskładnikowego adaptacyjnego uwierzytelnienia,

2.1.1.2. zabezpieczenia dostępu zarówno do wewnętrznych jak i zewnętrznych (SaaS) aplikacji poprzez wykorzystanie zabezpieczonego portalu SSO

2.1.1.3. zarządzania cyklem życia tożsamości (ang. lifecycle management, wymagający dodatkowej licencji czasowej)

2.1.2. 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.

2.1.3. 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")

2.1.4. Moduł MFA poprzez protokół Radius musi umożliwiać integrację z popularnymi koncentratorami VPN jak minimum Cisco Systems, Palo Alto Networks, Pulse Secure, Fortinet.

2.1.5. 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.

2.1.6. …System musi realizować usługę SSO dla aplikacji chmurowych oraz wewnętrznych, realizując w sposób scentralizowany bezpieczne uwierzytelnienie przy wykorzystaniu metod opisanych w punktach 2.02 oraz 2.03. 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

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

- Saml
- WS-Fed
- Użytkownik - hasło

2.1.7. 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.

2.1.8. 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).

2.1.9. Poprzez dodatkowe rozszerzenie licencyjne system musi realizować funkcję MFA wymuszane na chronionych serwerach Windows przy połączeniu uprzywilejowanym realizowanym w oparciu o moduł proxy opisany w punkcie 1.15. W ramach realizacji połączenia uprzywilejowanego moduł proxy musi auto uzupełnić poświadczenia i umożliwić użytkownikowi wpisanie kolejnego składnika MFA. Sesja musi być zestawiana w oparciu o koncepcję izolacji opisaną w punkcie 1.15. System musi umożliwiać wymuszenie weryfikacji trzeciego składnika MFA na poziomie aplikacji mobilnej (minimum możliwe do zastosowania: PIN oraz uwierzytelnianie biometryczne).

3. **Wymagana ochrona dostępu zdalnego,**

3.1. 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.

3.2. 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).

3.3. 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).

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

3.4. 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.

3.5. 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.

3.6. 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.

3.7. 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.

3.8. Rozwiązanie musi wspierać transfer plików w trakcie trwania sesji graficznej

3.9. Rozwiązanie musi posiadać interfejs REST API do automatyzacji procesu zarządzania użytkownikami.

3.10. 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)

3.11. Aplikacja mobilna Rozwiązania musi posiadać funkcję zapraszania innych użytkowników. Proces ten musi umożliwiać automatyczne założenie tożsamości użytkownika zewnętrznego w systemie PAS.

4. Usługi wsparcia

4.1. W ramach świadczenia wsparcia wymagana jest:

4.1.1. analiza wymagań, analiza środowiska, opracowanie koncepcji systemu i projektu przedwdrożeniowego:

4.1.1.1. Przeprowadzenie warsztatu technologicznego.

4.1.1.2. Przeprowadzenie analizy potrzeb Zamawiającego.

4.1.1.3. Przeprowadzenie analizy środowiska Zamawiającego.

4.1.1.4. Opracowanie architektury systemu.

4.1.1.5. Przygotowanie dokumentacji.

4.1.2. przygotowanie środowiska pod system, instalacja komponentów PAS, konfiguracja bazowa i integracja z systemami współdziałającymi

4.1.2.1. Przygotowanie lub modyfikacja posiadanego przez Zamawiającego środowiska,

4.1.2.2. Instalacja komponentów system,

4.1.2.3. Integracja systemu z systemami współdziałającymi (AD, syslog, SIEM, SMTP),

4.1.2.4. Opracowanie docelowej listy zasobów, które będą wprowadzane do systemu,

4.1.3. konfiguracja kont, wciąganie zasobów do systemu

4.1.3.1. Opracowanie struktury logicznej,

4.1.3.2. Przygotowanie przez Zamawiającego listy kont i haseł,

4.1.3.3. Przedstawienie listy wymaganych dostępów pomiędzy komponentami systemu a systemami docelowymi, które ma obejmować rozwiązanie,

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

4.1.3.4. Przeprowadzenie konfiguracji na systemie PAS w zakresie wciągania kont do systemu,

4.1.3.5. Przeprowadzenie konfiguracji na systemie PAS w zakresie zarządzania hasłami do kont objętych systemem,

4.1.3.6. Przeprowadzenie konfiguracji na systemie w zakresie nagrywania sesji dla w/w kont,

4.1.3.7. Konfiguracja MFA i SSO na potrzeby logowania do systemu,

4.1.3.8. Konfiguracja modułu zdalnego dostępu dla wskazanych administratorów.

4.1.3.9. Konfiguracja systemu wykrywania anomalii w sesjach uprzywilejowanych dla 5 przykładowych definicji incydentów;

4.1.4. dokumentacja powykonawcza i procedury administracyjne i utrzymaniowe:

4.1.4.1. Wspólne opracowanie i przygotowanie scenariuszy testów akceptacyjnych,

4.1.4.2. Przeprowadzenie testów,

4.1.4.3. Opracowanie planów i procedur odtworzenia systemu w przypadku częściowej lub całkowitej awarii systemu,

4.1.4.4. Wspólne wykonanie testów dla procedur odtworzeniowych na systemie,

4.1.4.5. Opracowanie dokumentacji powykonawczej dla wdrożonego system,

4.1.4.6. Opracowanie procedur administracyjnych i utrzymaniowych dla wypracowanego standardu konfiguracji kont i ich utrzymania w systemie.

4.1.4.7. Opracowanie dokumentacji i procedur realizacji zdalnego dostępu użytkowników

4.1.5. szkolenie z zakresu obsługi i utrzymania system:

4.1.5.1. Opracowanie scenariuszy warsztatowych wg wymagań Zamawiającego,

4.1.5.2. Przygotowanie środowiska i systemów (zasobów) do realizacji,

4.1.5.3. Przeprowadzenie szkolenia autorskiego z administratorami. Przykładowy zakres szkolenia:

4.1.5.3.1. Ogólny opis architektury, scenariusze instalacji i wdrożenia,

4.1.5.3.2. Konfiguraowania i adminsitracja,

4.1.5.3.3. Monitorownaie,

4.1.5.3.4. Zarządzanie uprawnieniami,

4.1.5.3.5. Diagnostyka problemów.

4.1.6. szkolenie z zakresu obsługi systemu dla użytkowników

4.1.6.1. Opracowanie scenariuszy warsztatowych wg wymagań Zamawiającego,

4.1.6.2. Przygotowanie środowiska i systemów (zasobów) do realizacji warsztatu,

4.1.6.3. Przeprowadzenie szkolenia autorskiego z użytkownikami wewnętrznymi oraz zewnętrznymi. Przykładowy zakres szkolenia:

4.1.6.3.1. Wprowadzenie do koncepcji systemu,

4.1.6.3.2. Dostęp do systemu,

4.1.6.3.3. Omówienie interfejsu użytkownika,

4.1.6.3.4. Praktyczne wykorzystanie systemu PAM do realizacji dostępu do zasobów chronionych,

4.1.6.3.5. Rozwiązywanie problemów

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

4.1.6.3.6. Przygotowanie nagrania (w formie pliku avi) ze szkolenia dla użytkowników wewnętrznych i zewnętrznych na potrzeby późniejszego wykorzystania przez Zamawiającego

4.1.7. Wymagane usługi profesjonalne rozwoju systemu. W ramach migracji Zamawiający wymaga usług konsultacji w ramach puli dni rozwojowych w zakresie czynności, związanych z eksploatacją oraz rozwojem systemu. W ramach konsultacji możliwe jest zlecanie m.in takich prac jak.:

4.1.7.1. implementacja krytycznych poprawek systemu zalecanych przez producenta

4.1.7.2. aktualizacja systemu do nowych wersji zalecanych przez producenta,

4.1.7.3. cykliczne, nie częściej niż raz na kwartał, przeglądy kwartalne systemu,

4.1.7.4. cykliczne, nie częściej niż dwa razy w roku, testy Disaster Recovery,

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

4.1.7.6. zgłaszanie problemów wymagających rozwiązania przez producenta, w ramach wykupionego przez Klienta wsparcia producenta,

4.1.7.7. wskazanie rozwiązania zastępczego, pozwalającego na zachowanie podstawowej funkcjonalności systemu do czasu przekazania rozwiązania przez producenta.

5. **Oczekiwany termin dostarczenia Systemu:**

Wykonawca dostarczy Zamawiającemu Przedmiot Zamówienia w terminie nie dłuższym niż 15 dni roboczych od dnia podpisania 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