Załącznik nr 1 – Opis przedmiotu zamówienia do Umowy nr UM.IN.271.84.2024 CRU …./2024

1. W ramach przedmiotowego postępowania wymagane jest dostarczenie licencji czasowych na okres 12 miesięcy produktu **MenageEngine Privileged AccessManager 360** dla 15 administratorów oraz 25 kluczy w następującym zakresie funkcjonalnym **:**

   1) Baza danych :

      - System obsługuje PostgreSQL jako instancje do przechowywania danych i działa na pojedynczej bazie danych.

   2) Zarządzanie hasłami :

      - System posiada centralne repozytorium haseł z możliwością definiowania właścicieli haseł i poziomów dostępu.
      - System posiada zdalny reset haseł dla różnych systemów operacyjnych (Windows, Linux, Unix) oraz baz danych (Oracle, MySQL).
      - System posiada funkcje polityki haseł obejmujące długość, wymuszanie specjalnych znaków, ograniczenia użycia loginu.

   3) Zdalne sesje :

      - System umożliwia logowania z przeglądarek wspierających protokół HTML5 dla sesji RDP, VNC, SQL, SSH i Telnet, bez potrzeby instalowania agentów.
      - System pozwala na tunelowanie sesji przez serwer zarządzania hasłami, bez bezpośredniego kontaktu z docelowym urządzeniem.

   4) Certyfikaty :

      - System daje możliwość zarządzania certyfikatami SSL, w tym ich skanowanie, odnawianie oraz przypisywanie do grup i użytkowników.
      - System integruje się z dostawcami certyfikatów, w tym wsparcie dla certyfikatów Wildcard.

   5) Funkcje bezpieczeństwa :

      - System posiada dwupoziomową autentykacja z wykorzystaniem narzędzi takich jak Google Authenticator, RSA SecurID czy YubiKey.
      - System śledzi i nagrywa sesje użytkowników z możliwością przerwania przez administratora.

   6) Integracje :

      - System integruje się z systemami zarządzania kolejkami zgłoszeń.
      - System współpracuje z platformami CI/CD oraz systemami SIEM .

   7) Dodatkowe funkcjonalności :

      - System obsługuje API REST, z możliwością generowania zapytań do systemu w celu pozyskania haseł.
      - System wspiera SCIM 2.0 (System for Cross-domain Identity Management), co pozwala na wymianę danych użytkowników między dostawcami tożsamości a PAM360.
      - System integruje się z Kubernetes i DevOps.

2. Usługi gwarancyjne/Wsparcie :

1) System musi być dostarczony wraz z usługą wsparcia technicznego.
2) Wsparcie techniczne musi uwzględniać rozwiązywanie problemów z dostępem do platformy, błędów działania oraz wydajności w następującym zakresie czasowym:

Priorytet	Czas podjęcia	Czas na rozwiązanie
Błąd krytyczny	Do 1 godziny dnia roboczego	Do 8 godzin dnia roboczego
Błąd istotny	Do 1 godziny dania roboczego	Do 5 dni roboczych

Przy czym:

- Błąd krytyczny to błąd, który uniemożliwia korzystanie z Systemu.
- Błąd istotny to błąd, inny niż błąd krytyczny, w szczególności taki błąd, który ma niewielki bezpośredni wpływ na działanie i bezpieczeństwo Systemu, a wszystkie podstawowe funkcjonalności są zachowane.
- Czas na rozwiązanie to czas od momentu zgłoszenia błędu do momentu wprowadzenia poprawek przywracających prawidłowe, bezbłędne korzystanie z Systemu.
- Czas podjęcia okres od momentu zgłoszenia błędu do momentu podjęcia pierwszych czynności diagnostycznych przez Wykonawcę.

3) Usługa konsultacji 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:
    - implementacja krytycznych poprawek systemu zalecanych przez producenta
    - aktualizacja systemu do nowych wersji zalecanych przez producenta,
    - cykliczne, nie częściej niż raz na pół roku, przeglądy kwartalne systemu,
    - przyjmowanie i obsługa zgłoszeń problemów: w godzinach od 08.00 – 16.00, 5 dni w tygodniu przyjmowanie zgłoszeń problemów oraz zgłaszanie problemów wymagających rozwiązania przez producenta. Czas reakcji Wykonawcy na zgłoszenie to 1 godzina.
4) Usługa wsparcia w ramach usuwania musi być dostępna z możliwością zgłaszania problemów za pomocą telefonu, wiadomości e-mail lub dedykowanego portalu www.
5) Wsparcie musi zapewniać dostęp do bazy wiedzy producenta oraz materiałów szkoleniowych producenta.
6) W ramach usługi wsparcia wymaga się od Wykonawcy wsparcia w zakresie dostosowywania zasad i najlepszych praktyk, przypadków użycia oraz architektury rozwiązania
7) Wykonawca w zakresie dostarczonych licencji czasowych wykona prace wdrożenia referencyjnego obejmującego implementację zdalnego dostępu przy pomocy kont domenowych lub lokalnych do:
    - Serwerów Windows w ilości nie mniejszej niż 5 i nie większej niż 25 systemów.
    - Serwerów Linux w ilości nie mniejszej niż 5 i nie większej niż 25 systemów.
    - Aplikacji Web opartych o HTML5 w ilości nie mniejszej niż 2 i nie większej niż 5 systemów.
    - Dostęp do aplikacji typu. „gruby klient” za pomocą RemoteApp.

3. Instruktaż dla pracowników Zamawiającego:

- Wykonawca przeprowadzi dla pracowników Zamawiającego instruktaż, który przygotuje wskazanych pracowników do samodzielnej pracy na Systemie, operowania Systemem z poziomu

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

- Lista uczestników instruktażu zostanie ustalona drogą mailową z Wykonawcą po podpisaniu umowy.
- Instruktaż zostanie zorganizowany w czasie trwania wdrożenia Systemu.
- Termin przeprowadzenia instruktażu zostanie ustalony pomiędzy Zamawiającym a Wykonawcą drogą mailową.
- 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.
- Instruktaż będzie trwał łącznie minimum 4 godziny zegarowe. Przy czym Zamawiający dopuszcza możliwość realizacji szkolenia w ramach cyklicznych warsztatów.
- Harmonogramy zajęć zostaną ustalone drogą mailową z Zamawiającym.
- Zakres tematyczny instruktażu będzie zawierał się w niniejszych obszarach:
  1) Architektura produktu
  2) Poruszanie się po interfejsie użytkownika
  3) Planowanie wdrożenia systemu wraz z architekturą systemu
  4) Instalacja konsoli zarządzania
  5) Tworzenie kont użytkowników uprzywilejowanych, definiowanie ról oraz przydzielanie poziomów dostępu.
  6) Praktyczne przykłady zarządzania politykami haseł, resetów oraz uprawnień.
  7) Szkolenie z konfiguracji oraz zarządzania zdalnymi sesjami dla protokołów RDP, SSH, VNC, Telnet oraz SQL.
  8) Obsługa RemoteApp, umożliwiająca bezpośrednie łączenie z aplikacjami systemu Windows z poziomu zdalnej konsoli.
  9) Monitorowanie aktywnych sesji z możliwością ich przerywania przez administratora, tzw. session shadowing, oraz nagrywanie sesji do późniejszego przeglądu.
  10) Zarządzanie certyfikatami i kluczami:
  11) Pełne zarządzanie cyklem życia certyfikatów SSL, w tym importowanie, odnawianie oraz skanowanie pod kątem podatności.
  12) Zarządzanie kluczami SSH, tworzenie, przypisywanie i usuwanie kluczy.
  13) Szkolenie z narzędzi do monitorowania i audytowania działań użytkowników oraz operacji na systemie.
  14) Generowanie raportów dotyczących sesji, haseł, zgodności polityk oraz interakcji z systemem.
  15) Wykorzystanie integracji z systemami SIEM do automatyzacji i monitorowania incydentów bezpieczeństwa.
  16) Konfiguracja RemoteApp, umożliwiająca bezpośrednie uruchamianie aplikacji Windows na zdalnych urządzeniach z poziomu scentralizowanej konsoli.
  17) Zarządzanie dostępem oraz kontrolą do uprzywilejowanych aplikacji przez administratorów i użytkowników.
  18) Włączanie oraz wyłączanie systemu w trakcie prac konserwacyjnych.