SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa, wdrożenie i uruchomienie systemu klasy Privileged Access Management (PAM)

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, wdrożenie i uruchomienie systemu klasy Privileged Access Management (PAM) wraz ze wsparciem technicznym producenta na okres **12 miesięcy**.

2. Zakres zamówienia

- Dostawa systemu klasy Privileged Access Management (PAM) umożliwiającego:
  - kontrolę dostępu uprzywilejowanego,
  - monitorowanie i rejestrowanie sesji administracyjnych,
  - analizę ryzyka działań administratorów,
  - zarządzanie poświadczeniami uprzywilejowanymi,
  - integrację z istniejącą infrastrukturą IT Zamawiającego,
  - obsługę minimum 150 zarządzanych zasobów(serwerów, urządzeń sieciowych, lub innych systemów objętych ochroną PAM),
  - obsługę minimum 50 jednoczesnych sesji.

- Wdrożenie, instalację i konfigurację systemu.
- Konfigurację raportów, alertów, retencji, archiwizacji, ról dostępowych, uwierzytelniania wieloskładnikowego.
- Przeprowadzenie warsztatów powdrożeniowych dla administratorów i operatorów obejmujących wszystkie elementy systemu.
- Opracowanie i przekazanie dokumentacji powykonawczej.
- Wsparcie techniczne producenta na okres **minimum 12 miesięcy**.

3. Warunki licencyjne

- Licencja musi mieć charakter bezterminowy, zwany również licencją wieczystą.
- Wykonawca musi dostarczyć wszystkie licencje, subskrypcje, dodatki, konektory, instancje zapasowe i inne prawa niezbędne do realizacji całego zakresu funkcjonalnego oprogramowania.
- Po zakończeniu okresu wsparcia technicznego Zamawiający musi zachować prawo do bezterminowego korzystania z ostatniej wersji oprogramowania, do której uzyskał uprawnienia w okresie obowiązywania wsparcia.
- Wygaśnięcie lub nieprzedłużenie wsparcia technicznego nie może powodować zablokowania oprogramowania, ograniczenia wcześniej nabytej funkcjonalności, utraty dostępu do zgromadzonych danych, uniemożliwienia generowania raportów z wcześniej zgromadzonych danych, przejścia oprogramowania do wersji bezpłatnej, demonstracyjnej albo wersji o ograniczonej funkcjonalności ani obowiązku ponownego zakupu licencji podstawowej.
- Licencja musi umożliwiać użytkowanie oprogramowania na potrzeby wewnętrzne Zamawiającego, zgodnie z zakresem ilościowym wskazanym w dokumentach zamówienia.
- Licencja nie może być uzależniona od cyklicznego uiszczania opłat subskrypcyjnych warunkujących dalsze działanie podstawowej funkcjonalności oprogramowania.
- Zamawiający musi posiadać możliwość przeniesienia instalacji oprogramowania na inny serwer lub środowisko w ramach tej samej jednostki organizacyjnej, w szczególności w przypadku wymiany sprzętu, awarii, migracji, odtworzenia środowiska albo zmiany architektury technicznej.

- Licencja musi pochodzić z legalnego i autoryzowanego kanału dystrybucji oraz umożliwiać Zamawiającemu korzystanie ze wsparcia technicznego producenta.

4. Wymagania dotyczące bezpieczeństwa

- System musi umożliwiać pracę z zastosowaniem zasady minimalnych niezbędnych uprawnień.
- Wykonawca musi dostarczyć dokumentację zawierającą wykaz uprawnień wymaganych do działania oprogramowania.
- Konsola musi działać z użyciem HTTPS. Wykonawca skonfiguruje certyfikat wskazany przez Zamawiającego i wyłączy nieszyfrowany dostęp HTTP, jeżeli pozwala na to architektura.
- System musi umożliwiać wymuszenie TLS 1.2 lub nowszego dla konsoli webowej i integracji, w zakresie wspieranym przez komponenty.
- Komunikacja katalogowa musi umożliwiać użycie LDAPS.
- System musi obsługiwać uwierzytelnianie kontami Active Directory oraz kontami lokalnymi systemu.
- System musi obsługiwać uwierzytelnianie wieloskładnikowe przy użyciu co najmniej jednego standardowego mechanizmu: TOTP, RADIUS, dostawca tożsamości, e-mail albo SMS.
- System musi posiadać kontrolę dostępu opartą na rolach, umożliwiającą rozdzielenie co najmniej roli administratora i operatora lub audytora.
- System musi umożliwiać tworzenie niestandardowych ról albo ograniczanie dostępu do raportów, funkcji administracyjnych.
- System musi audytować działania administratorów i techników systemu.
- Hasła i sekrety przechowywane przez system muszą być chronione silnym mechanizmem kryptograficznym, co najmniej AES-256 lub rozwiązaniem zapewniającym równoważny poziom bezpieczeństwa.
- System nie może wymagać przekazywania danych audytowych poza infrastrukturę Zamawiającego.
- System musi umożliwiać aktualizację do wersji usuwających ujawnione podatności bezpieczeństwa przez cały okres obowiązywania wsparcia technicznego.
- Producent musi publikować informacje o aktualizacjach, poprawkach lub nowych wersjach oprogramowania.
- System musi być dostarczony w aktualnej, stabilnej i wspieranej przez producenta wersji, przeznaczonej do użytkowania produkcyjnego.
- System nie może być wersją demonstracyjną, testową, czasową, edukacyjną, nieprzeznaczoną do zastosowań produkcyjnych ani wersją o funkcjonalności ograniczonej czasowo.

5. Wymagania dotyczące działania systemu

- System musi być dostarczony jako rozwiązanie instalowane lokalnie w infrastrukturze Zamawiającego. Dane nie mogą być przekazywane do chmury producenta.
- Zapewnienie kontroli dostępu opartej na rolach, uwierzytelniania wieloskładnikowego oraz audytu działań administratorów systemu.
- System musi umożliwiać tworzenie kopii zapasowej konfiguracji oprogramowania oraz jej odtworzenie.
- System musi być dostarczony z obsługiwaną bazą danych albo umożliwiać użycie zewnętrznego, wspieranego systemu bazodanowego. Zastosowany wariant musi zapewniać backup, odtwarzanie, kontrolę dostępu i obsługę zakładanej skali (rozmiaru bazy danych).

6. Minimalne wymagania funkcjonalne

1) Monitoring i nagrywanie sesji

a. Rejestrowanie sesji SSH.
b. Rejestrowanie sesji RDP.
c. Możliwość odtwarzania nagrań.
d. Indeksowanie działań użytkownika.
e. Wyszukiwanie w nagraniach.
f. Eksport nagrań.
g. Integralność i nienaruszalność zapisów (mechanizmy kryptograficzne).
h. Możliwość podglądu sesji w czasie rzeczywistym.
i. Możliwość zakończenia sesji przez operatora.
j. AI behavioral biometrics na poziomie sesji:
System musi analizować zachowanie użytkownika w czasie rzeczywistym (keystrokes, mouse dynamics) i wykrywać anomalie na podstawie profilu behawioralnego.
k. Automatyczna reakcja na anomalię (pause/kill):
System musi automatycznie wstrzymać lub zakończyć sesję na podstawie analizy behawioralnej.

2) Kontrola działań uprzywilejowanych

a. Definiowanie polityk dostępu.
b. Ograniczanie dostępu do określonych systemów.
c. Ograniczanie dostępu do określonych komend (dla SSH).
d. Blokowanie komend zdefiniowanych jako zabronione.
e. Definiowanie polityk per użytkownik / grupa / host.

3) Zarządzanie poświadczeniami

a. Centralne przechowywanie poświadczeń.
b. Automatyczną rotację haseł.
c. Obsługę kluczy SSH.
d. Możliwość przyznawania dostępu czasowego (JIT).

4) Integracje systemu

a. AD/LDAP.
b. RADIUS LUB SAML.
c. Eksport logów do SIEM.
d. REST API – udokumentowane API umożliwiające automatyzację w administracji.

7. Odbiór systemu

Wykonawca przygotuje plan testów, dane testowe i protokół wyników. Każdy scenariusz musi zostać wykonany w środowisku Zamawiającego albo w uzgodnionym środowisku demonstracyjnym.

Scenariusz odbioru:

1. Weryfikacja poprawnej integracji z usługą katalogową (np. Active Directory/LDAP), synchronizacji użytkowników i grup oraz poprawnego uwierzytelniania.
2. Weryfikacja możliwości przyznania użytkownikowi dostępu do kont uprzywilejowanych zgodnie z rolą oraz odebrania tych uprawnień.
3. Weryfikacja procesu pobierania lub użycia poświadczeń uprzywilejowanych zgodnie z przyjętą polityką bezpieczeństwa, z uwzględnieniem rejestracji operacji.
4. Weryfikacja automatycznej zmiany hasła konta uprzywilejowanego po zakończeniu sesji lub zgodnie z harmonogramem.

5. Weryfikacja zestawienia sesji do chronionego systemu za pośrednictwem PAM oraz poprawnego zakończenia sesji.
6. Weryfikacja rejestrowania informacji o sesji (użytkownik, czas rozpoczęcia i zakończenia, system docelowy, wykonane operacje – zgodnie z możliwościami rozwiązania) oraz możliwości ich odtworzenia.
7. Weryfikacja procesu uzyskania dostępu wymagającego akceptacji wskazanego przełożonego lub administratora.
8. Weryfikacja przyznania dostępu uprzywilejowanego na określony czas oraz automatycznego wygaśnięcia uprawnień.

8. Dokumentacja, warsztaty powdrożeniowe i wsparcie techniczne

a) Dokumentacja powykonawcza

Zamawiający wymaga, aby Wykonawca przygotował i przekazał kompletną dokumentację powdrożeniową w języku polskim, obejmującą co najmniej następujące elementy:

- Architektura wdrożenia i diagram przepływów danych.
- Wykaz serwerów, komponentów, portów, certyfikatów i kont serwisowych.
- Konfiguracja źródeł danych, repozytorium, retencji i archiwum.
- Lista utworzonych raportów i alertów.
- Konfiguracja bezpieczeństwa, ról i uwierzytelniania wieloskładnikowego.
- Procedury aktualizacji, backupu, odtwarzania i – jeżeli dotyczy – przełączenia wysokiej dostępności.
- Instrukcja operacyjna dla administratorów i operatorów.
- Dokumentacja musi być w języku polskim.

b) Warsztaty powdrożeniowe

Warsztaty muszą obejmować administrację systemem, zarządzanie źródłami danych, tworzenie raportów i alertów, analizę blokad kont, obsługę archiwum, integrację SIEM, zarządzanie rolami oraz podstawowe czynności utrzymaniowe i diagnostyczne.

- Czas trwania warsztatów: co najmniej 10 godzin, podzielonych na min. 2 spotkania.
- Zajęcia muszą być przeprowadzone w języku polskim.
- Warsztaty mogą się odbyć w formie wideokonferencji w dni robocze w godzinach 9.00 – 14.00 lub stacjonarnej w siedzibie Zamawiającego.
- Uczestnikom zapewnione zostaną materiały dydaktyczne w formie elektronicznej w języku polskim lub angielskim.
- Liczba uczestników: 7.

c) Wsparcie techniczne producenta

Zamawiający wymaga zapewnienia przez Wykonawcę wsparcia technicznego producenta systemu przez okres 12 miesięcy, obejmującego co najmniej następujące świadczenia:

- Dostęp do aktualizacji, poprawek bezpieczeństwa i nowych stabilnych wersji przez cały okres wsparcia.
- Możliwość zgłaszania incydentów technicznych pocztą elektroniczną, portalem i telefonicznie w języku polskim.
- Przekazanie procedury eskalacji zgłoszeń i kontaktów serwisowych.
- Zdalna pomoc techniczna w języku polskim.
- Pomoc techniczną producenta systemu.
- Dostęp do polskiej bazy wiedzy.