Opis zakresu szacowania

1. **Przedmiotem szacowania jest uruchomienie licencji rozwiązania Privilege Access Management (PAM) w infrastrukturze Zamawiającego**, które obejmuje w szczególności:
   1.1. Wykonanie Analizy środowiska Zamawiającego oraz sporządzenie Projektu Technicznego;
   1.2. Uruchomienie i konfiguracja rozwiązania PAM w najnowszej dostępnej wersji (rozwiązanie musi być kompletne i gotowe do pracy);
   1.3. Udzielenie lub zapewnienie udzielenia licencji/subskrypcji dla oprogramowania PAM na warunkach określonych przez producenta wraz z gwarancją i usługą wsparcia technicznego na okres minimum 12 miesięcy, w tym:
      1) możliwość pracy 5 użytkowników typu administrator i 10 użytkowników biznesowych,
      2) możliwość zapamiętania min. 50 danych logowania do systemów docelowych,
      3) możliwość podłączenia się do minimum 50-ciu systemów docelowych.
   1.4. Przeprowadzenie instruktażu dla Zamawiającego z uruchomienia, konfiguracji i administracji PAM;
   1.5. Sporządzenie i dostarczenie Zamawiającemu Dokumentacji Powykonawczej;
   1.6. Merytoryczne wsparcie administratorów rozwiązania PAM w ilości 160 godzin w okresie 12 miesięcy, licząc od dnia podpisania Końcowego Protokołu Odbioru.

2. **Opis funkcjonalny Privileged Access Management (PAM):**

Zarządzanie kontami i dostępami uprzywilejowanymi

2.1 Oprogramowanie musi posiadać funkcje zarządzania kontami uprzywilejowanymi oraz umożliwiać dostęp nadzorowany do:
   1) Systemów operacyjnych: Windows, Unix, Linux (Debian, Ubuntu, RedHat),
   2) Baz danych: Microsoft SQL, Microsoft SQL Cluster Service, MySQL, MariaBD, PostgreSQL,
   3) Systemów zarządzania infrastrukturą: DELL IDRAC, HP iLO,
   4) Urządzeń sieciowych Cisco, Dell, Extreme Networks, FortiGate oraz systemów bezpieczeństwa FortiGate,
   5) Środowisk wirtualizacyjnych: VMWare ESX/ESXi, vCenter (https, ssh), Microsoft Hyper-V,
   6) Środowiska chmurowego Microsoft Entra

2.2 Oprogramowanie musi zapewniać możliwość Wymuszenia odpowiedniej polityki zarządzania poświadczeniami uprzywilejowanymi i/lub poświadczeniami tymczasowymi oraz kluczami SSH w zakresie nie mniejszym niż:
   1) Automatyczna zmiana haseł i/lub kluczy SSH po ich wygaśnięciu
   2) Ustawienie złożoność haseł
   3) Określenie czas uzyskania dostępu do kont/systemów docelowych (określone dni i/lub przedziałów czasowych w danym dniu)
   4) Ustawiania wymogu zawnioskowania o dostęp lub uzyskania zgody na dostęp do poświadczeń systemu chronionego,
   5) Automatyczne nagrywanie sesji przy dostępie do systemu chronionego.

2.3 Oprogramowanie musi automatycznie porównywać hasło i/lub klucz SSH przechowywane w systemie oraz hasło i/lub klucz SSH przechowywane na systemie docelowym.

2.4 Oprogramowanie musi automatycznie synchronizować hasło przechowywane w systemie

oraz hasło przechowywane na systemie docelowym w przypadku wykrycia niezgodności.

2.5 Oprogramowanie musi wspierać środowisko LDAP (MS Active-Directory) do uwierzytelniania użytkowników.

Zarządzanie sesjami uprzywilejowanymi

2.6 Oprogramowanie musi umożliwiać zestawienie połączenia oraz monitoring sesji do systemu docelowego bez konieczności uprzedniego przekazania na stację użytkownika hasła konta uprzywilejowanego (po uwierzytelnieniu użytkownika oraz wskazaniu konta uprzywilejowanego produkt musi wprowadzić do wybranej aplikacji dane dostępowe, lub musi umożliwiać zestawienie połącznia do systemu docelowego z wykorzystaniem tymczasowych danych logowania, dzięki czemu dane dostępowe systemu docelowego nie są udostępniane stacji użytkownika). Nie jest dopuszczalne zestawianie połączeń do poniższych systemów poprzez wykorzystanie dodatkowych modułów pośredniczących klasy jumphost / bastion host, do których użytkownik może się interaktywnie zalogować, wybrać aplikacje i ręcznie zestawić sesję do systemu chronionego)

2.7 Oprogramowanie musi umożliwiać zestawianie i zarządzanie sesjami uprzywilejowanymi do systemów chronionych, w szczególności:

1) Do baz danych: Microsoft SQL, , MySQL, PostgreSQL, MariaDB, Microsoft SQL, Microsoft SQL Cluster Service, MySQL, MariaBD, PostgreSQL;
2) Do systemów zarządzania pozapasmowego: DELL IDRAC, HP iLO;
3) Do urządzeń sieciowych: Cisco, Dell, Extreme Networks, FortiGate oraz systemów bezpieczeństwa Fortigate;
4) Do środowisk wirtualizacyjnych VMWare ESX/ESXi, vCenter (https, ssh), Microsoft HyperV;
5) Do środowisk chmurowych Microsoft Entra, Microsoft 365.
6) Do systemów Unix/Linux i obsługiwać oraz zarządzać kluczami SSH
7) Do systemów Windows (konta LDAP)

2.8 Proponowane rozwiązanie powinno być w stanie zarządzać wieloma jednocześnie aktywnymi sesjami przy użyciu różnych protokołów połączeń i różnych kont uprzywilejowanych.

2.9 Oprogramowanie musi przechowywać nagrania sesji w zabezpieczonym kryptograficznie repozytorium.

2.10 Oprogramowanie musi posiadać wsparcie dla monitoringu i separacji sesji w Systemach operacyjnych: Windows, Unix, Linux (Debian, Ubuntu, RedHat).

2.11 Oprogramowanie musi zestawiać bezpośrednią sesję do docelowego systemu chronionego.

2.12 Dostęp zdalny do docelowych systemów chronionych nie może wymagać, aby istniały otwarte porty z sieci publicznej/Internetu do sieci wewnętrznej zamawiającego.

2.13 Oprogramowanie musi zapewniać rozliczalność w przypadku jednoczesnego wykorzystania konta współdzielonego przez więcej niż jednego użytkownika.

2.14 Oprogramowanie musi wykorzystywać mechanizmy indeksowania nagrań umożliwiające szybkie przeszukiwanie nagranych i monitorowanych sesji pod kątem występowania wskazanych słów kluczowych (wymagane są nie mniej niż następujące mechanizmy indeksowania: keystrokes). Nie jest dopuszczalnym dokonywanie indeksacji nagrań z wykorzystaniem mechanizmu OCR.

2.15 Oprogramowanie musi umożliwiać dostęp użytkowników do zasobu docelowego zgodnie z wymaganiami opisanymi w punkcie 2.6 przy wykorzystaniu przynajmniej następujących metod/narzędzi:

1) wykorzystanie różnych klientów RDP używanych na stacji, z której realizowany jest dostęp uprzywilejowany poprzez nie mniej niż: zdefiniowanie parametrów połączenia w ramach pliku konfiguracyjnego klienta RDP oraz możliwość interaktywnego odpytania użytkownika o właściwości systemu chronionego (takie jak adres, aplikacja kliencka, nazwa konta uprzywilejowanego) do którego będzie zestawione połączenie,
2) wykorzystanie przeglądarki internetowej obsługującej html5 w celu zapewnienia wsparcia dla użytkowników korzystających z innych systemów operacyjnych niż Windows (brak klienta RDP na stacji użytkownika). W ramach połączenia realizowanego za pomocą tej metody sesja uprzywilejowana (zestawiona w oparciu o dowolną aplikację skonfigurowaną w systemie proxy, zgodnie z wymaganiami opisanymi w punkcie 2.6) musi być tunelowana w html5,
3) wykorzystanie różnych klientów linii poleceń i protokołu SSH (np. Putty).

2.14 Proponowane rozwiązanie powinno umożliwić synchronizację umożliwiającą dodanie do systemu nowego użytkownika utworzonego w Active Directory.

2.15 Oprogramowanie musi umożliwiać transmisję plików oraz wykorzystanie schowka dla sesji w ramach wszystkich oferowanych mechanizmów zestawiania połączenia do systemów docelowych.

2.16 Rozwiązanie musi udostępniać funkcjonalność wstrzykiwania poświadczeń dla najpopularniejszych przeglądarek internetowych (Microsoft Edge, Google Chrome, Mozilla Firefox, Safari).

Zarządzanie incydentami bezpieczeństwa

2.17 W oferowanym rozwiązaniu musi istnieć mieć możliwość monitorowania sesji w czasie rzeczywistym podczas nagrywania.

2.18 Oprogramowanie musi mieć możliwość określenia przedziału czasu w jakim można uzyskać dostęp do przechowywanych danych kont uprzywilejowanych (okres w dniach kalendarzowych lub tygodnia lub określone godziny dnia).

2.19 Oprogramowanie musi generować odpowiedni alarm w przypadku wykorzystania konta uprzywilejowanego w niestandardowych godzinach (np. poza typowymi dla danego użytkownika godzinami pracy).

2.20 Oprogramowanie musi umożliwiać monitoring, ingerencję oraz zakończenie aktywnej sesji w czasie jej trwania przez administratorów oferowanego rozwiązania (zarówno do systemu PAM jak i zabezpieczanych systemów docelowych).

Architektura

2.21 Rozwiązanie musi być kompletne i po wdrożeniu gotowe do użycia.

2.22 Proponowanie rozwiązanie musi być dostarczone wraz z kompletem licencji i umów wymaganych do jego działania.

2.23 Zaleca się, aby całość rozwiązania dostarczona Zamawiającemu była od tego/przez tego samego producenta, poszczególne moduły funkcjonalne muszą integrować się ze sobą.

2.24 Oprogramowanie musi posiadać budowę modularną, tzn. możliwość rozbudowy funkcjonalnej o kolejne komponenty.

2.25 Rozwiązanie powinno być zaprojektowane w architekturze 2 warstwowej, z niezależnymi serwerami front-end (warstwa dostępu i prezentacji) i back-end (zarządzanie logiką systemu, poświadczeniami i bazą danych).

2.26 Wymagana jest możliwość niezależnego skalowania warstwy front-end i back-end.

2.27 Rozwiązanie powinno funkcjonować na dowolnym virtualizatorze, jak również na maszynie fizycznej.

2.28 Proponowane rozwiązanie powinno mieć zaplanowaną funkcję tworzenia kopii zapasowych. Kopie zapasowe muszą być możliwe do zapisania w sieci SAN, na serwerze NAS lub w innej lokalizacji sieciowej.

2.29 Producent musi udostępniać procedury opisujące sposób utwardzania każdego z komponentów Systemu. Utwardzanie każdego z komponentów musi być realizowane w oparciu o dobre praktyki producenta systemu operacyjnego oraz producenta rozwiązania PAM/PAS.

Integracje

2.30 Rozwiązanie musi umożliwiać integrację z mechanizmami wykorzystywanymi do uwierzytelniania użytkowników minimum: hasła, LDAP, klucze SSH, SAML, wieloskładnikowe uwierzytelnianie, klucze YubiKey 5.

2.31 Oferowane rozwiązanie powinno być w stanie wysyłać wszystkie logi w formatach Syslog/CEF do produktów SIEM i integrować się z rozwiązaniami SIĘM.

2.32 Oprogramowanie musi oferować możliwość integracji z dowolnym serwerem pocztowym i być w stanie wysyłać powiadomienia e-mail do jednej lub więcej osób/grup w przypadku wystąpienia predefiniowanych zdarzeń (nieprawidłowe logowanie użytkowników, wyświetlenie/użycie współdzielonego hasła itp.).

3. Wymagania dodatkowe

Wieloskładnikowe uwierzytelnienie oraz zabezpieczenie dostępu do kluczowych aplikacji poprzez funkcję Single Sign-On

3.1 Oprogramowanie musi realizować funkcję:

1) wieloskładnikowego uwierzytelnienia,
2) zabezpieczenia dostępu zarówno do zewnętrznych jak i do wewnętrznych aplikacji poprzez wykorzystanie funkcji SSO,
3) zarządzania cyklem życia tożsamości (ang. lifecycle management).

3.2 Wymagana jest możliwość obsługi minimum następujących składników uwierzytelniających MFA: hasło, sms, email oraz minimum jednego z mechanizmów: oauth2, aplikacja mobilna, klucze sprzętowe YubiKey 5.

3.3 Oprogramowanie musi realizować usługę SSO dla aplikacji wewnętrznych i chmurowych, realizując w sposób scentralizowany bezpieczne uwierzytelnienie przy wykorzystaniu metod opisanych w punkcie 2.1. Musi istnieć możliwość integracji z własnymi aplikacjami poprzez nie mniej niż następujące integracje:

1) Basic auth,
2) Oauth i/lub Oauth2,
3) Saml,
4) Użytkownik - hasło.

Ochrona dostępu zdalnego

3.4 Rozwiązanie/oprogramowanie musi realizować 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.

3.5 Rozwiązanie/oprogramowanie nie może wymagać instalowania dodatkowego oprogramowania po stronie stacji roboczej użytkownika zewnętrznego poza przeglądarką internetową oraz aplikacji mobilnej na jego urządzeniu mobilnym

3.6 Aplikacja mobilna używana w mechanizmach MFA oferowanego rozwiązania/oprogramowania musi posiadać wsparcie dla następujących platform mobilnych: IOS od wersji 12, Android od wersji 8.0.

3.7 W celu obsłużenia całości ruchu uprzywilejowanego do sieci Zamawiającego przez przeglądarkę internetową. Rozwiązanie/oprogramowanie musi posiadać wsparcie tunelowania sesji graficznych RDP przy użyciu HTML5.

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

4. Wdrożenie

4.1. PAM musi być uruchomiony w następującym zakresie:

1) PAM musi być zainstalowany w najnowszej wersji wraz z najnowszymi aktualizacjami.
2) Konfiguracja Oprogramowania PAM musi uwzględniać:
   a) Utworzenie kont użytkowników i grup w PAM zgodnie z wymaganiami Zamawiającego;
   b) Integrację uwierzytelniania i autoryzacji użytkowników PAM z usługą katalogową Active Directory wykorzystywaną przez Zamawiającego;
   c) Utworzenie do 5 kont systemów docelowych w PAM zgodnie z wymaganiami Zamawiającego;
   d) Utworzenie polityk związanych ze złożonością hasła zgodnie z wymaganiami Zamawiającego;
   e) Utworzenie harmonogramów zmiany hasła/ wygasania poświadczeń zgodnie z wymaganiami Zamawiającego;
   f) Utworzenie schematów wnioskowania o dostęp do hasła i/lub sesji zgodnie z wymaganiami Zamawiającego;
3) Dołączenie PAM do systemu monitoringu (Zabbix) Zamawiającego. Wykonawca określi kluczowe mierniki odnośnie wydajności i dostępności Oprogramowania PAM oraz określi wartości progowe dla tych liczników, dzięki którym możliwe będzie proaktywne monitorowanie PAM. W szczególności określone zostaną przez Wykonawcę dopuszczalne wartości wskaźników wydajnościowych wszystkich składników systemu w warunkach normalnych oraz ich wartości progowe, których przekroczenie będzie uznawane za sytuację alarmową i sytuację krytyczną.
4) Wykonanie testów akceptacyjnych:
   a) Uruchamianie i zatrzymywanie rozwiązania PAM;
   b) Weryfikacja procesu zarzadzania hasłami na kontach systemów docelowych;
   c) Weryfikacja procesu zarzadzania sesjami;
   d) Weryfikacja poprawności działania procedur;

4.2. Oferowane rozwiązanie PAM musi być uruchomiony w obecnym środowisku Zamawiającego z minimalnymi wymaganiami:

1) Uruchomienie na maszynach wirtualnych lub virtual appliance działających w środowisku VMware vSphere 7.0.3,
2) Zapewnione licencje pozwalające na jednoczesne łączenie się przynajmniej dwóch administratorów do systemu operacyjnego każdej wykorzystywanej w dostarczonym

rozwiązaniu maszyny wirtualnej (połączenia RDP lub SSH),

3) Zapewnione licencje pozwalające na jednoczesne łączenie się przynajmniej 20 kont/użytkowników do serwera bazodanowego,
4) Zapewnione licencje pozwalające na swobodną migrację maszyn wirtualnych pomiędzy 4 nodami klastra vSphere 7.0.3, zarządzanym przez środowisko vCenter. W skład klastra wchodzą poniższe serwery fizyczne:

   a) 3x serwer Dell PowerEdge R740 (VMware ESXi, 2 CPU, 32 core)
   b) serwer Dell PowerEdge R730 (VMware ESXi, 2 CPU, 12 core)

4.3. Proponowane rozwiązanie powinno mieć możliwość zaplanowania harmonogramu tworzenia kopii zapasowych. Kopie zapasowe muszą być możliwe do zapisania w sieci SAN, na serwerze NAS lub w innej lokalizacji sieciowej.

5. Instruktaż

5.1. Zamawiający wymaga od Wykonawcy przeprowadzenia instruktażu dla 2 administratorów oprogramowania PAM.
5.2. Instruktaż odbędzie się w siedzibie Zamawiającego w uzgodnionym na roboczo pomiędzy Wykonawcą a Zamawiającym terminie. W przypadku gdy nie będzie możliwości zorganizowania instruktażu w siedzibie Zamawiającego, dopuszcza się zorganizowanie instruktażu w formie zdalnej.
5.3. Zamawiający wymaga, aby instruktaż składał się z części teoretycznej i warsztatowej, i trwał minimum 16 godzin (min. 2 dni robocze).
5.3. Zapewnienie infrastruktury dla części warsztatowej leży po stronie Wykonawcy.
5.4. Zakres szkolenia:

1) Ogólna architektura Oprogramowania PAM;
2) Bezpieczeństwo Oprogramowania PAM;
3) Konfiguracja kont systemów docelowych w Oprogramowaniu PAM;
4) Zarządzanie użytkownikami w Oprogramowaniu PAM i integracja z innymi mechanizmami uwierzytelnienia i autoryzacji;
5) Polityki złożoności hasła, harmonogram zmian haseł, walidacja poprawności zmiany hasła;
6) Zarządzanie sesjami w Oprogramowaniu PAM;
7) Zarządzanie schematami wnioskowania i akceptacji dostępu hasła i/lub sesji w Systemie PAM;
8) Audyt i raportowanie w Oprogramowaniu PAM;
9) Procedura aktualizacji Oprogramowania PAM;
10) Procedura rozwiązywania problemów i zgłoszeń serwisowych;

6. Gwarancja i wsparcie techniczne

6.1. Oprogramowanie PAM powinno być objęte 12 miesięczną gwarancja i wsparciem technicznym producenta i/lub Wykonawcy (dopuszcza się udział partnerów i/lub podwykonawców).
6.2. Usługi w ramach gwarancji, w tym usuwanie Awarii, będą realizowane zgodnie z zasadami określonymi w umowie gwarancyjnej.

6.3. Zakres usług wsparcia technicznego obejmuje:

1) doradztwo i pomoc w zakresie obsługi Oprogramowania PAM;
2) analizę i rozwiązywanie problemów związanych z Oprogramowania PAM

oraz zaistniałych na styku pomiędzy Oprogramowaniem PAM i/lub Sprzętem Teleinformatycznym i innym oprogramowaniem użytkowanym przez Zamawiającego;

3) zapewnienie dostępu (za pośrednictwem strony internetowej) i możliwości korzystania z aktualizacji, poprawek Oprogramowania PAM, nowych wersji oprogramowania, oraz dokumentacji administracyjnej i technicznej dotyczącej oprogramowania PAM;
4) informowanie o znanych problemach z Oprogramowania PAM i sposobach ich rozwiązania drogą telefoniczną lub poprzez pocztę elektroniczną.