**OPZ systemu PIM/PAM**

Dostawa rozwiązania systemu do zarządzania uprawnieniami oraz aktywnością kont uprzywilejowanych **(ang. PIM/PAM)** wraz z kompletem niezbędnych licencji, wdrożenie systemu oraz świadczeniem usługi wsparcia technicznego (asysty) na okres 36 miesięcy w wymiarze (300 h), w tym z usługą szkolenia w trybie warsztatów z wdrożonego rozwiązania dla administratorów ARiMR.

Zamawiający posiada środowisko systemu bezpieczeństwa kont uprzywilejowanych (PAM- Privileged Access Management ), na które składają się następujące licencje:

|  |  |  |
| --- | --- | --- |
| Nazwa | Oznaczenie producenta | Ilość użytkowników |
| Privileged Standard User Subscription | PRIV-STANDARD-USER-SUBS | 300 |
| PAM Remote Vendor User with Advanced Remote Access | EXT-VENDOR-USER-SUBS | 200 |

**W ramach przedmiotowego postępowania wymagane jest dostarczenie dla administratorów będących pracownikami Zamawiającego licencji czasowych na 36 miesięcy (na zasadach subskrypcji) realizujących podstawowe funkcjonalności systemu, pochodzącego od tego samego producenta, nie mniej niż:**

* zarządzanie kontami i dostępami uprzywilejowanymi (szczegółowy opis wymagań systemu PIM/PAM)
* ochrona dostępu zdalnego (szczegółowy opis wymagań systemu PIM/PAM)
* wieloskładnikowe uwierzytelnienie oraz zabezpieczenie dostępu do kluczowych aplikacji poprzez portal Single Sign-On (szczegółowy opis wymagań systemu PIM/PAM)
* min. 100 kont uprzywilejowanych.

**W ramach przedmiotowego postępowania wymagane jest dostarczenie dla usługi tzw. kontraktorów (zewnętrznych dostawców) licencji czasowych na 36 miesięcy (na zasadach subskrypcji) realizujących podstawowe funkcjonalności systemu objętych serwisem producenta w okresie 36 miesięcy, pochodzącego od tego samego producenta, nie mniej niż:** zarządzanie kontami i dostępami uprzywilejowanymi (szczegółowy opis wymagań systemu PIM/PAM)

* ochrona dostępu zdalnego szczegółowy (szczegółowy opis wymagań systemu PIM/PAM)
* min. 400 kont uprzywilejowanych.

1. **Opis funkcjonalny systemu PIM/PAM**
   1. Dostarczony system musi umożliwiać uruchomienie zarówno na platformie fizycznej, jak i wirtualnej w ramach tej samej licencjioraz posiadać wykupienia wsparcia technicznego producenta dla wdrożonego oprogramowania na okres 36 miesięcy.
2. **Zarządzanie kontami i dostępami uprzywilejowanymi.**
   1. System musi posiadać funkcje zarządzania (automatycznej zmiany haseł, definiowania polityki dostępu) kontami uprzywilejowanymi w:
3. Systemach operacyjnych: Windows, Unix, Linux, iSeries (AS/400), zSeries (OS/390), Straus VOS
4. Bazach danych: Microsoft SQL, Microsoft SQL Cluster Service, Oracle, Informix, MySQL, Sybase Adaptive Server Enterprise, HeidiSQL, DB2, Informatica, MariaBD, MongoDB, PostgreSQL
5. Systemach zarządzania infrastrukturą, aplikacjach: DELL DRAC, IBM Tivoli,RSA authentication Manager, HP iLO, SAP Application Server
6. Urządzeniach sieciowych oraz systemach bezpieczeństwa: Cisco (routery, seria nexus, firewalle), HP, Checkpoint, Netscreen, F5, Infoblox NIOS, FireEye Malware Analysis, FortiGate, Aruba, Palo Alto Networks, A10, Riverbed, Gemalto
7. Narzędziach CI/CD: Chef, Jenkins, Kubernetes, Docker
8. Aplikacjach typu SaaS/ stronach web/ interfejach web, minimum takich jak: Facebook (konta marketingowe), Amazon Web Services (klucze API oraz konta uprzywilejowane, konto root), Zarządzanie Microsoft Azure (klucze API oraz konta uprzywilejowane)
9. Modułach: Microsoft Services, Scheduled tasks, IIS application Pool, IIS Directory Security, w rejestrach, COM+ , zarządzanie kontami w domenie Microsoft
10. Plikach konfiguracyjnych, tabelach baz danych
11. Środowiskach wirtualizacyjnych VMWare ESX/ESXi
    1. System musi zapewniać wsparcie (ochronę kont) dla dowolnego urządzenia obsługującego ODBC w wersji 2.7 lub wyższej
    2. System musi zapewniać wsparcie (możliwość zarządzania kontami uprzywilejowanymi wykorzystywanymi w obrębie systemu docelowego) dla systemów spoza listy "out of box" z wykorzystaniem skryptów lub innych mechanizmów realizowanych i wspieranych przez producenta rozwiązania dostępnych nieodpłatnie na oficjalnej stronie producenta rozwiązania. Producent powinien udostępniać nie mniej niż 200 unikalnych integracji udostępnionych w ramach wspomnianego portalu.
    3. W przypadku ochrony kont lokalnych administratorów na stacjach roboczych Windows oraz MAC OS proponowany system musi obsługiwać scenariusz potencjalnej niedostępności stacji w momencie wykonania polityki automatycznej zmiany hasła lokalnego administratora (realizowanej przez narzędzie ochrony kont). W przypadku systemów, które często znajdują się poza siecią lokalną Zamawiającego musi istnieć możliwość wykorzystania narzędzia / agenta instalowanego na stacji roboczej, który będzie integrował się z proponowanym rozwiązaniem (w ramach tej samej licencji czasowej) w celu zmiany hasła na stacji roboczej (gdy stacja zostanie podłączona do sieci lokalnej) i poinformowania narzędzia ochrony kont o realizacji zadania.
    4. System musi zapewniać wsparcie (możliwość zarządzania kontami uprzywilejowanymi wykorzystywanymi w obrębie systemu docelowego) dla systemów spoza listy "out of box" z wykorzystaniem skryptów lub innych mechanizmów realizowanych i wspieranych przez producenta rozwiązania w zakresie zmiany haseł poprzez: SSH / Telnet, API do zewnętrznych aplikacji, możliwość wykonywania zmian oraz weryfikacji spójności haseł poprzez symulację działań użytkownika w sesji aplikacji Web.
    5. System musi zapewniać możliwość automatycznego wykrywania kont w nowych urządzeniach Windows, usługach systemu Windows, zaplanowanych zadaniach, kontach serwisowych IIS itp., automatycznego dodania powyższych do produktu oraz automatycznie wymusić odpowiednią politykę zarządzania kontami uprzywilejowanymi
    6. System musi posiadać możliwość ochrony (zarządzania) oraz dynamicznego generowania (w formie pseudolosowej) nowego klucza SSH zgodne z określonym szablonem
    7. System musi automatycznie porównywać hasło/klucz SSH przechowywane w systemie oraz hasło/klucz SSH przechowywane na systemie docelowym
    8. System musi automatycznie synchronizować hasło (oraz klucz SSH) przechowywane w systemie oraz hasło (oraz klucz SSH) przechowywane na systemie docelowym w przypadku wykrycia niezgodności.
    9. System musi umożliwiać przechowywanie historii rotacji haseł (np. trzy ostatnie hasła dla danego systemu docelowego) oraz umożliwiać łatwy dostęp do tej historii (np. poprzez interfejs webowy)
    10. System musi wspierać różne środowiska LDAP do uwierzytelniania użytkowników, nie mniej niż Sun One, MS Active-Directory, IBM Tivoli, Novel eDirectory, Oracle Internet Directory
    11. System musi umożliwiać wykrywanie par kluczy SSH w danej infrastrukturze
    12. System musi umożliwiać zarządzanie i zapewniać bezpieczeństwo kluczy SSH używanych przez aplikacje w przypadku przechowywania kluczy w plikach konfiguracyjnych
    13. Producent musi udostępniać bezpłatnie dodatkową aplikację umożliwiającą automatyzację procesu tworzenia nowych skryptów do rotacji poświadczeń w systamach docelowych dostępnych z wykorzystaniem protokołu SSH. Aplikacja musi umożliwiać nagranie procesu ręcznego logowania użytkownika do systemu docelowego i rotacji poświadczeń, a następnie na podstawie nagrania musi automatycznie wygenerować skrypt / plugin który będzie wykorzystany przez silnik automatycznego zarządzania poświadczeniami konta.
12. **Zarządzanie sesjami uprzywilejowanymi.**
    1. System 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 dowolnie wybranej aplikacji dane dostępowe, dzięki czemu nie muszą być one udostępniane stacji użytkownika).
    2. Rozwiązanie musi udostępniać narzędzia do obsługi aplikacji instalowanych na systemie operacyjnym modułu separacji oraz nagrywania sesji. Jako obsługa rozumiane jest uruchomienie aplikacji oraz wypełnienie pól danymi dostępowymi automatycznie pobranymi z zabezpieczonego, centralnego repozytorium kont uprzywilejowanych.
    3. W przypadku zestawienia połączeń przez przeglądarkę internetową narzędzie musi posiadać moduł umożliwiający realizację procesu utwardzania przeglądarki internetowej przez którą realizowana jest sesja uprzywilejowana.
    4. System musi umożliwiać zestawianie i zarządzanie sesjami uprzywilejowanymi do systemów chronionych, 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):
13. Systemów operacyjnych: Windows, Unix, Linux, iSeries (AS/400), zSeries (OS/390)
14. Baz danych: Microsoft SQL, Oracle, MySQL, SAP HANA, HeidiSQL, DB2
15. Systemów zarządzania infrastrukturą, aplikacji: DELL DRAC, RSA authentication Manager, HP iLO, SAP GUI, BMC Remedy
16. Urządzeń sieciowych oraz systemów bezpieczeństwa Zamawiajacego: Cisco (routery, seria nexus, firewalle), HP, Checkpoint (SmartDashboard, https, ssh), F5 Networks, Palo Alto Networks
17. Narzędzi CI/CD (https, ssh): Chef, Jenkins, Kubernetes, Docker, Jfrog, GitHub
18. Aplikacji typu SaaS/ stron web/ interfejów web, minimum takich jak: Zarządzanie Microsoft Azure
19. Środowisk wirtualizacyjnych VMWare ESX/ESXi, vCenter (vSphere Client, https, ssh)
    1. System musi posiadać wsparcie (dla monitoringu i separacji sesji oraz realizacji funkcji Single Sign-On dla kont uprzywilejowanych) dla pozostałych aplikacji oraz systemów niż wcześniej wyszczególnionych poprzez możliwość wykorzystania nie mniej niż: uruchomienia aplikacji ze wskazanym zbiorem parametrów, zastosowania opisowego języka skryptowego, wbudowanego komponentu pozwalającego na obsługę własnych aplikacji web.
    2. Producent musi udostępniać bezpłatnie dodatkową aplikację umożliwiającą automatyzację procesu tworzenia komponentów połączeniowych dla nowych / nieznanych aplikacji Web poprzez nagranie ręcznego połączenia użytkownika do aplikacji, automatyczną identyfikację nazw formularzy wykorzystywanych do wpisania poświadczeń przez użytkownika a następnie na podstawie nagrania automatyczne wygenerowanie odpowiedniego skryptu umożliwiającego połączenie.
    3. System musi przechowywać nagrania sesji w zabezpieczonym kryptograficznie repozytorium uniemożliwiającym ich manipulację.
    4. Żaden z użytkowników włącznie z administratorem systemu nie może mieć wpływu na integralność składowanych nagrań (włącznie z brakiem możliwości ich usunięcia w zdefiniowanym okresie składowania danych).
    5. System musi umożliwiać ograniczanie dostępu do systemów docelowych oraz tworzenie list dopuszczalnych i niedopuszczalnych poleceń wykonywanych poprzez SSH.
    6. System musi zapewniać rozliczalność w przypadku jednoczesnego wykorzystania konta współdzielonego przez więcej niż jednego użytkownika.
    7. System 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, odpowiedzi okien systemu operacyjnego, komendy SQL). Nie jest dopuszczalnym dokonywanie indeksacji nagrań z wykorzystaniem mechanizmu OCR.
    8. System musi umożliwiać wykorzystanie przez moduł proxy funkcjonalności Microsoft Remote App w celu publikowania aplikacji dostępowych. Skrypty utwardzające (and. Hardening) muszą być dostarczone przez Producenta rozwiązania oraz uruchomione podczas instalacji rozwiązania
    9. System musi umożliwiać dostęp użytkowników do zasobu docelowego przy wykorzystaniu nie mniej niż następujących metod / narzędzi:
20. Interfejs Web proponowanego rozwiązania
21. 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, przy czym wspierana musi metoda uwierzytelnienia do systemu bazująca na certyfikatach PKI.
22. 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 1.15) musi być tunelowana w html5 i widoczna dla użytkownika jako nowa zakładka w przeglądarce.
23. Wykorzystanie różnych klientów linii poleceń i protokołu SSH (np. putty), przy czym wspierana musi metoda uwierzytelnienia do systemu bazująca na kluczach SSH.
    1. Dla połączeń uprzywilejowanych zestawianych z poziomu interfejsu graficznego system musi umożliwiać wybór czy sesją ma być zestawiona ze stacji użytkownika w oparciu o protokół RDP czy protokoł HTTPS (sesja tunelowana w html5).
    2. System musi wspierać tryb automatycznego, tymczasowego przypisywania konta użytkownika systemu Windows do grupy lokalnych administratorów po złożeniu stosownego wniosku (tzw. tryb dostępu Just-in-time / JIT). Nadane przez proponowany System uprawnienia JIT muszą być automatycznie odbierane po upływie czasu na który został nadany dostęp.
    3. System musi wspierać tryb automatycznego generowania krótkoterminowych certyfikatów SSH w chronionych systemach Linux/Unix dla administratorów po złożeniu stosownego wniosku. Wygenerowane krótkoterminowe certyfikaty muszą być podpisane przez uprzednio utworzony klucz CA oraz zawierać klucz publiczny, informację o tożsamości wnioskującego administratora i opcjonalnie dodatkowe restrykcje przypisanego do wnioskującego.
    4. System musi umożliwiać transmisję plików oraz wykorzystanie schowka dla sesji tunelowanych w html5.
    5. Po uwierzytelnieniu wieloskładnikowym w portalu graficznym rozwiązania system musi umożliwiać wygenerowanie klucza SSH na potrzeby bezpiecznego dostępu do systemów chronionych poprzez moduł proxy bez konieczności wpisywania dodatkowych składników uwierzytelniających.
    6. Dostęp do systemów docelowych musi podlegać polityce Role Based Access Control przypisanej do użytkownika który wygenerował i pobrał klucz SSH. System musi posiadać możliwość zabezpieczenia klucza podczas jego generowania poprzez wykorzystania pasphrase (o definiowalnej w oferowanym systemie długości oraz złożoności) oraz określenia w polityce systemu czasu ważności klucza.
24. **Zarządzanie incydentami bezpieczeństwa.**
    1. System musi posiadać funkcję kategoryzacji nagranych sesji użytkowników pod kątem ryzyka:

4.1.1. Ryzyko opisane musi być poprzez konfigurację przez administratora systemu zbioru wykrywanych w trakcie trwania sesji funkcji / poleceń i przypisanej do nich wagi.

4.1.2. Ryzyko musi być analizowane i przypisane zarówno dla zakończonych jak i aktywnych sesji. Informacje dotyczące poziomu ryzyka sesji muszą być widoczne zarówno w konsoli monitoringu sesji jak i w interfejsie obrazującym ryzyko / incydenty bezpieczeństwa (dashboard).

4.1.3.Administrator musi posiadać możliwość określenia akcji wykonanych przez użytkownika dla których sesja powinna być automatycznie zakończona / wstrzymana.

* 1. System musi posiadać wbudowane narzędzia analityczne umożliwiające automatyczne, bezobsługowe (bez konieczności definiowania reguł polityki bezpieczeństwa) wykrywanie podejrzanej aktywności kont uprzywilejowanych na bazie nauczonych automatycznie wzorców działania poszczególnych użytkowników (podejrzany czas pracy, nowy adres IP, zbyt duża ilość odwołań do repozytorium kont o hasła)
  2. System musi umożliwiać pobieranie danych o aktywnościach użytkowników z zewnętrznych systemów SIEM, wspierane muszą być nie mniej niż następujące rozwiązania posiadane przez Zamawiającego: Qradar, Splunk oraz zewnętrzne źródła informacji, minimum rsyslog (z systemów Unix/Linux), Windows Event Forwarder (z systemów Windows), Azure Function App.
  3. System musi umożliwiać podjęcie aktywnej akcji (co najmniej wymuszenie zmiany hasła konta uprzywilejowanego) w przypadku wykrycia anomalii wykorzystania kont uprzywilejowanych (minimum: kradzież hasła konta uprzywilejowanego; utworzenie nowego konta i próba zestawienia nim połączenia z serwerem).
  4. System musi generować odpowiedni alarm w przypadku wykrycia nadmiernego wykorzystania kont uprzywilejowanych przez danego użytkownika oraz w przypadku wykorzystania konta uprzywilejowanego w niestandardowych godzinach (np. poza typowymi dla danego użytkownika godzinami pracy)
  5. System musi umożliwiać wykrywanie incydentów polegających na bezpośrednim dostępie użytkownika do systemu docelowego (np. bez wcześniejszego wysłania wniosku do proponowanego rozwiązania o hasło systemu docelowego) oraz na utworzeniu w systemie docelowym niezarządzanego do tej pory konta uprzywilejowanego.
  6. Rozwiązanie musi posiadać funkcje reagowania na tego typu działania poprzez wyegzekwowanie zmiany hasła konta uprzywilejowanego przez proponowany system, dodanie konta nowo utworzonego do centralnego repozytorium oraz automatyczny reset poświadczeń.
  7. System musi wykrywać i wysyłać powiadomienia (alarmy) o wykrytych podatności środowiska dotyczących kont uprzywilejowanych: nieszyfrowana komunikacja do systemu pozwalająca na przejęcie danych dostępowych kont uprzywilejowanych, użycie kont serwisowych w wielu celach (jako konta serwisowe i jednocześnie interaktywne), konta z włączoną funkcją "Unconstrained Delegation" oraz konta usług podatne na ataki klasy Kerberoasting (ang. risky SPNs).
  8. System musi umożliwiać wykrywanie nowych, niezarządzanych kont uprzywilejowanych oraz połączeń, które zostały nawiązane bez uprzedniego pobrania hasła z centralnego repozytorium, realizowanych w środowisku Azure oraz opcjonalnie AWS.
  9. System musi umożliwiać monitoring, ingerencję oraz zakończenie aktywnej sesji graficznej w czasie jej trwania, a także określenie zbioru poleceń i uruchomionych funkcji systemu operacyjnego które spowodują automatyczne zakończenie / wstrzymanie sesji użytkownika (dla licencji czasowej użytkownika wewnętrznego).

1. **Architektura.**
   1. Całość rozwiązania dostarczona musi być przez tego samego producenta, poszczególne moduły funkcjonalne muszą integrować się ze sobą.
   2. System musi umożliwiać zainstalowanie bazy danych z centralnym repozytorium poświadczeń na odseparowanym, utwardzonym systemie operacyjnym, który nie będzie współdzielony z pozostałymi modułami rozwiązania (jak proxy izolujące sesje, interfejs graficzny, moduł rotacji poświadczeń czy silnik analityczny).
   3. System musi posiadać budowę modularną, tzn. możliwość rozbudowy funkcjonalnej o kolejne komponenty, dostępne w ramach oddzielnych licencji czasowych, odpowiedzialne za nie mniej niż:

* wieloskładnikowe uwierzytelnienie użytkowników oraz zabezpieczenie dostępu do kluczowych aplikacji Web (wewnętrznych oraz chmurowych) poprzez moduł Single Sign-On
* ochronę dostępu zdalnego dla pracowników i zewnętrznych dostawców
* 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)
* ochronę kont uprzywilejowanych w środowiskach DevOps
* ochronę kont uprzywilejowanych zaszytych w kodzie statycznych aplikacji i skryptów
* automatyczną klasyfikację ryzyka związanego ze zbyt obszernymi uprawnieniami w środowiskach chmurowych
* automatyczne wykrywanie oraz reagowanie na ataki dotyczące kontrolerów domeny i protokołu kerberos (OverPIM/PAMs-the-hash, golden ticket, PAC manipulation, DCSync)
* 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)
* moduł umożliwiający przechowywanie poświadczeń użytkownika biznesowego w centralnym. 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.
* 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. Producent musi udostępniać procedury opisujące sposób utwardzania każdego z komponentów Systemu oraz dostarczone w paczkach instalacyjnych skrypty automatyzujące proces utwardzania dostosowane do każdego z modułów funkcyjnych.
  2. Utwardzanie każdego z komponentów musi być realizowane w oparciu o dobre praktyki producenta systemu operacyjnego oraz producenta rozwiązania PIM/PAM.

5.5.1. Utwardzanie systemu operacyjnego modułu repozytorium poświadczeń musi być realizowane automatycznie przez instalator podczas procesu instalacji modułu.

* 1. Zaproponowane rozwiązanie musi uwzględniać nie mniej niż: jeden moduł składowania danych (poświadczeń, nagrań sesji etc), 5x moduł składowania danych na potrzeby Disaster Recovery/High Availability, 5x moduł do zmian i zarządzania kluczami oraz hasłami w systemach chronionych, 2 środowiska testowe pozwalające na odwzorowanie środowiska produkcyjnego
  2. Rozwiązanie nie może ograniczać liczby modułów odpowiedzialnych za izolację, monitoring oraz rejestrację sesji a także interfejsów Web, którymi użytkownik może podłączyć się do systemu ochrony kont uprzywilejowanych (dodanie kolejnych modułów nie może wymagać zakupu dodatkowych licencji czasowych producenta systemu ochrony kont uprzywilejowanych).
  3. System musi wspierać rozproszoną architekturę, w której poszczególne moduły funkcyjne (proxy pośredniczące, moduły rotujące poświadczenia, interfejsy graficzne) zainstalowane są w wielu lokalizacjach (odseparowanych geograficznie) oraz komunikują się z elementami centralnymi (repozytorium poświadczeń) z wykorzystaniem bezpiecznego protokołu komunikacji zapewniającego bezpieczeństwo danych podczas transmisji, pracującego na jednym porcie TCP (do zadeklarowania podczas instalacji systemu). W przypadku infrastruktury rozproszonej całość systemu musi być zarządzana z centralnego interfejsu graficznego.
  4. Zapewnienie wysokiej dostępności modułu składowania kont uprzywilejowanych musi być zaimplementowane na warstwie proponowanego oprogramowania (aplikacji), nie systemu operacyjnego/bazy danych na którym oprogramowanie jest zainstalowane.
  5. Produkt musi zapewniać ochronę kryptograficzną kopii zapasowych generowanych z produktu.
  6. Rozwiązanie musi posiadać funkcję implementacji modułów składowania kont uprzywilejowanych w formie rozproszonej, złożonej z aktywnego modułu, redundancji modułu aktywnego oraz zbioru aktywnych modułów rozproszonych geograficznie, świadczących (w trybie odczytu) część funkcji użytkownikom (np. mechanizmy wykonywania kopii zapasowych, udostępniania danych kont uprzywilejowanych aplikacjom, dostęp do interfejsu użytkownika.
  7. Proponowane rozwiązanie musi obsługiwać nie mniej niż 6 aktywnych repozytoriów poświadczeń.
  8. W przypadku infrastruktury rozproszonej całość systemu musi być zarządzana z centralnego interfejsu graficznego.
  9. Rozwiązanie, w którym składowane są chronione konta uprzywilejowane musi uwzględniać zapasowe komponenty typu Disaster Recovery w lokalizacjach odseparowanych geograficznie. Musi istnieć możliwość wykorzystania trybu wysokiej dostępności (ang high availability) pomiędzy dwoma systemami współdzielącymi przestrzeń dyskową z zaszyfrowaną bazą danych oraz modułów zaPIM/PAMowych (ang. Disaster Recovery) w innych lokalizacjach (musi istnieć możliwość wdrożenia do 4 modułów Disaster Recovery w ramach podstawowej licencji czasowej przy wdrożonym HA w lokalizacji podstawowej)

1. **Integracje.**
   1. System musi umożliwiać integrację z posiadanym przez Zamawiającego systemem SIEM Splunk Enterpse w celu wysyłania informacji o zarejestrowanych zdarzeniach w ramach monitorowanych sesji. System musi posiadać możliwość zdefiniowania typu zdarzeń które powinny być wysłane do systemu SIEM w celu ograniczenia utylizacji licencji.
   2. System musi umożliwiać integrację z biletowymi systemami zgłoszeń, nie mnie niż: BMC Remedy, ServiceNow oraz innym poprzez otwarte API, rozumianą jako weryfikację czy poprawne zgłoszenie istnieje w systemie biletowym i czy posiada odpowiedni status uprawniający do otrzymania poświadczeń uprzywilejowanych lub nawiązania połączenia uprzywilejowanego.
   3. System musi wspierać integrację z rozwiązaniami typu HSM obsługującymi standard PKCS11, wymagana jest integracja z dostępnymi na rynku systemami: Atos HSM Proteccio, Gemalto Luna/Safenet 1700 Hardware Security Module, Thales nShield Hardware Security Module, Utimaco CryptoServer, Crypto4A QxEDGE, Fortanix SDKMS, i4p Trident, Unbound Key Control, Utimaco CryptoServer.
   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, OpenID Connect (OIDC).
2. **Wymagania dodatkowe.**
   1. System musi posiadać skorelowaną ze sobą oficjalną metodykę implementacji.
   2. Metodyka ta musi zawierać minimum opis kroków, które należy wykonać w celu należytego i kompleksowego zaimplementowania rozwiązania typu PIM/PAM, 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).
   3. Metodyka poprzez analizę ryzyka musi umożliwiać pomoc w klasyfikacji kluczowych typów kont uprzywilejowanych oraz przypisanie ich do kolejnych etapów planowanej implementacji rozwiązania PIM/PAM.
3. **Wieloskładnikowe uwierzytelnienie oraz zabezpieczenie dostępu do kluczowych aplikacji poprzez portal Single Sign-On.**
   1. System musi realizować funkcję:
4. wieloskładnikowego adaptacyjnego uwierzytelnienia
5. zabezpieczenia dostępu zarówno do wewnętrznych jak i zewnętrznych (SaaS) aplikacji poprzez wykorzystanie zabezpieczonego portalu SSO.
6. zarządzania cyklem życia tożsamości (ang. lifecycle management, wymagający dodatkowej licencji czasowej)
   1. 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. 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")
   3. Moduł MFA poprzez protokół Radius musi umożliwiać integrację z popularnymi koncentratorami VPN jak minimum Cisco Systems, Palo Alto Networks, Pulse Secure, Fortinet.
   4. 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.
   5. System musi realizować usługę SSO dla aplikacji chmurowych oraz on-premises, realizując w sposób scentralizowany bezpieczne uwierzytelnienie.
   6. 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
  1. System musi posiadać gotowe integracje SSO z nie mniej niż następującymi aplikacjami: Office 365, Webex.
  2. 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).
  3. Poprzez dodatkowe licencje system musi realizować funkcję MFA wymuszane na chronionych serwerach Windows przy połączeniu uprzywilejowanym realizowanym w oparciu o moduł proxy.
  4. W ramach realizacji połączenia uprzywilejowanego moduł proxy musi auto uzupełnić poświadczenia i umożliwić użytkownikowi wpisanie kolejnego składnika MFA.
  5. System musi umożliwiać wymuszenie weryfikacji trzeciego składnika MFA na poziomie aplikacji mobilnej (minimum możliwe do zastosowania: PIN oraz uwierzytelnianie biometryczne).

1. **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.
   4. 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.
   5. 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.
   6. Aplikacja powinna umożliwiać zarządzanie utworzonymi użytkownikami (tworzenie nowych zaproszeń, nadawanie uprawnień, wyłączanie kont).
   7. Dostęp do aplikacji musi być możliwy poprzez wykorzystanie uwierzytelnienia biometrycznego, bez konieczności podawania danych dostępowych użytkownika (jak jego nazwa czy hasło).
   8. 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.
   9. 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.
   10. 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.
   11. 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.
   12. Rozwiązanie musi wspierać transfer plików w trakcie trwania sesji graficznej
   13. Rozwiązanie musi posiadać interfejs REST API do automatyzacji procesu zarządzania użytkownikami.
   14. Rozwiązanie musi wspierać konfigurację dla wielu instytucji, zarówno od strony Zamawiającego jak i zewnętrznych dostawców (Zamawiający może zarządzać dostępami wielu kontraktorów)
   15. Aplikacja mobilna Rozwiązania musi posiadać funkcję zapraszania innych użytkowników. Proces ten musi umożliwiać automatyczne założenie tożsamości użytkownika zewnętrznego w systemie PIM/PAM.