Załącznik nr 1 – Opis przedmiotu zamówienia

W ramach przedmiotowego postępowania wymagane jest dostarczenie dla 25 administratorów licencji czasowych, na 12 miesięcy, realizujących podstawowe funkcjonalności systemu, pochodzącego od tego samego producenta, nie mniej niż:

- zarządzanie kontami i dostępami uprzywilejowanymi (szczegółowy opis wymagań zawarty został punkcie 1)
- wieloskładnikowe uwierzytelnienie oraz zabezpieczenie dostępu do kluczowych aplikacji poprzez portal Single Sign-On (szczegółowy opis wymagań zawarty został punkcie 2)
- ochrona dostępu zdalnego (szczegółowy opis wymagań zawarty został punkcie 3)

1. Opis funkcjonalny systemu PAM/PAS

Zarządzanie kontami i dostępami uprzywilejowanymi

1.1. System musi posiadać funkcje zarządzania (automatycznej zmiany haseł, definiowania polityki dostępu) kontami uprzywilejowanymi w:
- 1.1.1 Systemach operacyjnych: Windows, Unix, Linux, iSeries (AS/400), zSeries (OS/390)
- 1.1.2 Bazach danych: Microsoft SQL, Microsoft SQL Cluster Service, Oracle, Informix, MySQL, Sybase Adaptive Server Enterprise, DB2, Informatica, MariaBD, MongoDB, PostgreSQL
- 1.1.3 Systemach zarządzania infrastrukturą, aplikacjach: DELL DRAC, RSA authentication Manager, HP iLO, SAP
- 1.1.4 Urządzeniach sieciowych oraz systemach bezpieczeństwa: Cisco (routery, seria nexus, firewalle), HP, Checkpoint, Netscreen, Infoblox NIOS, FireEye Malware Analysis, FortiGate, Aruba, Palo Alto Networks, A10, Riverbed
- 1.1.5 Narzędziach CI/CD: Chef, Jenkins, GitHub, Red Hat Ansible
- 1.1.6 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), Google Cloud Platform (Service Accounts, IAM Users), VMWare Cloud Foundation
- 1.1.7 Modułach: Microsoft Services, Scheduled tasks, IIS application Pool, IIS Directory Security, w rejestrach, COM+, zarządzanie kontami w domenie Microsoft
- 1.1.8 Plikach konfiguracyjnych, tabelach baz danych
- 1.1.9 Środowiskach wirtualizacyjnych VMWare ESX/ESXi

1.2. System musi zapewniać wsparcie (ochronę kont) dla dowolnego urządzenia obsługującego ODBC w wersji 2.7 lub wyższej

1.3. 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 250 unikalnych integracji udostępnionych w ramach wspomnianego portalu.

1.4. 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.

1.5. 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.

1.6. 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

1.7. System musi posiadać możliwość ochrony (zarządzania) oraz dynamicznego generowania (w formie pseudolosowej) nowego klucza SSH zgodne z określonym szablonem

1.8. System musi automatycznie porównywać hasło/klucz SSH przechowywane w systemie oraz hasło/klucz SSH przechowywane na systemie docelowym

1.9. System musi automatycznie synchronizować hasło (oraz klucz SSH) przechowywane w systemie oraz hasło (oraz klucz SSH) przechowywane na systemie docelowym w przypadku wykrycia niezgodności.

1.10. 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)

1.11. System musi wspierać różne środowiska LDAP do uwierzytelniania użytkowników, nie mniej niż Sun One, MS Active-Directory, IBM Tivoli, Novel eDirectory, Oracle Internet Directory

1.12. System musi umożliwiać wykrywanie par kluczy SSH w danej infrastrukturze

1.13. System musi umożliwiać zarządzanie i zapewniać bezpieczeństwo kluczy SSH używanych przez aplikacje w przypadku przechowywania kluczy w plikach konfiguracyjnych

1.14. Producent musi udostępniać bezpłatnie dodatkową aplikację umożliwiającą automatyzację procesu tworzenia nowych skryptów do rotacji poświadczeń w systemach 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.

Zarządzanie sesjami uprzywilejowanymi

1.15. 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). 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. W przypadku zestawienia połączeń przez przeglądarkę internetową narzędzie musi posiadać moduł umożliwiający realizację procesu utwardzania przeglądarki internetowej przez którą realizowana jest sesja uprzywilejowana (np. wyłączanie paska adresu, menu, narzędzi, widok theater mode, blokowanie wpisywania znaków podczas wypełniania danych dostępowych etc.)

1.16. System musi umożliwiać zestawianie i zarządzanie sesjami uprzywilejowanymi do systemów chronionych (w sposób opisany w punkcie 1.15 niniejszego dokumentu, 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):

1.16.1. Systemów operacyjnych: Windows, Unix, Linux, iSeries (AS/400), zSeries (OS/390)

1.16.2. Baz danych: Microsoft SQL, Oracle, MySQL, SAP HANA, HeidiSQL

1.16.3. Systemów zarządzania infrastrukturą, aplikacji: DELL DRAC, RSA authentication Manager, HP iLO, SAP GUI, BMC Remedy

1.16.4. Urządzeń sieciowych oraz systemów bezpieczeństwa: Cisco (routery, seria nexus, firewalle), HP, Checkpoint, Radware, F5 Networks, FortiGate, Palo Alto Networks

1.16.5 Narzędzi CI/CD (https, ssh): Chef, Jenkins, Docker, Jfrog

1.16.5. Aplikacji typu SaaS/ stron web/ interfejów web, minimum takich jak: Facebook (konta marketingowe), Amazon Web Services (konsola zarządzania, IAM, integracja z STS), Zarządzanie Microsoft Azure

1.16.6. Środowisk wirtualizacyjnych VMWare ESX/ESXi, vCenter (vSphere Client, https, ssh)

1.17. System musi posiadać wsparcie (dla monitoringu i separacji sesji oraz realizacji funkcji Single Sign-On dla kont uprzywilejowanych) dla innych aplikacji oraz systemów niż wskazane w punkcie 1.16 poprzez możliwość wykorzystania nie mniej niż: uruchomienia aplikacji ze wskazanym zbiorem parametrów, zastosowania opisowego języka skryptowego, wbudowanego komponentu pozwalającego na obsługę własnych aplikacji web.

1.18. 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 zgodnie z opisem zawartym w punkcie 1.15 niniejszego dokumentu.

1.19. System musi przechowywać nagrania sesji w zabezpieczonym kryptograficznie repozytorium uniemożliwiającym ich manipulację. 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)

1.20. System musi umożliwiać ograniczanie dostępu do systemów docelowych oraz tworzenie list dopuszczalnych i niedopuszczalnych poleceń wykonywanych poprzez SSH

1.21. System musi zapewniać rozliczalność w przypadku jednoczesnego wykorzystania konta współdzielonego przez więcej niż jednego użytkownika

1.22. 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.

1.23. System musi umożliwiać wykorzystanie przez moduł proxy opisany w punkcie 1.15 funkcjonalności Microsoft Remote App w celu publikowania aplikacji dostępowych. Skrypty utwardzające (and. Hardening) muszą być dostarczone przez Producenta rozwiązania oraz uruchomione podczas instalacji rozwiązania

1.24. System musi umożliwiać dostęp użytkowników do zasobu docelowego zgodnie z wymaganiami opisanymi w punkcie 1.15 przy wykorzystaniu nie mniej niż następujących metod / narzędzi:

1.24.1. Interfejs Web proponowanego rozwiązania

1.24.2. 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.

1.24.3. 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.

1.24.4. Wykorzystanie różnych klientów linii poleceń i protokołu SSH (np. putty), przy czym wspierana musi metoda uwierzytelnienia do systemu bazująca na kluczach SSH.

1.25. 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 protokół HTTPS (sesja tunelowana w html5 - mechanizm zestawiania sesji opisany w punkcie 1.23)

1.26. 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.

1.27. 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.

1.28. System musi umożliwiać transmisję plików oraz wykorzystanie schowka dla sesji tunelowanych w html5 (mechanizm zestawiania sesji opisany w punkcie 1.2.3)

1.29. Po uwierzytelnieniu wieloskładnikowym w portalu graficznym rozwiązania system musi umożliwiać wygenerowanie klucza SSH na potrzeby bezpiecznego dostępu do systemów chronionych poprzez moduł proxy opisany w punkcie 1.24.4 bez konieczności wpisywania dodatkowych składników uwierzytelniających. 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 passphrase (o definiowalnej w oferowanym systemie długości oraz złożoności) oraz określenia w polityce systemu czasu ważności klucza.

Zarządzanie incydentami bezpieczeństwa

1.30. System musi posiadać funkcję kategoryzacji nagranych sesji użytkowników pod kątem ryzyka. Ryzyko opisane musi być poprzez konfigurację przez administratora systemu zbioru wykrywanych w trakcie trwania sesji funkcji / poleceń i przypisanej do nich wagi. 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). Administrator musi posiadać możliwość określenia akcji wykonanych przez użytkownika dla których sesja powinna być automatycznie zakończona / wstrzymana.

1.31. 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 liczba odwołań do repozytorium kont o hasła)

1.32. System musi umożliwiać pobieranie danych o aktywnościach użytkowników z zewnętrznych systemów SIEM, wspierane muszą być nie mniej niż następujące rozwiązania: Arcsight, Qradar, Splunk, LogRhythm, RSA, McAfee oraz zewnętrzne źródła informacji, minimum rsyslog (z systemów Unix/Linux), Windows Event Forwarder (z systemów Windows), AWS CloudTrail, Azure Function App

1.33. System musi umożliwiać podjęcie aktywnej akcji (co najmniej wymuszenie zmiany hasła konta uprzywilejowanego) w przypadku wykrycia anomalii wykorzystania kont uprzywilejowanych (nie mniej niż: kradzież hasła konta uprzywilejowanego; utworzenie nowego konta i próba zestawienia nim połączenia z serwerem)

1.34. 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)

1.35. 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. 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.

1.36. System musi umożliwiać wykrywanie nowych, niezarządzanych kont uprzywilejowanych oraz połączeń, które zostały nawiązane bez uprzedniego pobrania hasła z centralnego repozytorium, realizowanych w środowisku AWS i Azure

1.37. 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)

Architektura

1.38. Całość rozwiązania dostarczona musi być przez tego samego producenta, poszczególne moduły funkcjonalne muszą integrować się ze sobą

1.39. 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).

1.40. 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 oraz zabezpieczenie dostępu do kluczowych aplikacji Web (wewnętrznych oraz chmurowych) poprzez moduł Single Sign-On dla użytkowników biznesowych (wymagania opisane w sekcji 2)
- ochronę dostępu zdalnego dla pracowników i zewnętrznych dostawców (wymagania opisane w sekcji 2 oraz 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)
- 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

1.41. 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. Utwardzanie każdego z komponentów musi być realizowane w oparciu o dobre praktyki producenta systemu operacyjnego oraz producenta rozwiązania PAM/PAS. Utwardzanie systemu operacyjnego modułu repozytorium poświadczeń musi być realizowane automatycznie przez instalator podczas procesu instalacji modułu.

1.42. 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

1.43. 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).

1.44. 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.

1.45. 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

1.46. Produkt musi zapewniać ochronę kryptograficzną kopii zapasowych generowanych z produktu

1.47. 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, możliwość zestawiania sesji uprzywilejowanych w sposób opisany w punkcie 1.15). Proponowane rozwiązanie musi obsługiwać nie mniej niż 6 aktywnych repozytoriów poświadczeń. W przypadku infrastruktury rozproszonej całość systemu musi być zarządzana z centralnego interfejsu graficznego.

1.48. 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 zapasowych (ang. Disaster Recovery) w innych lokalizacjach (musi istnieć możliwość wdrożenia do 4 modułów Disaster Recovery w ramach podstawowej licencji czasowej przy wdrożonym HA w okalizacji podstawowej)

Integracje

1.49. System musi umożliwiać integrację z systemami SIEM w celu wysyłania informacji o zarejestrowanych zdarzeniach w ramach monitorowanych sesji. Musi istnieć możliwość zdefiniowania typu zdarzeń, które powinny być wysłane do systemu SIEM.

1.50. 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

1.51. System musi wspierać integrację z rozwiązaniami typu HSM obsługującymi standard PKCS11, wymagana jest integracja z systemami: Atos HSM Proteccio, Thales Luna, Entrust nShield, Utimaco CryptoServer, Crypto4A QxEDGE, Fortanix SDKMS, i4p Trident, Unbound Key Control, Utimaco CryptoServe.

1.52. 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)

Wymagania dodatkowe

1.53. System musi posiadać skorelowaną ze sobą oficjalną metodykę implementacji, udostępnianą przez producenta systemu na stronie internetowej producenta. Metodyka ta musi zawierać 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.

1.54. Proponowany system musi znajdować się w kwadracie "Leaders" wszystkich raportów Gartner Magic Quadrant for Privileged Access Management począwszy od raportu wydanego za rok 2018 włącznie.

2. Wieloskładnikowe uwierzytelnienie, SSO oraz ochrona poświadczeń użytkowników

Podstawowe funkcjonalności systemu

2.1. System musi realizować funkcję:
- wieloskładnikowego adaptacyjnego uwierzytelnienia
- zabezpieczenia dostępu zarówno do wewnętrznych jak i zewnętrznych aplikacji (SaaS) poprzez wykorzystanie zabezpieczonego portalu SSO
- zarządzania cyklem życia tożsamości (ang. lifecycle management, wymagający dodatkowej licencji czasowej)
- przechowywania poświadczeń użytkownika biznesowego w centralnym repozytorium zainstalowanym w środowisku Zamawiającego. Wymagane jest, aby poświadczenia użytkowników w ramach repozytorium składowane były w formacie zaszyfrowanym przy wykorzystaniu zarówno kluczy symetrycznych, nie mniej niż AES256, jak również asymetrycznych, nie mniej niż RSA2048. Musi istnieć możliwość integracji z systemem PAM/PAS (wymagania opisane w punkcie 1) na potrzeby realizacji tego wymagania.

2.2. System musi być dostarczony jako usługa zewnętrzna (SaaS) wraz z modułem konektora, umożliwiającym integrację ze środowiskiem usług katalogowych AD/LDAP oraz uruchomienie serwera Radius dla klientów sieciowych Zamawiającego.

2.3. Rozwiązanie nie może ograniczać licencyjnie liczby konektorów możliwych do zainstalowania w środowisku Zamawiającego

2.4. Rozwiązanie musi wspierać obsługę języka polskiego minimum dla interfejsu użytkownika i aplikacji mobilnej dostępnej dla systemów operacyjnych Android i iOS

2.5. Proponowany system musi znajdować się w kwadracie "Leaders" raportu Gartner Magic Quadrant for Access Management wydanego za rok 2022.

2.6. System musi zapewniać dodatkowy komponent (poprzez dodatkową subskrypcję, nieuwzględniony w obecnej fazie projektu) jako rozszerzenie modułu SSO, pozwalający na realizację dla dowolnej aplikacji web nie mniej niż następujących funkcjonalności:
- rejestrowanie wszystkich działań użytkowników z wykorzystaniem podejścia „krokowego”. System musi wywoływać zrzut ekranu okna przeglądarki użytkownika wraz z odpowiednimi metadanymi dla co najmniej następujących czynności wykonywanych przez użytkownika podczas monitorowanej sesji internetowej: kliknięcie myszką, naciśnięcie klawiszy „enter” lub „tab”. System musi umożliwiać wyszukiwanie wszystkich nagranych sesji za pomocą dowolnego wprowadzania tekstu oraz filtrowanie zdarzeń związanych z bezpieczeństwem według dat i działań.
- zidentyfikowanie, kiedy sesja wysokiego ryzyka pozostaje otwarta i wymaga ponownego uwierzytelnienia, aby upewnić się, że osoba, która zainicjowała sesję internetową, jest osobą uprawnioną,
- ochronę sesji internetowej na punkcie końcowym za pomocą rozszerzenia przeglądarki

- kontrolowanie wartości wprowadzanych przez użytkownika do pól tekstowych aplikacji web. System musi umożliwiać generowanie incydentów w przypadku wykrycia nadużyć, dla nie mniej niż następujących sytuacji: wartość liczbowa wprowadzona przez użytkownika przekracza zdefiniowany w systemie próg, użytkownik przechodzi do miejsca w aplikacji, które jest szczególnie wrażliwe i zbudowana dla niego została polityka monitorująca. Jako reakcje na incydenty systemu musi udostępniać nie mniej niż: oznaczenie zdarzenia w systemie monitoringu sesji web, wysłanie powiadomienia na zdefiniowany adres email, wysłanie powiadomienia typu push do aplikacji mobilnej wybranego użytkownika. Tworzenie reguł musi być możliwe poprzez wykorzystanie pluginu zainstalowanego w przeglądarce administratora, bez konieczności dostępu do interfejsu graficznego rozwiązania.

2.7. System musi zapewniać dodatkowy komponent (poprzez dodatkową subskrypcję, nieuwzględniony w obecnej fazie projektu) jako rozszerzenie modułu SSO, pozwalający na realizację dla dowolnej aplikacji web funkcjonalności certyfikacji dostępu umożliwiającej przeprowadzanie cyklicznych kampanii mających na celu automatyzację procesu nadawania i odwoływania dostępu użytkownika na podstawie procesu akceptacyjnego

2.8. System musi zapewniać funkcjonalność certyfikacji dostępu (poprzez dodatkową subskrypcję, nieuwzględnioną w obecnej fazie projektu) w celu automatycznej weryfikacji, nadawania lub cofania uprawnień, jakie użytkownik posiada w systemie PAM/PAS (wymagania opisane w punkcie 1).

2.9. System musi zapewniać dodatkowy komponent (poprzez dodatkową subskrypcję, nieuwzględniony w obecnej fazie projektu) jako rozszerzenie modułu SSO, pozwalający na realizację dla aplikacji funkcjonalności: zarządzania cyklem życia użytkownika, polegającej na pobieraniu atrybutów konta użytkownika z systemu HR (wymagane jest wsparcie dla nie mniej niż BambooHR, SAP SuccessFactors, Workday, UltiPro) i przekazaniu ich do docelowej aplikacji web w ramach procesu tworzenia konta nowego użytkownika.

2.10. System musi zapewniać dodatkowy komponent (poprzez dodatkową subskrypcję, nieuwzględniony w obecnej fazie projektu) jako rozszerzenie modułu SSO, pozwalający na realizację integracji pomiędzy różnymi systemami źródłowymi i docelowymi, rozumianą jako możliwość pobrania danych wejściowych z systemu źródłowego (np. z wykorzystaniem API) i przekazania ich z zmienionej lub zmodyfikowanej formie do systemu docelowego (np. również z wykorzystaniem API). System musi udostępniać interfejs użytkownika umożliwiających opisanie wymaganych przepływów danych w ujęciu no-code (bez konieczności opisywania wymaganych założeń za pomocą języków skryptowych). System musi wspierać integrację z rozwiązaniami klasy EDR (minimum CrowdStrike), rozwiązaniami bezpieczeństwa (ProofPoint) i rozwiązaniem PAM/PAS (wymagania opisane w punkcie 1) z wykorzystaniem gotowych szablonów integracji dostępnych w formie out of the box.

2.11. System musi zapewniać dodatkowy komponent (poprzez dodatkową subskrypcję, nieuwzględniony w obecnej fazie projektu) jako rozszerzenie modułu MFA, pozwalający na realizację silnego uwierzytelniania wieloskładnikowego na poziomie systemu operacyjnego, wymuszanego podczas podnoszenia uprawnień oraz uruchamiania aplikacji realizowanego przez użytkownika. Warunki wymuszające egzekwowanie MFA muszą być opisane w ramach polityki powiązanej z kontrolą aplikacji uruchamianych na systemie operacyjnym. Wymagana jest możliwość budowanie polityki kontrolującej aplikacje w oparciu o warunki dopasowujące nie mnie niż: Filename, Checksum, Parameters, Location type, Owner, Product name, File description, Company name, Original filename, File version, Product version, Source, Parent process. Wymagane jest wsparcie dla nie mniej niż następujących systemów operacyjnych: Windows 7 x32 & x64, Windows 8/8.1 x32 & x64, Windows 10 x32 & x64, Windows 11 x64, Windows Server 2008 x32 & x64, Windows Server 2008 R2 x64, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, macOS Big Sur 11, macOS Monterey 12, macOS Ventura 13.

Wieloskładnikowe uwierzytelnianie

2.12. Wymagana jest możliwość obsługi minimum następujących składników uwierzytelniających: hasło, sms, email, oauth, aplikacja mobilna, phone call, pytanie bezpieczeństwa, składniki kompatybilne ze

standardem Fido2 (np. token sprzętowy, Windows hello, touch id), certyfikat użytkownika, karta PIV/CAC, Qrcode generowany w ramach procesu uwierzytelnienia do interfejsu Systemu (umożliwiający uwierzytelnienie użytkownika przy użyciu aplikacji mobilnej uprzednio zarejestrowanej w systemie).

2.13. 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")

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

2.15. System musi posiadać edytor graficzny do tworzenia niestandardowych przepływów uwierzytelniania, umożliwiający tworzenie reguł uwierzytelniania, z nie mniej niż następującymi możliwościami:

- możliwość zbudowania przepływu uwierzytelniania do portalu użytkownika, wymuszającego wskazaną kombinacje składników uwierzytelniających w oparciu o warunki typu if-else (mechanizm ten musi umożliwiać szczegółowe definiowanie zależności np. jeśli użytkownik jako pierwszy składnik wybierze hasło, jako drugi składnik musi wybrać otp, natomiast jeśli jako pierwszy składnik wybierze aplikację mobilną – nie będzie poproszony o drugi składnik. W przeciwnych wypadkach wymagane będzie uwierzytelnianie w oparciu o QRCode) i filtry (nie mniej niż adres IP, plik cookie, dzień tygodnia, data, zakres dat, zakres czasowy, System operacyjny urządzenia, przeglądarka, kraj, poziom ryzyka, uwierzytelnianie certyfikatu)
- aplikacje internetowe, możliwość zbudowania przepływu uwierzytelniania, wymuszającego wskazaną kombinacją składników uwierzytelniających w oparciu o warunki typu if-else (mechanizm ten musi umożliwiać szczegółowe definiowanie zależności np. jeśli użytkownik jako pierwszy składnik wybierze hasło, jako drugi składnik musi wybrać otp, natomiast jeśli jako pierwszy składnik wybierze aplikację mobilną – nie będzie poproszony o drugi składnik. W przeciwnych wypadkach wymagane będzie uwierzytelnianie w oparciu o QRCode) i filtry (nie mniej niż adres IP, plik cookie uwierzytelniania, dzień tygodnia, data, zakres dat, zakres czasu, system operacyjny urządzenia, Przeglądarka, Rola, Kraj, Zarządzane urządzenie, Poziom ryzyka, Uwierzytelnianie certyfikatu)
- ogólny profil uwierzytelniania, możliwość zbudowania przepływu uwierzytelniania, wymuszającego wskazaną kombinacją składników uwierzytelniających w oparciu o warunki typu if-else (mechanizm ten musi umożliwiać szczegółowe definiowanie zależności np. jeśli użytkownik jako pierwszy składnik wybierze hasło, jako drugi składnik musi wybrać otp, natomiast jeśli jako pierwszy składnik wybierze aplikację mobilną – nie będzie poproszony o drugi składnik. W przeciwnych wypadkach wymagane będzie uwierzytelnianie w oparciu o QRCode) i filtry.

2.16. System musi udostępniać aplikację do generowania kodów OTP dostępną dla systemu operacyjnego Windows. Podczas uruchamiania aplikacja po zarejestrowaniu musi wymuszać od użytkownika podaniu kodu PIN zdefiniowanego podczas procesu rejestracji.

2.17. System musi posiadać wbudowane narzędzie obrazujące na bieżąco minimalny i maksymalny poziom AAL (Authenticator Assurance Level) możliwy do uzyskania za pomocą składników uwierzytelniających wybranych w profilu uwierzytelniającym.

2.18. System musi posiadać moduł integracji z systemem ADFS umożliwiający wymuszanie mechanizmu MFA bez konieczności modyfikacji zintegrowanej aplikacji.

2.19. System musi posiadać wbudowany moduł analizujący zachowanie i profilowanie użytkownika w oparciu o nie mniej niż następujące parametry: historia profilu logowania, charakterystyka godzin i dni tygodnia logowań, charakterystyka zmian geolokalizacyjnych użytkownika, obecność zaufanego certyfikatu na urządzeniu, z którego zestawiane jest połączenie, lokalizacja z której realizowane jest połączenie. W zależności od wyliczonego poziomu ryzyka musi istnieć możliwość przypisania odpowiednich profili uwierzytelniających oraz blokowania dostępu.

2.20. System musi umożliwiać wysłanie powiadomień o wystąpieniu ryzykownych zdarzeń z wykorzystaniem webhook

2.21. System musi posiadać ochronę przed atakami klasy phishing (potwierdzenie, iż użytkownik loguje się do odpowiedniego portalu) poprzez wybór przez użytkownika końcowego obrazka wyświetlanego przy każdym logowaniu do portalu

2.22. Platforma SaaS musi posiadać certyfikację SOC2 Type 2

SSO

2.23. System musi realizować usługę SSO dla aplikacji chmurowych oraz wewnętrznych, realizując w sposób scentralizowany bezpieczne uwierzytelnienie przy wykorzystaniu metod opisanych w punkcie 2. 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

2.24. 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.

2.25. 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)

2.26. Dla aplikacji web, które nie wspierają protokołów SSO (jak SAML) musi istnieć możliwość integracji z wykorzystaniem uwierzytelniania w oparciu o nazwę użytkownika i hasło. Dla tego typu aplikacji użytkownik musi mieć możliwość samodzielnego podania w systemie danych uwierzytelniających. Podczas połączenia plugin zainstalowany w przeglądarce użytkownika musi dokonywać procesu automatycznego uzupełniania poświadczeń we właściwe pola aplikacji web. System musi umożliwiać składowanie poświadczeń wprowadzonych przez użytkownika w centralnym repozytorium zainstalowanym w środowisku Zamawiającego. Wymagane jest, aby poświadczenia użytkowników w ramach repozytorium składowane były w formacie zaszyfrowanym przy wykorzystaniu zarówno kluczy symetrycznych, nie mniej niż AES256, jak również asymetrycznych, nie mniej niż RSA2048. Musi istnieć możliwość integracji z systemem PAM/PAS (wymagania opisane w punkcie 1) na potrzeby realizacji tego wymagania.

2.27. System musi automatycznie rozpoznawać wizyty na nowych stronach web, gdzie użytkownik zostanie poproszony o uwierzytelnienie. Dane uwierzytelniające podane przez użytkownika muszą zostać przechwycone i zapisane w repozytorium haseł oraz odpowiednia nowa aplikacja web musi zostać dodana do katalogu aplikacji w portalu SSO. System musi umożliwiać składowanie poświadczeń wprowadzonych przez użytkownika w centralnym repozytorium zainstalowanym w środowisku Zamawiającego. Wymagane jest, aby poświadczenia użytkowników w ramach repozytorium składowane były w formacie zaszyfrowanym przy wykorzystaniu zarówno kluczy symetrycznych, nie mniej niż AES256, jak również asymetrycznych, nie mniej niż RSA2048. Musi istnieć możliwość integracji z systemem PAM/PAS (wymagania opisane w punkcie 1) na potrzeby realizacji tego wymagania.

Repozytorium poświadczeń

2.28. System musi umożliwiać składowanie poświadczeń oraz notatek wprowadzonych przez użytkownika w centralnym repozytorium zainstalowanym w środowisku Zamawiającego. Wymagane jest, aby poświadczenia użytkowników w ramach repozytorium składowane były w formacie zaszyfrowanym przy wykorzystaniu zarówno kluczy symetrycznych, nie mniej niż AES256, jak również asymetrycznych, nie mniej niż RSA2048. Musi istnieć możliwość integracji z systemem PAM/PAS (wymagania opisane w punkcie 1) na potrzeby realizacji tego wymagania.

2.29. System musi umożliwiać udostępnienie przez użytkownika (właściciela) poświadczeń i notatek innemu użytkownikowi lub grupie użytkowników.

2.30. System musi zapewnić wtyczkę do przeglądarki użytkownika z wbudowaną funkcją generatora haseł. Generator haseł musi umożliwiać określenie co najmniej długości hasła i stopnia złożoności nowo generowanego hasła (system musi umożliwiać wybór, czy w nowo generowanym haśle mają być użyte cyfry, symbole, wielkie i małe litery)

2.31. System musi umożliwiać zdefiniowanie mechanizmu TOTP w interfejsie graficznym systemu dla aplikacji web które wymagają TOTP podczas procesu uwierzytelniania. Właściciel biznesowy aplikacji wraz ze zdefiniowany TOTP oraz administrator systemu muszą mieć możliwość udostępnienia zintegrowanego z aplikacją web TOTP innym użytkownikom.

2.32. System musi posiadać możliwość definiowania w interfejsie nowego właściciela aplikacji oraz poświadczeń, umożliwiający tym samym dostęp w przypadku gdy dotychczasowy właściciel opuści organizację.

3 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).

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, Android. 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, zgodnie z wymaganiami punktu 1.24.3. niniejszego dokumentu.

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 gwarancyjne - Wsparcie

4.1. System musi być dostarczony wraz z usługą wsparcia technicznego dostarczoną przez producenta rozwiązania.

4.2. Wsparcie techniczne musi uwzględniać rozwiązywanie problemów z dostępem do platformy, błędów działania, wydajności i aktualizacji agenta Systemu. W następującym zakresie czasowym:

Priorytet	Czas podjęcia	Czas na rozwiązanie
Błąd krytyczny	ↄ 2 godzin dnia roboczego	ↄ 8 godzin dnia roboczego
Błąd istotny	ↄ 6 godzin dania roboczego	ↄ 5 dni roboczych

Przy czym:

1) Błąd krytyczny to błąd, który uniemożliwia korzystanie z Systemu.
2) 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.
3) Czas na rozwiązanie to czas od momentu zgłoszenia błędu do momentu wprowadzenia poprawek przywracających prawidłowe, bezbłędne korzystanie z Systemu.
4) Czas podjęcia - okres od momentu zgłoszenia błędu do momentu podjęcia pierwszych czynności diagnostycznych przez Wykonawcę.

4.3 W ramach wsparcia Zamawiający wymaga

4.3.1 usług 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.:

4.3.1.1 implementacja krytycznych poprawek systemu zalecanych przez producenta

4.3.1.2 aktualizacja systemu do nowych wersji zalecanych przez producenta,

4.3.1.3 cykliczne, nie częściej niż raz na pół roku, przeglądy kwartalne systemu,

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

4.3.1.5 przyjmowanie i obsługa zgłoszeń problemów: 24 godziny na dobę, 7 dni w tygodniu przyjmowanie zgłoszeń problemów oraz zgłaszanie problemów wymagających rozwiązania przez producenta, w ramach wykupionego przez Klienta wsparcia producenta. Czas reakcji Wykonawcy na zgłoszenie to 30 min

4.3.2 Usługa wsparcia w ramach usuwania musi być dostępna z możliwością zgłaszania problemów za pomocą telefonu, wiadomości e-mail lub dedykowanego portalu www.

4.4. Wsparcie musi zapewniać dostęp do bazy wiedzy producenta oraz materiałów szkoleniowych producenta.

4.5. W ramach usługi wsparcia wymaga się od konsultanta wsparcia w zakresie dostosowywania zasad i najlepszych praktyk, przypadków użycia oraz architektury rozwiązania

4.6. Oferent w zakresie dostarczonych licencji czasowych wykona prace wdrożenia referencyjnego obejmującego implementację zdalnego dostępu przy pomocy kont domenowych lub lokalnych do:

4.6.1. Serwerów Windows w ilości nie mniejszej niż 5 i nie większej niż 25 systemów.

4.6.2. Serwerów Linux w ilości nie mniejszej niż 5 i nie większej niż 25 systemów.

4.6.3. Aplikacji Web opartych o HTML5 w ilości nie mniejszej niż 2 i nie większej niż 5 systemów.

4.6.4. Dostęp do aplikacji typu ERP tzw. „gruby klient" instalowany na stacji przesiadkowej.

4.6.5. Szkolenie dla *administratorów* systemu PAM - max do 8h. dostępne w formule zdalnej.

4.6.6. Instrukcje dla użytkowników PAM w formacie PDF beż szkoleń indywidulanych.

4.6.7. Wdrożenie standardowej infrastruktury (maksymalnie 2 wystąpienia danego komponentu).

5. Instruktaż dla pracowników Zamawiającego

5.1 Wykonawca przeprowadzi dla nie więcej niż 3 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.

5.2 Lista uczestników instruktażu zostanie ustalona drogą mailową z Wykonawcą po podpisaniu umowy.

5.3 Instruktaż zostanie zorganizowany w czasie trwania wdrożenia Systemu.

5.4 Termin przeprowadzenia instruktażu zostanie ustalony pomiędzy Zamawiającym a Wykonawcą drogą mailową.

5.5 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.

5.6 Instruktaż będzie trwał łącznie minimum 4 godziny zegarowe. Przy czym Zamawiający dopuszcza możliwość realizacji szkolenia w ramach cyklicznych warsztatów.

5.7 Harmonogramy zajęć zostaną ustalone drogą mailową z Zamawiającym.

5.8 Wykonawca musi posiadać certyfikację producenta Systemu w zakresie prowadzenia instruktażu z wdrożonego u Zamawiającego Systemu.

5.9 Dla uczestników instruktażu Wykonawca przygotuje środowisko testowe z zainstalowaną wersją Systemu tożsamą dla wdrożonego u Zamawiającego Systemu pozwalające na zapoznanie się, z elementami interfejsu graficznego oraz wykonanie ćwiczeń w warunkach możliwie zbliżonych do realnych.

5.10 Wykonawca zapewni dla każdego uczestnika wersję elektroniczną materiałów dydaktycznych zawierających streszczenie/omówienie wszystkich zagadnień zawartych w programie instruktażu oraz prezentacje wykorzystane podczas instruktażu.

5.11 Jeśli na potrzeby realizacji instruktażu powstaną materiały edukacyjne będące utworami w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2022 poz. 2509) będą udostępnione na wolnej licencji zapewniającej licencjobiorcy prawo do dowolnego wykorzystywania utworów do celów komercyjnych i niekomercyjnych, tworzenia i rozpowszechniania kopii utworów w całości lub we fragmentach oraz wprowadzania zmian i rozpowszechniania utworów zależnych.

5.12 Zakres tematyczny instruktażu będzie zawierał się w niniejszych obszarach:

- Architektura produktu
- Poruszanie się po interfejsie użytkownika
- Planowanie wdrożenia systemu wraz z architekturą systemu
- Instalacja konsoli zarządzania i agentów na stacjach końcowych
- Konfiguracja reguł filtrujących/analizujących dla dedykowanego systemu końcowego.
- Wykonanie przykładowych scenariuszy.
- Analiza i raportowanie wyników.

- Konfiguracja zadań.
- Zarządzanie użytkownikami i rolami