Załącznik nr 1 do Zaproszenia

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa oprogramowanie typu PAM (Privileged Account Management) do zarządzania kontami uprzywilejowanymi

Rozdział I. Przedmiot zamówienia

1. Przedmiotem zamówienia jest dostawa oprogramowania PAM (Privileged Access Management), umożliwiającego jednoczesną pracę 600 użytkowników/administratorów Zamawiającego, służącego do zabezpieczania tożsamości, poprzez monitorowanie i wykrywanie nieuprawnionego dostępu uprzywilejowanego do zasobów o kluczowym znaczeniu, w modelu subskrypcyjnym obowiązującej przez okres 12/24/36 miesięcy, zwanego dalej Oprogramowaniem lub PAM.
2. Zamówienie w zakresie podstawowym obejmuje:
   1) Dostawę Oprogramowania umożliwiającego jednoczesną pracę 600 użytkowników/administratorów Zamawiającego, z uwzględnieniem wymagań opisanych w rozdziale II;
   2) Instalację Oprogramowania na środowisku testowym, zgodnie z wymaganiami opisanymi w rozdziale III
   3) Świadczenie gwarancji dla Oprogramowania przez okres 36 miesięcy, zgodnie z wymaganiami opisanymi w rozdziale IV
3. Zamówienie w zakresie prawa opcji obejmuje:
   1) Wdrożenie Oprogramowania dostarczonego w ramach zamówienia podstawowego, w tym: dokumentację, instalację, konfigurację, uruchomienie w środowisku produkcyjnym, zgodnie z wymaganiami opisanymi w rozdziale V.
   2) Przeprowadzenie przeszkolenia dla maksymalnie 10 osób wskazanych przez Przedstawiciela Zamawiającego w zakresie administrowania i zarządzania, zgodnie z wymaganiami opisanymi w rozdziale V.
   3) Konsultacje i asystę w zakresie dostarczonego Oprogramowania w wymiarze do 600 godzin, zgodnie z wymaganiami opisanymi w rozdziale V
   4) Dostarczenie Oprogramowania – do 50% zamówienia podstawowego, umożliwiającego jednoczesną pracę max dla 300 użytkowników/administratorów Zamawiającego, zgodnie z wymaganiami opisanymi w rozdziale V
4. Oprogramowanie musi umożliwiać instalacje w rozproszonym środowisku produkcyjnym Zamawiającego oraz w środowisku testowym.

Rozdział II. Wymagane funkcjonalności Oprogramowania

1. Opis funkcjonalny Oprogramowania

Zarządzanie kontami i dostępami uprzywilejowanymi

1.1. Oprogramowanie musi posiadać funkcje zarządzania (automatycznej zmiany haseł, definiowania polityki dostępu) kontami uprzywilejowanymi w:
   a) Systemach operacyjnych: Windows, Unix, Linux,

b) Bazach danych: Microsoft SQL, Microsoft SQL Cluster Service, Oracle, MySQL, Sybase Adaptive Server Enterprise, DB2, MariaBD, MongoDB, PostgreSQL,
c) Systemach zarządzania infrastrukturą, aplikacjach: DELL DRAC, RSA authentication Manager, HP iLO,
d) Urządzeniach sieciowych oraz systemach bezpieczeństwa: Cisco (routery, seria nexus, firewalle), HP, Checkpoint, Infoblox NIOS, FireEye Malware Analysis, FortiGate, Aruba, Palo Alto Networks, Riverbed, F5 Networks, Huawei
e) Aplikacjach typu SaaS/ stronach web/ interfejsach web, minimum takich jak: Zarządzanie Microsoft Azure (klucze API oraz konta uprzywilejowane),
f) Modułach: Microsoft Services, Scheduled tasks, IIS application Pool, IIS Directory Security, w rejestrach, COM+, zarządzanie kontami w domenie Microsoft,
g) Plikach konfiguracyjnych, tabelach baz danych,
h) Środowiskach wirtualizacyjnych VMWare ESX/ESXi, vCenter (vSphere Client, https, ssh)

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

1.3. Oprogramowanie musi zapewniać wsparcie (możliwość zarządzania kontami uprzywilejowanymi wykorzystywanymi w obrębie systemu docelowego) dla systemów spoza listy "out of box"(systemów obsługiwanych przez dostarczone Oprogramowanie) 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. Oprogramowanie 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.

1.5. Oprogramowanie musi zapewniać możliwość automatycznego wykrywania kont w nowych systemach Windows, usługach systemu Windows, zaplanowanych zadaniach, kontach serwisowych IIS itp., automatycznego dodania powyższych do produktu oraz automatycznie wymusić odpowiednią politykę zarządzania kontami uprzywilejowanymi

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

1.7. Oprogramowanie musi automatycznie porównywać hasło/klucz SSH przechowywane w systemie oraz hasło/klucz SSH przechowywane na systemie docelowym

1.8. Oprogramowanie musi automatycznie synchronizować hasło (oraz klucz SSH) przechowywane w systemie oraz hasło (oraz klucz SSH) przechowywane na systemie docelowym w przypadku wykrycia niezgodności.
1.9. Oprogramowanie 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)
1.10. Oprogramowanie musi wspierać różne środowiska LDAP do uwierzytelniania użytkowników, nie mniej niż MS Active-Directory, IBM Tivoli, Oracle Internet Directory
1.11. Oprogramowanie musi umożliwiać wykrywanie par kluczy SSH w danej infrastrukturze
1.12. Oprogramowanie musi umożliwiać zarządzanie i zapewniać bezpieczeństwo kluczy SSH używanych przez aplikacje w przypadku przechowywania kluczy w plikach konfiguracyjnych
1.13. Producent musi udostępniać bezpłatnie dodatkową aplikację umożliwiającą automatyzację procesu tworzenia nowych skryptów do rotacji poświadczeń w systemach docelowych dostępnych z wykorzystaniem protokołu SSH. Oprogramowanie 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

1.14. 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 dowolnie wybranej aplikacji dane dostępowe, dzięki czemu nie muszą być one udostępniane stacji użytkownika). Oprogramowanie 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.)
1.15. Oprogramowanie musi umożliwiać zestawianie i zarządzanie sesjami uprzywilejowanymi do systemów chronionych (w sposób opisany w punkcie 1.14 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):

a) Systemów operacyjnych: Windows, Unix, Linux,
b) Baz danych: Microsoft SQL, Oracle, MySQL,
c) Systemów zarządzania infrastrukturą, aplikacjach: DELL DRAC, RSA authentication Manager, HP iLO,
d) Urządzeń zarządzania infrastrukturą, aplikacji: Cisco (routery, seria nexus, firewalle), HP, Checkpoint, F5 Networks, FortiGate, Palo Alto Networks
e) Aplikacji typu SaaS/ stronach web/ interfejsach web, minimum takich jak: Zarządzanie Microsoft Azure
f) Środowisk wirtualizacyjnych VMWare ESX/ESXi, vCenter (vSphere Client, https, ssh)

1.16. Oprogramowanie 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.

1.17. 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 1.14 niniejszego dokumentu.

1.18. Oprogramowanie 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)

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

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

1.21. 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, odpowiedzi okien systemu operacyjnego, komendy SQL). Nie jest dopuszczalnym dokonywanie indeksacji nagrań z wykorzystaniem mechanizmu OCR.

1.22. Oprogramowanie musi umożliwiać wykorzystanie przez moduł proxy opisany w punkcie 1.14 funkcjonalności Microsoft Remote App w celu publikowania

aplikacji dostępowych. Skrypty utwardzające (and. Hardening) muszą być dostarczone przez Producenta rozwiązania oraz uruchomione podczas instalacji rozwiązania

1.23. Oprogramowanie musi umożliwiać dostęp użytkowników do zasobu docelowego zgodnie z wymaganiami opisanymi w punkcie 1.14 przy wykorzystaniu nie mniej niż następujących metod / narzędzi:
   a) interfejs Web proponowanego rozwiązania
   b) wykorzystanie 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
   c) 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 1.14) musi być tunelowana w html5 i widoczna dla użytkownika jako nowa zakładka w przeglądarce
   d) wykorzystanie klientów linii poleceń i protokołu SSH (np. putty), przy czym wspierana musi metoda uwierzytelnienia do systemu bazująca na kluczach SSH.

1.24. 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 podpunkt c)

1.25. Oprogramowanie 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 Oprogramowanie uprawnienia JIT muszą być automatycznie odbierane po upływie czasu, na który został nadany dostęp.

1.26. Oprogramowanie 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.

1.27. Oprogramowanie musi umożliwiać transmisję plików oraz wykorzystanie schowka dla sesji tunelowanych w html5 (mechanizm zestawiania sesji opisany w punkcie 1.23 podpunkt c)

1.28. Po uwierzytelnieniu wieloskładnikowym w portalu graficznym rozwiązania system musi umożliwiać wygenerowanie klucza SSH na potrzeby bezpiecznego dostępu do systemów chronionych 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

1.29. Oprogramowanie 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.

1.30. Oprogramowanie 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)

1.31. Oprogramowanie 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), Azure Function App

1.32. Oprogramowanie 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)

1.33. Oprogramowanie 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)

1.34. Oprogramowanie 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.

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

1.36. Oprogramowanie 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)

Wymagania związane z architekturą

1.37. Oprogramowanie musi pochodzić od jednego producenta, poszczególne moduły funkcjonalne muszą integrować się ze sobą

1.38. Oprogramowanie 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).

1.39. Oprogramowanie musi posiadać budowę modularną, tzn. możliwość rozbudowy funkcjonalnej o kolejne komponenty tego samego producenta (funkcjonalności mogą być dostępne w ramach oddzielnych licencji czasowych) w poniższych obszarach zarządzania tożsamością:

a) wieloskładnikowe uwierzytelnienie użytkowników oraz zabezpieczenie dostępu do kluczowych aplikacji Web (wewnętrznych oraz chmurowych) poprzez moduł Single Sign-On
b) ochronę dostępu zdalnego dla pracowników i zewnętrznych dostawców
c) 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.
d) zapewnienie funkcjonalności certyfikacji dostępów celu automatycznej weryfikacji, nadawania lub cofania uprawnień, jakie użytkownik posiada w Oprogramowaniu PAM
e) agentowe ograniczanie uprawnień użytkowników na stacjach Windows oraz serwerach Windows, Linux 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 oraz aplikacji (np. przeglądarek internetowych, pamięci LSASS, SAM i innych)

f) dodatkowy komponent 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 budowania polityki kontrolującej aplikacje w oparciu o warunki dopasowujące nie mniej 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 10 x32 & x64, Windows 11 x64, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022.
g) ochronę sekretów używanych w środowiskach DevOps umożliwiając automatyczne pobieranie poświadczeń z centralnego repozytorium przez narzędzia wykorzystywane w procesach CI/CD oraz przez platformy konteneryzacyjne
h) Automatyczne wykrywanie oraz synchronizację sekretów zarządzanych przez centralny system PAM do natywnych sejfów w środowiskach cloud takich jak Azure, Google Cloud lub AWS
i) ochronę kont uprzywilejowanych zaszytych w kodzie statycznych aplikacji i skryptów
j) automatyczną klasyfikację ryzyka związanego ze zbyt obszernymi uprawnieniami w środowiskach chmurowych
k) budowanie polityk dostępowych w modelu Just-In-Time nadających uprawnienia na podstawie zdefiniowanych reguł bezpieczeństwa
l) nadanie wymaganych uprawnień na podstawie wniosku złożonego w ramach systemu przez użytkownika końcowego na określony czas
m) 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). Oprogramowanie musi udostępniać interfejs użytkownika umożliwiających opisanie wymaganych przepływów danych w ujęciu no-code (bez konieczności opisywania wymaganych założeń za pomocą języków skryptowych)

1.40. Dostawca musi posiadać produkt pozwalający na rozszerzenie obszaru PAM o zarządzanie cyklem życia certyfikatów SSL/TLS, odpowiedzialne za nie mnie niż:

a) automatyczne wykrywanie certyfikatów TLS na serwerach w środowisku IT organizacji
b) zarządzanie certyfikatami SSL/TLS pozwalające na: automatyczny proces odnowienia certyfikatów na serwerach, generowanie nowych certyfikatów, ochronę kluczy prywatnych przed nieautoryzowanym dostępem
c) zabezpieczenie kluczy SSH używanych do nawiązywania połączenia z serwerami i systemami w środowisku IT. Jako zabezpieczanie należy rozumieć: proces automatycznego wykrywania kluczy SSH, bezpieczne składowanie kluczy prywatnych, automatyczna rotacja kluczy SSH
d) integrację z innymi systemami Certificate Authority (CA), między innymi: Microsoft Certificate Services, OpenSSL, DigiCert, RedHat Certificate System, itp.
e) integrację z systemami klasy SIEM w celu automatyzacji procesu monitoringu oraz raportowania incydentów bezpieczeństwa powiązanych z nadużyciem certyfikatów w organizacji
f) generowanie polityk bezpieczeństwa definiujących kryteria dotyczące złożoności certyfikatów
g) generowanie i zarządzanie certyfikatami służącymi do podpisu kodu źródłowego aplikacji (Code Signing Certificate Management)

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 Oprogramowania PAM/PAS. Utwardzanie systemu operacyjnego modułu repozytorium poświadczeń musi być realizowane automatycznie przez instalator podczas procesu instalacji modułu.

1.42. Oprogramowanie musi uwzględniać nie mniej niż: jeden moduł składowania danych (poświadczeń, nagrań sesji etc), 4x moduł składowania danych na potrzeby Disaster Recovery/High Availability, 4x moduł do zmian i zarządzania kluczami oraz hasłami w systemach chronionych, 2 środowiska testowe pozwalające na odwzorowanie środowiska produkcyjnego.

1.43. Oprogramowanie 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. Oprogramowanie 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. Oprogramowanie musi zapewniać ochronę kryptograficzną kopii zapasowych generowanych z produktu

1.47. Oprogramowanie 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 1.14). 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 5 modułów Disaster Recovery w ramach podstawowej licencji czasowej przy wdrożonym HA w lokalizacji podstawowej).

Integracje

1.49. Oprogramowanie 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. Oprogramowanie musi umożliwiać integrację z biletowymi systemami zgłoszeń, nie mniej niż: HPSM, Jira 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. Oprogramowanie musi wspierać integrację z rozwiązaniami typu HSM obsługującymi standard PKCS11, wymagana jest integracja z systemami: Thales Luna, Entrust nShield, Utimaco CryptoServer.

1.52. Oprogramowanie 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).

Wymagania dodatkowe

1.53. Oprogramowanie 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 2022 włącznie

2. Wieloskładnikowe uwierzytelnienie oraz zabezpieczenie dostępu do kluczowych aplikacji poprzez portal Single Sign-On

2.1. Oprogramowanie musi realizować funkcje:
   a) wieloskładnikowego adaptacyjnego uwierzytelnienia
   b) zabezpieczenia dostępu zarówno do wewnętrznych jak i zewnętrznych (SaaS) aplikacji poprzez wykorzystanie zabezpieczonego portalu SSO
   c) zarządzania cyklem życia tożsamości (ang. lifecycle management, wymagający dodatkowej licencji czasowej)
   d) przechowywania poświadczeń użytkownika biznesowego w centralnym repozytorium opisanym w punkcie 1.38.

2.2. Wymagana jest możliwość obsługi minimum następujących składników uwierzytelniających MFA: hasło, sms, email, oauth, aplikacja mobilna, pytanie bezpieczeństwa, Qrcode generowany w ramach procesu uwierzytelnienia do interfejsu Systemu, umożliwiający uwierzytelnienie użytkownika przy użyciu aplikacji mobilnej uprzednio zarejestrowanej w systemie.

2.3. Oprogramowanie 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 typu "Threat Intelligence").

2.4. Moduł MFA poprzez protokół Radius musi umożliwiać integrację z popularnymi koncentratorami VPN jak minimum Cisco Systems, Palo Alto Networks, Pulse Secure, Fortinet, F5 Networks.

2.5. Oprogramowanie musi realizować usługę SSO dla aplikacji chmurowych oraz wewnętrznych, realizując w sposób scentralizowany bezpieczne uwierzytelnienie przy wykorzystaniu metod opisanych w punktach 2.2 oraz 2.3. 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

2.6. Oprogramowanie musi posiadać gotowe integracje SSO z nie mniej niż następującymi aplikacjami: Adobe Sign, Office 365/Microsoft 365.

2.7. Dla użytkowników zewnętrznych którzy chcą skorzystać z aplikacji web w centrum danych Zamawiającego Oprogramowanie 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).

2.8. Poprzez dodatkowe rozszerzenie licencyjne system musi realizować funkcję MFA wymuszane na chronionych serwerach Windows przy połączeniu uprzywilejowanym realizowanym w oparciu o moduł proxy opisany w punkcie 1.14. W ramach realizacji połączenia uprzywilejowanego moduł proxy musi auto uzupełnić poświadczenia i umożliwić użytkownikowi wpisanie kolejnego składnika MFA. Sesja musi być zestawiana w oparciu o koncepcję izolacji opisaną w punkcie 1.14. Oprogramowanie musi umożliwiać wymuszenie weryfikacji trzeciego składnika MFA na poziomie aplikacji mobilnej (minimum możliwe do zastosowania: PIN oraz uwierzytelnianie biometryczne).

2.9. Oprogramowanie musi umożliwiać składowanie poświadczeń oraz notatek wprowadzonych przez użytkownika w portalu dostępowym do aplikacji WEB 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.

2.10. Oprogramowanie musi udostępniać plugin, możliwy do zainstalowania w przeglądarce internetowej, realizujący funkcję generatora haseł.

3. Ochrona dostępu zdalnego

3.1. Oprogramowanie musi realizować funkcję bezpiecznego, uprzywilejowanego dostępu zdalnego dla użytkowników oprogramowania PAM (pracowników zewnętrznych lub wewnętrznych organizacji), bez konieczności instalacji rozwiązań klasy VPN (site-2-site lub client-site) po stronie sieci lub stacji roboczej firmy zewnętrznej.

3.2. Oprogramowanie nie może wymagać instalowania dodatkowego oprogramowania po stronie stacji roboczej użytkownika poza przeglądarką internetową (wsparcie dla nie mniej niż przeglądarki Chrome, Edge).

3.3. Oprogramowanie musi umożliwiać użycie dedykowanej przeglądarki WEB, korzystającej z mechanizmów zabezpieczeń polegających na izolacji stacji roboczej użytkownika końcowego poprzez zabezpieczenie plików cookie przed atakami typu; Cookie/Session Theft.

3.4. Oprogramowanie musi umożliwiać zestawienie połączenia szyfrowanego pomiędzy stacją roboczą użytkownika systemu a siecią Zamawiającego bez konieczności otwierania ruchu przychodzącego do sieci Zamawiającego. W celu realizacji niniejszego punktu Oprogramowanie musi umożliwiać utworzenie usługi 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 zdalnego usługa 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. Usługa powinna umożliwiać zarządzanie utworzonymi użytkownikami (tworzenie nowych zaproszeń, nadawanie uprawnień, wyłączanie kont). Dostęp do usługi musi być możliwy poprzez wykorzystanie uwierzytelnienia biometrycznego, bez konieczności podawania danych dostępowych użytkownika (jak jego nazwa czy hasło).

3.5. Oprogramowanie musi obsługiwać uniwersalne uwierzytelnienie biometryczne (bez konieczności wpisywania przed zestawieniem połączenia danych dostępowych, jak użytkownik - hasło) realizowane przy użyciu stosowanych powszechnie urządzeń klasy smartphone.

3.6. Oprogramowanie 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.

3.7. Oprócz realizacji funkcji uwierzytelnienia biometrycznego, Oprogramowanie musi posiadać funkcję potwierdzenia tożsamości dla kluczowych operacji realizowanych przez aplikację SaaS, np. nadawanie uprawnień administracyjnych innym użytkownikom.

3.8. W celu obsłużenia całości ruchu uprzywilejowanego do sieci Zamawiającego przez przeglądarkę internetową. Oprogramowanie musi posiadać wsparcie tunelowania sesji graficznych RDP przy użyciu HTML5 oraz protokołu SDP, zgodnie z wymaganiami punktu 1.24 podpunkt c niniejszego dokumentu.
3.9. Oprogramowanie musi wspierać transfer plików w trakcie trwania sesji graficznej
3.10. Oprogramowanie musi posiadać interfejs REST API do automatyzacji procesu zarządzania użytkownikami.
3.11. Oprogramowanie 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)

Rozdział III. Wymagania w zakresie dostawy i instalacji Oprogramowania

1. Wykonawca jest zobowiązany do dostarczenia subskrypcji i instalacji Oprogramowania w terminie do 20 Dni Roboczych od zawarcia Umowy. Zamawiający dopuszcza dostarczenie Oprogramowania drogą elektroniczną.
2. Dostawa i wszelkie czynności z nią związane realizowane będą przez Wykonawcę w Dni Robocze w godzinach 8:00 - 16:00.
3. Instalacja Oprogramowania na zaprojektowanym przez Wykonawcę we współpracy z Zamawiającym środowisku testowym Zamawiającego.
4. Wykonawca w ramach instalacji przygotuje działającą konsolę i wszelkie niezbędne komponenty Oprogramowania do instalacji, zgodnie z wymaganiami funkcjonalnymi opisanymi w Rozdziale II.
5. Odbiór Oprogramowania przez Zamawiającego będzie polegał na weryfikacji ilościowej dostarczonego Oprogramowania, poprawności instalacji oraz weryfikacji spełniania wymagań opisanych w rozdziale II.
6. Odbiór Oprogramowania zostanie potwierdzony Protokołem odbioru Oprogramowania.
7. Zamawiający zastrzega sobie prawo do korzystania ze wsparcia osób trzecich w trakcie odbiorów przedmiotu zamówienia.

Rozdział IV. Wymagania w zakresie Gwarancji

1. Wykonawca udziela Zamawiającemu Gwarancji na wykonany przedmiot Umowy oraz zobowiązuje się, do zapewnienia Gwarancji producenta dla dostarczonego Oprogramowania przez okres min. 36 m-cy od dnia podpisania przez obie Strony bez zastrzeżeń Protokołu Odbioru Wdrożenia, w wariancie wsparcia Wykonawcy realizowanego w trybie 365/24/7.
2. W ramach gwarancji na dostarczone Oprogramowanie, mają być zapewnione następujące świadczenia:
   2.1. dostęp do strony/portalu producenta pod wskazanym przez Wykonawcę adresem do aktualizacji Oprogramowania, w szczególności poprzez dostarczanie nowych wersji Oprogramowania, dostarczanie wersji podwyższonych, wydań

uzupełniających, nowych sygnatur oraz poprawek programistycznych, bez dodatkowych opłat;

2.2. Wsparcie w korzystaniu z Oprogramowania polegające w szczególności na:

2.2.1. świadczeniu Zamawiającemu pomocy w zakresie obsługi Zgłoszeń, w formie elektronicznej w systemie udostępnionym przez Wykonawcę Serwisie Zgłoszeń przez 24 godziny na dobę, 7 dni w tygodniu, w języku polskim;

2.2.2. świadczenia usług konsultacji w zakresie czynności, związanych z eksploatacją Oprogramowania, takich jak:

2.2.2.1. implementacja krytycznych poprawek systemu zalecanych przez producenta

2.2.2.2. aktualizacja systemu do nowych wersji zalecanych przez producenta, nie częściej niż 2 razy do roku,

2.2.2.3. cykliczne, nie częściej niż 1 raz do roku, przegląd systemu,

2.2.2.4. cykliczne, nie częściej niż dwa razy w roku, opracowanie dodatkowych procedur i instrukcji oraz ich aktualizacja,

Czynności, o których mowa powyżej zostaną odebrane Protokołem Odbioru Usługi Gwarancji, którego wzór stanowi Załącznik nr …. do Umowy.

2.3. Zapewnienia elektronicznego dostępu Zamawiającego do informacji w języku polskim lub angielskim na temat oferowanego Oprogramowania - pod wskazanym przez Wykonawcę adresem internetowym,

2.4. W czasie niedostępności Serwisu Zgłoszeń, Wykonawca zobowiązuje się do przyjmowania Zgłoszeń i udzielania informacji o ich statusie za pomocą poczty elektronicznej na adres wskazany przez Wykonawcę lub przez telefon na numer wskazany przez Wykonawcę.

2.5. Przyjmowaniu zgłoszeń problemów oraz zgłaszanie problemów wymagających rozwiązania przez producenta, w ramach wykupionego wsparcia producenta.

3. Wykonawca zagwarantuje rozwiązanie Zgłoszenia lub zastosowania obejścia w czasie nie dłuższym niż (stanowi kryterium oceny ofert), licząc od momentu Zgłoszenia:

Rodzaj Zgłoszenia	Czas na wykonanie czynności	
	Reakcja na Zgłoszenie Awarii*	Rozwiązanie Zgłoszenia - Naprawa lub zastosowanie tymczasowego rozwiązania**
Zgłoszenie Awarii niekrytycznej	do 8 godzin	do 24 godzin
Zgłoszenie Awarii krytycznej	do 4 godzin	do 8 godzin

*) Czas reakcji – czas od chwili Zgłoszenia Awarii do chwili kontaktu inżyniera serwisowego Wykonawcy z Zamawiającym,

**) Czas naprawy – czas liczony od chwili Zgłoszenia Awarii do momentu usunięcia Awarii potwierdzonej diagnostyką lub testem lub zastosowanie tymczasowego rozwiązania

4. Wykonawca poinformuje Zamawiającego o zastosowaniu tymczasowego rozwiązania i rozwiązaniu Zgłoszenia. Zamawiający uzna Zgłoszenie za rozwiązane po weryfikacji czy przedmiot Zgłoszenia został rozwiązany, co zostanie potwierdzone za pośrednictwem co najmniej jednego kanału komunikacji wskazanego w ust. 2

5. W przypadku zastosowania tymczasowego rozwiązania Wykonawca zobowiązany jest do wskazania rozwiązania zastępczego, pozwalającego na zachowanie podstawowej funkcjonalności Oprogramowania do czasu przekazania rozwiązania przez producenta.
6. Wykonawca odpowiada za potwierdzenie przyjęcia Zgłoszenia i zdiagnozowania nieprawidłowości. Wykonawca zobowiązany jest do niezwłocznego podjęcia wszelkich niezbędnych działań zmierzających do rozwiązania Zgłoszenia i przywrócenia w pełni prawidłowego działania Oprogramowania.
7. W ramach obsługi Zgłoszeń, Zamawiający udostępnieni Wykonawcy informacje, które okażą się konieczne do należytej ich obsługi (m.in. opisy objawów, logi).

Rozdział V. Wymagania w zakresie prawa opcji

1. **Wymagania w zakresie Wdrożenia Oprogramowania**, tj. dokumentacji, instalacji, konfiguracji, uruchomienia w środowisku produkcyjnym.
   1.1. Wykonawca zobowiązuje się do realizacji Wdrożenia w terminie do 70 Dni Roboczych od dnia zlecenia opcji.
   1.2. Wykonawca w terminie do 5 Dni Roboczych od dnia Zlecenia opcji, opracuje i przekaże do akceptacji Przedstawiciela Zamawiającego harmonogram Wdrożenia. Harmonogram musi uwzględniać w szczególności daty prowadzonych prac wdrożeniowych w środowisku Zamawiającego, z uwzględnieniem podziału na etapy, o których mowa w ust. 1.4
   1.3. Przedstawiciel Zamawiającego w terminie do 5 Dni Roboczych od przekazania przez Wykonawcę harmonogramu, zaakceptuje go lub przekaże uwagi. Przedłożony przez Zamawiającego harmonogram będzie wiążący dla Wykonawcy i Zamawiającego.
   1.4. Wykonawca w dniu akceptacji harmonogramu przystąpi do Wdrożenia Oprogramowania z uwzględnieniem poniższych etapów:
      1.4.1. analiza wymagań, analiza środowiska, opracowanie koncepcji wdrożenia i projektu przedwdrożeniowego, w szczególności:
         1.4.1.1. Przeprowadzenie warsztatu technologicznego.
         1.4.1.2. Przeprowadzenie analizy potrzeb wdrożeniowych Zamawiającego.
         1.4.1.3. Przeprowadzenie analizy środowiska Zamawiającego.
         1.4.1.4. Opracowanie i uzgodnienie z Zamawiającym docelowej architektury dla Oprogramowania.
         1.4.1.5. Zestawienie listy wymaganych dostępów pomiędzy komponentami Oprogramowania a systemami docelowymi Zamawiającego, które ma obejmować rozwiązanie,
         1.4.1.6. Przygotowanie dokumentacji zgodnie z wymaganiem określonymi w pkt 2 (w zakresie Projektu technicznego).
      1.4.2. Instalacja Oprogramowania, konfiguracja bazowa na środowisku produkcyjnym Zamawiającego oraz rekonfiguracja środowiska testowego,
      1.4.3. Przygotowanie lub modyfikacja posiadanego przez Zamawiającego środowiska,
      1.4.4. Integracja Oprogramowania z systemami współdziałającymi (np. AD, syslog, SIEM, SMTP),
      1.4.5. Opracowanie docelowej listy zasobów, które będą wprowadzane do systemu z poniższych obszarów:
         1.4.5.1. Konta Administratorów domeny
         1.4.5.2. Konta domenowe administratorów IT
         1.4.5.3. Konta lokalne na serwerach Windows
         1.4.5.4. Konta root na serwerach Linux

1.4.5.5. Konta administracyjne dla środowisk wirtualizacyjnych
1.4.5.6. Konta administracyjne platform PaaS/IaaS
1.4.6. Definicja oraz konfiguracja polityk bezpieczeństwa,
1.4.7. Przeprowadzenie konfiguracji i importu kont uprzywilejowanych do PAM, z uwzględnieniem przygotowanych i przekazanych przez Zamawiającego listy kont i haseł,
1.4.8. Przeprowadzenie konfiguracji w zakresie automatycznego zarządzania hasłami,
1.4.9. Przeprowadzenie konfiguracji na systemie w zakresie nagrywania sesji dla w/w kont,
1.4.10. Konfiguracja MFA i SSO na potrzeby logowania do systemu,
1.4.11. Konfiguracja modułu zdalnego dostępu dla wskazanych administratorów,
1.4.12. Konfiguracja funkcjonalności wykrywania anomalii w sesjach uprzywilejowanych dla 5 przykładowych definicji incydentów;

1.5. Wykonawca co najmniej na 3 Dni Roboczych przed przystąpieniem do prac wdrożeniowych, które mogą spowodować przerwy w działaniu produkcyjnego Środowiska Zamawiającego, zobowiązany jest zgłosić elektronicznie na adres Przedstawiciela Zamawiającego potrzebę wyznaczenia okna serwisowego (rozumianego jako ograniczenie dostępności środowiska Zamawiającego). W zgłoszeniu Wykonawca zobowiązany jest określić przewidywany zakres prac i czas ich wykonania.
1.6. W przypadku niedotrzymania terminu, o którym mowa w punkcie poprzedzającym, Zamawiający może nie dopuścić Wykonawcy do realizacji Wdrożenia.
1.7. Wykonawca przyjmuje do wiadomości, że okno serwisowe może być wyznaczone w porze nocnej od godz. 22 do godz. 6 oraz w soboty i w niedziele. Czas trwania okna serwisowego nie może każdorazowo przekroczyć 4 godzin, przy czym w każdym przypadku Wykonawca zobowiązany jest do organizowania i wykonywania prac w ramach Wdrożenia w sposób minimalizujący okresy przerw w działaniu Środowiska Zamawiającego. Zamawiający dopuszcza wydłużenie czasu trwania okna serwisowego na uzasadniony wniosek Wykonawcy.
1.8. Działanie dostarczonego Oprogramowania nie może powodować obniżenia wydajności eksploatowanego środowiska Zamawiającego.
1.9. W przypadku, gdy zaoferowany przez Wykonawcę Oprogramowanie nie będzie współdziałać ze środowiskiem Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu pracy tego środowiska, Wykonawca przywróci i pokryje wszystkie koszty związane z przywróceniem środowiska Zamawiającego do sprawnego działania (tj. działania sprzed instalacji).
1.10. Po wykonaniu instalacji, konfiguracji i uruchomieniu dostarczonego Oprogramowania w środowisku produkcyjnym Zamawiający dokona weryfikacji Wdrożenia.
1.11. Wykonawca zobowiązany jest do poinformowania Zamawiającego o gotowości do przystąpienia do odbioru Wdrożenia, tj. weryfikacji Wdrożenia w środowisku produkcyjnym z 2 dniowym wyprzedzeniem.
1.12. Weryfikacja Wdrożenia będzie wykonywana przez Zamawiającego w obecności Wykonawcy na podstawie opracowanych Planów i Scenariuszy Testów Akceptacyjnych, o których mowa w pkt. 2
1.13. W przypadku, gdy Wdrożenie nie przejdzie pozytywnej weryfikacji, Wykonawca zobowiązuje się do usunięcia nieprawidłowości oraz do przedstawienia Wdrożenia do ponownego odbioru w terminie nie dłuższym niż 5 Dni Roboczych od dnia wniesienia zastrzeżeń przez Przedstawiciela Zamawiającego w Protokole Odbioru

Wdrożenia. Ponowny odbiór Wdrożenia będzie polegał na powtórzeniu weryfikacji Wdrożenia.

1.14. Niezależnie od powyższej procedury, Wykonawca zobowiązany jest do dochowania terminów określonych w Zleceniu.

1.15. Odbiór Wdrożenia zostanie potwierdzony Protokołem Odbioru Wdrożenia bez zastrzeżeń, którego wzór stanowi Załącznik nr … do Umowy.

2. Wymagania w zakresie Dokumentacji

2.1. Wykonawca w ramach Wdrożenia zobowiązany jest przygotować i dostarczyć Dokumentację:

2.1.1. Projekt Techniczny,

2.1.2. Plan i Scenariusze Testów Akceptacyjnych,

2.1.3. Dokumentacja Powykonawcza

2.1.4. Procedury bezpieczeństwa, operacyjne i administracyjne.

2.2. Projekt Techniczny musi zawierać co najmniej informacje określone w Załączniku …. do OPZ - Wzór Projektu Technicznego/Dokumentacji Powykonawczej;.

2.2.1. Plan Testów Akceptacyjnych oraz Scenariusze Testów Akceptacyjnych, uwzględniający wymagania w zakresie Wdrożenia i odbiorów, w tym:

2.2.2. opis i listę scenariuszy,

2.2.3. terminy testów akceptacyjnych,

2.2.4. kategoryzację błędów i warunki odbioru,

2.2.5. opisy ról oraz odpowiedzialności osób zaangażowanych w przeprowadzenie testów,

2.2.6. sposób przeprowadzenia kolejnych iteracji testów po naprawie błędów,

2.2.7. opis środowiska testowego,

2.2.8. podejście do testowania,

2.2.9. scenariusze i przypadki testowe,

2.3. Scenariusze Testów Akceptacyjnych, muszą:

2.3.1. zapewniać jednoznaczną weryfikację spełniania przez Oprogramowanie założeń wdrożeniowych i wymagań określonych w Rozdziale II,

2.3.2. zapewniać możliwość weryfikacji prawidłowej instalacji i konfiguracji w środowisku Zamawiającego.

2.4. Dokumentacja Powykonawcza, zawierającą co najmniej informacje, o których mowa w Załączniku nr 2 do OPZ - Wzór Projektu Technicznego/Dokumentacji Powykonawczej;

2.5. Dokumentacja Powykonawcza musi zawierać elementy/opisy/schematy potwierdzające spełnianie przez Wdrożone Oprogramowanie postawionych przez Zamawiającego wymagań.

2.6. Wykonawca wraz z Dokumentacją Powykonawczą opracuje i przekaże Przedstawicielowi Zamawiającego Procedury bezpieczeństwa, operacyjne i administracyjne Wdrożonego Oprogramowania, zawierającą co najmniej informacje, o których mowa w Załączniku nr 2 do OPZ - Wzór Procedur bezpieczeństwa, operacyjnych i administracyjnych.

2.7. Wymagania w zakresie dostawy Dokumentacji:

2.7.1. Wykonawca w terminie do 20 Dni Roboczych od dnia Zlecenia opcji, opracuje i przekaże do akceptacji Zamawiającego Dokumentację,

2.7.2. Wykonawca w terminie do 10 Dni Roboczych od dnia podpisania Protokołu Odbioru Wdrożenia bez zastrzeżeń, opracuje i przekaże do akceptacji

Zamawiającego Dokumentację Powykonawczą i Procedury bezpieczeństwa, operacyjne i administracyjne.

2.7.3. Wykonawca zobowiązuje się dostarczyć Dokumentację w formie elektronicznej z wykorzystaniem jednego lub kilku z następujących formatów zapisu plików:

a) MS Word i PDF;
b) MS Excel (w przypadku dużych zestawień tabelarycznych);
c) HTML;
d) JPG, GIF, PNG;
e) w przypadku schematów - w wersji edytowalnej wektorowej;

oraz innych za uprzednią zgodą Zamawiającego.

2.7.4. Dokumentacja musi być przekazana do Przedstawiciela Zamawiającego w języku polskim w formie elektronicznej.

2.7.5. Odbiór dokumentacji zostanie potwierdzony podpisanym przez Strony Protokołem Odbioru Dokumentacji, którego wzór stanowi Załącznik nr … do Umowy.

3. Wymagania w zakresie przeszkolenia:

3.1. Wykonawca w terminie do 20 Dni Roboczych od Zlecenia opcji zobowiązany jest do przeprowadzenia przeszkolenia dla maksymalnie 10 osób wskazanych przez Przedstawiciela Zamawiającego w zakresie administrowania i zarządzania Oprogramowaniem.

3.2. Zakres merytoryczny przeszkoleń proponowanych przez Wykonawcę musi zapewniać prawidłową obsługę Oprogramowania w zakresie integracji Oprogramowania w ramach infrastruktury Zamawiającego oraz jego prawidłowe użytkowanie przez pracowników Zamawiającego, w szczególności w zakresie instalacji i konfiguracji, administrowania i utrzymania z uwzględnieniem ról wymaganych dla prawidłowego utrzymania Oprogramowania.

3.3. Minimalne wymagania dotyczące zakresu przeszkolenia zostały wskazane w załączniku nr 1 do OPZ

3.4. Wykonawca zapewni poniżej określone warunki dotyczące przeszkolenia:

3.4.1. wszyscy uczestnicy przeszkolenia otrzymają materiały szkoleniowe w języku polskim lub angielskim w formie elektronicznej;

3.4.2. przeszkolenia będą prowadzone w języku polskim;

3.4.3. prowadzący przeszkolenie musi posiadać kwalifikacje i odpowiednią wiedzę z zakresu obejmującego przeszkolenie;

3.4.4. środowisko szkoleniowe oraz wszelkie niezbędne materiały i oprogramowanie;

3.4.5. przeszkolenia będą prowadzone on-line,

3.4.6. każdy uczestnik przeszkolenia otrzyma imienne potwierdzenie udziału w szkoleniu.

3.5. Przeszkolenie zostanie przeprowadzone co najmniej w dwóch grupach, w terminach uzgodnionych z Zamawiającym. Wykonawca jest zobowiązany do przedstawienia Zamawiającemu propozycji co najmniej 4 różnych terminów przeszkolenia. Zamawiający w trybie roboczym, po przekazaniu Zlecenia opcji uzgodni z Wykonawcą termin i listę osób uczestniczących w przeszkoleniu.

3.6. Przeszkolenie każdego uczestnika będzie obejmowało co najmniej 24 godziny zegarowych wykładów i ćwiczeń, rozłożonych po maksymalnie 8 godzin zegarowych dziennie.

3.7. Wykonawca przedstawi do akceptacji Przedstawiciela Zamawiającego na co najmniej 10 dni przed rozpoczęciem przeszkolenia, informacje dotyczące:

3.7.1. terminu,
3.7.2. zakresu przeszkolenia;
3.7.3. agendy;
3.7.4. kwalifikacji Wykładowców;
3.7.5. materiałów szkoleniowych wraz z ich zakresem.

3.8. Akceptacja przez Przedstawiciela Zamawiającego wymagań określonych w pkt. 3.7 stanowi warunek rozpoczęcia przeszkolenia i zostanie potwierdzona drogą elektroniczną przez Przedstawiciela Zamawiającego.

3.9. Prawidłowe przeprowadzenie przeszkolenia zostanie potwierdzone podpisaniem bez zastrzeżeń przez Przedstawiciela Zamawiającego i Wykonawcę Protokołu Odbioru Przeszkolenia, którego wzór stanowi Załącznik nr … do Umowy.

3.10. Wszelkie koszty związane z realizacją przeszkolenia ponosi Wykonawca.

4. Wymagania w zakresie konsultacji i asysty dotyczących dostarczonego Oprogramowania:

4.1. Zamawiający może, w każdym czasie realizacji Umowy, kierować do Wykonawcy Zlecenia w zakresie konsultacji i asysty dotyczące dostarczonego Oprogramowania w wymiarze do 600 godzin, w szczególności w zakresie:

4.1.1. wykonania prac o charakterze analitycznym, projektowo-programistycznym i wdrożeniowym, związanych z potrzebami zmian w Środowisku Zamawiającego, z zastrzeżeniem, że Zlecenie nie może prowadzić do zmiany kodu źródłowego dostarczonego Oprogramowania,

4.1.2. dostosowania do wymagań integracyjnych z innymi systemami Zamawiającego,

4.1.3. przygotowania i prowadzenie przeszkoleń, dla wskazanych przez Zamawiającego pracowników Resortu Finansów. Konieczność przeprowadzenia przeszkoleń będzie ujęta w zleceniu przez Zamawiającego. Przeszkolenia będą organizowane w formule „online”.

4.2. Zlecenia przekazywane będą na adres email wskazany Umowie.

4.3. Terminy realizacji Zleceń będą określane każdorazowo w Zleceniu, na podstawie uzgodnionej przez Strony pracochłonności. Wzór Zlecenia stanowi Załącznik Nr ….. do Umowy.

4.4. Zamawiający przekaże Wykonawcy w Zleceniu opis wymaganych prac oraz wstępny harmonogram ich realizacji.

4.5. Wykonawca w terminie do 5 (pięciu) Dni Roboczych od otrzymania Zlecenia przekaże Zamawiającemu:

4.5.1. analizę Zlecenia,

4.5.2. akceptację lub korektę oszacowanej przez Zamawiającego liczby Roboczogodzin (pracochłonność) w podziale na zadania zdefiniowane w harmonogramie realizacji na formularzu Zlecenia,

4.5.3. w przypadku wprowadzenia korekty do oszacowanej przez Zamawiającego pracochłonności, Wykonawca przedstawi Zamawiającemu uzasadnienie korekty i warunki wykonania Zlecenia.

4.6. Wykonawca może zwrócić się do Zamawiającego o wydłużenie terminu, o którym mowa w pkt 4.3., jeśli do przygotowania analizy i ewentualnej korekty oszacowanej przez Zamawiającego liczby Roboczogodzin konieczne jest wykonanie dodatkowych analiz, badań lub testów. Wniosek musi zawierać uzasadnienie, obejmujące wykaz koniecznych do przeprowadzenia w tym zakresie prac. Zamawiający nie uwzględni wniosku, który w sposób nieuzasadniony będzie zmierzał do opóźnienia realizacji Zlecenia.

4.7. Przedstawiciele Stron dokonają uzgodnienia ostatecznej treści Zlecenia. Uzgodniony opis w Zleceniu może podlegać ponownej analizie i określeniu liczby Roboczogodzin.
4.8. W przypadku braku zgody Zamawiającego na wskazaną przez Wykonawcę liczbę Roboczogodzin, Zamawiający może odstąpić od zlecenia Wykonawcy.
4.9. Podstawą wykonania Zmiany jest podpisane przez Strony Zlecenie.

5. **Wymagania w zakresie dostarczenia Oprogramowania – do 50% zamówienia podstawowego, umożliwiającego jednoczesną pracę max dla 300 użytkowników/administratorów Zamawiającego**:
   5.1. Zamawiający w każdym czasie realizacji Umowy zastrzega możliwość nabycia do 50% z ogólnej liczby Oprogramowania zamówienia podstawowego, umożliwiającego jednoczesną pracę max dla 300 użytkowników/administratorów Zamawiającego.
   5.2. Dostarczone w ramach opcji Oprogramowanie musi być identyczne z dostarczonymi w ramach zamówienia podstawowego, z uwzględnieniem jego aktualizacji.
   5.3. Wykonawca zobowiązuje się dostarczyć licencje w terminie maksymalnie do 10 Dni Roboczych od dnia przesłania Zamówienia Opcji.
   5.4. Dostawa musi być zrealizowana poprzez udostępnienie Zamawiającemu, pod adresem internetowym, możliwości pobrania licencji i kluczy licencyjnych drogą elektroniczną lub przekazania na adres Przedstawiciela Zamawiającego.
   5.5. W terminie do 3 Dni Roboczych od dnia dostawy, Zamawiający dokona odbioru polegającego na zweryfikowaniu zgodności dostarczonego Oprogramowania z przedmiotem zamówienia, co zostanie potwierdzone podpisanym przez Przedstawiciela Zamawiającego bez zastrzeżeń Protokołem Odbioru (Załącznik nr ….. do Umowy), który zostanie przekazany Wykonawcy na wskazany w Umowie adres e-mail.
   5.6. W przypadku zastrzeżeń do realizowanej przez Wykonawcę dostawy, Przedstawiciel Zamawiającego przekaże Wykonawcy na wskazany w Umowie adres e-mail Protokół Odbioru z zastrzeżeniami. Wykonawca zobowiązany jest w terminie do 2 Dni Roboczych od dnia przekazania uwag Zamawiającego do ich uwzględnienia. Po usunięciu nieprawidłowości przez Wykonawcę, Przedstawiciel Zamawiającego przystąpi do ponownego odbioru przedmiotu zamówienia, zgodnie z procedurą opisaną w punkcie 5.5. Postanowienia niniejszego punktu stosuje się jednokrotnie.
   5.7. Należyte wykonanie przedmiotu Umowy zostanie potwierdzone podpisaniem przez Zamawiającego i Wykonawcę Protokołu Odbioru bez zastrzeżeń.