Krajowe Centrum
Monitorowania
Ratownictwa Medycznego

Lotnicze Pogotowie Ratunkowe

ul. Księżycowa 5
01-934 Warszawa
tel. (22) 22-99-931/932
fax. (22) 22-99-933

NIP: 522-25-48-391
KRS: 0000144355
www.kcmrm.pl
e-mail: centrala@lpr.com.pl

OPIS PRZEDMIOTU ZAMÓWIENIA

Zakup oprogramowania i licencji klasy PIM/PAM/PSM wraz z usługą wsparcia technicznego

Spis treści

Lotnicze Pogotowie Ratunkowe
ul. Księżycowa 5
01-934 Warszawa
tel. (22) 22-99-931/932
fax. (22) 22-99-933

NIP: 522-25-48-391
KRS: 0000144355
www.kcmrm.pl
e-mail: centrala@lpr.com.pl

1. SŁOWNIKI I SKRÓTY

Dla potrzeb niniejszego opracowania przyjmuję się następujące definicje skrótów i pojęć:

Skrót/pojęcie	Definicja
Dni Robocze	Oznacza każdy dzień tygodnia od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy, w godz. od 8:00 do 15:35.
Dokumentacja	Wytworzone przez Wykonawcę w ramach realizacji Umowy i podlegające zatwierdzeniu przez Zamawiającego materiały w formie papierowej, jak również informacje zapisane na innych nośnikach, w tym nośnikach elektronicznych, w szczególności Wykaz Ilościowo-Cenowy.
Incydent serwisowy	Oznacza zgłoszenie do Wykonawcy przez Zamawiającego lub osoby wskazane przez Zamawiającego, w trybie 24/7, nieprawidłowości w działaniu Oprogramowania. Wykonawca zobowiązany jest do rejestracji zgłoszenia oraz usuwania Błędów i usterek lub dostarczenia procedur obejścia, powodujących przywrócenie działania Oprogramowania i rozwiązania zgłoszenia pod warunkiem, że na przedstawioną przez Wykonawcę propozycję obejścia Zamawiający wyrazi pisemną zgodę.
Oprogramowanie Standardowe/Oprogramowanie	Oznacza oprogramowanie powszechnie dostępne i eksploatowane na dzień złożenia oferty, będące przedmiotem dostaw w ramach realizacji niniejszego przedmiotu zamówienia, którego producentem jest Wykonawca lub podmiot trzeci. Zamawiający dopuszcza zastosowanie Oprogramowania Standardowego w poniższych obszarach: 1) system operacyjny; 2) oprogramowanie bazodanowe; 3) oprogramowanie do tworzenia raportów; 4) oprogramowanie do archiwizacji i tworzenia kopii bezpieczeństwa; 5) oprogramowanie antywirusowe; 6) oprogramowanie ETL (ang. Extract, Transform and Load); 7) komunikator (np. oparty o protokół XMPP); 8) oprogramowanie do wirtualizacji; 9) oprogramowanie serwera pocztowego; 10) oprogramowanie serwera aplikacyjnego, kontener aplikacji (z wyłączeniem kodu aplikacji udostępnianej użytkownikowi), serwera WWW; 11) oprogramowanie narzędziowe do monitorowania i diagnozy Systemu; 12) oprogramowanie sterujące i zarządzające centralami telefonicznymi.

Skrót/pojęcie	Definicja
	Zamawiający dopuszcza zastosowanie Oprogramowania Standardowego, którego producentem jest Wykonawca lub podmiot trzeci również w innych obszarach pod warunkiem, że zastosowanie takiego oprogramowania nie ograniczy kompatybilności z innymi dostępnymi na rynku rozwiązaniami technicznymi oraz dalszej rozbudowy Systemu i świadczenia serwisu gwarancyjnego przez inne podmioty niż Wykonawca i podmiot trzeci , co wymaga udzielenia licencji dla Oprogramowania na polach eksploatacji określonych w umowie , którego producentem jest Wykonawca lub podmiot trzeci.
PRM	Państwowe Ratownictwo Medyczne.
SWD PRM	Systemy Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego wraz z zainstalowanym oprogramowaniem standardowym, aplikacyjnym oraz infrastrukturą sprzętową.
Umowa	Umowa zawarta pomiędzy Wykonawcą a Zamawiającym na potrzeby realizacji niniejszego przedmiotu zamówienia.
Usługa Serwisu	Usługa świadczona w ramach gwarancji udzielonej przez Wykonawcę, polegająca na zapewnieniu przez Wykonawcę poprawności i ciągłości prawidłowego działania Oprogramowania oraz jego poszczególnych komponentów.
Użytkownik	Zamawiający oraz jego pracownicy.
Wykonawca/Dostawca	Podmiot realizujący zamówienie.
Zamawiający	Lotnicze Pogotowie Ratunkowe.

2. Cel zamówienia

Celem zamówienia jest dostawa Oprogramowania do obsługi kont uprzywilejowanych wraz z licencjami dla minimum 10 operatorów (administratorów), umożliwiającego podłączenie do 500 zarządzanych urządzeń docelowych. Dostarczone oprogramowanie musi zawierać wsparcie producenta z prawami do uaktualniania i wsparciem technicznym przez okres 36 miesięcy od daty zakupu. Produkty objęte przedmiotowym zamówieniem mają charakter powszechnie dostępnych na rynku (typu Commercial off-the-shelf - COTS).

Przedmiot zamówienia zostanie dostarczony w terminie nie dłuższym niż 30 dni od dnia podpisania umowy.

Lotnicze Pogotowie Ratunkowe
ul. Księżycowa 5
01-934 Warszawa
tel. (22) 22-99-931/932
fax. (22) 22-99-933

NIP: 522-25-48-391
KRS: 0000144355
www.kcmrm.pl
e-mail: centrala@lpr.com.pl

3. Wymagania niefunkcjonalne

KOD WYMAGANIA	PODSTAWOWE WYMAGANIA OPROGRAMOWANIA
WNF.01	Uprawnienia z licencji na korzystanie z Oprogramowania do ochrony kont uprzywilejowanych Zamawiający nabywa z chwilą jego Odbioru.
WNF.02	Wykonawca oświadcza i gwarantuje, że warunki korzystania z Oprogramowania typu PIM/PAM/PSM nie wymagają ponoszenia dodatkowych opłat na rzecz Wykonawcy lub producentów takiego Oprogramowania. Wynagrodzenie obejmuje całość wynagrodzenia za korzystanie z Oprogramowania.
WNF.03	Wykonawca gwarantuje, że jeżeli w ramach opłat należnych producentowi Oprogramowania mieści się opłata za jakiekolwiek dodatkowe świadczenia, w szczególności dostarczanie aktualizacji lub poprawek błędów lub inne usługi serwisowe, nieprzedłużenie korzystania z tych świadczeń przez Zamawiającego nie może powodować ustania licencji na korzystanie z Oprogramowania lub uprawniać do wypowiedzenia umowy licencyjnej.
WNF.04	Wykonawca dostarczy Oprogramowanie na informatycznych nośnikach danych lub w innej postaci umożliwiającej prawidłową instalację tego Oprogramowania oraz certyfikaty autentyczności, klucze instalacyjne oraz inne dokumenty i zabezpieczenia najpóźniej w dacie Odbioru tego Oprogramowania, chyba że z Umowy wynika inna data przekazania.
WNF.05	Informatyczne nośniki danych, kopie, certyfikaty autentyczności, klucze instalacyjne oraz inne dokumenty i zabezpieczenia, o których mowa w poprzednim ustępie, powinny być zgodne z wymaganiami określonymi przez producenta Oprogramowania. Zamawiający jest uprawniony do weryfikacji, czy certyfikaty autentyczności, klucze instalacyjne oraz inne dokumenty i zabezpieczenia są wystarczające i zgodne z wymogami określonymi przez producenta. W tym celu Zamawiający może zwracać się do osób trzecich, w tym producenta Oprogramowania.
WNF.06	Wykonawca jest odpowiedzialny, względem Zamawiającego, za wszelkie wady prawne, a w szczególności za ewentualne roszczenia osób trzecich wynikające z naruszenia praw własności intelektualnej, w tym praw wynikających z ustawy o prawie autorskim i prawach pokrewnych.
WNF.07	Usługa serwisu (maitanance) będzie obejmowała aktualizacje oferowanego oprogramowania do najnowszych wersji udostępnionych przez producenta oprogramowania przez okres 36 miesięcy od daty protokolarnego odbioru Oprogramowania. W ramach tej usługi Zamawiający ma prawo zgłaszać błędy w Oprogramowaniu do jego serwisu oraz mieć dostęp do bazy wiedzy i aktualizacji zakupionego Oprogramowania.

WNF.08	Udzielone licencje na Oprogramowanie do ochrony kont uprzywilejowanych nie m mieć ograniczeń czasowych. Dostarczone licencje będą nadane bezterminowo.
WNF.09	Przedmiot zamówienia musi zostać dostarczony wraz z wszystkimi licencjami na systemy operacyjne/bazy danych/połączenia terminalowe jak również każde inne wymagane do uruchomienia systemu jeżeli rozwiązanie wymaga takich systemów/aplikacji.
WNF.10	W ramach realizacji przedmiotu zamówienia Wykonawca zapewni usługę wsparcia technicznego realizowaną przez producenta Oprogramowania. Usługa ma być świadczona przez 36 miesięcy od momentu dostawy oprogramowania - 24h na dobę 7 dni w tygodniu. W ramach usługi Zamawiający będzie posiadać możliwość zgłaszania błędów drogą telefoniczną lub elektroniczną za pośrednictwem poczty email lub strony WWW. Oferowane Oprogramowanie powinno mieć możliwość zakupu usługi wsparcia technicznego na kolejne lata po upływie 36 miesięcy liczonych od dnia dostawy oprogramowania. W ramach wsparcia Wykonawca winien zapewnić, w okresie użytkowania oferowanej licencji, elektronicznego dostęp do nowej wersji oprogramowania i udoskonaleń do wersji bieżących oferowanych przez producenta oprogramowania (nowe edycje produktów, wydania uzupełniające, aktualizacje, poprawki programistyczne).
WNF.11	W ofercie Wykonawca powinien przedstawić: 1) nazwy licencji wraz liczbą licencjonowanych jednostek; 2) koszty licencji wraz z usługą wsparcia technicznego przez okres 36 miesięcy; 3) oświadczenie o spełnianiu każdego wymagania wraz ze wskazaniem miejscaw dokumentacji oprogramowania.
WNF.13	Powszechna dostępność jest rozumiana jako możliwość kupna bądź pobrania przez dowolny podmiot bądź osobę fizyczną, szczegółowej wiedzy na temat produktu (np. w postaci kompletu dokumentacji technicznej, wersji demonstracyjnych lub testowych, innych nośników wiedzy nt. produktu).
WNF.14	Dostarczone licencje, powinny umożliwiać realizację pośrednictwa w dostępie do między innymi następującej infrastruktury sprzętowej będącej w posiadaniu Zamawiającego: 1) Cisco Catalyst 9300-24T-E; 2) HPE MSA 2050 SAN Dual Controller SFF; 3) HPE ProLiant DL380 Gen10 8SFF; 4) PALO ALTO PA-820; 5) Cisco 7206 Series; 6) Cisco Catalyst C3KXNM10G; 7) Cisco Catalyst 2960 XR; 8) PALO ALTO PA-820; 9) PRIMERGY RX2540 M4; 10) Fujitsu ETHERNUS DX200 S4; 11) QNAP TS-832XU-RP; 12) HPE DATA PROTECTOR; 13) Cisco C3750;

	14) Urządzenia szyfrujące HSM; 15) BIG-IP Virtual Edition Best Bundle 1 Gbps; 16) BIG-IP Virtual Edition Local Traffic Manager 300 Mbps; 17) Cisco Catalyst C9300-48T-E -port data only; 18) Cisco Catalyst C9200-24T-E - port data only; 19) Cisco ISR 4461/K9; 20) Cisco ISR 4451 VSEC/K9.
WNF.15	Dostarczone licencje muszą umożliwiać realizację pośrednictwa w dostępie do co najmniej następującej infrastruktury programowej: 1) bazujące na systemie Linux Redhat: CentOS; 2) systemów z rodziny MS Windows: Windows Server 2012 i wyższych, Windows 10, Windows 7; 3) systemów z rodziny produktów Vmware: Vmware vCenter Server, ESX, ESXi- usługi Microsoft Services: Scheduled tasks, IIS application Pool, IIS Directory Security, w rejestrach, COM+, zarządzanie kontami w domenie Microsoft.
WNF.16	Oprogramowanie musi zapewniać wsparcie (możliwość zarządzania kontami uprzywilejowanymi wykorzystywanymi w obrębie systemu docelowego) w formie "out of box" dla systemów docelowych takich jak: Cisco, Microsoft Windows, Microsoft SQL, Linux/Unix, Oracle, MySQL, VMWare,
WNF.17	Dla oferowanego Oprogramowania muszą istnieć na terenie Polski autoryzowani partnerzy usługowi oraz autoryzowany serwis zapewniający wsparcie techniczne dla dostarczonego systemu.
WNF.18	Oprogramowanie stanowiące przedmiot zamówienia powinno być opisane na publicznie i powszechnie dostępnych stronach www producenta.
WNF.19	Oprogramowanie musi pochodzić z oficjalnego kanału dystrybucji na terenie Unii Europejskiej i stanowić Oprogramowanie Standardowe.
WNF.20	Zamawiający wymaga dostarczenia najnowszej wersji Oprogramowania, zapewniającej zgodność i wymagana funkcjonalność całości dostarczonego przedmiotu zamówienia.
WNF.21	Warunki licencyjne dostarczonego Oprogramowania będą dopuszczać uruchomienie zarówno na maszynie wirtualnej jak i na fizycznej platformie sprzętowej, korzystając z tej samej licencji.
WNF.22	Zamawiający będzie miał zapewnioną możliwość pobierania aktualizacji oraz nowych wersji oprogramowania, samodzielnie, przez dedykowaną stronę www.
WNF.23	W przypadku dostarczenia Appliance programowego przez Wykonawcę, Zamawiający wymaga dostarczenia Oprogramowania w postaci Virtual

	Appliance dla wersji posiadanej przez Zamawiającego infrastruktury Vmware: 6.7.
WNF.24	Dostarczone Oprogramowanie musi być kompletne wraz z licencjami pozwalającymi na uruchomienie minimum następujących funkcjonalności: 1) zarządzanie kontami uprzywilejowanymi w ramach organizacji; 2) monitoring wykorzystania kont uprzywilejowanych; 3) nagrywanie i archiwizowanie sesji zdalnych; zabezpieczenie środowiska przed przerwami w pracy poprzez wbudowaną automatykę reagowania na awarie.
WNF.25	Zarządzanie kontami uprzywilejowanymi proponowanego rozwiązania musi umożliwiać podłączenie do 500 zarządzanych systemów docelowych.
WFN.26	Oprogramowanie musi posiadać funkcję chroniącą pliki, foldery i klucze rejestru wykorzystywane przez program przed zapisem i modyfikacją.
WFN.27	Oprogramowanie musi posiadać ochronę przed różnymi typami wirusów, robaków i koni trojańskich, przed zagrożeniami z Internetu i poczty elektronicznej, a także złośliwym kodem oraz mieć możliwość wykrywania oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka oraz narzędzi hakerskich.

4. Wymagania w zakresie funkcjonalności

KOD WYMAGANIA	OPIS PODSTAWOWYCH WYMAGAŃ FUNKCJONALNYCH
WF.01	Zamawiający wymaga oprogramowania ochrony kont uprzywilejowanych pracującego w architekturze klient – serwer.
WF.02	Przedmiot zamówienia powinien udostępniać portal WWW (dostępny przez 3 najpopularniejsze przeglądarki internetowe: Edge, Chrome, Firefox) dla użytkowników końcowych, w którym widoczne będą przypisane im dostępy i za pomocą którego możliwe będzie uruchomienie sesji do udostępnionych zasobów, bez potrzeby dodatkowego podawania haseł do zasobów docelowych.
WF.03	Przedmiot zamówienia, w którym składowane są chronione konta uprzywilejowane umożliwiać musi implementację zapasowych komponentów typu Disaster Recovery w lokalizacjach odseparowanych geograficznie, musi istnieć możliwość wykorzystania trybu wysokiej dostępności pomiędzy dwoma systemami w jednym centrum danych oraz modułów zapasowych Disaster Recovery w dwóch innych lokalizacjach.

KOD WYMAGANIA	OPIS PODSTAWOWYCH WYMAGAŃ FUNKCJONALNYCH
WF.04	Oprogramowanie musi być kompatybilne z systemami działającymi w infrastrukturze Zamawiającego: 1) systemy operacyjne oparte o architekturę Microsoft Windows; 2) systemy operacyjne oparte o architekturę Unix / Linux; 3) oprogramowanie do wirtualizacji Vmware w wersji co najmniej 6.7.
WF.05	Możliwość integracji z Active Directory na poziomie funkcjonalności domeny Windows Serwer 2016 i nowszym w zakresie uwierzytelniania użytkowników.
WF.06	Wszystkie zaoferowane przez Wykonawcę komponenty rozwiązania w całości będą pochodzić od jednego producenta /wytwórcy oprogramowania.
WF.08	Zaoferowane rozwiązanie musi być skalowalne w przypadku dodawania nowych zasobów oraz nowych usług.
WF.10	Dostarczone rozwiązanie musi umożliwiać monitoring i rejestrowanie użycia kont uprzywilejowanych oraz dogłębną analizę wykorzystania uprawnień.
WF.11	Dostarczone rozwiązanie musi umożliwiać rejestrowanie i archiwizowanie sesji zdalnych.
WF.12	Dostarczone rozwiązanie musi zapewniać zabezpieczanie przed przerwami w pracy poprzez wbudowane mechanizmy reagowania na występującą awarie.
WF.13	W przypadku wystąpienia awarii dostarczonego Oprogramowania powinno umożliwiać odtworzenie systemu z kopii zapasowej (ang. Backup) w pełni funkcjonującego środowiska produkcyjnego.
WF.14	System musi zapewniać poufność transmitowanych danych poprzez mechanizm szyfrowania.
WF.15	System powinien zapewniać wsparcie dla protokołów komunikacyjnych, pozostawiając dowolność w dopasowaniu do konkretnego systemu (np.: ssh, telnet, RDP, VNC, http/https, odbc, etc.)
WF.16	Rozwiązanie musi umożliwiać usługę pośredniczenia w dostępie do systemów i urządzeń dla użytkowników domenowych, rejestrując obsługiwane sesje, oraz obsługując minimum następujące protokoły: 1) SSH; 2) RDP; 3) VNC; 4) TELNET; 5) HTTP/HTTPS.

KOD WYMAGANIA	OPIS PODSTAWOWYCH WYMAGAŃ FUNKCJONALNYCH
WF.17	Zamawiający wymaga dostawy jednolitego oprogramowania obsługującego cały system rejestrowania sesji i zarzadzania kontami i tożsamościami uprzywilejowanymi.
WF.18	Przedmiot zamówienia musi zapewniać wsparcie dla dowolnego urządzenia obsługującego SSH.
WF.19	Przedmiot zamówienia musi zapewniać wsparcie dla dowolnego urządzenia obsługującego ODBC w wersji 2.7 lub wyższej.
WF.20	Przedmiot zamówienia musi zapewnić możliwość zarządzania kontami uprzywilejowanymi w systemach operacyjnych: 1) Windows; 2) Unix/Linux; 3) Komponentów oprogramowania Microsoft: Microsoft Services, IIS application Pool, IIS Directory Security, w rejestrach, COM+ oraz zarządzanie kontami w domenie.
WF.21	Przedmiot zamówienia musi zapewnić możliwość zarządzania kontami uprzywilejowanymi w systemach baz danych: 1) Microsoft SQL Server; 2) Oracle; 3) Mysql; 4) PostgreSQL.
WF.22	Przedmiot zamówienia musi zapewniać wsparcie dla kont lokalnego administratora zarówno na stacjach roboczych jak i na serwerach.
WF.23	Przedmiot zamówienia nie może posiadać ograniczeń w postaci maksymalnej liczby wspieranych systemów docelowych i przypisanych im kont uprzywilejowanych.
WF.24	Przedmiot zamówienia 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.
WF.25	Przedmiot zamówienia musi zostać dostarczony z kompletem licencji minimum dla następującej liczby funkcjonalności: 1) ochrona kont uprzywilejowanych; 2) zarządzanie i monitorowanie sesji uprzywilejowanych;

KOD WYMAGANIA	OPIS PODSTAWOWYCH WYMAGAŃ FUNKCJONALNYCH
	3) ograniczanie dostępu do zbiorów poleceń w połączeniach terminalowych; 4) raportowanie wykorzystania kont uprzywilejowanych; 5) rejestrowanie sesji uprzywilejowanych.
WF.26	Oprogramowanie musi obsługiwać monitorowanie i ochronę nawet kilkudziesięciu jednoczesnych połączeń od jednego użytkownika końcowego, do różnych systemów poprzez różne lub jedno konto uprzywilejowane.
WF.27	Oprogramowanie musi mieć wbudowane mechanizmy rozliczalności, autentykacji i autoryzacji.
WF.28	Przedmiot zamówienia musi umożliwiać integrację z mechanizmami wykorzystywanymi do uwierzytelniania użytkowników: 1) LDAP (nie mniej niż: Sun One, MS AD, IBM Tivoli, Novel eDirectory, Oracle Internet Directory); 2) RADIUS (TACACS); 3) Windows NTLM; 4) SAML; 5) Wieloskładnikowe uwierzytelnianie (2FA); 6) Baza lokalnych danych uwierzytelniania; 7) RSA SecurID; 8) Oracle SSO.
WF.29	Przedmiot zamówienia musi wykrywać i poddawać analizie niestandardowe działania podejmowane przez użytkowników systemu.
WF.30	Przedmiot zamówienia powinien gromadzić i poddawać analizie niestandardowe działania wysokiego ryzyka oraz reagować na nie.
WF.31	Automatycznie powiadamianie (alertowanie) w czasie rzeczywistym o zagrożeniach występujących w infrastrukturze.
WF.32	Przedmiot zamówienia musi posiadać (i zostać dostarczony z odpowiednimi licencjami) wbudowane narzędzia analityczne umożlwiające automatyczne, bezobsługowe (bez konieczności definiowania reguł polityki bezpieczeństwa) wykrywanie podejrzanej aktywności kont uprzywilejowanych na bazie nauczonych automatycznie wzorców działania poszczególnych użytkowników (podejrzany czas pracy, nowy adres IP, zbyt duża ilość odwołań do repozytorium kont o hasła).
WF.33	Przedmiot zamówienia musi generować (i zostać dostarczony z odpowiednimi licencjami) odpowiedni alarm w przypadku wykrycia nadmiernego wykorzystania kont uprzywilejowanych przez danego użytkownika oraz

KOD WYMAGANIA	OPIS PODSTAWOWYCH WYMAGAŃ FUNKCJONALNYCH
	w przypadku wykorzystania konta uprzywilejowanego w niestandardowych godzinach.
WF.34	Przedmiot zamówienia musi umożliwiać (i zostać dostarczony z odpowiednimi licencjami) wykrywanie incydentów polegających na bezpośrednim dostępie użytkownika do systemu docelowego (np. bez wcześniejszego wystąpienia o hasło do systemu docelowego), utworzenie na systemie docelowym niezarządzanego do tej pory konta uprzywilejowanego.
WF.35	Przedmiot zamówienia musi wykrywać (i zostać dostarczony z odpowiednimi licencjami) podatności środowiska dotyczące kont uprzywilejowanych: nieszyfrowana komunikacja do systemu pozwalająca na przejęcie danych dostępowych kont uprzywilejowanych, użycie kont serwisowych w wielu celach (jako konta serwisowe i jednocześnie interaktywne).
WF.36	Przedmiot zamówienia musi posiadać funkcję (i zostać dostarczony z odpowiednimi licencjami) 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 również podczas trwania bieżących 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 w wyniku których akcji wykonanych przez użytkownika sesja powinna być automatycznie zakończona.
WF.37	Przedmiot zamówienia musi posiadać funkcję (i zostać dostarczony z odpowiednimi licencjami): Identyfikacji ataków na kontroler domeny: Golden Ticket, Over-Pass-the-Hash, PAC manipulation dla minimum czterech kontrolerów zarządzania uprawnieniami administratorów kontrolera domeny, pozwalającą m.in. na ograniczenie możliwości nieautoryzowanego tworzenia nowych administratorów kontrolera domeny - dla minimum 4 kontrolerów.
WF.38	Przedmiot zamówienia musi posiadać możliwość rozbudowy funkcjonalnej o kolejne komponenty odpowiedzialne za nie mniej niż agentowe ograniczanie uprawnień użytkowników na stacjach Windows poprzez: 1) usuwanie kont lokalnych administratorów i podnoszenie uprawnień w kontekście konkretnych obiektów (skryptów, aplikacji, instalacji, dll i innych) dla konkretnych użytkowników; 2) kontrolę aplikacyjną; 3) blokowanie wycieku poświadczeń (np. haseł) z repozytoriów systemu operacyjnego oraz aplikacji (np. przeglądarek internetowych, pamięci LSASS, SAM i innych).

KOD WYMAGANIA	OPIS PODSTAWOWYCH WYMAGAŃ FUNKCJONALNYCH
ARCHITEKTURA SYSTEMU	
WAR.01	Przedmiot zamówienia poprzez wewnętrzne jego mechanizmy powinien zapewniać jego wysoką dostępność 24 godziny, 7 dni w tygodniu, 365 dni w roku.
WAR.02	Przedmiot zamówienia musi zapewniać wsparcie dla kluczy kryptograficznych używanych do szyfrowania danych wewnątrz Systemu zgodnych z FIPS 140-2.
WAR.03	Przedmiot zamówienia musi umożliwiać dostęp użytkowników do systemu docelowego następującymi narzędziami: 1) Interfejs Web rozwiązania zabezpieczenia kont uprzywilejowanych; 2) wykorzystanie dowolnych narzędzi RDP używanych na stacji z której realizowany jest dostęp uprzywilejowany; 3) wykorzystanie dowolnych narzędzi linii poleceń i protokołu SSH / Telnet (np. putty).
WAR.04	Przedmiot zamówienia dla realizacji podstawowych funkcjonalności musi działać bez konieczności instalacji agenta na systemie docelowym do nagrywania sesji oraz ochrony kont uprzywilejowanych za wyjątkiem kontrolerów domen.
WAR.05	Przedmiot zamówienia musi umożliwiać segregowanie obowiązków poprzez umożliwienie dostępu danemu administratorowi tylko do wybranych zasobów.
WAR.06	Musi istnieć możliwość wykorzystania trybu wysokiej dostępności pomiędzy dwoma systemami w jednym centrum danych oraz modułów zapasowych Disaster Recovery w innych lokalizacjach.
WAR.07	Zaproponowane rozwiązanie musi uwzględniać nie mniej niż: 1) jeden system składowania danych; 2) 1x system High Availability; 3) 2x system Disaster Recovery; 4) 3x moduł do zmian i zarządzania kluczami oraz hasłami w systemach chronionych.
WAR.08	Przedmiot zamówienia nie może licencyjnie ograniczać ilości 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 producenta systemu ochrony kont uprzywilejowanych).
WAR.09	Zapewnienie wysokiej dostępności modułu składowania kont uprzywilejowanych musi być zaimplementowana na warstwie proponowanego oprogramowania, nie systemu operacyjnego na którym oprogramowanie jest zainstalowane.

KOD WYMAGANIA	OPIS PODSTAWOWYCH WYMAGAŃ FUNKCJONALNYCH
WAR.10	Przedmiot zamówienia musi posiadać funkcję implementacji modułów składowania kont uprzywilejowanych w formie rozproszonej, złożonej z aktywnego modułu, redundancji modułu aktywnego oraz zbioru modułów rozproszonych geograficznie, świadczących (w trybie odczytu) część funkcji użytkownikom (np. mechanizmy wykonywania kopii zapasowych, udostępniania danych kont uprzywilejowanych aplikacjom).
WAR.11	Przedmiot zamówienia musi spełniać międzynarodowe certyfikacje minimum Common Criteria Level (EAL) 2+.
ZARZĄDZANIE	
WFZA.01	Dostarczone rozwiązanie musi umożliwiać centralne zarzadzanie poprzez jednolity panel administracyjny, obsługujący administratorów w wielu strefach czasowych.
WFZA.02	Przedmiot zamówienia musi posiadać możliwość odzwierciedlenia zmian zachodzących w organizacji (usługa katalogowa Active Directory/LDAP) takich jak dodawanie użytkowników, usuwanie użytkowników, zmiana przynależności użytkownika do grup, ról itd.
WFZA.03	Rozwiązanie powinno umożliwiać generowanie spersonalizowanych raportów jak i możliwość tworzenia spersonalizowanych interfejsów (np. dodanie elementu graficznego jak logo firmy).
WFZA.04	Przedmiot zamówienia powinien umożliwiać realizacje operacji masowych, edycji lub dodawania atrybutów do wskazanych kont w tym samym czasie.
ZARZĄDZANIE KONTAMI UPRZYWILEJOWANYMI W APLIKACJACH	
WFZAP.01	Przedmiot zamówienia musi zapewniać wsparcie SDK przy wykorzystaniu języków C/C++, Java, CLI (Command Line Interface - Windows, Linux), .Net Framework, COM (Windows).
WFZAP.02	Przedmiot zamówienia musi umożliwiać zarządzanie i ochronę oraz eliminację poświadczeń uprzywilejowanych zaszytych w aplikacjach i skryptach.
WFZAP.03	Przedmiot zamówienia musi umożliwiać zarządzanie poświadczeniami uprzywilejowanymi, wykorzystywanymi przez aplikacje, przechowywanymi w formie zaszyfrowanej.
WFZAP.04	Przedmiot zamówienia musi zapewniać uwierzytelnianie aplikacji i skryptów przed udostępnieniem poświadczeń kont uprzywilejowanych. Wymagane są co najmniej następujące mechanizmy uwierzytelnienia: adres IP, użytkownik systemu operacyjnego, ścieżka, skrót (hash) programu.
WFZAP.05	Przedmiot zamówienia musi wspierać tzw. tryb bezpołączeniowy czyli np. scenariusz w którym z powodu utraty komunikacji sieciowej aplikacja traci

KOD WYMAGANIA	OPIS PODSTAWOWYCH WYMAGAŃ FUNKCJONALNYCH
	kontakt z zabezpieczonym repozytorium składowania haseł. W takim scenariuszu aplikacja musi mieć lokalny dostęp do hasła umożliwiając zachowanie ciągłości działania aplikacji. Musi istnieć możliwość wyboru miejsca składowania poświadczeń lokalnie (cache): w pamięci systemu operacyjnego lub również w pliku w formacie zaszyfrowanym, co pozwala na zapisanie danych nawet w przypadku restartu systemu operacyjnego. Składowanie poświadczeń lokalnie musi być automatycznie wyłączane w przypadku wykonywania zmian haseł przez rozwiązanie.
WFZAP.06	Przedmiot zamówienia musi zapewniać bezpieczeństwo oraz automatyczne zarządzanie poświadczeniami w serwerach aplikacyjnych co najmniej JBOSS, Tomcat bez zmian w kodzie aplikacji (przez modyfikacje/przekierowanie używanego data source aplikacji).
WFZAP.07	Przedmiot zamówienia musi umożliwiać implementację w różnych trybach (w trybie agentowym i bezagentowym) aby zapewnić elastyczność w stosunku do różnych aplikacji. W trybie agentowym wymagana jest możliwość włączenia funkcji składowania danych dostępowych lokalnie (local cache) w formacie zaszyfrowanym.
BEZPIECZEŃSTWO	
WFBS.01	Przedmiot zamówienia musi zapewniać możliwość ograniczonego dostępu lub podglądu haseł uprzywilejowanych.
WFBS.02	Przedmiot zamówienia musi zapewniać możliwość budowania polityk dostępu w oparciu o role poprzez wbudowane mechanizmy oraz na podstawie przynależności do odpowiednich grup w Active Directory/LDAP.
WFBS.03	Komunikacja pomiędzy wszystkimi komponentami systemu musi być szyfrowana.
WFBS.04	Rozwiązanie musi zapewniać możliwość szyfrowania kopii zapasowych generowanych bezpośrednio z produktu.
WFBS.05	Przedmiot zamówienia musi zapewniać ochronę kryptograficzną wszystkich zapisanych danych (haseł, kluczy ssh oraz nagrań).
WFBS.06	Przedmiot zamówienia powinien zapewniać integralność oraz ochronę kryptograficzną przechowywanych danych takich jak poświadczenia uwierzytelniające, polityki, nagrania sesji, itd.) uniemożliwiających jakiekolwiek ingerencje np. modyfikacje bądź usuniecie.
WFBS.07	Przedmiot zamówienia musi wspierać wielostopniowe zarządzanie uprawnieniami, dla wielu administratorów systemów końcowych, gdzie każdy

KOD WYMAGANIA	OPIS PODSTAWOWYCH WYMAGAŃ FUNKCJONALNYCH
	może mieć inne uprawnienia przydzielone do systemów i/lub kont uprzywilejowanych, którymi może zarządzać.
INTEGRACJA	
WFIN.01	Rozwiązanie musi posiadać możliwość integracji z systemami typu SIEM w celu wymiany informacji o zarejestrowanych zdarzeniach w ramach monitorowanych sesji zarządzanych kontach uprzywilejowanych.
WFIN.02	Przedmiot zamówienia musi posiadać wbudowane API lub inne wbudowane mechanizmy integracyjne umożliwiające wymianę informacji z systemami do obsługi zgłoszeń (ang. Ticketing System).
WFIN.03	Przedmiot zamówienia musi wspierać integrację z rozwiązaniami typu HSM obsługującymi standard PKCS11.S.
RAPORTOWANIE	
WFRA.01	Przedmiot zamówienia musi posiadać wskazanie kont użytkowników, które realizowały z powodzeniem lub bez powodzenia logowanie do systemów informatycznych (np. aplikacji, systemów operacyjnych) w wybranych odstępach czasowych.
WFRA.02	Przedmiot zamówienia musi mieć możliwość prezentacji aktywności danego konta ze szczególnym uwzględnieniem zmiany hasła oraz historii aktywnych sesji.
WFRA.03	Przedmiot zamówienia powinien zapewniać możliwość zdefiniowania haromonogramu automatycznego generowania raportów jak również generować raport „na żądanie”.
WFRA.04	Szczegółowe generowanie raportów w oparciu o zdefiniowane harmonogramy dla raportów podstawowych takich, takich jak aktywność użytkownika, inwentaryzacja kont uprzywilejowanych, naruszenie polityk.
WFRA.05	Raportowanie zmian wprowadzonych przez użytkowników systemu (w tym administratorów).
WFRA.06	Przedmiot zamówienia musi umożliwiać raportowanie udanych i nieudanych prób logowania do dostarczonego przez Wykonawcę rozwiązania.
WFRA.07	Przedmiot zamówienia musi umożliwiać ograniczenie dostępu do raportów dla użytkowników / administratorów systemu.
WFRA.08	Przedmiot zamówienia musi umożliwiać wysłanie powiadomień e-mail z informacja o wygenerowanych raportach.

KOD WYMAGANIA	OPIS PODSTAWOWYCH WYMAGAŃ FUNKCJONALNYCH
WFRA.09	Przedmiot zamówienia musi generować raporty co najmniej w następujących formatach: 1) Formatted Microsoft Excel; 2) CSV.
WFRA.10	Przedmiot zamówienia musi umożliwiać raportowanie wszystkich logowań do Systemu.
WFRA.11	Przedmiot zamówienia musi umożliwiać raportowanie wszystkich zmian haseł oraz ich wykorzystania.
WFRA.12	Przedmiot zamówienia musi umożliwiać raportowanie informacji o zablokowanych kontach.
WFRA.13	Przedmiot zamówienia musi umożliwiać raportowanie niezgodności haseł z przyjętą w organizacji polityką bezpieczeństwa.
WFRA.14	Przedmiot zamówienia musi umożliwiać wysłanie powiadomienia email dla aktywności związanej z kontem uprzywilejowanym.
WFRA.15	Przedmiot zamówienia musi umożliwiać wysłanie powiadomienia email dla użytkownika wnioskującego o dostęp do systemu docelowego w przypadku zakończenia procesu weryfikacji.
WFRA.16	Przedmiot zamówienia musi umożliwiać wysłanie powiadomienia email do użytkownika w przypadku wygaśnięcia hasła i nie przypisaniu nowego (np. w sytuacji konieczności ręcznej zmiany haseł).
WFRA.17	Przedmiot zamówienia musi umożliwiać wysyłanie powiadomień e-mail dla następujących zdarzeń: 1) dostęp systemowy; 2) zmiany systemowe; 3) wykorzystanie hasła; 4) żądanie użycia hasła oraz akceptacja.
WFRA.18	Przedmiot zamówienia musi umożliwiać wykrywanie kluczy SSH odbiegających od przyjętej polityki i generowanie raportów zawierających te informacje.
WFRA.19	Przedmiot zamówienia musi umożliwiać generowanie raportów użycia prywatnych kluczy SSH.
WFRA.20	Przedmiot zamówienia musi udostępniać narzędzie umożliwiające wykrywanie par kluczy SSH w danej infrastrukturze oraz określenie relacji zaufania bazujących na kluczach SSH.

KOD WYMAGANIA	OPIS PODSTAWOWYCH WYMAGAŃ FUNKCJONALNYCH
WFRA.21	Przedmiot zamówienia musi zapewniać bezpieczne przechowywanie i kontrolowany dostęp do prywatnych kluczy SSH.
WFRA.22	Przedmiot zamówienia musi umożliwiać wygenerowanie raportu zawierającego wszystkie informacje o niezgodnościach haseł przechowywanych w produkcie w stosunku do hasłem przechowywanych w systemach docelowych (raporty).
	ZARZADZANIE KONTAMI UPRZYWILEJOWANYMI
WFKU.01	Przedmiot zamówienia musi mieć możliwość definiowania polityki zmiany hasła na systemie docelowym zgodnie z ustawiona polityka (np. co „X” dni, „X” miesięcy, „X” lat).
WFKU.02	Przedmiot zamówienia powinien umożliwiać zmianę haseł na pojedynczym systemie docelowym, grupie systemów docelowych oraz wszystkich systemów jednocześnie zgodnie z przyjętymi kryteriami.
WFKU.03	Przedmiot zamówienia musi umożliwiać zmianę hasła i grupy haseł systemów docelowych w sposób: 1) automatyczny, zgodnie ze zdefiniowana polityka bezpieczeństwa (z podziałem na dni, miesiące lub lata); 2) ręczny, zainicjowany przez administratora; 3) automatyczny, w sytuacji braku synchronizacji hasła pomiędzy Systemem a systemem docelowym.
WFKU.04	Przedmiot zamówienia musi umożliwiać zmianę haseł na pojedynczym systemie docelowym lub wskazanej grupie systemów docelowych w określonym momencie zgodnie z przyjętym kryterium.
WFKU.05	Przedmiot zamówienia musi posiadać funkcję dynamicznego generowania (w formie pseudolosowej) nowego hasła (lub kluczy SSH) zgodne z określonym szablonem (np. dla hasła: ilość znaków specjalnych, małych/ dużych znaków, ilość znaków w haśle etc).
WFKU.06	System musi zapewniać możliwość określenia polityki złożoności hasła dla systemu docelowego: 1) długość hasła; 2) złożoność hasła.
WFKU.07	Przedmiot zamówienia musi umożliwiać generowanie haseł jednokrotnego użycia dla przechowywanych w systemie kont uprzywilejowanych.
WFKU.08	Przedmiot zamówienia musi umożliwiać transparentne połączenie do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego.

KOD WYMAGANIA	OPIS PODSTAWOWYCH WYMAGAŃ FUNKCJONALNYCH
WFKU.09	Przedmiot zamówienia musi posiadać wsparcie (możliwość zarządzania kontami) dla innych systemów (dostępnych z poziomu sieciowego) niż domyślnie wspierane.
WFKU.10	Przedmiot zamówienia musi umożliwiać ograniczanie dostępu do systemów docelowych oraz tworzenie pozytywnych i negatywnych list poleceń wykonywanych poprzez SSH, Telnet.
WFKU.11	Przedmiot zamówienia musi automatycznie synchronizować hasło przechowywane w produkcie oraz hasło przechowywane na systemie docelowym w przypadku wykrycia niezgodności.
WFKU.12	Przedmiot zamówienia musi zapewniać możliwość automatycznego wykrywania kont w nowych urządzeniach Windows, usługach systemu Windows, zaplanowanych zadaniach, kontach serwisowych IIS itp., automatycznego dodania powyższych do Systemu oraz automatycznie wymusić odpowiednią politykę zarządzania kontami uprzywilejowanymi.
WFKU.13	Przedmiot zamówienia musi posiadać funkcję zmiany hasła i grupy haseł systemów docelowych w sposób: 1) automatyczny, zgodnie ze zdefiniowaną polityką (co „X" dni, „X" tygodni, „X" miesięcy lub „X" lat); 2) ręczny, zainicjowany przez administratora; 3) automatyczny, w sytuacji braku synchronizacji hasła pomiędzy Systemem a systemem docelowym.
WFKU.14	Przedmiot zamówienia musi automatycznie porównywać hasło przechowywane w produkcie oraz hasło przechowywane na systemie docelowym.
WFKU.15	Przedmiot zamówienia 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).
WFKU.16	Przedmiot zamówienia musi umożliwiać zdefiniowanie gwarantowanej liczby unikalnych haseł wprowadzonych per system docelowy (np. ostatnie „X" haseł musi się różnić względem siebie).
WFKU.17	W przypadku wykrycia niezgodności hasła przechowywanego w produkcie w stosunku do hasła przechowywanego w systemie docelowym, System musi wystawić odpowiednie powiadomienie.
WFKU.18	Przedmiot zamówienia musi mieć funkcjonalność cyklicznej weryfikacji hasła.
WFKU.19	Przedmiot zamówienia musi umożliwiać wykrywanie kluczy SSH odbiegających od przyjętej polityki i generowanie raportów zawierających te informacje.
WFKU.20	Przedmiot zamówienia musi zapewniać bezpieczne przechowywanie i kontrolowany dostęp do prywatnych kluczy SSH .

KOD WYMAGANIA	OPIS PODSTAWOWYCH WYMAGAŃ FUNKCJONALNYCH
WFKU.21	Przedmiot zamówienia musi umożliwiać automatyczną rotację kluczy SSH.
WFKU.22	Przedmiot zamówienia musi posiadać funkcje wnioskowania o dostęp do systemu docelowego przez zdefiniowane grupy osób. Wniosek musi być potwierdzony przez wskazany zbiór osób na kilku poziomach (np. wskazana ilość administratorów bezpieczeństwa i ich przełożonych).
WFKU.23	Przedmiot zamówienia musi umożliwiać użytkownikowi wnioskowanie o dostęp do określonych systemów docelowych we skazanych przez użytkownika godzinach.
NAGRYWANIE SESJI KONT UPRZYWILEJOWANCH	
WFSKU.01	Przedmiot zamówienia musi umożliwiać nagrywanie sesji uprzywilejowanych w: 1) systemach Windows; 2) systemach UNIX/Linux; 3) routerach oraz przełącznikach (narzędzia ssh takie jak putty, secureCRT); 4) bazach danych typu SQL; 5) w dostępie aplikacji web przez przeglądarki internetowe; 6) aplikacjach do zarządzania środowiskami do wirtualizacji (Vmware Client).
WFSKU.02	Przedmiot zamówienia musi umożliwiać nagrywanie sesji wraz z podglądem sesji aktywnej oraz możliwością ingerencji administratora w sesję aktywną z możliwością przerwania aktywnej sesji włącznie.
WFSKU.03	Nagrywanie sesji nie może mieć żadnego wpływu na wydajność systemu docelowego.
WFSKU.04	Przedmiot zamówienia musi mieć zaimplementowane algorytmy umożliwiające kompresję wynikowego pliku wideo w celu ograniczenia jego rozmiaru.
WFSKU.04	Przedmiot zamówienia musi przechowywać nagrania sesji w zabezpieczonym kryptograficznie repozytorium zapewniającym ich integralność i zabezpieczającym przed ingerencja.
WFSKU.05	Przedmiot zamówienia musi wykorzystywać mechanizmy indeksowania nagrań umożliwiające szybkie przeszukiwanie nagranych i monitorowanych sesji pod kątem występowania wskazanych słów kluczowych.
WFSKU.06	Przedmiot zamówienia musi umożliwiać odtworzenie zarejestrowanych nagrań sesji.
WFSKU.07	Przedmiot zamówienia musi posiadać funkcje rejestrowania wszystkich znaków wpisywanych z klawiatury użytkownika.
WFSKU.08	Przedmiot zamówienia musi umożliwiać monitoring, ingerencję oraz zakończenie aktywnej sesji RDP oraz SSH w czasie jej trwania, a także określenie zbioru

KOD WYMAGANIA	OPIS PODSTAWOWYCH WYMAGAŃ FUNKCJONALNYCH
	poleceń i uruchomionych funkcji systemu operacyjnego które spowodują automatyczne zakończenie sesji użytkownika.
WFSKU.09	Przedmiot zamówienia musi zapewniać możliwość uruchomienia oraz zestawienia połączenia za pomocą różnych aplikacji klienckich ze stacji monitorującej do systemów docelowych, dodatkowo umożliwiając automatyczne wprowadzenie do nich danych konta uprzywilejowanego.
WFSKU.10	Przedmiot zamówienia musi umożliwiać definiowanie dokładnych reguł określających warunki nagrywania sesji użytkownika (np. wybrany zbiór systemów docelowych).
WFSKU.11	Przedmiot zamówienia musi umożliwiać ograniczanie dostępu do systemów docelowych oraz tworzenie list dopuszczalnych i niedopuszczalnych poleceń wykonywanych poprzez SSH.
WFSKU.12	Przedmiot zamówienia musi zapewniać rozliczalność w przypadku jednoczesnego wykorzystania konta współdzielonego przez więcej niż jednego użytkownika.
WFSKU.13	Przedmiot zamówienia musi posiadać możliwość monitorowania dostępu do środowisk wirtualizacyjnych Vmware przy użyciu SSH (powercli) oraz Vmware vSphere Web Client.

5. Warunki udzielenia licencji

KOD WYMAGANIA	OPIS WYMAGAŃ MINIMALNYCH
WR.01	Licencje na oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej: klucze lub licencje dostępne do pobrania na stronie www producenta oprogramowania.
WR.02	W przypadku licencji dostępnych w formie elektronicznej na stronie producenta, Wykonawca przekaże dane autoryzacyjne lub Zamawiający poda konto do portalu producenta, jakie posiada, a do którego licencje maja być dołączone.
WR.03	Oprogramowanie musi posiadać od dnia podpisania protokołu odbioru końcowego, minimum 36 miesięczne wsparcie techniczne producenta oprogramowania dla licencji (tj. licencji dostarczonych w ramach niniejszego postępowania).

WR.04	Wsparcie techniczne zapewniające aktualizacje oprogramowania do najnowszej wersji oraz wsparcie telefoniczne, email lub stronę www producenta w przypadku problemów z oprogramowaniem.
WR.05	Dostarczone licencje powinny obejmować możliwość korzystania ze wszystkich wymaganych funkcjonalności dla co najmniej 10 kont uprzywilejowanych.
WR.06	Oprogramowanie nie może licencyjnie ograniczać ilości 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 producenta systemu ochrony kont uprzywilejowanych).

6. ŚWIADCZENIE SERWISU GWARANCYJNEGO I GWARANCJI

KOD WYMAGANIA	OPIS WYMAGAŃ MINIMALNYCH
WUSU.1	Zaoferowany model wsparcia technicznego musi zapewniać możliwość aktualizacji oprogramowania do najnowszej wersji oraz wsparcie telefoniczne, email lub stronę www producenta w przypadku problemów z oprogramowaniem.
WUSU.2	Czas reakcji na zgłoszenie (rozumienie jako podjęcie działań diagnostycznych oraz kontakt ze zgłaszającym) nie może przekroczyć 60 minut od momentu zarejestrowania zgłoszenia.
WUSU.4	Naprawa usterki/wady w Oprogramowaniu musi nastąpić maksymalnie w następnym dniu roboczym od momentu reakcji na zgłoszenie.
WUSU.5	Dopuszcza się, aby Wykonawca zastosował czasowe obejście rozwiązania problemu (ang. Workaround) w uzgodnieniu i akceptacją przez Zamawiającego, jednak docelowe rozwiązanie usterki/wady musi zostać dostarczone i zaimplementowane w czasie 30 dni liczonych od dnia następnego po dniu wdrożenia tymczasowego obejścia problemu.
WUSU.5	Zamawiający wymaga, aby gwarancja była realizowana w języku polskim przez Wykonawcę mającego status autoryzowanego wsparcia technicznego producenta/ wytwórcy Oprogramowania.
WUSU.7	Zamawiający wymaga, aby w ramach udzielonej usługi gwarancji Wykonawca dostarczył każdorazowo procedurę: 1) aktualizacji komponentów systemu do najnowszej wersji wraz z rekomendacją wdrożenia; 2) wycofania aktualizacji – powrotu do poprzedniej wersji (ang. Rollback).

7. WYMAGANIA W ZAKRESIE DOKUMENTACJI

Wykonawca dostarczy Dokumentację spełniającą wymagania określone w poniższej tabeli.

KOD WYMAGANIA	OPIS WYMAGAŃ MINIMALNYCH
DOK.1	Zamawiający wymaga, aby Wykonawca przygotował, zgodnie z ogólnie akceptowalnymi standardami w dziedzinie dokumentowania Wykaz Ilościowo-Cenowy. Wykaz Ilościowo-Cenowy zawiera co najmniej następujące informacje: 1) nazwa; 2) producent; 3) kod produktu/model (Part Number); 4) opis; 5) ilość; 6) cena jednostkowa brutto w PLN; 7) cena jednostkowa netto w PLN; 8) wartość brutto w PLN.
DOK. 2	Zamawiający wymaga, aby Wykonawca dostarczył dokumenty poświadczające: 1) posiadany status autoryzowanego sprzedawcy / dystrybutora 2) posiadany status autoryzowanego wsparcia technicznego producenta dla przedstawionego w ofercie oprogramowania.
DOK. 3	Wykonawca zobowiązany jest do dostarczenia procedur hardeningu systemu operacyjnego na którym zostanie zainstalowane zaoferowane przez Wykonawcę rozwiązanie.

ZASADY ODBIORU PRZEDMIOTU UMOWY

I.Zasady Ogólne

1. Przedmiot zamówienia należy dostarczyć zgodnie z zasadami i terminami wskazanymi w Umowie.
2. Przedmiot zamówienia będzie zrealizowany nie później niż w ciągu 30 dni od dnia podpisania Umowy.
3. Odbiór zostanie przeprowadzony w biurze Zamawiającego przy ul. Maszewskiej 20, w Warszawie , lokal U1, pierwsze piętro w obecności przedstawicieli Wykonawcy w godz. 8:00 – 15:35 lub elektronicznie na zasadach określonych w Umowie.
4. Szczegółowe zasady realizacji przedmiotu zamówienia określa umowa.

II. Odbiór

Celem czynności kontrolnych prowadzonych w ramach odbioru ilościowo – jakościowego jest sprawdzenie kompletności dostarczonego przedmiotu umowy i potwierdzenie zgodności z ilością określoną w umowie oraz sprawdzenie wymagań funkcjonalnych i potwierdzenie zgodności ze szczegółowym opisem przedmiotu Umowy.