OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa licencji systemu zarządzania dostępem uprzywilejowanym (PAM) wraz z serwisem producenta oraz usługą wdrożenia w dwóch niezależnych sieciach IT i OT

1. Przedmiot zamówienia

1.1. Przedmiotem zamówienia jest dostawa licencji na system klasy PAM (Privileged Access Management), służący do ochrony kont uprzywilejowanych i kluczy SSH, pośredniczenia w dostępie uprzywilejowanym, monitorowania i rejestrowania sesji uprzywilejowanych oraz raportowania wykorzystania kont uprzywilejowanych, dla dwóch niezależnych instancji – w sieci IT oraz w sieci OT Zamawiającego – wraz z serwisem producenta oraz usługą wdrożenia.

1.2. W skład przedmiotu zamówienia wchodzą:

Lp.	Element przedmiotu zamówienia	Ilość
1.	Licencja terminowa na system PAM dla co najmniej 5 użytkowników – zgodnie z rozdz. 2 i 3	2 kpl. (1 – sieć IT, 1 – sieć OT) na 24 miesięcy
2.	Serwis (wsparcie producenta i dystrybutora, aktualizacje) dla obu instancji (IT i OT) – zgodnie z rozdz. 4	24 miesięcy
3.	Usługa wdrożenia systemu PAM w dwóch niezależnych sieciach IT i OT, wraz z instruktażem administratorów	1 usługa

1.4. Zamówienie obejmuje dostawę licencji dla dwóch instancji systemu PAM: jednej przeznaczonej dla sieci IT i jednej dla sieci OT Zamawiającego. Instancje muszą działać jako dwa całkowicie niezależne systemy, zgodnie z pkt 2.5 i rozdz. 5. Wymagania z rozdz. 3 dotyczą każdej z instancji.

1.5. Kod CPV: 48730000-4 Pakiety oprogramowania zabezpieczającego; 72268000-1 Usługi dostawy oprogramowania; 72265000-0 Usługi konfiguracji oprogramowania.

2. Wymagania ogólne

2.1. Licencje muszą być wystawione na Zamawiającego, obejmować zakres określony w pkt 7–9 tabeli w rozdz. 3 i zostać udzielone na okres 24 miesięcy od dnia podpisania protokołu odbioru licencji. Liczba użytkowników: co najmniej 5 dla instancji IT i co najmniej 5 dla instancji OT.

2.2. Wygaśnięcie licencji terminowej nie może powodować utraty dostępu Zamawiającego do poświadczeń zapisanych w sejfie, nagrań sesji ani logów zdarzeń – Zamawiający musi mieć możliwość ich odczytu i eksportu.

2.3. System musi być instalowany w infrastrukturze Zamawiającego (on-premise), w środowisku wirtualizacyjnym Hyper-V lub VMware (pkt 3 tabeli), odrębnym dla sieci IT i dla sieci OT. Działanie funkcji systemu, w tym aktywacja licencji, nie może wymagać połączenia z chmurą producenta. Instancja OT musi zapewniać pełną funkcjonalność w środowisku bez dostępu do Internetu, z możliwością aktualizacji w trybie offline.

2.4. Wykonawca wskaże w ofercie minimalne wymagania sprzętowe (procesor, pamięć RAM, przestrzeń dyskowa, w tym na nagrania sesji przez okres **24** miesięcy) odrębnie dla instancji IT i OT, z uwzględnieniem klastra active-active z arbitrem (pkt 5–6 tabeli).

2.5. Instancje dla sieci IT i OT muszą być od siebie całkowicie niezależne. Każda instancja musi działać samodzielnie, z własnym sejfem poświadczeń, bazą danych, kontami użytkowników, konfiguracją i licencją, bez wspólnej konsoli zarządzania, synchronizacji danych lub konfiguracji ani połączeń sieciowych między instancjami. Klaster active-active (pkt 5 tabeli) może być zestawiony wyłącznie w ramach jednej sieci. Pośrednik (pkt 18–19 tabeli) instancji IT nie może być umieszczony w sieci OT, i odwrotnie.

2.6. System musi być dostarczony w najnowszej wersji dostępnej na dzień dostawy. Interfejs użytkownika i dokumentacja muszą być dostępne w języku polskim lub angielskim .

2.7. Wykonawca przekaże dokumenty potwierdzające udzielenie licencji i rejestrację serwisu u producenta na rzecz Zamawiającego, z uwzględnieniem wymagania z pkt 49 tabeli.

3. Wymagania funkcjonalne systemu PAM

Oferowany system musi spełniać co najmniej poniższe wymagania minimalne, odrębnie w każdej z instancji (IT i OT).

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
A. Ogólne – architektura		
1.	System PAM musi być rozwiązaniem bezagentowym, tj. umożliwiającym nawiązywanie sesji z wykorzystaniem serwerów proxy, bez potrzeby instalacji oprogramowania (agenta) na systemie, do którego będzie nawiązywana sesja.	
2.	System musi umożliwiać uwierzytelnianie wieloskładnikowe i obsługiwać wiele platform i systemów operacyjnych. System PAM ma zabezpieczać dostęp do maszyn fizycznych, maszyn wirtualnych, sprzętu sieciowego, w tym co najmniej: routerów, przełączników, zapór sieciowych, a także aplikacji, baz danych itp.	
3.	System musi być dostarczany w formie zamkniętej platformy wirtualnej, przygotowanej do implementacji w infrastrukturze Hyper-V lub VMware. Przez zamkniętą platformę Zamawiający rozumie wyspecjalizowane rozwiązanie, w ramach którego zainstalowana jest całość oprogramowania (system operacyjny, baza danych, aplikacja), realizująca wszystkie funkcjonalności systemu.	
4.	Rozwiązanie nie może wymagać wdrożenia kolejnych komponentów jako osobnych maszyn wirtualnych lub fizycznych. Do prawidłowego działania wszystkich dostępnych funkcjonalności wymagane jest posiadanie tylko jednej maszyny wirtualnej.	
5.	Rozwiązanie musi oferować możliwość wdrożenia drugiej instancji i konfiguracji klastra typu active-active.	
6.	Rozwiązanie musi posiadać możliwość wdrożenia komponentu zarządzającego klastrem w postaci arbitra.	
B. Licencjonowanie		
7.	System PAM musi zostać dostarczony z kompletem licencji dla co najmniej 5 użytkowników, którzy będą korzystali z systemu PAM (w każdej z instancji – IT i OT), obejmującym co najmniej następujące funkcjonalności: – ochronę kont uprzywilejowanych, – ochronę kluczy SSH, – zarządzanie i monitorowanie sesji uprzywilejowanych, – rejestrowanie sesji uprzywilejowanych, – raportowanie wykorzystania kont uprzywilejowanych.	
8.	Dostarczone licencje na system PAM do ochrony kont uprzywilejowanych zostaną udzielone na okres 24 miesięcy (licencje terminowe).	
9.	Dostarczone licencje na system PAM nie mogą w żaden sposób limitować liczby chronionych systemów docelowych.	
10.	System powinien być dostarczony wraz z serwisem na okres 24 miesięcy, umożliwiającym korzystanie ze wsparcia producenta oraz dystrybutora oraz pobieranie aktualizacji przygotowanych przez producenta.	
11.	W ramach zakupionych licencji użytkownicy systemu muszą mieć możliwość skorzystania z mechanizmu prywatnego sejfu do przechowywania haseł, notatek, plików itp.	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
12.	W ramach zakupionej licencji rozwiązanie powinno umożliwiać korzystanie z dodatkowych modułów: – modułu pozwalającego na automatyczne wyszukiwanie urządzeń w sieci, – modułu pozwalającego na tworzenie automatycznych zadań wykonywanych na zarządzanych urządzeniach, – modułu pozwalającego na zarządzanie rozwiązaniem za pomocą API.	
C. Funkcjonalności		
Zarządzanie kontami i dostęp do systemów docelowych		
13.	System PAM musi zapewniać możliwość zarządzania co najmniej: – użytkownikami w systemach operacyjnych Windows, Unix/Linux, – kontami domenowymi Microsoft Active Directory, – kontami lokalnymi VMware ESX/ESXi, – kontami na urządzeniach, m.in.: Cisco, Aruba, Alcatel, Check Point, FortiGate, Huawei, IBM AIX, Brocade, – kontami baz danych: Microsoft SQL Server, Oracle, MySQL, PostgreSQL, – kontami do zarządzania i monitorowania serwerów, m.in. iLO, iDRAC, – kontami aplikacji webowych: Facebook, Google, Twitter (X), LinkedIn, Instagram, OpenStack, AWS, – kontami w innych, niewymienionych systemach i urządzeniach, do których dostęp odbywa się za pomocą protokołów: SSH, RDP, VNC, Telnet, HTTP/HTTPS, X11, – kluczami SSH.	
14.	System PAM musi umożliwiać utworzenie poświadczeń typu Just-in-Time (JIT), które będą tworzone lub aktywowane na czas trwania sesji.	
15.	System PAM musi zapewniać usługę pośredniczenia w dostępie do systemów i urządzeń dla użytkowników domenowych oraz użytkowników zewnętrznych, rejestrując obsługiwane sesje i obsługując co najmniej następujące protokoły: SSH, RDP, VNC, Telnet, HTTP/HTTPS, X11.	
16.	System PAM musi wspierać również protokoły bez rejestracji sesji: Cassandra, Elasticsearch, LDAP, LDAPS, MongoDB, MySQL, Oracle, PostgreSQL, Redis, Solr, SQL Server, RDS, Sybase, Windows RM, Windows RPC, Windows SMB.	
17.	System PAM musi umożliwiać dostęp użytkowników do systemu docelowego za pomocą następujących narzędzi: – przeglądarki internetowej, – klienta RDP, – klienta protokołu SSH/Telnet (np. PuTTY), – klienta serwerów bazodanowych, w tym co najmniej DBeaver.	
18.	System PAM musi umożliwiać wykorzystanie pośrednika w komunikacji pomiędzy systemem PAM a systemem docelowym.	
19.	Pośrednik musi być dostępny jako obraz dla usługi konteneryzacji Docker.	
Uwierzytelnianie		
20.	System PAM musi wspierać co najmniej następujące mechanizmy uwierzytelniania: LDAP, RADIUS, TACACS+, Active Directory, OpenID, SAML.	
21.	System PAM musi zapewniać możliwość uwierzytelniania dwuskładnikowego.	
22.	System PAM musi wspierać integrację z rozwiązaniami uwierzytelniania dwuskładnikowego, takimi jak Google Authenticator i Microsoft Authenticator.	
23.	System PAM musi obsługiwać monitorowanie i ochronę kilkudziesięciu jednoczesnych połączeń od jednego użytkownika końcowego do różnych systemów, poprzez wiele kont uprzywilejowanych lub jedno konto.	
Polityki dostępu		

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
24.	System PAM musi ograniczać administratorowi możliwość dostępu do haseł lub ograniczać podgląd haseł uprzywilejowanych.	
25.	System PAM musi umożliwiać budowanie polityk kontroli dostępu w oparciu o role, np. na podstawie przynależności do grup AD/LDAP.	
26.	System PAM musi umożliwiać budowanie polityk kontroli dostępu wymuszających: – możliwość rozpoczęcia sesji, – możliwość podglądu hasła, – podanie powodu rozpoczęcia sesji, – podanie powodu podglądu hasła, – możliwość rozpoczęcia sesji bez akceptacji w przypadku awarii, – możliwość podglądu hasła bez akceptacji w przypadku awarii, – konieczność akceptacji rozpoczęcia sesji przez innego administratora (administratorów), – konieczność akceptacji podglądu hasła przez innego administratora (administratorów), – akceptację na kilku poziomach, – dostęp do urządzeń i poświadczeń docelowych określonego typu, producenta, lokalizacji, – zakres godzin, dni oraz dat, w których użytkownik systemu będzie miał dostęp do poświadczeń.	
27.	System PAM musi umożliwiać udostępnienie poświadczenia do użytku dla użytkownika poza polityką dostępową, która jest do niego przypisana. Udostępnienie musi dawać możliwość wyboru czasu trwania takiego dostępu.	
28.	System PAM musi oferować możliwość wykorzystania kont uprzywilejowanych niezapisanych w samym systemie – kont prywatnych użytkowników.	
Logi i raportowanie		
29.	System PAM musi posiadać log wszystkich zdarzeń systemowych.	
30.	System PAM musi umożliwiać wskazanie kont użytkowników, które realizowały logowanie do stacji lub serwera.	
31.	System PAM musi umożliwiać raportowanie wszystkich zmian wprowadzonych przez administratorów.	
32.	System PAM musi umożliwiać raportowanie wszystkich logowań do systemu.	
33.	System PAM musi umożliwiać raportowanie oparte na nietypowym źródle, czasie i długości połączenia do systemu docelowego.	
34.	Rozwiązanie musi posiadać graficzną wizualizację przedstawiającą status bezpieczeństwa aktywnych oraz historycznych sesji do systemów zdalnych.	
35.	System PAM musi umożliwiać ograniczenie dostępu do raportów dla wskazanej grupy użytkowników lub administratorów.	
Zarządzanie hasłami		
36.	System PAM musi mieć możliwość zmiany wartości hasła na systemie docelowym zgodnie z ustawioną polityką, m.in.: – umożliwiać zdefiniowanie wymagań dotyczących długości hasła i znaków w haśle (małe i duże litery, cyfry, znaki specjalne), – automatycznie generować hasła kont systemów docelowych w sposób pseudolosowy, – generować unikalne hasła dla kont systemów docelowych, – wymuszać automatyczną zmianę hasła po jego podglądzie.	
37.	System PAM musi umożliwiać przezroczyste (transparentne) połączenie do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego.	
Zarządzanie sesjami i nagrania		
38.	System PAM musi umożliwiać podgląd zestawionej sesji w czasie rzeczywistym.	
39.	System PAM musi umożliwiać przerwanie lub zawieszenie trwającej sesji.	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
40.	System PAM musi posiadać menu pozwalające na zawieszenie lub przerwanie wszystkich sesji oraz zablokowanie dostępu do samego rozwiązania w przypadku sytuacji krytycznej.	
41.	System PAM musi umożliwiać ograniczanie dostępu do systemów docelowych oraz tworzenie białych i czarnych list poleceń wykonywanych w systemie docelowym (audyt poleceń).	
42.	Audyt poleceń musi umożliwiać podjęcie co najmniej akcji „zablokuj polecenie" i „rozłącz sesję" po wykryciu audytowanego polecenia, a także automatyczne umieszczenie na liście zablokowanych użytkowników użytkownika, który próbował wykonać blokowane polecenie.	
43.	Nagrywanie sesji nie może mieć żadnego wpływu na wydajność systemu docelowego.	
44.	System PAM musi umożliwiać konfigurację parametrów nagrań, w tym: – liczby klatek na sekundę, – jakości pojedynczej klatki, – formatu pojedynczej klatki: JPG lub PNG, – okresu przechowywania nagrań.	
45.	System PAM musi rejestrować znaki wprowadzone z klawiatury przez użytkownika, co najmniej dla sesji SSH i RDP, oraz umożliwiać szybkie przeszukiwanie zapisanych danych pod kątem występowania wskazanych słów kluczowych.	
46.	System PAM musi umożliwiać wyświetlenie w nagraniu sesji momentów aktywności ekranowej oraz wprowadzania danych z klawiatury przez użytkownika.	
47.	System PAM musi umożliwiać utworzenie oddzielnego zestawu ustawień w oparciu o: – politykę dostępową, – urządzenie docelowe, – poświadczenie, – adres źródłowy.	
48.	System PAM musi umożliwiać odtworzenie i pobranie zarejestrowanych nagrań sesji.	
Pozostałe		
49.	Oprogramowanie dostarczone w ramach realizacji zamówienia musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, że zaoferowany produkt posiada wsparcie producenta na terenie Polski.	
50.	System PAM musi być kompletny i pozwalać na uruchomienie co najmniej następujących funkcjonalności: – zarządzanie kontami uprzywilejowanymi w ramach organizacji, – monitorowanie wykorzystania kont uprzywilejowanych, – nagrywanie i archiwizowanie sesji zdalnych, – zagwarantowanie skalowalności rozwiązania w przypadku dodawania nowych zasobów oraz nowych usług.	
51.	System PAM musi umożliwiać personalizację wyglądu aplikacji, co najmniej poprzez umieszczenie logo Zamawiającego w głównym oknie aplikacji.	

W celu potwierdzenia zgodności oferowanego rozwiązania z wymaganiami Zamawiający żąda złożenia wraz z ofertą:

- wypełnionej tabeli z załączniku nr 2.1 do Formularza ofertowego, ze wskazaniem producenta, nazwy i wersji oferowanego systemu;
- dokumentacji producenta (np. karty produktu, specyfikacji technicznej, opisu licencjonowania) potwierdzającej spełnienie wymagań z rozdz. 3, w tym model licencjonowania, brak limitu chronionych systemów docelowych oraz pracę w infrastrukturze Hyper-V lub VMware;

- w przypadku zaoferowania rozwiązania spoza oficjalnego kanału dystrybucyjnego producenta w Polsce – dokumentu potwierdzającego wsparcie producenta na terenie Polski (pkt 49 tabeli).

Jeżeli z dokumentów producenta nie wynika jednoznacznie spełnienie danego wymagania, Wykonawca może złożyć oświadczenie producenta lub jego autoryzowanego przedstawiciela.

4. Serwis producenta

4.1. Wykonawca zapewni serwis producenta systemu PAM dla obu instancji (IT i OT) przez okres 24 miesięcy, liczony od dnia podpisania protokołu odbioru licencji, obejmujący wsparcie producenta oraz dystrybutora i pobieranie aktualizacji przygotowanych przez producenta (pkt 10 tabeli).

4.2. W ramach serwisu Zamawiający otrzyma co najmniej dostęp do nowych wersji i aktualizacji oprogramowania, w tym poprawek bezpieczeństwa platformy wirtualnej, dostęp do bazy wiedzy i dokumentacji producenta oraz możliwość zgłaszania problemów. Dla instancji OT producent powinien udostępniać aktualizacje w postaci pakietów do instalacji w trybie offline.

4.3. Zgłoszenia przyjmowane są przez portal producenta lub dystrybutora, e-mailem lub telefonicznie, w języku polskim lub angielskim. Czas reakcji na zgłoszenie: nie dłuższy niż **16** godzin roboczych; dla zgłoszeń krytycznych (niedostępność systemu lub sejfu poświadczeń) – nie dłuższy niż **8** godzin.

5. Wdrożenie w sieciach IT i OT

5.2. Zasady wdrożenia w sieciach IT i OT

5.2.1. Wdrożenie obejmuje dwa niezależne środowiska: sieć IT oraz sieć OT Zamawiającego. W każdej z sieci Wykonawca wdroży odrębną instancję systemu PAM, zgodnie z pkt 2.5.

5.2.2. W trakcie prac Wykonawca nie może zestawiać połączeń między siecią IT a siecią OT, także tymczasowych, ani podłączać do sieci OT urządzeń lub nośników, które wcześniej były wykorzystywane w sieci IT, bez zgody Zamawiającego. Pakiety instalacyjne i aktualizacyjne dla instancji OT będą przenoszone w sposób uzgodniony z Zamawiającym, po weryfikacji ich integralności (suma kontrolna lub podpis producenta).

5.2.3. Instancja IT obejmie wyłącznie systemy docelowe w sieci IT, a instancja OT – wyłącznie systemy docelowe w sieci OT. Dostęp użytkowników do instancji OT będzie możliwy wyłącznie z wyznaczonego segmentu sieci OT (np. strefy zdemilitaryzowanej OT lub stanowisk inżynierskich).

5.2.4. W sieci OT Wykonawca zastosuje bezpieczną konfigurację, w szczególności:

- automatyczna zmiana haseł (pkt 36 tabeli) oraz poświadczenia typu JIT (pkt 14 tabeli) na stacjach HMI, serwerach SCADA, stacjach inżynierskich i urządzeniach sterowania zostaną włączone wyłącznie dla kont wskazanych przez Zamawiającego, po weryfikacji zależności (usługi, aplikacje, połączenia między systemami) i potwierdzeniu zgodności z zaleceniami dostawców systemów sterowania; dla pozostałych kont hasła będą wyłącznie przechowywane w sejfie, a ich zmiana będzie wykonywana ręcznie w oknach serwisowych;
- moduł automatycznego wyszukiwania urządzeń i moduł zadań automatycznych (pkt 12 tabeli) będą uruchamiane wyłącznie dla systemów wskazanych przez Zamawiającego i w uzgodnionych oknach serwisowych; aktywne skanowanie sterowników PLC i RTU jest niedopuszczalne;
- dostęp użytkowników zewnętrznych (pkt 15 tabeli) do systemów OT będzie wymagał akceptacji upoważnionej osoby Zamawiającego dla każdej sesji (pkt 26 tabeli), ograniczenia czasowego i rejestrowania sesji, a podgląd sesji w czasie rzeczywistym (pkt 38 tabeli) będzie dostępny dla dyżurnego operatora;
- zostanie skonfigurowany i przetestowany dostęp w przypadku awarii (pkt 26 lit. e–f tabeli) oraz procedura dostępu do systemów sterowania w przypadku niedostępności systemu PAM, w tym przechowywanie kopii poświadczeń awaryjnych w zabezpieczonej formie offline (np. zaplombowana koperta w sejfie fizycznym);

- audyt poleceń (pkt 41–42 tabeli) zostanie uruchomiony w pierwszej kolejności w trybie wyłącznie rejestrowania, a akcje blokowania poleceń, rozłączania sesji i automatycznego blokowania użytkowników – po akceptacji Zamawiającego;
- zostanie uzgodniona z Zamawiającym procedura użycia funkcji zawieszenia wszystkich sesji i zablokowania dostępu (pkt 40 tabeli).

5.2.5. Prace w sieci OT Wykonawca będzie prowadził wyłącznie w oknach serwisowych uzgodnionych z Zamawiającym, zgodnie z obowiązującymi u Zamawiającego procedurami bezpieczeństwa, w sposób niepowodujący przerw ani zakłóceń w procesie technologicznym. Objęcie zarządzaniem systemów w sieci OT poprzedzi instalacja pilotażowa na wskazanym przez Zamawiającego, ograniczonym zakresie systemów.

5.3. Zakres wdrożenia (odrębnie dla sieci IT i dla sieci OT)

5.3.1. Opracowanie harmonogramu wdrożenia systemu w obu sieciach.

5.3.2. Przeprowadzenie analizy przedwdrożeniowej (inwentaryzacja kont uprzywilejowanych, systemów docelowych, zależności i procesów dostępu) oraz opracowanie odrębnego projektu technicznego wdrożenia dla sieci IT i dla sieci OT, przedkładanego do akceptacji Zamawiającego. Prace instalacyjne mogą rozpocząć się po akceptacji projektu.

5.3.3. Instalacja i konfiguracja każdej z instancji w klastrze active-active z arbitrem (pkt 5–6 tabeli) w tym: utwardzenie konfiguracji (zmiana domyślnych haseł, ograniczenie dostępu do interfejsów zarządzania), konfiguracja kopii zapasowych, integracja z usługą katalogową jeśli występuje, uruchomienie uwierzytelniania dwuskładnikowego (pkt 21 tabeli), przekazywanie logów do systemu SIEM właściwego dla danej sieci oraz umieszczenie logo Zamawiającego. Dla instancji OT – konfiguracja pracy bez dostępu do Internetu.

5.3.4. Objęcie zarządzaniem systemów docelowych wskazanych przez Zamawiającego, w tym konfiguracja polityk dostępu, akceptacji, zakresów czasowych, rejestrowania sesji i parametrów nagrań (pkt 44 tabeli) oraz – w zakresie uzgodnionym z Zamawiającym – zmiany haseł.

5.3.5. Konfiguracja ról i grup dostępu, raportów i dostępu do raportów, zgodnie z macierzą uprawnień uzgodnioną z Zamawiającym na etapie analizy przedwdrożeniowej.

5.3.6. Przygotowanie i przeprowadzenie scenariuszy testowych w każdej z sieci. Proponowane scenariusze zostaną przedłożone Zamawiającemu do akceptacji i muszą obejmować co najmniej:

- zestawienie sesji przez proxy dla każdego typu systemu docelowego i każdego narzędzia dostępu, rejestrację, odtworzenie i pobranie nagrania (pkt 48 tabeli) oraz zablokowanie polecenia z czarnej listy;
- akceptację dostępu z podaniem powodu, dostęp w określonym zakresie czasu oraz dostęp w przypadku awarii;
- zmianę hasła dla każdego typu systemu objętego zmianą haseł, w tym automatyczną zmianę po podglądzie;
- przełączenie awaryjne węzłów klastra oraz odtworzenie systemu z kopii zapasowej;
- dla instancji OT – aktualizację w trybie offline;
- brak dostępu do interfejsów zarządzania spoza wyznaczonego segmentu oraz brak połączeń między instancjami IT i OT.

5.3.7. Przekazanie odrębnej dla sieci IT i dla sieci OT dokumentacji powykonawczej w języku polskim, obejmującej co najmniej opis architektury i konfiguracji, wykaz systemów docelowych i kont objętych zarządzaniem, macierz uprawnień i polityk dostępu, protokoły z testów oraz procedury administracyjne (aktualizacja – dla sieci OT również w trybie offline, kopia zapasowa i odtworzenie, dostęp awaryjny). Hasła zostaną przekazane w sposób uzgodniony z Zamawiającym, odrębnie od dokumentacji.

5.3.8. Przeprowadzenie instruktażu stanowiskowego dla administratorów Zamawiającego (co najmniej 2 osób, w wymiarze co najmniej 4 godzin), odrębnie dla instancji IT i OT, obejmującego obsługę i

administrowanie systemem, procedury dostępu awaryjnego, odtwarzania z kopii zapasowej i aktualizacji w trybie offline.

5.3.9. Osoby realizujące wdrożenie po stronie Wykonawcy przed przystąpieniem do prac podpiszą zobowiązanie do zachowania poufności informacji uzyskanych w trakcie realizacji zamówienia, w szczególności dotyczących architektury i zabezpieczeń sieci IT i OT. Wykonawca nie może zachować kopii poświadczeń uzyskanych w trakcie wdrożenia; po zakończeniu prac hasła kont użytych przez Wykonawcę zostaną zmienione. Jeżeli Wykonawca będzie miał dostęp do danych osobowych (np. w nagraniach sesji), strony zawrą umowę powierzenia przetwarzania danych osobowych.

5.3.10. Wykonawca udzieli gwarancji na prawidłowe działanie wykonanej konfiguracji na okres nie krótszy niż **24** miesięcy od dnia odbioru wdrożenia w danej sieci.

6. Terminy realizacji i odbiór

6.1. Termin dostawy licencji i aktywacji serwisu producenta: do **20** dni od dnia zawarcia umowy.

6.3. Odbiór licencji nastąpi na podstawie protokołu odbioru, po przekazaniu dokumentów licencyjnych dla obu instancji oraz potwierdzenia rejestracji serwisu producenta.

6.4. Odbiór wdrożenia nastąpi odrębnie dla sieci IT i dla sieci OT, na podstawie protokołów odbioru podpisanych po pozytywnym wyniku testów z pkt 5.3.6, przekazaniu dokumentacji z pkt 5.3.7 i przeprowadzeniu instruktażu z pkt 5.3.8. Po odbiorze wdrożenia w obu sieciach strony podpiszą protokół odbioru końcowego.

7. Rozwiązania równoważne

7.1. Wskazanie w OPZ nazw systemów, urządzeń, aplikacji i narzędzi, z którymi oferowany system musi współpracować (m.in. Hyper-V, VMware ESX/ESXi, Microsoft Windows, Microsoft Active Directory, Cisco, Aruba, Alcatel, Check Point, FortiGate, Huawei, IBM AIX, Brocade, Microsoft SQL Server, Oracle, MySQL, PostgreSQL, iLO, iDRAC, Facebook, Google, Twitter (X), LinkedIn, Instagram, OpenStack, AWS, Cassandra, Elasticsearch, MongoDB, Redis, Solr, Sybase, PuTTY, DBeaver, Docker, Google Authenticator, Microsoft Authenticator), wynika z infrastruktury i narzędzi wykorzystywanych przez Zamawiającego i nie stanowi wskazania oferowanego produktu.

7.2. Pozostałe nazwy własne, znaki towarowe lub normy wskazane w OPZ mają charakter przykładowy. Zamawiający dopuszcza rozwiązania równoważne, zgodnie z art. 99 ust. 5 i art. 101 ust. 4 ustawy Prawo zamówień publicznych. Wykonawca, który powołuje się na rozwiązanie równoważne, jest obowiązany wykazać, że oferowane rozwiązanie spełnia wymagania określone przez Zamawiającego.