Opis Przedmiotu Zamówienia

1. **Wykonawca zobowiązany jest do:**

1.1 dostarczenia 1 x FUDO PAM virtual appliance z licencjami niezbędnymi do uruchomienia;
1.2 przedłużenie gwarancji na posiadany sprzęt FUDO PAM nr ser. 10000284;
1.3 opracowanie projektu wdrożeniowego obejmującego instalację i konfigurację FUDO PAM oraz integrację z oprogramowaniem/sprzętem aktualnie działającym w środowisku Zamawiającego, uruchomienie i skonfigurowanie wszystkich wymaganych urządzeń i oprogramowania w oparciu o wstępny projekt wdrożeniowy oraz przygotowanie dokumentacji post-technicznej;
1.4 przeprowadzenia warsztatu dla pracowników w zakresie zarządzania, administrowania i działania w ramach dostarczonego rozwiązania;
1.5 zapewnienia pomocy technicznej eksperta;
1.6 udzielenia 24-miesięcznej gwarancji, zgodnie z którą Wykonawca musi zapewnić wsparcie techniczne i serwis dla dostarczonego i aktywnego produktu;
1.7 budowy klastra FUDO PAM virtual appliance z posiadanym urządzeniem FUDO PAM nr ser. 10000284;
1.8 dostarczenia FUDO PAM virtual appliance dla odrębnej infrastruktury;
1.9 dostarczenie licencji minimum:
- Fudo 200 x Support – Standard,
- Fudo 200x Non-refundable HD per Appliance,
- Licence Support – Standard.

2. **Rozwiązanie do zarządzania dostępem uprzywilejowanym lub równoważne spełniające określone wymagania.**

2.1 Maszyny wirtualne - rozwiązanie, które powinno obejmować oprogramowanie działające na maszynach wirtualnych. Zamawiający zapewni zasoby niezbędne do uruchomienia maszyn wirtualnych.
2.2 Rozwiązanie All-In-One - nie wymaga integracji z żadnym z istniejących elementów infrastruktury sieciowej (nie obejmuje implementacji w warstwach 2 i 3 modelu OSI) ani zakupu dodatkowych licencji.
2.3 Rozwiązanie umożliwia rejestrację i zarządzanie procesem dostępu uprzywilejowanego za pomocą protokołów opisanych poniżej, do nieograniczonej liczby serwerów, gdzie serwer rozumiany jest jako unikalny adres IP z określonym protokołem komunikacyjnym.
2.4 Rozwiązanie składa się z co najmniej następujących modułów:
2.4.1 Moduł zarządzania sesjami uprzywilejowanymi i rejestracji - funkcjonalność Manager Sesji;
2.4.2 Moduł zarządzania hasłami dla kont na zdefiniowanych serwerach - min. dla systemów Windows, Windows Server i Unix (Linux Red Hat, Linux Suse, Linux Debian, Linux Ubuntu, FreeBSD 10+) oraz urządzeń sieciowych Cisco i baz danych MySQL - funkcjonalność Managera Haseł;
2.4.3 Moduł do raportowania aktywności i przeglądu wydajności w ramach zarejestrowanych sesji;
2.4.4 Moduł do zarządzania i przekazywania haseł do aplikacji - Funkcjonalność Application to Application Password Management (AAPM).

3. **Szczegółowy opis wymienionych modułów (w tym AAPM)**

3.1 Rozwiązanie nie powinno wymagać instalacji dodatkowego oprogramowania (agentów) ani na monitorowanych serwerach, ani na stacjach klienckich, z których będą wykonywane połączenia.
3.2 Rozwiązanie powinno posiadać mechanizmy analizy behawioralnej, które będą automatycznie wykrywać anomalie w sesjach uprzywilejowanych, zbudowane na podstawie zachowań użytkowników i indywidualnych wzorców składniowych.
3.3 Rozwiązanie pozwala na monitorowanie i rejestrację następujących protokołów:
3.3.1 dla protokołów graficznych:
a) RDP - w tym sesje wielomonitorowe;
b) VNC;
3.3.2 dla protokołów tekstowych:
a) SSH (w tym funkcja Proxy Jump);
b) Telnet - podwójne uwierzytelnianie dozwolone (ograniczenie protokołu);

3.3.3 w ramach aplikacji:
a) HTTP / HTTPS;
b) MySQL,
c) MS SQL i inne oparte na złączu TDS;
3.3.4 inny:
a) systemy automatyki przemysłowej (SCADA) - min. protokół MODBUS;
b) żądany protokół TCP - dozwolona jest tylko rejestracja sesji w formacie PCAP;
c) protokoły HTTP / HTTPS.

3.4 W zakresie protokołu RDP rozwiązanie musi wspierać połączenie z wykorzystaniem:
3.4.1 sesje z szyfrowania TLS;
3.4.2 sesje TLS z uwierzytelnianiem NLA;
3.4.3 sesje nieszyfrowane;
3.4.4 za pomocą wbudowanego klienta (z poziomu przeglądarki internetowej).

3.5 W zakresie protokołu SSH rozwiązanie musi oferować:
3.5.1 obsługę podsystemu SFTP - przeglądanie i pobieranie przesyłanych plików;
3.5.2 obsługę tuneli X11;
3.5.3 obsługę przekazywania tunelu agenta SSH;
3.5.4 za pomocą wbudowanego klienta (z poziomu przeglądarki internetowej).

3.6 W odniesieniu do protokołu HTTP / HTTP, wymagana jest pełna graficzna reprezentacja sesji, czyli rejestracja wszystkich elementów na stronie internetowej wraz z możliwością odtworzenia sesji w formie filmu, przedstawiającego prawdziwą stronę internetową (bez konieczności korzystania z dodatkowej stacji przesiadkowej).

3.7 Rozwiązanie musi umożliwiać zainicjowanie sesji na dwa sposoby; poprzez wywołanie połączenia z poziomu aplikacji natywnej za pośrednictwem określonego protokołu oraz z poziomu przeglądarki internetowej, bezpośrednio poprzez stronę internetową. uruchamiając nowe połączenie z danym protokołem – przynajmniej dla protokołów RDP (rdp: //) i SSH (ssh://):
3.7.1 funkcja uruchamiania sesji za pośrednictwem przeglądarki internetowej musi być dostępna tylko dla użytkowników, którzy zostali odpowiednio uwierzytelnieni przed wejściem na stronę główną, z której będzie prowadzone połączenie. Wspomniane uwierzytelnianie musi być również możliwe dla użytkowników zdefiniowanych w katalogu zewnętrznym - co najmniej Active Directory, LDAP i Radius.

3.8 Rozwiązanie pozwala na przeglądanie i zarządzanie sesjami na żywo m.in.: wszystkimi niedokończonymi sesjami:
3.8.1 w ramach procedury, wyznaczony użytkownik musi mieć możliwość dołączenia do sesji - przynajmniej w przypadku protokołów RDP, VNC, SSH i telnet – w celu dokonania przeglądu bieżących działań;
3.8.2 w rozwiązaniu musi istnieć możliwość łatwego zidentyfikowania, podmiotu aktualnie wykonującego akcje tzn.: wpisywanie znaków na klawiaturze lub używanie przycisku myszy - użytkownik inicjujący sesję lub operator dołączający do sesji;
3.8.3 w rozwiązaniu musi istnieć możliwość podglądu wprowadzonych kodów/znaków wysyłanych w ramach sesji, przy czym włączenie tej funkcji nie może być możliwe bez zgody min. dwóch operatorów (użytkowników z wyższymi uprawnieniami/rolą niż zwykły użytkownik);
3.8.4 operator przeglądający sesje na żywo, musi mieć możliwość natychmiastowego odłączenia tejże sesji i zablokowania użytkownika (poza statusem użytkownika wynikającym z synchronizacji z zasobami zewnętrznymi);
3.8.5 operator oglądający sesję na żywo musi być w stanie zatrzymać sesję bez potrzeby odłączenia użytkownik oraz wznowienie sesji w dowolnym momencie.

3.9 Administracja, monitorowanie, weryfikacja i podgląd zapisanych sesji wewnątrz rozwiązania odbywa się za pośrednictwem przeglądarki internetowej.

3.10 Podgląd monitorowanych sesji, zarówno na żywo, jak i nagranych wcześniej, nie wymaga instalowania dodatkowego oprogramowania (dotyczy również wtyczek do przeglądarek, np. Flash).

3.11 W rozwiązaniu analiza i rejestracja sesji dla wyżej wymienionych protokołów będzie odbywać się wyłącznie na samym urządzeniu.

3.12 Funkcja monitorowania sesji zapewniona przez rozwiązanie musi umożliwiać operatorowi uzyskanie informacji co najmniej o następujących zdarzeniach:
- 3.12.1 rozpoczęcie sesji;
- 3.12.2 zakończenie sesji;
- 3.12.3 dołączenie do operatora lub osoby z zaproszeniem na sesję;
- 3.12.4 odłączenie takiego operatora lub uczestników zewnętrznych/wewnętrznych.

3.13 Wyżej wymieniona funkcja musi być zaimplementowana co najmniej przy użyciu protokołu syslog i za pośrednictwem poczty elektronicznej.

3.14 Rozwiązanie musi być w stanie zainicjować sesję za pomocą powiadomień z dokładnym powodem, powinno również zachować wprowadzony tekst w wewnątrz metadanych sesji:
- 3.14.1 dane wejściowe muszą być zaimplementowane przed ustanowieniem sesji z serwerem docelowym (systemem);
- 3.14.2 wprowadzanie danych wejściowych musi być wykonywane, co najmniej dla protokołów:
  - a) RDP;
  - b) VNC;
  - c) Protokół SSH;
  - d) telnet.

3.15 Rozwiązanie pozwala kontrolować i ustawiać ograniczenia nad właściwościami sesji przy użyciu określonych protokołów:
- 3.15.1 dla protokołu RDP minimum:
  - a) ograniczenie maksymalnej rozdzielczości ekranu sesji;
  - b) ograniczenie głębi kolorów, min. do 8 i 16 bpp;
  - c) blokowanie funkcji schowka.

3.16 Dla protokołu SSH minimum:
- a) blokowanie przekierowania portów;
- b) blokowanie tunelu X11;
- c) blokowanie przekazywania agentów SSH;
- d) blokowanie podsystemu SFTP i przesyłanie plików za pomocą SCP.

3.17 Rozwiązanie zapewnia możliwość uwierzytelniania poprzez serwery zewnętrzne: Active Directory, Radius, LDAP (w tym OpenLDAP).

3.18 Rozwiązanie pozwala na pełną synchronizację użytkowników z Active Directory, w tym:
- a) wybrane grupy w domenie Active Directory;
- b) dana organizacja lub dane (OU);
- c) kilka domen Active Directory - również wtedy, gdy "nazwa użytkownika" jest duplikowana w dwóch domenach lub więcej;
- d) użytkownicy i grupy są wyodrębnione przy pomocy zdefiniowanych filtrami.

3.19 Rozwiązanie rejestruje cały ruch sieciowy w odniesieniu do danej sesji (rejestracja protokołu raw).

3.20 Rozwiązanie pozwala na selektywne wskazywanie systemów, dla których nagrywanie sesji zostało pierwotnie włączone.

3.21 Rozwiązanie umożliwia użytkownikowi zastąpienie loginu i hasła innym poświadczeniami określonymi na serwerze docelowym.

3.22 Dla sesji graficznych rozwiązanie pozwala na uruchomienie spersonalizowanego ekranu logowania przed nawiązaniem połączenia z docelowym serwerem (systemem).

3.23 W przypadku sesji graficznych i tekstowych (przynajmniej dla protokołów SSH i telnet) rozwiązanie musi umożliwiać połączenie z serwerem (systemem) bez znajomości nazwy domeny (FQHN), bądź też adresu IP serwera (systemu), a jedynie nazwy zdefiniowanej przez operatora; przekazywanie tych informacji może odbywać się np. w formacie "user # servername", jak również za pośrednictwem wyboru danego elementu z listy lub menu rozwijanego.

3.24 Rozwiązanie ma możliwość wyegzekwowania zgody operatora przed ustanowieniem sesji.

3.25 Rozwiązanie musi współpracować z systemami klasy SIEM - przynajmniej przy użyciu protokołu syslog.

3.26 Rozwiązanie posiada zaimplementowane rozszerzone oznaczanie powiadomień wewnętrznych wysyłanych bezpośrednio do SIEM (tagowanie), pozwalające na ustawienie odpowiednich kategorii logów/zdarzeń w takim systemie – niedopuszczalna jest konieczność wyszukiwania komunikatów dziennika zdarzeń według słów kluczowych w celu ich kategoryzacji.

3.27 Rozwiązanie pozwala na zdefiniowanie konkretnego dostępu do puli niezbędnych adresów IP wraz z podsieciami (np. maska/24) - przynajmniej dla protokołów RDP, VNC, SSH i telnet

3.28 Dla protokołu RDP - rozwiązanie musi umożliwiać dostęp do podsieci systemów VDI. wykorzystując np. Connection Broker, bez konieczności definiowania każdego systemu VDI osobno.

3.29 Rozwiązanie umożliwia umieszczanie komentarzy do oglądanych sesji – w trybie live, ostatnio utworzonych i wcześniej zapisanych nagrań – podczas odtwarzania.

3.30 Rozwiązanie umożliwia automatyczne zakończenie sesji po wykryciu predefiniowanego ciągu znaków oraz generowanie notyfikacji do administratora.

3.31 Rozwiązanie umożliwia dodatkowe zatwierdzenie połączenia uprzywilejowanego przez przełożonego (stronę trzecią) po prawidłowym uwierzytelnieniu użytkownika.

3.32 Akceptacja i/lub odrzucenie sesji uprzywilejowanej przez przełożonego (funkcja wymaga zatwierdzania w ramach Bezpiecznej konfiguracji) jest również możliwa za pomocą dedykowanej aplikacji dostępnej na urządzenia mobilne.

3.33 Rozwiązanie umożliwia funkcję Just-in-Time (JIT) - dostęp do zasobów poprzez żądania, gdzie system rozróżnia dwa typy zapytań dostępnych dla użytkownika:

- 3.33.1 natychmiastowe - żądania można ustawić od teraz i będzie ono aktywne przez np.: następne 2, 4, 6, 12 lub 24 godziny;
- 3.33.2 zaplanowane - użytkownik wybiera datę rozpoczęcia i datę zakończenia, co oznacza, że dostęp zostanie przyznany na cały okres od daty rozpoczęcia do daty zakończenia.

3.34 Rozwiązaniem posiada funkcje przeszukiwania (skanowanie) kontrolerów domeny w celu wyodrębnienia kont o różnych poziomach uprawnień (automatyczne wykrywanie) i dodanie ich do odpowiednich sejfów i/lub gniazd zasłuchiwania.

3.35 Funkcja automatycznego wykrywania (odnajdowania) wykonuje skanowanie Active Directory tylko przy użyciu połączenia LDAP i obsługuje ją w dwóch trybach:

- 3.35.1 wdrażanie (onboarding) – proces, podczas którego rozwiązaniem będzie udzielanie odkrytym kontom dostępu do połączeń;
- 3.35.2 kwarantanna - funkcja może wysłać niezaufane konta do kwarantanny i zablokować je na serwerze docelowym.

3.36 Rozwiązanie umożliwia wyszukiwanie sesji w trybie pełno tekstowym.

3.37 Wyszukiwanie musi być możliwe w równym stopniu dla kanału wejściowego (np. wpisywanych poleceń) jak również dla danych wyjściowych pojawiających się na ekranie trawiącej sesji.

3.38 Powyższe zapisy dotyczą w równym stopniu sesji graficznych dla protokołów RDP i VNC, i określaj całość treści pojawiających się na ekranie.

3.39 Możliwość wyszukiwania musi być natychmiastowa, z wyjątkiem sesji graficznych, w których można wykorzystać silnik indeksujący OCR.

3.40 Mechanizm OCR musi być zaimplementowany co najmniej dla sesji HTTP/HTTPS (zarówno dla formy tekstowej, jak i graficznej), VNC i RDP poprzez rozpoznawanie i zapisywanie we wszystkich znakach i tekstach, które były wyświetlane w ramach sesji w głównej bazie danych; dotyczy to zarówno tekstów (poleceń) wprowadzanych na klawiaturze, jak i znaków/fraz, które pojawiły się w dowolnym miejscu na ekranie sesji graficznej (okna aplikacji, dane edytowanych dokumentów, "wyskakujące" okna powiadomień, nazwy plików itp.).

3.41 Przygotowanie sesji do weryfikacji musi odbywać się wewnętrznie, tzn. dane nie mogą być przesyłane do chmury lub innego dedykowanego urządzenia.

3.42 Funkcja wyszukiwania musi być wyłączona co najmniej na poziomie określonego użytkownika na serwerze.

3.43 Rozwiązanie pozwala na przyznanie czasowego dostępu do pojedynczej sesji – zarówno w zakresie zakończonej i zapisanej, jak i niedokończonej ("live"):

- 3.43.1 w ramach sesji niedokończonej ("live"), operator musi mieć możliwość określenia, czy sesja ma być udostępniana tylko w trybie podglądu, czy też z opcją dołączenia/udostępnienia sesji uczestnikom zewnętrznym;
- 3.43.2 musi istnieć możliwość cofnięcia udzielonego dostępu do wspólnej sesji w dowolnym momencie.

3.44 Rozwiązaniem posiada możliwość monitorowania, raportowania i analizowania aktywności/efektywności użytkowników podczas sesji, z uwzględnieniem modułu analizy biznesowej:

3.44.1 analiza sesji powinna szczegółowo przedstawiać, w jaki sposób produktywność użytkowników / organizacji rozwijała się w każdym okresie;
3.44.2 konfigurowalny parametr definiujący próg aktywności powinien pozwolić na szybką identyfikację sesji, użytkowników lub organizacji, które nie przekroczyły wymaganego poziomu aktywności, a także wspomóc proces wskazywania wartości progowej, przy której dana liczba użytkowników lub sesji osiąga wymagany poziom aktywności;
3.44.3 musi istnieć możliwość określenia aktywności sesji w skali 0% -100%, wynikającej z liczby zarejestrowanych zdarzeń wejściowych (wysłany kod klucza, a dla sesji graficznych każde użycie mysz; ruch i kliknięcia przycisków funkcyjnych - jeśli dla danego protokołu rejestracja takich elementów została aktywowana);
3.44.4 komponent analizy produktywności powinien umożliwiać porównywanie aktywności organizacji lub użytkowników w określonych odstępach czasu.

3.45 Rozwiązanie musi być w stanie zdefiniować hierarchię użytkowników i operatorów, przynajmniej pod względem:
3.45.1 konto regularnego dla użytkownika;
3.45.2 konta operatora z dostępem do standardowego trybu podglądu;
3.45.3 konta operatora z trybem przeglądu konfiguracji;
3.45.4 konta operatora z możliwością dostosowania konfiguracji;
3.45.5 konta operatora z możliwością zarządzania systemem (np. restart urządzenia).

3.46 Rozwiązanie musi być w stanie zdefiniować dostęp dla operatora co najmniej do:
3.46.1 wskazanych serwerów (systemy) oraz zapisanych i trwających sesji;
3.46.2 wyznaczonych użytkowników wraz z zapisanymi i trwającymi sesjami.

3.47 Rozwiązanie musi umożliwiać nałożenie znaczników czasu na nagrane sesje przez uprawnione podmioty (przynajmniej przez KIR i PWPW).

3.48 Rozwiązanie musi mieć opcję zdefiniowania polityki sesji/przechowywania danych, czyli określenia okresu, po którym sesje zostaną usunięte z urządzenia:
3.48.1 musi istnieć możliwość zdefiniowania różnych czynników przechowywania sesji/danych.

3.49 Rozwiązanie musi posiadać możliwość integracji z zewnętrznym repozytorium haseł firmowych:
3.49.1 CyberArk;
3.49.2 Thycotic;
3.49.3 LAPS.

3.50 Rozwiązanie musi posiadać funkcjonalność sprawdzania hasła.

3.51 Rozwiązanie musi być zintegrowane ze standardem uwierzytelniania opisanym w RFC 6287 (OATH).

3.52 Rozwiązanie musi umożliwiać zdefiniowanie zestawu poleceń lub ciągów znaków, które (wprowadzone podczas sesji lub występujące w treści sesji) wywołają akcję zdefiniowaną przez operatora, co najmniej jako:
3.52.1 informacje wysyłane za pomocą protokołu syslog;
3.52.2 informacje przesyłane do systemu SIEM;
3.52.3 notyfikacja operatora za pośrednictwem poczty elektronicznej;
3.52.4 natychmiastowe zakończenie aktywnej sesji z dodatkową opcją automatycznego blokowania podejrzanego użytkownika, niezależnie od stanu użytkownika wynikającego z synchronizacji z zasobami zewnętrznymi;
3.52.5 zatrzymanie trwającej sesji.

3.53 Zestaw poleceń lub ciągów wspomnianych powyżej musi być możliwy do zdefiniowania za pomocą mechanizmu wyrażeń regularnych (regexp), mechanizm symboli wieloznacznych nie będzie uważany za równoważny.

3.54 Wyżej opisana funkcjonalność musi być możliwa do osiągnięcia przynajmniej dla protokołów:
3.54.1 RDP;
3.54.2 VNC;
3.54.3 Protokół SSH;
3.54.4 Telnet.

3.55 Wymienione funkcje powinny rozpoznawać polecenia lub ciągi znaków w następujących przypadkach:

3.55.1 poprawne egzekwowanie reguły co najmniej dla protokołów VNC, RDP – w zakresie danych wejściowych i danych sesji dostępnych po indeksowaniu po zakończeniu sesji;
3.55.2 dla innych protokołów - podczas trwającej sesji, natychmiast po rozpoznaniu danego ciągu znaków, identycznie dla danych wejściowych i wyjściowych pojawiających się na ekranie sesji;
3.55.3 konfigurowanie ograniczenia tylko dla danych wejściowych/wyjściowych, które pojawiają się na ekranie nawiązanej sesji.

3.56 Rozwiązanie musi posiadać opcję zapisu sesji w formie nagrania wideo (zapis liniowy) w formacie umożliwiającym odtworzenie nagrania przy użyciu programu VLC 3.0 lub wersji najnowszej:
3.56.1 taki zapis musi być możliwy dla protokołów graficznych (co najmniej VNC i RDP) i tekstowych (co najmniej SSH i telnet).

3.57 Zarządzanie skryptami rozwiązania dla udokumentowanego API musi mieć opcję co najmniej:
3.57.1 tworzenia, modyfikowania i usuwanie kont użytkowników;
3.57.2 tworzenia, modyfikowania i usuwanie serwerów (systemów docelowych);
3.57.3 tworzenia, modyfikowania i usuwanie dostępu do serwerów (systemów) – w odniesieniu do kont;
3.57.4 tworzenia, modyfikowania i usuwanie adresów IP i portów, z którymi użytkownicy będą się łączyć;
3.57.5 tworzenia, modyfikowania i usuwanie relacji między kontami, serwerami, czy poszczególnymi dostępami;
3.57.6 pobieranie listy sesji - z możliwością wyróżnienia sesji, które nie zostały jeszcze zakończone;
3.57.7 blokowanie użytkownika - niezależnie od stanu synchronizacji użytkownika pod kątem zasobów zewnętrznych.

3.58 Rozwiązanie musi pozwalać na odzyskiwanie systemu co najmniej do poprzedniej wersji po wadliwej aktualizacji.

3.59 Funkcja ta musi być dostępna bezpośrednio z poziomu interfejsu zarządzania, bez konieczności korzystania z wiersza poleceń lub dedykowanej konsoli zarządzania (terminala).

4. Szczegółowa specyfikacja modułu zarządzania hasłami

4.1 Rozwiązanie musi obsługiwać funkcję zmiany haseł w systemach Unix przy użyciu uprzywilejowanego konta z dostępem za pomocą klucza SSH.

4.2 Rozwiązanie umożliwia definiowanie sekwencji poleceń wyzwalających modyfikację hasła.

4.3 Rozwiązanie umożliwia weryfikację czy hasło nie zostało zmienione w sposób nieautoryzowany.

4.4 Rozwiązanie przechowuje historię hasła do konta i ma możliwość odzyskania wybranego hasła.

4.5 Rozwiązanie pozwala zdefiniować złożoność automatycznie generowanych haseł.

5. Specyfikacja modułu zarządzania hasłami i mechanizmu przekazywania

5.1 Rozwiązanie zapewnia bezpieczną wymianę haseł pomiędzy aplikacjami - funkcjonalność AAPM.

5.2 Autoryzacja dostępu do danych w systemie AAPM powinna opierać się na adresie IP oraz jednorazowym lub statycznym haśle.

5.3 Moduł musi współpracować przynajmniej z oprogramowaniem, które działa pod kontrolą systemu operacyjnego:
a) Windows Server 2012 lub nowszy;
b) Linux - Red Hat 6 lub nowszy (lub równoważna, ale nie starsza, inna dystrybucja);
c) FreeBSD 10 lub nowszy.

6. Specyfikacja techniczna

6.1 Rozwiązanie zapewnia kryptograficzną ochronę wszystkich zapisanych danych (szyfrowanie i integralność) na poziomie bezpieczeństwa nie niższym niż poziom gwarantowany przez kod AES 256:

6.1.1 dostawca/producent rozwiązania nie powinien mieć możliwości odszyfrowania jakichkolwiek danych przechowywanych na urządzeniu bez dostępu do oryginalnych kluczy szyfrujących (brak kluczy serwisowych);

6.1.2 kryptograficzna ochrona przechowywanych danych musi być realizowana co najmniej na poziomie bazy danych (dane są szyfrowane wewnątrz bazy), a także na poziomie nośnika, na którym działa system (szyfrowanie całego systemu plików, również dla instalacji wirtualnej), a funkcja szyfrowania nośników musi być integralną częścią rozwiązania.

6.2 Rozwiązanie posiada możliwość konfiguracji klastra:

6.2.1 minimalna liczba węzłów w klastrze: 2;

6.2.2 musi istnieć możliwość świadczenia usług w trybie wysokiej dostępności przy użyciu wirtualnego ("pływającego") adresu IP.

6.3 Rozwiązanie nie może pracować w trybie "hot standby", tzn. wszystkie węzły klastra muszą aktywnie uczestniczyć we wdrażaniu funkcjonalności rozwiązania, zgodnie ze zdefiniowaną polityką, np.: musi istnieć możliwość określenia, który węzeł klastra będzie obsługiwał dany zestaw sesji.

6.4 Musi istnieć możliwość ręcznej zmiany roli węzła w klastrze, np. przeniesienia funkcjonalności z węzła, który ma zostać przeniesiony lub modyfikacja węzła w obrębie instancji.

6.5 Rozwiązanie posiada zarezerwowaną przestrzeń dyskową na dane (użytkową) pozwalającą na rejestrację i przechowywanie zebranych danych (monitorowanych sesji) przez minimalny okres (ustalony osobno dla każdej pojemności pamięci urządzenia) – 180 dni dla sesji RDP, przy założeniu przechowywania minimum 50 sesji RDP dziennie, gdzie jedna sesja trwa średnio 8 godzin. a szacowany rozmiar pojedynczej sesji jest równy, średnio 300 MB.

6.6 Rozwiązanie musi dysponować wystarczającą ilością pamięci masowej, która pozwoli na jednoczesną rejestrację do min. 100 sesji tekstowych (dla protokołów SSH, telnet) lub min. 30 sesji (dla protokołów RDP, VNC) - liczonych dla pojedynczego urządzenia lub dla klastra z tylko jednym aktywnym węzłem.

6.7 Urządzenie musi pracować w następującym trybie:

6.7.1 serwer, do transmisji (warstwa 5+ modelu OSI);

6.7.2 aplikacja - nasłuchiwanie na wskazanym adresie IP/adresach i portach;

6.7.3 tryb routera (brama, warstwa 3 modelu OSI) - wysyłanie pakietów/ruchu tylko do zdefiniowanych serwerów (systemów) pomiędzy dwoma segmentami sieci IP;

6.7.4 tryb mostka (warstwa 2 modelu OSI) - wysyłanie całego ruchu sieciowego między dwoma punktami końcowymi w ramach zwykłego połączenia Ethernet, ale nie może zakłócać pakietów, które nie są częścią ruchu sieciowego należącego do sesji i będących w równym stopniu obsługiwanymi przez urządzenie.

6.8 Rozwiązanie musi umożliwiać zdefiniowanie własnego certyfikatu/klucza dla połączeń szyfrowanych (dla protokołów RDP i SSH) oraz przeniesienie istniejących certyfikatów/klucza z serwera (systemu), do którego zdefiniowany jest dostęp - obsługa fraz szyfrujących certyfikat/klucz.

6.9 Rozwiązanie musi umożliwiać weryfikację certyfikatu/klucza serwera (systemu), do którego zdefiniowany jest dostęp – przynajmniej dla protokołów RDP i SSH:

6.9.1 w przypadku protokołu RDP musi istnieć możliwość weryfikacji certyfikatu serwera docelowego (systemu) na podstawie zdefiniowanego początkowo certyfikatu CA (zaimportowanego).

6.10 Rozwiązanie obsługuje pakiety oznaczone zgodnie ze standardem 801.1q (VLAN).

6.11 Rozwiązanie obsługuje agregację 802.3ad (LACP) dla każdego typu interfejsu sieciowego - tj. zarówno dla interfejsów używanych do nasłuchiwania, interfejsu przesyłania danych (interfejsów), jak i interfejsu zarządzania.

6.12 Rozwiązanie musi mieć możliwość monitorowania wybranych parametrów pracy za pomocą protokołu SNMP, wersja min. v3.

6.13 Rozwiązanie musi umożliwiać podstawową diagnostykę sieci:

6.14 Potwierdzenie komunikacji za pomocą sygnalizacji ICMP (ping):

6.14.1 potwierdzenie komunikacji za pomocą połączenia TCP (połączenie z dowolnym portem o dowolnym adresie IP).

6.15 Rozwiązanie musi współpracować z następującymi usługami sieciowymi:

6.15.1 NTP;
6.15.2 serwer nazw (DNS).

6.16 Rozwiązanie obsługuje polską klawiaturę (programistę).

6.17 Rozwiązanie posiada dokumentację oraz interfejs użytkownika w języku polskim i angielskim.

6.18 Rozwiązanie posiada wsparcie techniczne w języku polskim i angielskim.

7. Specyfikacja obsługi rozwiązania

7.1 Wsparcie dla rozwiązania musi być aktywne - tj. w ciągu ostatnich 2 kwartałów od daty końcowego wdrożenia, rozwiązanie otrzymało min. 3 aktualizacje (pakiety takie jak: aktualizacja wersji głównej, wydanie pomocnicze, poprawki błędów, hot patche).

7.2 Rozwiązanie musi zawierać wszystkie niezbędne licencje do uruchomienia powyższych funkcjonalności, w tym licencje systemu operacyjnego - jeśli są niezbędne do jego uruchomienia.

8. Specyfikacja maszyny wirtualnej

8.1 Rozwiązanie musi działać co najmniej na następujących platformach wirtualizacji:

a) VMware 7.x;
b) VMware 8.x;
c) KVM / OpenStack / Proxmox lub jakikolwiek inny oparty na KVM lub qemu hypervisor.

9. W ramach przedmiotowego postepowania wymagane jest dostarczenie Zamawiającemu licencji wieczystych realizujących wszystkie funkcjonalności systemu dla minimum 200 urządzeń aktywnych (serwerów) Zamawiającego.

10. Do oferowanych licencji oprogramowania należy zapewnić 2 letnie (24 miesięcy) wsparcie techniczne (Support) producenta.