OPIS PRZEDMIOTU ZAMÓWIENIA

I Przedmiot zamówienia obejmuje:

1. dostarczenie systemu do rejestracji sesji zdalnych, zwanego dalej „Systemem" wraz ze sprzętem niezbędnym do prawidłowego działania Systemu zwanym dalej „Sprzętem" zgodnie z opisem przedmiotu zamówienia i przeniesie na rzecz Zamawiającego własności Sprzętu wraz z oprogramowaniem oraz udzielenie lub zapewnienie udzielenia licencji do oprogramowania niezbędnego do prawidłowego działania Systemu,
2. opracowanie projektu wdrożeniowego obejmującego instalację i konfigurację Systemu oraz integrację z systemami obecnie funkcjonującymi u Zamawiającego,
3. uruchomienie i dokonanie konfiguracji Sprzętu i oprogramowania w oparciu o założenia projektu wdrożeniowego w 10 lokalizacjach Zamawiającego,
4. przeprowadzenie instruktażu stanowiskowego w każdej z 10 lokalizacji dla minimum 3 pracowników Zamawiającego z zakresu funkcjonowania dostarczonego Systemu i administrowania nim,
5. udzielenie 36-miesięcznej gwarancji, w ramach której zostanie zapewniona opieka serwisowa dla dostarczonego i uruchomionego Systemu wraz ze Sprzętem niezbędnym do prawidłowego działania Systemu,
6. wykonanie dokumentacji powykonawczej,
7. zapewnienie 500 roboczogodzin asysty technicznej eksperta.

II System musi posiadać następujące cechy, parametry i funkcjonalności dla każdej lokalizacji:

1. System musi zapewniać wysoką dostępność i niezawodność (tzw. HA – ang. High Availability) poprzez zastosowanie wdrożenia klastrowego, łącznie z wszystkimi jego składnikami sprzętowymi, programowymi i licencyjnymi. W każdej z 10 lokalizacji wymagany jest dwuczłonowy klaster z automatycznym przełączeniem urządzeń w przypadku awarii jednego z nich. W takim przypadku Zamawiający dopuszcza możliwość zerwania sesji zdalnych trwających w czasie wystąpienia awarii.

2. rozwiązanie nie powinno wymagać instalowania dodatkowego oprogramowania (agentów) ani na monitorowanych serwerach ani na stacjach klienckich, z których wykonywane są połączenia

3. rozwiązanie powinno posiadać mechanizmy analityki behawioralnej, która automatycznie wykrywa anomalie w sesjach uprzywilejowanych bazując na wzorcach budowanych na podstawie zachowań użytkowników

4. rozwiązanie pozwala na monitorowanie i rejestrację protokołów:
    a. graficznych:
        i. RDP – włączając w to sesje wielomonitorowe
        ii. ICA / StoreFront (Citrix)
        iii. VNC
    b. tekstowych:
        i. SSH
        ii. telnet – dopuszcza się konieczność podwójnego uwierzytelnienia (ograniczenie protokołu)
    c. aplikacyjnych:
        i. HTTP/HTTPS
        ii. MySQL
        iii. MS SQL i innych, opartych o konektor TDS
        iv. Oracle – może być realizowane przez tzw. RemoteApp

d. innych:
    i. systemy automatyki przemysłowej (SCADA) – min. protokół MODBUS
    ii. dowolnego protokołu TCP – dopuszcza się wyłącznie rejestrację sesji w formacie PCAP
    iii. protokołów HTTP/HTTPS

5. w zakresie obsługi protokołu RDP rozwiązanie musi umożliwić połączenie z wykorzystaniem:
a) sesji szyfrowania TLS
b) sesji szyfrowania TLS z uwierzytelnieniem NLA
c) sesji nieszyfrowanej

2) w zakresie obsługi protokołu SSH rozwiązanie musi oferować:
a) obsługę podsystemu SFTP – przegląd i pobieranie przesłanych plików
b) obsługę tunelu X11

3) W zakresie sesji HTTP/HTTPs wymagana jest, graficzna reprezentacja sesji WWW, czyli zarejestrowanie wszystkich elementów występujących na stronie wraz z możliwością odtworzenia sesji przedstawiającą rzeczywistą stronę WWW.

4) rozwiązanie musi umożliwiać rozpoczęcie sesji zarówno przez wywołanie połączenia z poziomu aplikacji realizującej dany protokół jak i z poziomu przeglądarki internetowej, poprzez stronę uruchomienie połączenia z danym protokołem za pomocą aplikacji wspomagającej obsługującej dany protokół – przynajmniej dla protokołów RDP (rdp://) i SSH (ssh://)
a) funkcja rozpoczęcia sesji poprzez przeglądarkę internetową musi być dostępna tylko dla użytkowników, który przed tym poprawnie się uwierzytelnioną
b) powyższe uwierzytelnienie musi być możliwe także dla użytkowników zdefiniowanych w zewnętrznym katalogu – przynajmniej Active Directory, LDAP i Radius

5) rozwiązanie umożliwia podgląd i zarządzanie sesjami “na żywo”, tzn. niezakończonymi:
a) w ramach tego podglądu musi być możliwość dołączenia do sesji – przynajmniej dla protokołów RDP, VNC, SSH i telnet
b) musi istnieć możliwość łatwej identyfikacji kto wprowadził dany znak lub wywołał kliknięcie myszy – użytkownik inicjujący sesję lub operator dołączający do sesji
c) musi być możliwość podglądu wprowadzanych kodów znakowych przesyłanych w sesji, przy czym włączenie tej funkcji nie może być możliwe bez zgody min. dwóch operatorów (użytkowników urządzenia o wyższych uprawnieniach niż zwykły użytkownik)
d) operator przeglądający sesję “na żywo” musi mieć możliwość natychmiastowego rozłączenia sesji i blokowania użytkownika (niezależnie od stanu użytkownika wynikającego z synchronizacji z zewnętrznymi zbiorami użytkowników)
e) operator przeglądający sesję “na żywo” musi mieć możliwość zatrzymania sesji bez jej rozłączania i wznowienia jej w dowolnym momencie

6) administracja, monitorowanie oraz podgląd zapisanych w rozwiązaniu sesji odbywa się poprzez przeglądarkę WWW

7) podgląd monitorowanych sesji, zarówno “na żywo” jak i wcześniej nagranych, nie wymaga instalowania dodatkowego oprogramowania (dotyczy także wtyczek do przeglądarek, np. Flash)

8) w rozwiązaniu analiza i rejestracja sesji dla ww. protokołów odbywa się wyłącznie na urządzeniu; nie dopuszcza się stosowania tzw. „stacji przesiadkowych”

9) funkcjonalność monitoringu sesji realizowana przez rozwiązanie musi umożliwić informowanie operatora co najmniej o następujących o zdarzeniach:
a) rozpoczęcia sesji

b) zakończenia sesji
c) dołączenia operatora lub osoby posiadającej zaproszenie do sesji
d) rozłączenie się takiego operatora lub osoby

10) ww. funkcja musi być realizowana przynajmniej z wykorzystaniem protokołu syslog i poprzez e-mail
11) rozwiązanie musi umożliwić podanie przez nawiązującego sesję powodu jej rozpoczęcia i zapisywać wprowadzony tekst w metadanych sesji
    a) wprowadzenie ww. tekstu musi być realizowane przed nawiązaniem sesji do serwera (systemu) docelowego
    b) wprowadzenie ww. tekstu musi być realizowane co najmniej dla protokołów:
        i) RDP
        ii) VNC
        iii) SSH
        iv) telnet
12) rozwiązanie pozwala na kontrolę i ograniczenie właściwości sesji protokołowych:
    a) dla protokołu RDP minimum:
        i) ograniczenie maksymalnej rozdzielczości ekranu sesji
        ii) ograniczenie głębi kolorów, min. do 8 i 16 bpp
        iii) blokowanie funkcji schowka
    b) dla protokołu SSH minimum:
        i) blokowanie przekazywania portów (port forwarding)
        ii) blokowanie tunelu X11
        iii) blokowanie przekazywania agenta SSH
        iv) blokowanie podsystemu SFTP i przesyłania plików z wykorzystaniem scp
13) rozwiązanie posiada możliwość uwierzytelniania poprzez zewnętrzne serwery: Active Directory, Radius, LDAP (w tym OpenLDAP)
14) rozwiązanie umożliwia synchronizację użytkowników z Active Directory, w tym:
    a) z wybranymi grupami w domenie Active Directory
    b) tylko w zakresie danej lub danych organizacji (OU)
    c) z kilkoma domenami Active Directory – także w sytuacji, gdy nazwy użytkowników w domenach się powtarzają w dwóch lub więcej domenach
    d) z użytkownikami i grupami wskazanymi na podstawie zdefiniowanego filtru
15) rozwiązanie nagrywa cały ruch sieciowy związany z daną sesją (rejestracja surowego protokołu)
16) rozwiązanie pozwala na selektywne wskazanie systemów, dla których ma być włączone nagrywanie sesji
17) rozwiązanie umożliwia podmianę loginu i hasła wprowadzonego przez użytkownika na inny, znany na systemie docelowym
18) dla sesji graficznych rozwiązanie umożliwia uruchomienie własnego ekranu logowania przed nawiązaniem połączenia z serwerem (systemem) docelowym
19) dla sesji graficznych i tekstowych (przynajmniej dla SSH i telnet) rozwiązanie musi umożliwić połączenie z serwerem (systemem) bez znajomości ani nazwy domenowej (FQHN) ani adresu IP tego serwera (systemu), a jedynie nazwy zdefiniowanej przez operatora; przekazywanie tej informacji może być zrealizowane np. w formacie “użytkownik#nazwaserwera” jak i wybór z listy lub z rozwijalnego menu
20) rozwiązanie posiada możliwość wymuszenia akceptacji operatora przed nawiązywaniem sesji

21) rozwiązanie musi współpracować z systemami klasy SIEM – przynajmniej z wykorzystaniem protokołu syslog
22) rozwiązanie ma zaimplementowane oznakowanie komunikatów systemowych wysyłanych do systemu SIEM (tagowanie) umożliwiające kategoryzację wydarzeń w takim systemie – niedopuszczalna jest konieczność przeszukiwania komunikatów logów wg słów kluczowych w celu ich kategoryzacji
23) rozwiązanie umożliwia zdefiniowanie dostępu do puli dla systemów z wykorzystaniem adresacji IP zawierającej określających całe podsieci (np. maska /24) – przynajmniej dla protokołów RDP, VNC, SSH I telnet
24) dla protokołu RDP – rozwiązanie musi umożliwiać dostęp do podsieci systemów VDI za pomocą tzw. Connection Broker, bez konieczności definiowania każdego systemu typu VDI z osobna
25) rozwiązanie umożliwia komentowanie przeglądanych sesji – zarówno w trybie “na żywo” jak i zapisanych wcześniej – w trakcie odtwarzania
26) rozwiązanie umożliwia automatyczne przerwanie sesji po wykryciu wcześniej zdefiniowanego ciągu znaków oraz alert administratora
27) rozwiązanie umożliwia wprowadzenie konieczności dodatkowej akceptacji połączenia uprzywilejowanego przez nadzorcę (osobę trzecią) po poprawnym uwierzytelnieniu się użytkownika
28) potwierdzenie i/lub odrzucenie sesji uprzywilejowanej przez nadzorcę możliwe jest również przy pomocy dedykowanej aplikacji dostępnej na urządzenia mobilne.
29) rozwiązanie umożliwia przeszukiwanie sesji w trybie pełnotekstowym
    a) wyszukiwanie musi być możliwe zarówno dla kanału wejściowego (np. wpisywane komendy) jak i danych wyjściowych, pojawiających się na ekranie nawiązanej sesji
    b) powyższe dotyczy to także sesji graficznych w protokołach RDP i VNC, a co za tym idzie wszystkich treści pojawiających się na ekranie
    c) możliwość wyszukiwania musi być natychmiastowa, z wyjątkiem sesji graficznych, dla których dopuszcza się zastosowanie mechanizmu indeksującego OCR
    d) przygotowanie sesji do wyszukiwania musi być realizowane wewnętrznie, tzn. dane nie mogą być wysyłane do chmury lub innego dedykowanego urządzenia
30) rozwiązanie umożliwia udzielenie czasowego dostępu do pojedynczej sesji – zarówno zakończonej i zapisanej jak niezakończonej (“na żywo”)
    a) w ramach sesji niezakończonej (“na żywo”) operator musi mieć możliwość określenia czy sesja ma być udostępniona tylko w trybie podglądu czy z możliwością dołączenia do sesji
    b) musi być możliwość wycofania udzielonego dostępu do współdzielonej sesji w każdej chwili
31) rozwiązanie ma mieć możliwość monitorowania, raportowania oraz analizy aktywności użytkownika podczas sesji, uwzględniający moduł analityki biznesowej
    a) Analiza sesji powinna przedstawiać szczegółowo jak kształtowała się produktywność użytkowników/organizacji w zadanym przedziale czasu.
    b) Konfigurowalny parametr określający próg aktywności powinien pozwalać na szybkie identyfikowanie sesji, użytkowników czy organizacji, które nie przekroczyły wymaganego poziomu aktywności oraz wspomagać ustalenie wartości progowej, przy której zadana liczba użytkowników lub sesji osiąga wymagany poziom aktywności.
    c) w szczególności musi być możliwość określenia aktywności sesji w skali 0%-100%, wynikająca z liczby zarejestrowanych zdarzeń wejścia (wysłany kod klawiszowy, a dla sesji graficznych wysłane zdarzenie naciśnięcia klawisza myszy i ruchu myszy – jeżeli protokół to rejestruje)

d) Komponent analizy produktywności powinien pozwalać porównać aktywność organizacji lub użytkowników w zadanych przedziałach czasu.

32) rozwiązanie musi mieć możliwość definiowania hierarchii użytkowników i operatorów, co najmniej w zakresie:
    a) zwykłego konta użytkownika
    b) konta operatora z dostępem do przeglądu
    c) konta operatora z możliwością przeglądu konfiguracji
    d) konta operatora z możliwością zmiany konfiguracji
    e) konta operatora z możliwością zarządzania systemem (np. restart urządzenia)
33) rozwiązanie musi posiadać możliwość zdefiniowania dostępu dla operatora co najmniej do:
    a) wskazanych serwerów (systemów) oraz zapisanych i trwających do nich sesji
    b) wskazanych użytkowników oraz zapisanych i trwających sesji tychże
34) rozwiązanie musi umożliwić wprowadzenie znakowania czasowego do zapisu sesji przez podmioty kwalifikowane (co najmniej przez KIR i PWPW)
35) rozwiązanie musi umożliwić zdefiniowanie polityki retencji sesji, tj. okresu, po którym sesje będą kasowane z urządzenia
    a) musi istnieć możliwość zdefiniowania innej polityki retencji
36) rozwiązanie musi mieć możliwość integracji z zewnętrznym repozytorium haseł firm takich jak:
    a) CyberArk
    b) Lieberman
    c) Thycotic
    d) Hitachi
37) rozwiązanie musi integrować się ze standardem uwierzytelnienia opisanym w dokumencie RFC 6749 (OAuth2)
38) rozwiązanie musi umożliwić zdefiniowanie zestawu komend lub ciągów znaków, których wprowadzenie w trakcie trwania sesji lub pojawienie się w treści sesji wywoła zdefiniowane przez operatora działanie, co najmniej:
    a) informacja wysłana z wykorzystaniem protokołu syslog
    b) informacja wysłana do systemu SIEM
    c) informacja wysłana do operatora poprzez e-mail
    d) natychmiastowe zakończenie rozpoczętej sesji z możliwością automatycznego zablokowania konta użytkownika niezależnie od stanu użytkownika wynikającego z synchronizacji z zewnętrznymi zbiorami użytkowników
    e) zatrzymanie rozpoczętej sesji
39) ww. zestaw komend lub ciągów znaków musi być możliwy do zdefiniowania z wykorzystaniem mechanizmu wyrażeń regularnych (regexp) przy czym mechanizm wildcard nie będzie uznany za równoważny
40) wyżej opisana funkcjonalność musi być realizowana co najmniej dla protokołów:
    a) RDP
    b) VNC
    c) SSH
    d) telnet
41) funkcjonalność wyżej opisanego rozpoznawania komend lub ciągu znaków musi:
    a) być realizowana dla protokołów co najmniej VNC, RDP – w zakresie danych wejściowych i danych sesji dostępnych po zindeksowaniu po zakończeniu sesji

b) dla pozostałych protokołów – w trakcie trwającej sesji niezwłocznie po rozpoznaniu danego ciągu znaków w danych wejściowych i danych wyjściowych, pojawiających się na ekranie nawiązanej sesji
c) mieć możliwość ograniczenia tylko dla danych wejściowych lub wyjściowych, pojawiających się na ekranie nawiązanej sesji

42) rozwiązanie musi umożliwiać zapisanie sesji w postaci nagrania wideo (zapis liniowy) w formacie umożliwiającym odtworzenie nagrania za pomocą programu VLC 3.0 w wersji lub nowszej
a) zapis taki musi być możliwy zarówno dla protokołów graficznych (przynajmniej VNC i RDP) jak i tekstowych (przynajmniej SSH i telnet)
43) rozwiązanie musi mieć możliwość zarządzania skryptowego z wykorzystaniem udokumentowanego API umożliwiającego co najmniej:
a) tworzenie, zmianę i usuwanie kont użytkowników
b) tworzenie, zmianę i usuwanie serwerów (systemów docelowych)
c) tworzenie, zmianę i usuwanie dostępu do ww. serwerów (systemów) – dotyczy kont na tychże
d) tworzenie, zmianę i usuwanie adresów IP i portów, do których będą się łączyć użytkownicy
e) tworzenie, zmianę i usuwanie relacji między kontami, serwerami, dostępami
f) pobieranie listy sesji – z możliwością rozróżnienia sesja, które nie zostały jeszcze zakończone
g) blokowanie użytkownika – niezależnie od stanu użytkownika wynikającego z synchronizacji z zewnętrznymi zbiorami użytkowników
44) rozwiązanie musi umożliwić powrót co najmniej do poprzedniej wersji po wykonaniu uaktualnienia
a) funkcja ta musi być dostępna bezpośrednio z interfejsu zarządzania, bez konieczności uruchamiania linii komend lub dedykowanej konsoli zarządzającej
45) rozwiązanie musi wspierać zmianę haseł w systemach Unix za pomocą uprzywilejowanego konta z dostępem z wykorzystaniem klucza SSH
46) rozwiązanie umożliwia definiowanie sekwencji komend wywołujących zmianę hasła
47) rozwiązanie umożliwia weryfikację czy hasło nie zostało zmienione w sposób nieuprawniony
48) rozwiązanie przechowuje historię haseł do kont i umożliwia odzyskanie wybranego hasła
49) rozwiązanie umożliwia zdefiniowanie złożoności automatycznie generowanych haseł
50) rozwiązanie umożliwia bezpieczną wymianę haseł pomiędzy aplikacjami – funkcjonalność AAPM
51) autoryzacja dostępu systemu AAPM do danych ma odbywać się na podstawie adresu IP oraz hasła jednorazowego lub statycznego
52) moduł musi współpracować przynajmniej z systemami uruchomionymi pod kontrolą systemu operacyjnego:
a) Windows Server 2012 lub nowszego
b) Linux – Red Hat 6 lub nowszego (lub równoważna, ale nie starsza, inna dystrybucja)
c) FreeBSD 10 lub nowszego
53) rozwiązanie zapewnia ochronę kryptograficzną wszystkich zapisanych danych (szyfrowanie oraz integralność) na poziomie bezpieczeństwa nie gorszym niż poziom gwarantowany przez szyfr AES256
a) producent rozwiązania nie może mieć możliwość odszyfrowania zapisywanych na urządzeniu danych bez dostępu do oryginalnych kluczy szyfrujących (brak tzw. “kluczy serwisowych”)
54) rozwiązanie ma możliwość konfiguracji klastrowej:

a) musi być możliwość udostępnianie usług w trybie wysokiej dostępności z wykorzystaniem wirtualnego (“pływającego”) adresu IP
b) rozwiązanie nie może pracować w trybie “hot standby”, tj. wszystkie węzły klastra muszą brać aktywny udział w realizacji funkcjonalności rozwiązania, zgodnie ze zdefiniowaną polityką, tj. musi być możliwe określenie który węzeł klastra będzie obsługiwał dany zestaw sesji
c) musi być możliwość ręcznej zmiany roli węzła w klastrze, np. w celu przeniesienia obsługi funkcjonalności rozwiązania z węzła, który będzie relokowany

55) rozwiązanie posiada przestrzeń dyskową na dane (użytkową) umożliwiającą rejestrację i przechowywanie gromadzonych danych (monitorowanych sesji) przez okres minimum 2 lata licząc dla sesji RDP, przy założeniu przechowywania minimum 200 sesji RDP dziennie, gdzie jedna sesja trwa średnio 8 godzin dziennie i jest uruchamiana przez 365 dni w roku, a jej szacunkowa wielkość to około 130 MB
56) rozwiązanie musi posiadać wydajność umożliwiającą jednoczesną rejestrację do min. 100 sesji tekstowych (dla protokołów SSH, telnet) lub min. 30 sesji (dla protokołów RDP, VNC) – liczone dla pojedynczego urządzenia lub dla klastra z aktywnym tylko jednym węzłem,
57) rozwiązane musi być dostarczone z licencją pozwalającą na nieograniczone definiowanie obiektów (np. skonfigurowanego połączenia, użytego protokołu, użytkowników, ról i innych definiowanych obiektów) oraz na nielimitowane aktywne monitorowanie jednocześnie dowolnej ilości sesji bez względu na jej rodzaj. Licencje muszą pozwalać na przenoszenie pomiędzy urządzeniami (np. w przypadku wymiany sprzętu) oraz możliwość przenoszenia pomiędzy jednostkami organizacyjnymi resortu sprawiedliwości. Licencjobiorcą jest Ministerstwo Sprawiedliwości a podmiotami uprawnionymi do korzystania z licencji są jednostki podległe lub nadzorowane przez Ministra Sprawiedliwości oraz jednostki sądownictwa powszechnego.
58) urządzenie musi pracować w trybie:
a) serwera tzw. “przesiadkowego” (warstwa 5+ modelu OSI)
b) aplikacji – nasłuchując na wskazanym lub wskazanych adresach IP i portach
c) trybie routera (gateway, warstwa 3 modelu OSI) – przesyłając ruch wyłącznie do zdefiniowanych serwerów (systemów) między dwoma segmentami sieci IP
d) trybie mostka (bridge, warstwa 2 modelu OSI) – przesyłając cały ruch sieciowy pomiędzy dwoma segmentami sieci Ethernet, przy czym nie może ingerować w pakiety nie będące częścią ruchu sieciowego należącego do sesji obsługiwanej przez urządzenie
59) rozwiązanie musi umożliwić zdefiniowanie własnego certyfikatu / klucza dla połączeń szyfrowanych (dla protokołów RDP i SSH) jak również przeniesienie istniejących certyfikatów / klucza z serwera (systemu), do którego dostęp jest zdefiniowany – obsługa fraz szyfrujących certyfikat / klucz
60) rozwiązanie musi umożliwić weryfikację certyfikatu / klucza serwera (systemu), do którego dostęp jest zdefiniowany – przynajmniej dla protokołów RDP i SSH
a) w przypadku protokołu RDP musi być możliwość weryfikacji certyfikatu serwera (systemu) docelowego na podstawie zdefiniowanego w urządzeniu (zaimportowanego) certyfikatu CA
61) rozwiązanie obsługuje pakiety tagowane wg standardu 801.1q (VLAN-y)
62) rozwiązanie obsługuje agregację sieciową 802.3ad (LACP) dla dowolnego typu interfejsu sieciowego – tj. zarówno dla interfejsów wykorzystywanych do nasłuchu, interfejsu lub interfejsów przekazywania danych jak i dla interfejsu zarządzania

63) rozwiązanie musi umożliwić monitorowanie wybranych parametrów pracy z wykorzystaniem protokołu SNMP w wersji min. v3
64) rozwiązanie musi umożliwić podstawową diagnostykę sieciową:
    a) potwierdzenie komunikacji za wykorzystaniem sygnalizacji ICMP (ping)
    b) potwierdzenie komunikacji z wykorzystaniem połączenia TCP (połączenie z dowolnym portem dowolnego adresu IP)
65) rozwiązanie musi współpracować z następującymi usługami sieciowymi:
    a) NTP
    b) name server (DNS)
66) rozwiązanie posiada wsparcie dla polskiej klawiatury (programisty)
67) rozwiązanie musi zawierać wszystkie niezbędne licencje do uruchomienia wyżej opisanej funkcjonalności, włączając w licencje na system operacyjny – jeżeli takie są niezbędne do jej uruchomienia
68) rozwiązanie posiada min. 4 interfejsy sieciowe 1 GbE (1000Base-T)
    a) rozwiązanie musi mieć możliwość rozszerzenia obsługi ww. interfejsów o tryb bypass, tj. funkcję przesyłu pakietów także, gdy urządzenie główne jest wyłączone i nie pracuje
69) rozwiązanie powinno mieć możliwość rozbudowy o światłowodowe interfejsy sieciowe pracujące w standardzie 802.1ae z wykorzystaniem interfejsów 10GBASE-SX i -LX i złącz SFP+
70) rozwiązanie musi mieć możliwość dołączenia zewnętrznego udziału dyskowego z wykorzystaniem sieci SAN (protokół Fibre Channel) – w celu zwiększenia przestrzeni przechowywania danych zapisanych sesji

III Dodatkowe wymagania:

1. Oferowane produkty będą pochodziły z oficjalnego kanału dystrybucyjnego producenta na terenie Unii Europejskiej.
2. Zamawiający wymaga, aby dostarczone urządzenia były wolne od wad, fabrycznie nowe - bez śladów używania i bez uszkodzenia, wprowadzone na rynek zgodnie z przepisami obowiązującymi na terenie Rzeczpospolitej Polskiej, wyprodukowane nie wcześniej niż 6 miesięcy od daty dostawy sprzętu, urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych zabezpieczających przed uszkodzeniem w trakcie transportu i składowania, z załączonymi kartami gwarancyjnymi, dokumentami producenckimi i instrukcjami obsługi w języku polskim, a jeśli są one niedostępne to w języku angielskim. Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu realizacji procedur opisanych w zakresie Zamówienia, przy czym Wykonawca jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo uczestniczenia podczas czynności rozpakowywania.
3. Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej (tzn. najnowszej opublikowanej przez producenta) na dzień dostawy Systemu .
4. Oferowane urządzenia w dniu składania ofert nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
5. Wykonawca udostępni oprogramowanie umożliwiające zdalne zgłaszanie i monitorowanie statusu zgłoszenia serwisowego. .
6. Zamawiający w ramach udzielonej gwarancji musi mieć możliwość zgłaszania awarii i zapytań o pomoc techniczną do Wykonawcy. Bardzo istotnym elementem jest brak ograniczeń, co do liczby zgłoszeń.
7. Wszelkie prace wykonywane przez Wykonawcę w Systemie nie mogą skutkować utratą praw gwarancyjnych do istniejącej i rozszerzonej konfiguracji danego urządzenia i oprogramowania.

8. Na wniosek Wykonawcy Zamawiający może wyrazić zgodę w formie pisemnej na wykonanie prac zdalnie w całości lub części, pod warunkiem przestrzegania przez Wykonawcę zasad bezpieczeństwa określonych przez Zamawiającego. Zgodę taką należy uzyskać dla każdej z lokalizacji niezależnie. Zamawiający zastrzega sobie prawo do wycofania udzielonej zgody w dowolnym momencie bez konieczności podawania przyczyny i wcześniejszego informowania Wykonawcy.
9. Wykonawca będzie realizował zgłoszenia awarii/usterek systemu w następujący sposób:
    - awaria krytyczna, tj. niedostępność systemu dla wszystkich użytkowników: czas reakcji do 1 godziny od chwili zgłoszenia awarii przez Zamawiającego, czas naprawy (przywrócenia funkcjonalności systemu) do 8 godzin od chwili zgłoszenia awarii przez Zamawiającego;
    - usterka (niepowodująca niedostępności systemu): czas reakcji do 4 godzin od chwili zgłoszenia usterki przez Zamawiającego, czas naprawy (przywrócenia funkcjonalności systemu) do 96 godzin od chwili zgłoszenia usterki przez Zamawiającego.
10. Obsługa zgłoszeń musi obejmować co najmniej:
    - wymiany uszkodzonego sprzętu przez Wykonawcę,
    - aktualizację i konfigurację oprogramowania Systemu oraz Sprzętu
11. Zamawiający może zawiesić czas naprawy do 40 dni kalendarzowych w przypadkach wymagających udzielenia przez producenta Systemu informacji technologicznych niedostępnych w opublikowanych materiałach produktowych oraz w przypadku konieczności interwencji producenta w szczególności polegających na wprowadzaniu zmian takich jak przygotowanie odpowiednich poprawek w produktach. W przypadku wystąpienia opóźnień leżących po stronie producenta Systemu Wykonawca zobowiązany jest poinformować Zamawiającego o zaistniałym fakcie.
12. Czynności związane z instalacją w infrastrukturze Zamawiającego oraz uruchomieniem i konfiguracją systemu muszą być przeprowadzone przez personel Wykonawcy we współpracy z personelem IT Zamawiającego.
13. Dostawa musi obejmować wszystkie wymagane przez producentów oferowanego rozwiązania komponenty do jego prawidłowego podłączenia i konfiguracji w rozwiązaniu Zamawiającego takie jak między innymi: okablowanie, adaptery, wtyczki, listwy mocujące, urządzenia zasilające itp.(sieć energetyczna Zamawiającego o parametrach: 230 V ± 10%, 50 Hz).
14. Wykonawca zapewni do 500 roboczogodzin asysty technicznej eksperta.
15. W roboczogodzinę asysty technicznej eksperta nie wlicza się czasu dojazdu oraz ilości osób zapewniających wsparcie tzn. nie ma znaczenia ile osób będzie świadczyło asystę techniczną eksperta w danej roboczogodzinie/roboczogodzinach u Zamawiającego. Rozliczenie roboczogodzin wsparcia asysty technicznej eksperta odbywać się będzie miesięcznie za faktycznie wykorzystane roboczogodziny na podstawie miesięcznych Protokołów odbioru asysty technicznej eksperta. Do godzin asysty technicznej eksperta nie wlicza się roboczogodzin usług wykonywanych w ramach realizacji zgłoszeń awarii lub usterek systemu
16. Asysta techniczna eksperta będzie dotyczyła oferowanego przez Wykonawcę Systemu i Sprzętu i będzie polegała w szczególności na wprowadzaniu zmian w konfiguracji Systemu i Sprzętu.
17. Zamawiający będzie przekazywać Wykonawcy zlecenia, w których każdorazowo określi przedmiot zlecenia oraz określi maksymalny, oczekiwany termin realizacji zlecenia.
18. Wykonawca w terminie wyznaczonym przez Zamawiającego, nie krótszym niż jeden dzień roboczy od otrzymania zlecenia, przekaże Zamawiającemu propozycję sposobu wykonania zlecenia zawierającą w szczególności wycenę prac zawartych w zleceniu, tj. proponowaną liczbę roboczogodzin niezbędnych do wykonania zlecenia.
19. Zamawiający może zaakceptować propozycję sposobu wykonania zlecenia albo odrzucić ją, co jest równoznaczne z nieudzieleniem zlecenia albo zażądać od Wykonawcy, w wyznaczonym terminie, dodatkowych wyjaśnień, informacji do przedstawionej propozycji sposobu wykonania zlecenia.

20. W przypadku akceptacji propozycji sposobu wykonania zlecenia, Zamawiający przedłoży Wykonawcy zaakceptowane zlecenie zawierające w szczególności: zakres prac, liczbę roboczogodzin niezbędną do wykonania prac, kwotę wynagrodzenia należnego za zrealizowanie zlecenia, termin wykonania prac.
21. Rozliczenie asysty technicznej odbywać się będzie na podstawie podpisanych bez zastrzeżeń, przez Zamawiającego, Protokołów odbioru asysty technicznej eksperta.
22. W ramach roboczogodzin asysty technicznej ekspert na wezwanie Zamawiającego ma obowiązek przybyć do wskazanego w umowie miejsca/siedziby na terenie Warszawy i tam realizować zgłoszenie.
23. Świadczenie usługi asysty technicznej jest uprawnieniem Zamawiającego. Niewykorzystanie wszystkich przewidzianych w Umowie roboczogodzin nie rodzi po stronie Wykonawcy żadnych roszczeń w stosunku do Zamawiającego.
24. Wykonawca w ramach gwarancji dla dostarczonego i uruchomionego Systemu oraz Sprzętu, zainstaluje na wezwanie i w uzgodnieniu z Zamawiającym wszystkie poprawki, usprawnienia i nowe wersje oprogramowania dla Systemu i Sprzętu, udostępniane przez producenta wdrożonego Systemu oraz Sprzętu.
25. W ramach gwarancji Zamawiającemu przysługuje prawo do instalacji i używania wszystkich poprawek, usprawnień i nowych wersji oprogramowania dla Systemu i Sprzętu udostępnianych przez producenta Systemu nie powodując ponoszenia dodatkowych kosztów finansowych przez Zamawiającego.
26. W ramach wdrożenia Wykonawca przeprowadzi w każdej z 10 lokalizacji Zamawiającego instruktaż stanowiskowy dla minimum 3 pracowników Zamawiającego w wymiarze 8 godzin zegarowych. Instruktaż musi być przeprowadzony przez inżyniera/inżynierów dokonujących bezpośrednio wdrożenia Systemu po stronie Wykonawcy. Instruktaż zostanie przeprowadzony po konfiguracji i instalacji Systemu. Instruktaż stanowiskowy musi obejmować całość zagadnień związanych z czynnościami administracyjnymi i funkcjonowaniem wdrożonego Systemu w środowisku produkcyjnym Zamawiającego z zapewnieniem poniżej określonych warunków:
    - wszyscy uczestnicy otrzymają materiały szkoleniowe w języku polskim w formie papierowej i/lub elektronicznej,
    - instruktaż będzie prowadzony w języku polskim,
    - koszty opracowania, transportu i powielenia materiałów ponosi Wykonawca,
    - potwierdzeniem prawidłowej realizacji instruktażu stanowiskowego będzie podpisany bez zastrzeżeń przez Zamawiającego Protokół odbioru instruktażu.
27. Wykonawca opracuje i dostarczy następującą dokumentację dotyczącą projektu wdrożeniowego:
    a. Projekt Wdrożenia Systemu, który musi zawierać, w szczególności: Opis funkcjonalny Systemu, Wykaz Oprogramowania i Sprzętu potrzebnego do realizacji projektu wraz z ich specyfikacją techniczną, Szczegółowy opis architektury proponowanego rozwiązania wraz z opisem integracji z infrastrukturą techniczną Zamawiającego oraz harmonogramem wdrożenia dla każdej z 10 lokalizacji Zamawiającego.
    b. Dokumentację testów akceptacyjnych wdrożenia Systemu, która musi dokumentować działania, jakie należy wykonać, aby uzyskać potwierdzenie, że wdrożony System jest zgodny z opisem przedmiotu zamówienia.
28. Wykonawca opracuje i dostarczy dokumentację powykonawczą, która musi być jednym spójnym dokumentem, bez względu na jej objętość I musi zawierać wszystkie procedury administracyjne i operacyjne oraz inne informacje, istotne w eksploatacji Systemu, w szczególności:
    a. procedury i instrukcje dotyczące instalacji, konfiguracji i aktualizacji oprogramowania,
    b. procedury dotyczące wykonywania i przechowywania kopii bezpieczeństwa,
    c. procedury odtwarzania danych i systemu po awarii,

d. instrukcje dla użytkowników i administratorów w tym:
e. procedury oraz instrukcje konfiguracji reguł monitorowania sesji dla wszystkich ich rodzajów i protokołów,
f. procedury zarządzania użytkownikami i hasłami,
g. procedury raportowania oraz instrukcje konfiguracji modułu raportowania w tym:
   i. procedury audytu zmian w systemie,
   ii. procedury audytu działań administratorów i użytkowników (np. rozliczalność),
   iii. procedura kontroli zdarzeń dotyczących bezpieczeństwa,
h. inne niezbędne dokumenty, jakie powstaną w trakcie realizacji wdrożenia Systemu, uzgodnione z przedstawicielem Zamawiającego.

Zamawiający dopuszcza posiadanie przez Systemem funkcjonalności które nie są wymagane przez Zamawiającego lecz mogą stanowić dodatkową funkcjonalność rozwiązania ocenianą przez Zamawiającego dla każdej z poniższych funkcjonalności opcjonalnych niezależnie:

1. rozwiązanie posiada interfejs użytkownika w języku polskim,
2. rozwiązanie posiada wsparcie techniczne w języku polskim,
3. rozwiązanie posiada dokumentację w języku polskim.

IV Lokalizacje fizyczne Zamawiającego w których będzie realizowana umowa:

1. ….
2. ….
3. ….
4. ….
5. ….
6. ….
7. ….
8. ….
9. ….
10. ….

Kryteria oceny
W pełni polski interfejs użytkownika
Wsparcie i serwis na terenie polski

+
Ilość licencji (bez limitu) zapsy w opz