

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

wersja ujednolicona po zmianie treści Zapytania ofertowego nr 1

Zmiany wprowadzone niniejszą wersją oznaczono kolorem żółtym (oznaczenie robocze – do usunięcia przed publikacją)

1. Dostawa i wdrożenie systemu monitorowania sieci przemysłowej – 1 sztuka

Przedmiotem zamówienia jest:

1. wdrożenie systemu monitorowania sieci przemysłowej służącego do monitorowania sieci przemysłowej, składającego się z sond sprzętowych oraz oprogramowania do zarządzania i analizy ruchu sieciowego (system IDS),
2. dostawa licencji oraz sond sprzętowych,
3. udzielenie wsparcia dla administratorów Zamawiającego,
4. organizacja i realizacja szkoleń dla administratorów Zamawiającego.

1. Funkcjonalność i specyfikacja.

Zgodność z normami i standardami.

Oferowane rozwiązanie oraz sposób jego wdrożenia muszą być zgodne z obowiązującymi, aktualnymi na dzień składania ofert wydaniami następujących norm i standardów: PN-EN IEC 62443 (bezpieczeństwo systemów automatyki przemysłowej i sterowania – IACS/OT), w szczególności części 62443-3-3 (wymagania bezpieczeństwa systemu) oraz 62443-4-2 (wymagania bezpieczeństwa dla komponentów); ISO/IEC 27001 (system zarządzania bezpieczeństwem informacji); ISO/IEC 27002 (zabezpieczenia bezpieczeństwa informacji); ISO 22301 (system zarządzania ciągłością działania). Wykonawca potwierdzi zgodność oferowanego rozwiązania z powyższymi normami w treści oferty oraz, na żądanie Zamawiającego, przedstawi stosowne dokumenty, certyfikaty lub oświadczenia producenta. W zakresie, w jakim norma nie ma bezpośredniego zastosowania do konkretnego elementu rozwiązania, Wykonawca wskaże to wraz z uzasadnieniem.

1. Oprogramowanie musi być w 100% niezależne od dostawców automatyki oraz zawierać wsparcie dla urządzeń przemysłowych wykorzystywanych przez Zamawiającego.
2. Przetwarzane dane w systemie nie mogą być przesyłane poza infrastrukturę Zamawiającego.
3. Całość rozwiązania, tj. system IDS wraz z silnikiem analitycznym oraz wszystkie sondy systemowe – zarówno sondy fizyczne, jak i wirtualne – muszą pochodzić od jednego producenta. Producent systemu IDS musi być jednocześnie producentem sond, a rozwiązanie powinno stanowić spójny, zintegrowany produkt, zaprojektowany i rozwijany jako całość. Przez pochodzenie od jednego producenta rozumie się sytuację, w której jeden podmiot jest właścicielem projektu całego rozwiązania i ponosi wyłączną odpowiedzialność za projekt i rozwój warstwy sprzętowej i programowej, oprogramowanie układowe (firmware) sond, aktualizacje i poprawki bezpieczeństwa, obsługę podatności, dokumentację techniczną, zgodność wyrobu oraz wsparcie serwisowe i gwarancję, przy jednym kanale wsparcia producenta i jednej ścieżce aktualizacji. Wymagania nie spełnia rozwiązanie polegające na integracji, rebrandingu lub oznakowaniu własną marką sprzętu i oprogramowania pochodzących od różnych podmiotów, w którym odpowiedzialność za oprogramowanie układowe, poprawki bezpieczeństwa i podatności warstwy sprzętowej pozostaje po stronie podmiotu innego niż producent systemu IDS. Zamawiający nie wymaga, aby producent prowadził samodzielnie proces fizycznej produkcji urządzeń; korzystanie z podwykonawców produkcyjnych (EMS) nie narusza wymagania, o ile producent pozostaje właścicielem projektu rozwiązania oraz podmiotem wyłącznie odpowiedzialnym w zakresie wskazanym powyżej.

4. System IDS musi posiadać interfejs graficzny min. w języku polskim i angielskim, który ma być dostępny przez przeglądarkę internetową. Dostęp do interfejsu musi być zabezpieczony protokołem szyfrowania TLS. Zamawiający musi mieć możliwość importu własnego certyfikatu.
5. System IDS nie może ograniczać wielkości przestrzeni dla przechowywanych logów i archiwalnego ruchu sieciowego. Musi umożliwiać ustawienie czasu przechowywania informacji o anomaliach i archiwum ruchu sieciowego. Wymaganie dotyczy licencji oraz konstrukcji systemu IDS i nie ustanawia po stronie Zamawiającego obowiązku udostępnienia przestrzeni dyskowej większej niż wskazana w lit. 1 części „Parametry minimalne rozwiązania i skala wdrożenia”.
6. System IDS musi umożliwiać konfigurowanie poziomów dostępu dla użytkowników.
7. System IDS musi umożliwiać aktualizację bazy danych, oprogramowania, podatności w trybie offline.
8. System IDS musi umożliwiać synchronizację czasu przy użyciu protokołu NTP.
9. System IDS musi zapewniać:
 - a. pasywne monitorowanie sieci przemysłowej Zamawiającego,
 - b. automatyczne tworzenie graficznej mapy urządzeń min.: PLC, HMI, RTU, IED, stacje operatorskie SCADA, wraz z możliwością filtrowania po urządzeniach, protokołach, portach.
 - c. szczegółową inwentaryzację urządzeń,
 - d. automatyczne odzwierciedlenie połączeń komunikacyjnych,
 - e. informowanie o zmianach min.: utrata urządzenia, pojawienie się nowego urządzenia, zmiana komunikacji,
 - f. wykrywanie podatności urządzeń i oprogramowania w sieci przemysłowej wykorzystując powszechnie znane podatności CVE na podstawie bazy MITRE i/lub NIST,
 - g. budowę mapy topologii sieci przemysłowej wraz z informacją o sposobie komunikacji,
 - h. obsługę LLDP, CDP, CIP, SSDP.
10. System IDS musi posiadać mechanizmy alarmujące, które będą działać w trakcie budowania modelu sieci przemysłowej w celu wykrywania zagrożeń w procesie nauki.
11. System IDS musi posiadać zaimplementowane mechanizmy wsparcia i rozumienia komend dla głównych protokołów OT i IT.
12. System IDS musi mieć możliwość dodawania nowego typu protokołu.
13. System IDS musi działać na kopii ruchu oraz musi być w 100% pasywny. Nie może generować żadnego dodatkowego ruchu w monitorowanej sieci ani mieć wpływu na komunikację w sieci przemysłowej.
14. Kopia ruchu sieciowego musi się odbywać na bazie kopii dostarczanej ze SPAN/mirror portów przełączników, lub w trybie w pełni pasywnym, z wykorzystaniem TAP-a pasywnego, bez wpięcia systemu IDS w linię (tryb in-line jest niedopuszczalny).
15. System IDS musi umożliwiać analizę ruchu sieciowego: Packet Capture (pliki PCAP).
16. System IDS musi monitorować i klasyfikować cyberincydenty oraz zdarzenia operacyjne.
17. System IDS powinno być oparte na technologii uczenia maszynowego i umożliwiać modelowanie sieci w czasie maksymalnie 5 dni.
18. System IDS musi umożliwiać generowanie potencjalnych wektorów ataku, bazując na analizie ruchu sieciowego oraz rekomendować sposoby zwiększenia bezpieczeństwa.
19. System IDS musi umożliwiać integrację z systemami typu SIEM (np. poprzez Syslog)

20. System IDS musi zapewniać w trybie ciągłym monitoring online sieci przemysłowej z alarmowaniem w czasie rzeczywistym wykorzystując metody /techniki behawioralne.
21. System IDS musi umożliwiać sortowanie alarmów zgodnie z min.: stopniem, ważności, typie, czasie wystąpienia.
22. System IDS musi umożliwiać wysyłanie wiadomości e-mail w razie wystąpienia alarmów.
23. System IDS musi gromadzić informacje o zaistniałych alarmach min.: opis techniczny alarmu, stopień oraz ważność, rekomendacje, plik z ruchem sieciowym.
24. System IDS musi pozwalać na głęboką analizę pakietów (DPI) dla min. protokołów: MODBUS RTU, DNP3.
25. System IDS musi wspierać analizę ML/AI dla protokołów min.: Profinet, Profibus, Powerlink, Modbus RTU, Modbus TCP/IP, TASE2, DNP3, OPC UA, OPC, EtherCAT, GE EGD, EtherNet/IP, BUSZ, CIP, IEC-61850, SRTP, BACnet.
26. System IDS musi identyfikować anomalie w ruchu sieciowym oraz incydenty w tej sieci.
27. System IDS musi obsługiwać incydenty w zakresie min.: wykrywania, rejestrowania, analizy, ustawienia priorytetu, ustawienia statusu, podejmowanie działań naprawczych, rekomendacji.
28. System IDS musi wykrywać zagrożenia min.:
 - a. malware/"zero-day",
 - b. atak DOS/DDOS,
 - c. atak typu ATP,
 - d. spyware, skanowanie sieci,
 - e. zagrożenia Man-in-the-Middle,
 - f. anomalie min.: rozpoznawanie częstotliwości komunikacji urządzeń, niezgodność, komend, skanowanie PLC, skanowanie urządzeń sterujących,
 - g. wykrywanie połączeń do innej sieci LAN/internet,
 - h. wykrywanie połączeń do kluczowych urządzeń wraz z prezentacją sposobu komunikacji.
29. System IDS musi pozwalać na generowanie raportów w zakresie analizy danych.
30. System IDS musi umożliwiać instalację sond programowych w środowisku Linux.
31. System IDS musi umożliwiać szyfrowaną komunikację z sondami sprzętowymi.
32. System IDS musi umożliwiać zapamiętywanie widoków graficznych skonfigurowanych przez użytkownika.
33. System IDS musi zapewniać funkcjonalność budowy oraz utrzymania Software Bill of Materials (SBOM) dla monitorowanej infrastruktury przemysłowej, realizowaną w sposób pasywny, bez ingerencji w pracę urządzeń końcowych.
34. System IDS musi mieć możliwość ukrywania urządzeń typu MULTICAST/BROADCAST.
35. System IDS musi mieć możliwość wykrywania producenta urządzenia min. na podstawie adresu MAC.
36. System IDS musi umożliwiać eksport listy urządzeń do pliku CSV i/lub PDF z podziałem na podsieć.
37. System IDS musi umożliwiać eksport protokołów do pliku CSV i/lub PDF z informacją w której podsieci zostały one wykryte.
38. System IDS musi mieć możliwość eksportu co najmniej do pliku PCAP wybranych pakietów.
39. System IDS musi mieć możliwość zdalnej zmiany konfiguracji oraz firmware sond sprzętowych.

40. Sonda sprzętowa musi posiadać możliwość przechowywania danych na karcie pamięci w formie zaszyfrowanej min. AES128.
41. Sonda sprzętowa musi mieć możliwość instalacji na szynie DIN.
42. Sonda sprzętowa musi być zasilana napięciem 24 VDC z podtrzymaniem baterijnym do 30 minut przy zaniku zasilania z sieci.
43. Sonda sprzętowa musi wspierać: DHCP, stały adres IP.
44. Sonda sprzętowa musi być zabezpieczona przed ingerencją tzn.: dane muszą zostać skasowane przy próbie odczytu pamięci FLASH.
45. Sonda sprzętowa musi generować alarm w systemie IDS podczas próby otwarcia obudowy.
46. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS485.
47. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS422.
48. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS232.
49. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący CAN.
50. Sonda sprzętowa musi posiadać min. jeden interfejs monitorujący RJ45 10/100Mbps pracujący w trybie Span-port. Interfejs monitorujący RJ45 nie może identyfikować się w sieci poprzez adres MAC oraz musi być pozbawiony funkcji Tx. Wymaganie stosuje się z uwzględnieniem lit. f części „Parametry minimalne rozwiązania i skala wdrożenia”.
51. Sonda sprzętowa musi umożliwiać przekazywanie do systemu IDS wskazaną część ruchu sieciowego min.: dla wybranych urządzeń logicznych, protokołu.
52. Sonda sprzętowa musi umożliwiać przekazywać do systemu IDS strumień sieciowy w formacie IPFIX.

2. Dostawa, wdrożenie.

1. Wykonawca dostarczy:

- a. sondy sprzętowe w liczbie 3 szt. do monitorowania sieci przemysłowej,
- b. licencję wieczystą na system IDS dla nielimitowanej liczby monitorowanych urządzeń,
- c. usługi wsparcia serwisowego producenta systemu IDS na okres co najmniej 12 miesięcy od dnia podpisania protokołu odbioru końcowego bez zastrzeżeń.
- d. gwarancję na dostarczone sondy sprzętowe na okres co najmniej 24 miesięcy od dnia podpisania protokołu odbioru końcowego bez zastrzeżeń, na warunkach określonych we wzorze umowy.

Serwis producenta systemu IDS ma obejmować:

- Dostęp do dokumentacji technicznej i instrukcji systemu IDS w języku polskim.
- Dostęp do nowych wersji systemu IDS.
- Dostęp do aktualizacji i poprawek systemu IDS.
- Dostęp do aktualizacji oprogramowania sond sprzętowych.
- Wymianę uszkodzonych sond sprzętowych w razie awarii.
- Przekazanie danych kontaktowych do działu technicznego producenta systemu IDS.
- Wsparcie administratorów Zamawiającego w zakresie obsługi systemu IDS podczas wdrożenia i późniejszej eksploatacji.
- Wsparcie administratorów Zamawiającego przy identyfikacji problemów a także ich rozwiązywaniu lub zastosowaniu obejścia.

2. Wykonawca zainstaluje i zalicencjonuje oraz skonfiguruje system IDS w środowisku serwerowym wskazanym przez Zamawiającego.
3. Licencje systemowe (tj. licencje systemu operacyjnego oraz oprogramowania wirtualizacyjnego) oraz sprzęt serwerowy zapewni Zamawiający.
4. Wykonawca przeprowadzi instalację sond sprzętowych w miejscach wskazanych przez Zamawiającego. Miejsce w szafach zapewni Zamawiający a Wykonawca wykona wszystkie niezbędne połączenia pomiędzy dostarczonym sprzętem a istniejącą infrastrukturą oraz zapewni wymagane okablowanie. Instalacja sond sprzętowych nie może powodować przerw działania sieci ani wprowadzać zakłóceń do sieci.
5. Wykonawca przeprowadzi pełną konfigurację i wdrożenia systemu u Zamawiającego (konfiguracja serwera, oprogramowania, konfiguracja switchy itp.), zapewniając pełną funkcjonalność i sprawność systemu pod nadzorem Zamawiającego.
6. Wykonawca przekaze Zamawiającemu wszelkie hasła, użyte w oprogramowaniu wraz z opisem ich funkcji i uprawnień w systemie.
7. Dla całego powyższego zakresu dot. instalacji, konfiguracji i parametryzacji Wykonawca przeprowadzi testy sprawdzające prawidłowość jego wykonania i działania.
8. Wszystkie powyższe prace mają być zrealizowane w siedzibie i pod nadzorem Zamawiającego.
9. Wykonawca przeprowadzi szkolenie dla administratorów Zamawiającego z konfiguracji i administracji systemem IDS. Zamawiający dopuszcza realizację szkolenia zdalnie. Termin szkolenia zostanie uzgodniony w późniejszym terminie pomiędzy Zamawiającym a Wykonawcą.
10. Wykonawca przygotuje dokumentację powykonawczą opisującą wszystkie prace oraz sposób konfiguracji poszczególnych urządzeń 14 dni od dnia zakończenia wdrożeń przedmiotu zamówienia, przed podpisaniem protokołu odbioru końcowego. Zakończenie wdrożenia i jego odbiór nastąpi po odebraniu dokumentacji powykonawczej.

Warunki realizacji zamówienia.

Miejsce i skala wdrożenia.

Wdrożenie zostanie zrealizowane w lokalizacjach Zamawiającego wskazanych na etapie podpisania umowy. Zakres obejmuje monitorowanie sieci przemysłowej (OT) Zamawiającego przy użyciu sond sprzętowych oraz centralnego systemu IDS. Szczegółowy wykaz punktów instalacji sond, liczby monitorowanych segmentów sieci oraz lokalizacji zostanie przekazany Wykonawcy po zawarciu umowy, w ramach uzgodnienia harmonogramu; Zamawiający udostępni niezbędne informacje techniczne o topologii sieci w zakresie koniecznym do prawidłowego wdrożenia.

Parametry minimalne rozwiązania i skala wdrożenia.

Poniższe wartości stanowią wymagania minimalne i służą doborowi rozwiązania. Wykonawca potwierdzi ich spełnienie w tabeli zgodności stanowiącej Załącznik nr 6 do Zapytania ofertowego.

- a) liczba lokalizacji objętych monitorowaniem: 3,
- b) liczba punktów podłączenia sond sprzętowych (monitorowanych segmentów sieci): 3, zgodnie z liczbą dostarczanych sond,
- c) szacunkowa liczba monitorowanych urządzeń w sieci przemysłowej (PLC, HMI, RTU, przełączniki, pozostałe): do 100. Wartość ma charakter szacunkowy i służy wyłącznie doborowi wydajności rozwiązania; licencja na system IDS pozostaje Nielimitowana pod względem liczby monitorowanych urządzeń,

- d) protokoły przemysłowe występujące w sieci Zamawiającego: co najmniej protokoły wskazane w pkt 24 i 25 niniejszego OPZ; szczegółowy wykaz Zamawiający przekaże Wykonawcy po zawarciu umowy,
- e) prędkość portów przełączników, z których pobierana będzie kopia ruchu (SPAN/mirror): 1000 Mbps – przełączniki Cisco C1300-48T-4X (48 portów 10/100/1000 Mb/s, 4 porty uplink 10G SFP+),
- f) prędkość interfejsu monitorującego sondy sprzętowej: nie niższa niż rzeczywisty wolumen ruchu kierowanego na port lustrzany. Jeżeli wolumen ten przekracza 100 Mbps, interfejs monitorujący sondy musi obsługiwać prędkość 1000 Mbps; wymaganie pkt 50 stosuje się z uwzględnieniem niniejszego zastrzeżenia,
- g) wydajność analizy ruchu: sonda sprzętowa oraz system IDS muszą zapewniać analizę rzeczywistego ruchu sieciowego występującego w monitorowanych segmentach bez utraty pakietów. Spełnienie tego wymagania podlega weryfikacji podczas testów akceptacyjnych; stwierdzenie utraty pakietów zobowiązuje Wykonawcę do dostosowania rozwiązania, w tym rozbudowy sprzętowej, na własny koszt w ramach wynagrodzenia ofertowego,
- h) minimalny okres przechowywania (retencji) alarmów, incydentów oraz logów systemowych: 12 miesięcy,
- i) minimalny okres przechowywania archiwalnego zapisu ruchu sieciowego (PCAP): co najmniej 7 dni w trybie nadpisywania najstarszych danych (rolling), w ramach przestrzeni dyskowej udostępnionej na macierzy dyskowej wskazanej w lit. l. Niezależnie od powyższego, fragmenty zapisu ruchu sieciowego powiązane z zarejestrowanymi alarmami i incydentami muszą być przechowywane przez okres wskazany w lit. h,
- j) bufor lokalny sondy sprzętowej: pojemność zapewniająca ciągłość zapisu przez co najmniej 72 godziny w przypadku braku łączności z systemem IDS. Wymaganie odnosi się do strumienia danych przekazywanych przez sondę do systemu IDS (metadane ruchu, zapis w formacie IPFIX, zdarzenia i alarmy wraz z powiązаныmi fragmentami ruchu sieciowego), a nie do pełnego zapisu ruchu sieciowego pobieranego z portu lustrzanego. Wymaganie odnosi się do średniego typowego obciążenia eksploatacyjnego. Jako wartość referencyjną do wyliczenia wymaganej pojemności bufora przyjmuje się średnie obciążenie eksploatacyjne 1 Mb/s (jeden megabit na sekundę) agregatu danych przekazywanych do systemu IDS przez jedną sondę; wymaganie nie odnosi się do maksymalnej przepływności interfejsu monitorującego wskazanej w lit. e i f. Bufor lokalny sondy musi zapewniać co najmniej 64 GB pojemności użytkowej przeznaczonej na dane buforowane, przy zapisie w formie zaszyfrowanej zgodnie z pkt 40. Zamawiający nie określa wymaganego ani dopuszczalnego poziomu kompresji danych; jej zastosowanie pozostaje decyzją Wykonawcy i może wyłącznie wydłużyć rzeczywisty czas buforowania. Po wypełnieniu bufora sonda musi kontynuować zapis w trybie nadpisywania najstarszych danych, bez utraty danych o zarejestrowanych alarmach i incydentach, oraz zasygnalizować ten stan w systemie IDS po przywróceniu łączności.
- k) liczba kont administracyjnych oraz liczba jednoczesnych sesji użytkowników systemu IDS: nielimitowana,
- l) środowisko serwerowe zapewniające przez Zamawiającego, na którym zostanie uruchomiony centralny system IDS (sprzęt dostarczany w ramach odrębnego postępowania Zamawiającego): klaster dwóch serwerów Lenovo ThinkSystem SR650 V4 w obudowie 2U, każdy wyposażony w procesor Intel Xeon 6515P (16 rdzeni, 2,3 GHz), pamięć RAM 128 GB DDR5 (4 × 32 GB RDIMM), dyski lokalne 2 × 480 GB SSD SATA w konfiguracji RAID 1, kontroler RAID ThinkSystem 940-16i 4 GB z podtrzymaniem SuperCap, interfejsy sieciowe 4 × 1 GbE RJ45 (OCP) oraz 2 × 10 GbE, moduł TPM 2.0, zdalne zarządzanie Lenovo XClarity Controller XCC3 Premier i zasilanie redundantne 2 × 1300 W. Przestrzeń dyskowa na dane zapewniająca jest przez macierz Lenovo ThinkSystem DE4200 (kontrolery dual-active, cache 64 GB, 12 × 10 TB SAS 7,2K, ok. 120 TB pojemności surowej) podłączoną do serwerów,

m) system operacyjny oraz platforma wirtualizacyjna środowiska, o którym mowa w lit. l: Microsoft Windows Server 2025 Datacenter x64 (licencja OEM na 16 rdzeni, po jednej na każdy węzeł klastra) wraz z rolą Hyper-V. Licencje systemu operacyjnego oraz platformy wirtualizacyjnej zapewnia Zamawiający; edycja Datacenter obejmuje nielimitowaną liczbę wirtualnych instancji systemu Windows Server uruchamianych na tym serwerze,

n) oferowane rozwiązanie musi być możliwe do uruchomienia w środowisku, o którym mowa w lit. l oraz m, tj. jako aplikacja instalowana bezpośrednio w systemie Microsoft Windows Server 2025 Datacenter albo jako maszyna wirtualna uruchamiana w środowisku Hyper-V, z obsługą systemów gościnnych Windows oraz Linux, bez konieczności stosowania platformy sprzętowej lub wirtualizacyjnej innej niż wskazana w lit. l i m, n1) jeżeli oferowane rozwiązanie, w tym sondy programowe, o których mowa w pkt 30, wymaga systemu operacyjnego innego niż Microsoft Windows Server, Wykonawca zapewni ten system operacyjny wraz z niezbędnymi licencjami oraz jego wsparciem w ramach wynagrodzenia ofertowego,

o) Wykonawca poda w tabeli zgodności minimalne zasoby wymagane przez oferowane rozwiązanie: liczbę rdzeni procesora lub vCPU, pojemność pamięci RAM, wymaganą przestrzeń dyskową, wymagany system operacyjny oraz platformę wirtualizacyjną,

p) jeżeli oferowane rozwiązanie wymaga zasobów przekraczających parametry wskazane w lit. l, Wykonawca zapewni je we własnym zakresie, w ramach wynagrodzenia ofertowego. Wykonawca potwierdzi w tabeli zgodności, że oferowane rozwiązanie będzie działać prawidłowo w środowisku serwerowym o parametrach określonych w lit. l oraz że zapewni analizę ruchu bez utraty pakietów, zgodnie z lit. g.

Środowisko serwerowe i infrastruktura Zamawiającego.

Zamawiający zapewnia środowisko serwerowe (wirtualizacyjne lub sprzętowe) o parametrach niezbędnych do uruchomienia centralnego systemu IDS, zasilanie, miejsce w szafach teletechnicznych, dostęp do portów SPAN/mirror lub punktów podłączenia TAP-ów pasywnych oraz łączność sieciową w zakresie koniecznym do wdrożenia. Wykonawca dostarcza sondy sprzętowe, licencje, oprogramowanie systemu IDS oraz realizuje instalację, konfigurację, testy, szkolenie i dokumentację. Udostępnienie środowiska serwerowego zostanie potwierdzone protokołem. Zasady rozpoczęcia biegu terminu realizacji zamówienia w związku z udostępnieniem środowiska określa § 4 wzoru umowy oraz Rozdział 4 Zapytania ofertowego

Wykonawca potwierdzi w tabeli zgodności, stanowiącej Załącznik nr 6 do Zapytania ofertowego, minimalne wymagania środowiska serwerowego dla oferowanego rozwiązania, zgodnie z lit. o powyżej, oraz zgodność oferowanego rozwiązania z parametrami środowiska wskazanymi w lit. l i m. Złożenie tabeli zgodności wraz z ofertą stanowi potwierdzenie spełnienia tego wymogu.

Podział obowiązków (Zamawiający / Wykonawca).

Po stronie Zamawiającego pozostaje: udostępnienie środowiska serwerowego, przygotowanie portów lustrzanych/TAP, zapewnienie dostępu do lokalizacji i infrastruktury, wskazanie administratorów do szkolenia i odbioru oraz udzielenie informacji o topologii sieci. Po stronie Wykonawcy pozostaje: dostawa sprzętu i licencji, instalacja, konfiguracja, integracja, przeprowadzenie testów, szkolenie, przekazanie dokumentacji powykonawczej oraz zapewnienie wsparcia i gwarancji zgodnie z umową. Wszelkie elementy niezbędne do prawidłowego działania rozwiązania, a nieprzypisane wprost Zamawiającemu, zapewnia Wykonawca w ramach wynagrodzenia.

Zasady odbioru i testy akceptacyjne.

Odbiór końcowy nastąpi na podstawie protokołu odbioru podpisanego przez Strony, po pozytywnym przeprowadzeniu testów akceptacyjnych potwierdzających zgodność wdrożonego rozwiązania z niniejszym OPZ. Testy obejmą co najmniej: poprawność działania sond i systemu IDS na kopii ruchu, poprawność

wykrywania i alarmowania, budowę mapy topologii, wykrywanie podatności, poprawność interfejsu w języku polskim, mechanizmy uprawnień oraz brak wpływu systemu na monitorowaną sieć (potwierdzenie pełnej pasywności). Warunkiem odbioru jest również przekazanie kompletnej dokumentacji powykonawczej oraz przeprowadzenie szkolenia.

Szkolenie administratorów.

Wykonawca przeprowadzi szkolenie dla administratorów Zamawiającego w wymiarze co najmniej 16 godzin (2 dni robocze) w języku polskim, obejmujące: obsługę i konfigurację systemu IDS, zarządzanie sondami, interpretację alarmów i incydentów, zarządzanie użytkownikami i uprawnieniami, aktualizacje oraz podstawową diagnostykę. Szkolenie zakończy się przekazaniem materiałów szkoleniowych w języku polskim. Termin szkolenia zostanie uzgodniony z Zamawiającym w ramach harmonogramu.

Wsparcie serwisowe i poziomy SLA.

Wykonawca zapewni wsparcie serwisowe zgodnie z umową. Czasy reakcji liczone od zgłoszenia wynoszą co najmniej: dla awarii krytycznej (brak działania systemu IDS lub utrata monitorowania) – reakcja do 4 godzin w dni robocze i przystąpienie do usuwania niezwłocznie; dla awarii istotnej (ograniczona funkcjonalność) – reakcja do 8 godzin roboczych; dla usterki oraz zgłoszeń zwykłych – reakcja do 2 dni roboczych. Zgłoszenia przyjmowane są co najmniej za pośrednictwem poczty elektronicznej oraz telefonicznie w godzinach roboczych. Szczegółowe warunki wsparcia i gwarancji określa wzór umowy.

Potwierdzenie zgodności oferowanego rozwiązania z OPZ.

Wykonawca potwierdzi spełnienie wszystkich wymagań OPZ poprzez wypełnienie formularza wymagań (tabeli zgodności) stanowiącego załącznik do zapytania, wskazując dla każdego wymagania sposób jego spełnienia oraz nazwę, model i wersję oferowanego rozwiązania. Na żądanie Zamawiającego Wykonawca przedstawi karty katalogowe, dokumentację producenta lub oświadczenia potwierdzające deklarowane parametry.

Dokumentacja powykonawcza.

Dokumentacja powykonawcza zostanie przekazana w języku polskim, w formie edytowalnej oraz PDF, przed podpisaniem protokołu odbioru końcowego, i obejmie co najmniej: opis wdrożonej architektury rozwiązania i topologii podłączenia sond, konfigurację systemu IDS i sond sprzętowych, wykaz kont i uprawnień, wykaz haseł przekazany w sposób zabezpieczony, procedury eksploatacyjne i aktualizacyjne, protokoły z testów akceptacyjnych oraz dane kontaktowe wsparcia producenta. Dokumentację powykonawczą Wykonawca prześle nie później niż w terminie 14 dni kalendarzowych od zakończenia prac wdrożeniowych, zgodnie z pkt 10 powyżej oraz § 4 ust. 1 lit. b wzoru umowy, przed podpisaniem protokołu odbioru końcowego.