

Załącznik nr 10 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

w postępowaniu prowadzonym w trybie otwartej procedury konkurencyjnej pn.
**„Wdrożenie kompleksowych rozwiązań w zakresie cyberbezpieczeństwa
dla Przedsiębiorstwa Komunalnego w Tucholi Sp. z o.o.,
w ramach projektu „Cyberbezpieczne Wodociągi”**

CZĘŚĆ IV – Dostawa oprogramowania IDS wraz z niezbędnymi licencjami i wdrożeniem

Przedmiotem zamówienia jest dostawa i wdrożenie systemu monitorowania bezpieczeństwa sieci IT/OT/ICS wraz z sondami monitorującymi, szkoleniem i wsparciem technicznym

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja i uruchomienie kompletnego systemu klasy IDS/NDR przeznaczonego do pasywnego monitorowania bezpieczeństwa sieci przemysłowej IT/OT/ICS Zamawiającego.

System ma umożliwiać w szczególności automatyczną identyfikację zasobów OT, analizę komunikacji sieciowej, wykrywanie anomalii, zagrożeń i nieautoryzowanej aktywności oraz wspomagać analizę incydentów bezpieczeństwa.

Przedmiot zamówienia obejmuje co najmniej:

1. dostawę licencji systemu centralnego zarządzania i analizy umożliwiającej monitorowanie minimum 80 urządzeń fizycznych OT/ICS,
2. dostawę minimum 3 niezależnych sond sprzętowych przeznaczonych do pasywnego monitorowania ruchu sieciowego,
3. instalację i konfigurację systemu,
4. instalację i konfigurację sond,
5. integrację sond z systemem centralnym,
6. wykonanie wstępnej inwentaryzacji monitorowanej infrastruktury,
7. utworzenie mapy urządzeń i komunikacji,
8. konfigurację podstawowych reguł, alarmów i mechanizmów detekcji,
9. przeprowadzenie testów poprawności działania,
10. wykonanie dokumentacji powdrożeniowej,
11. przeprowadzenie szkolenia administratorów,
12. zapewnienie aktualizacji, gwarancji i wsparcia technicznego przez okres minimum 36 miesięcy.

Dostarczone rozwiązanie musi stanowić kompletny, wzajemnie kompatybilny system, gotowy do użytkowania po zakończeniu wdrożenia.

2. Architektura rozwiązania

System musi składać się co najmniej z:

- centralnego komponentu zarządzającego i analitycznego,
- minimum 3 sond monitorujących ruch sieciowy,
- interfejsu administracyjnego umożliwiającego centralne zarządzanie całym rozwiązaniem.

System musi umożliwiać monitorowanie minimum 80 urządzeń fizycznych występujących w sieci OT/ICS Zamawiającego.

Dopuszcza się rozwiązanie licencjonowane:

- według liczby monitorowanych urządzeń,
- według liczby sond,

pod warunkiem zapewnienia pełnej wymaganej funkcjonalności dla minimum 80 urządzeń oraz minimum 3 punktów monitorowania.

Centralny komponent systemu może być dostarczony jako urządzenie fizyczne, maszyna wirtualna lub rozwiązanie równoważne umożliwiające pracę w infrastrukturze Zamawiającego.

System musi działać lokalnie w infrastrukturze Zamawiającego (on-premise).

Podstawowe funkcje monitorowania, detekcji i analizy bezpieczeństwa nie mogą wymagać stałego połączenia z usługami chmurowymi producenta.

3. Pasywne monitorowanie sieci OT

System musi prowadzić monitoring sieci OT w sposób pasywny.

Monitorowanie nie może wymagać:

- instalowania agentów na monitorowanych urządzeniach OT,
- aktywnego skanowania urządzeń w normalnym trybie monitorowania,
- ingerencji w konfigurację sterowników PLC, urządzeń automatyki lub systemów SCADA,
- modyfikowania analizowanego ruchu sieciowego.

Sondy muszą umożliwiać analizę kopii ruchu przekazywanej co najmniej poprzez port SPAN/Mirror przełącznika sieciowego lub urządzenie TAP.

Awaria sondy monitorującej nie może powodować przerwania komunikacji pomiędzy monitorowanymi urządzeniami OT.

4. Automatyczna inwentaryzacja infrastruktury OT

System musi automatycznie identyfikować urządzenia komunikujące się w monitorowanej sieci.

Dla wykrytych urządzeń system powinien umożliwiać prezentację co najmniej:

- adresu IP,
- adresu MAC, jeżeli informacja jest dostępna,
- nazwy urządzenia lub hosta, jeżeli jest możliwa do ustalenia,
- producenta urządzenia, jeżeli jest możliwy do ustalenia,
- rodzaju lub kategorii urządzenia,
- wykorzystywanych protokołów,
- usług sieciowych,
- informacji o komunikacji z innymi urządzeniami,
- czasu pierwszej i ostatniej obserwacji urządzenia.

System musi umożliwiać prowadzenie aktualizowanej automatycznie inwentaryzacji zasobów OT.

Administrator musi mieć możliwość uzupełniania lub korygowania informacji dotyczących wykrytych urządzeń.

5. Wizualizacja infrastruktury i komunikacji

System musi automatycznie tworzyć mapę urządzeń oraz występujących pomiędzy nimi połączeń.

Mapa musi umożliwiać co najmniej:

- wizualizację wykrytych urządzeń,
- prezentację komunikacji pomiędzy urządzeniami,
- identyfikację wykorzystywanych protokołów,

- identyfikację nowych lub wcześniej niewystępujących połączeń.

Administrator powinien mieć możliwość filtrowania prezentowanych informacji oraz przechodzenia z mapy do szczegółowych informacji dotyczących urządzenia lub komunikacji.

6. Analiza komunikacji OT/ICS

System musi umożliwiać analizę protokołów stosowanych w sieciach IT oraz OT/ICS.

Wymagana jest obsługa protokołów odpowiednich dla środowiska Zamawiającego, w szczególności protokołów przemysłowych wykorzystywanych przez urządzenia automatyki, sterowniki PLC, systemy SCADA, urządzenia pomiarowe i systemy telemetryczne.

System powinien umożliwiać rozbudowę obsługi protokołów poprzez aktualizacje producenta bez konieczności wymiany sond sprzętowych, o ile wymagania sprzętowe nowych wersji nie przekroczą możliwości dostarczonych urządzeń.

7. Wykrywanie zagrożeń i anomalii

System musi umożliwiać wykrywanie co najmniej:

- pojawienia się nowego urządzenia w monitorowanej sieci,
- nowych połączeń pomiędzy urządzeniami,
- nietypowych zmian komunikacji,
- komunikacji z nieznanymi lub nieautoryzowanymi urządzeniami,
- zmian sposobu wykorzystania protokołów,
- prób skanowania sieci,
- podejrzanej aktywności sieciowej,
- zdarzeń mogących wskazywać na próbę ataku,
- znanych zagrożeń rozpoznawanych przez mechanizmy detekcyjne systemu.

System musi umożliwiać wykorzystanie mechanizmów opartych co najmniej na:

- regułach i sygnaturach,
- analizie zachowania urządzeń i komunikacji,
- wykrywaniu odstępstw od wcześniej obserwowanego sposobu działania sieci.

System powinien umożliwiać określanie poziomu istotności lub ryzyka wykrytych zdarzeń.

8. Monitoring parametrów i zmian w środowisku OT

System powinien umożliwiać obserwowanie zmian dotyczących komunikacji przemysłowej oraz parametrów możliwych do odczytania z analizowanego ruchu sieciowego.

W przypadku protokołów umożliwiających taką analizę system powinien pozwalać na wykrywanie nietypowych lub nieoczekiwanych zmian wartości lub sposobu komunikacji urządzeń OT.

Funkcja ta nie może wymagać instalowania agentów na urządzeniach końcowych.

9. Podatności i informacje o zagrożeniach

System musi umożliwiać identyfikację potencjalnych podatności wykrytych urządzeń na podstawie informacji możliwych do pozyskania z monitorowanego ruchu oraz bazy wiedzy producenta.

System powinien umożliwiać prezentację co najmniej:

- urządzenia, którego może dotyczyć podatność,
- identyfikatora podatności CVE, jeżeli jest dostępny,
- poziomu ryzyka lub istotności,
- opisu podatności.

Baza informacji o podatnościach i zagrożeniach musi być aktualizowana w okresie obowiązywania wsparcia.

10. Alarmy i obsługa zdarzeń

System musi posiadać centralny mechanizm obsługi alarmów.

Dla alarmu powinny być dostępne co najmniej:

- data i czas wystąpienia,
- źródło zdarzenia,
- urządzenie lub urządzenia uczestniczące w zdarzeniu,
- typ zdarzenia,
- poziom istotności,
- opis zdarzenia.

Administrator musi mieć możliwość:

- przeglądania alarmów,
- filtrowania alarmów,
- wyszukiwania zdarzeń,
- potwierdzania lub zmiany statusu alarmu,
- analizowania historii zdarzeń.

11. Integracja z systemami zewnętrznymi

System musi umożliwiać przekazywanie informacji o zdarzeniach do zewnętrznych systemów bezpieczeństwa.

Wymagana jest możliwość integracji co najmniej poprzez jeden lub kilka powszechnie stosowanych mechanizmów, takich jak:

- Syslog,
- API REST,
- SNMP,
- webhook,
- format CEF lub równoważny.

Rozwiązanie powinno umożliwiać integrację z systemami klasy SIEM/SOC oraz innymi systemami monitorowania bezpieczeństwa.

12. Sondy monitorujące

Należy dostarczyć minimum 3 kompletne sondy sprzętowe.

Każda sonda musi:

- być przeznaczona do ciągłego monitorowania ruchu sieciowego,
- posiadać co najmniej jeden interfejs umożliwiający odbiór monitorowanego ruchu,
- posiadać interfejs umożliwiający komunikację z centralnym systemem,
- umożliwiać pracę w sieciach Ethernet,
- pracować bez konieczności instalowania dodatkowego oprogramowania na monitorowanych urządzeniach,
- umożliwiać centralne zarządzanie,
- przysyłać wyniki analiz lub dane wymagane przez centralny system w sposób zabezpieczony przed nieuprawnionym dostępem,
- sonda sprzętowa powinna posiadać pasywny interfejs monitorujący RS485, RS422, RS232.
- sonda posiadać powinna co najmniej jeden interfejs monitorujący RJ45 Ethernet o przepustowości co najmniej 100Mbps (sonda negocjuje z siecią prędkość pomiędzy 10Mbps a 100Mbps) pracujący w trybie „Span-port” (dwa interfejsy RJ45 w trybie „pass-through”),
- interfejs komunikacyjny sondy powinien wspierać DHCP,
- powinna istnieć możliwość rozbudowy systemu w przyszłości o sondy softwarowe, które można zainstalować w środowisku LINUX,

- wymagane jest podtrzymanie baterijne sondy oraz zasilanie sondy napięciem stałym. Sonden muszą być fabrycznie nowe i objęte wsparciem producenta przez minimum 36 miesięcy. Dopuszcza się sondy o konstrukcji przeznaczonej do montażu w szafie RACK, na szynie DIN lub innej konstrukcji odpowiedniej dla miejsca instalacji.

13. Bezpieczeństwo systemu

Komunikacja pomiędzy sondami a systemem centralnym musi być zabezpieczona przed nieuprawnionym dostępem.

System musi posiadać:

- mechanizm uwierzytelniania użytkowników,
- możliwość tworzenia kont administratorów,
- możliwość różnicowania uprawnień użytkowników,
- rejestrowanie istotnych czynności administracyjnych,
- mechanizmy aktualizacji oprogramowania.

Interfejs administracyjny powinien wykorzystywać szyfrowaną komunikację HTTPS lub rozwiązanie równoważne.

14. Wdrożenie

W ramach realizacji zamówienia Wykonawca wykona co najmniej:

1. analizę środowiska Zamawiającego w zakresie niezbędnym do wdrożenia,
2. uzgodnienie miejsc instalacji sond,
3. instalację systemu centralnego,
4. instalację 3 sond,
5. konfigurację komunikacji sond z systemem centralnym,
6. konfigurację monitorowania wskazanych segmentów sieci OT,
7. uruchomienie automatycznej inwentaryzacji,
8. przygotowanie początkowej mapy urządzeń i komunikacji,
9. konfigurację podstawowych alarmów i reguł bezpieczeństwa,
10. dostosowanie konfiguracji do specyfiki środowiska Zamawiającego,
11. wykonanie testów działania,
12. usunięcie stwierdzonych podczas testów nieprawidłowości,
13. przekazanie systemu do eksploatacji.

Wdrożenie nie może powodować niezgodzonych przerw w funkcjonowaniu infrastruktury technologicznej Zamawiającego.

15. Dokumentacja powdrożeniowa

Po zakończeniu wdrożenia Wykonawca przekaze dokumentację obejmującą co najmniej:

- opis wdrożonego rozwiązania,
- schemat logiczny rozwiązania,
- lokalizację sond,
- opis konfiguracji systemu,
- sposób komunikacji sond z systemem centralnym,
- podstawowe procedury administracyjne,
- procedurę wykonywania aktualizacji,
- procedurę zgłaszania problemów do wsparcia technicznego.

Dokumentacja musi zostać dostarczona w języku polskim w formie elektronicznej.

16. Szkolenie

Wykonawca przeprowadzi szkolenie dla minimum 2 administratorów Zamawiającego.

Szkolenie musi obejmować co najmniej:

- architekturę rozwiązania,
- obsługę interfejsu administracyjnego,
- analizę wykrytych urządzeń,
- korzystanie z mapy sieci,
- analizę komunikacji,
- obsługę alarmów,
- analizę zdarzeń bezpieczeństwa,
- podstawową konfigurację reguł i alarmów,
- generowanie raportów,
- podstawową diagnostykę systemu.

Szkolenie może zostać przeprowadzone stacjonarnie lub zdalnie, jeżeli Zamawiający dopuści taką formę.

Materiały szkoleniowe należy przekazać w języku polskim.

17. Licencja, aktualizacje i wsparcie

Wykonawca zapewni przez minimum do dnia 31.12.2026 od odbioru systemu:

- prawo do użytkowania systemu dla minimum 80 monitorowanych urządzeń,
- prawo do użytkowania wszystkich 3 dostarczonych sond,
- aktualizacje oprogramowania,
- aktualizacje mechanizmów detekcyjnych,
- aktualizacje informacji o podatnościach i zagrożeniach,
- poprawki bezpieczeństwa,
- dostęp do nowych wersji oprogramowania w ramach wykupionego poziomu wsparcia,
- wsparcie techniczne producenta lub autoryzowanego partnera.

Wsparcie musi obejmować co najmniej możliwość zgłaszania incydentów i problemów technicznych drogą elektroniczną.

Dla awarii krytycznych uniemożliwiających korzystanie z systemu wymagany czas podjęcia zgłoszenia nie może przekraczać 1 dnia roboczego.

18. Wymagania dotyczące licencji

Wszystkie wymagane licencje muszą zostać dostarczone legalnie i pochodzić z oficjalnego kanału dystrybucji producenta.

Licencja musi obejmować minimum 80 urządzeń fizycznych OT/ICS.

Dopuszcza się zaoferowanie licencji bez limitu liczby urządzeń.

Jeżeli do realizacji wymaganych funkcjonalności konieczne są dodatkowe licencje, moduły lub subskrypcje, Wykonawca musi uwzględnić je w cenie oferty na cały okres realizacji projektu.

Zamawiający nie może być zobowiązany do zakupu dodatkowych licencji niezbędnych do realizacji funkcjonalności określonych w OPZ.

20. Wymagania w zakresie posiadanych przez Wykonawcę certyfikowanych systemów zarządzania:

ISO 20000-1 lub równoważne w zakresie: sprzedaży technicznych systemów bezpieczeństwa. Projektowania i wdrażania rozwiązań informatycznych

b) ISO 27001 lub równoważne w zakresie: sprzedaży technicznych systemów bezpieczeństwa. Projektowania i wdrażania rozwiązań informatycznych

c) ISO 9001 lub równoważne - w zakresie: sprzedaży technicznych systemów bezpieczeństwa. Projektowania i wdrażania rozwiązań informatycznych

d) ISO 14001 lub równoważne w zakresie: sprzedaży technicznych systemów bezpieczeństwa. Projektowania i wdrażania rozwiązań informatycznych

23. Odbiór

Warunkiem odbioru będzie co najmniej:

- zainstalowanie systemu centralnego,
- uruchomienie wszystkich 3 sond,
- potwierdzenie komunikacji sond z systemem centralnym,
- wykrywanie urządzeń znajdujących się w monitorowanych segmentach,
- utworzenie mapy komunikacji,
- potwierdzenie generowania zdarzeń i alarmów,
- wykonanie testu integracji z systemem zewnętrznym, jeżeli integracja będzie wymagana przez Zamawiającego,
- przeprowadzenie szkolenia,
- przekazanie dokumentacji,
- przekazanie wymaganych licencji i danych dotyczących wsparcia.

Z odbioru zostanie sporządzony protokół odbioru i przekazany Zamawiającemu.

Oświadczenie Wykonawcy.

Oświadczam, że składając ofertę świadom jestem jej złożenia i zapewniam, że wykonam zamówienie zgodnie z oczekiwaniami Zamawiającego.

Składając ofertę oświadczam, że spełniam warunki udziału w postępowaniu.

Oświadczam, że wykonam zamówienie zgodnie z wymaganiami zawartymi w niniejszym Opisie Przedmiotu Zamówienia.

....., dnia