

Załącznik nr 5 do IWZ**OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)**

Przedmiotem zamówienia jest audyt, dostawa, wdrożenie, szkolenie i uruchomienie dedykowanych sond sprzętowych oraz systemu klasy IDS dla protokołów przemysłowych warstwy OT w zakresie systemu SCADA obejmującego produkcję wody w ZUW I, ZUW III i ZUW V.

1. Audyt bezpieczeństwa środowiska OT

Wykonawca przed przystąpieniem do wdrożenia przeprowadzi audyt (weryfikację architektury sieciowej) infrastruktury SCADA w obiektach ZUW I, ZUW III i ZUW V. Badanie zostanie zakończone raportem z rekomendacjami optymalizacyjnymi. Forma i zakres raportu musi być zaakceptowany przez wskazany personel Zamawiającego.

2. Sondy sprzętowe IDS dla środowiska przemysłowego – 3 szt.:

- 1) obudowa i konstrukcja: Przemysłowa, wzmocniona obudowa (np. aluminium/metal); brak ruchomych części mechanicznych (w tym dysków HDD – wymagane nośniki SSD/eMMC); chłodzenie pasywne (bez wentylatorów – fanless);
- 2) montaż: przystosowana do montażu w szafach automatyki na standardowej szynie DIN (DIN-rail 35mm);
- 3) wydajność (przepustowość): przepustowość analizy ruchu w warstwie aplikacji (DPI - Deep Packet Inspection) na poziomie minimum 100 Mbps;
- 4) wpływ na sieć (opóźnienia): praca w trybie w pełni pasywnym (out-of-band / SPAN / TAP). Sonda nie może wprowadzać żadnych opóźnień (0 ms) do ruchu sterującego w sieci produkcyjnej OT ani stanowić punktu awarii (Single Point of Failure);
- 5) Interfejsy sieciowe: minimum 3 porty 10/100/1000Base-T (RJ-45), w tym min. 1 port dedykowany wyłącznie do pasywnego nasłuchu (konektory SPAN z przełączników przemysłowych), min. 1 port izolowany galwanicznie/logicznie, dedykowany do zarządzania i bezpiecznej komunikacji z centralnym systemem IDS;
- 6) Zasilanie: obsługa standardowych napięć w szafach automatyki (np. w zakresie 12V – 48V DC). Maksymalny pobór mocy nie większy niż 50 W;
- 7) Warunki środowiskowe pracy: zakres temperatur pracy: od 0°C do +60°C, wilgotność względna: od 5% do 95% (bez kondensacji). Stopień ochrony obudowy: minimum IP30;
- 8) Odporność i certyfikaty : odporność na wstrząsy i wibracje zgodna ze standardami przemysłowymi (np. IEC 60068). Odporność na zakłócenia elektromagnetyczne (EMI/EMC) spotykane w obiektach wodociągowych i przepompowniach (zgodność m.in. z CE, FCC, lub normami EN 61000-6-2/EN 61000-6-4);

- 9) Rozpoznawane protokoły OT: natywne wsparcie (wbudowane dekodery DPI) dla protokołów stosowanych w systemach SCADA, w tym obowiązkowo: Modbus TCP, PROFINET, DNP3, IEC 60870-5-104;
- 10) Gwarancja i Serwis: minimum 5 lat gwarancji na sprzęt. Serwis realizowany w systemie door-to-door lub wymiana sprzętu w trybie NBD (Next Business Day).

3. **Centralny System klasy IDS dla warstwy OT – 1 szt.**

System będzie pełnił rolę centralnego punktu zarządzania, analizy i korelacji zdarzeń zbieranych przez sondy sprzętowe zlokalizowane na obiektach ZUW I, ZUW III i ZUW V. System wdrożony lokalnie (on-premise) na infrastrukturze wirtualnej Zamawiającego (dostarczony w formie wirtualnego urządzenia - Virtual Appliance). Licencja musi obejmować zarządzanie minimum 3 sondami sprzętowymi (z możliwością rozbudowy) oraz monitorowanie minimum 500 urządzeń końcowych (węzłów/zasobów IP/MAC) bez ograniczeń czasowych (licencja wieczysta). System musi umożliwiać co najmniej:

- 1) Wykrywanie i mapowanie zasobów (Asset Discovery): Pasywne, zautomatyzowane wykrywanie urządzeń w sieci OT bez aktywnego skanowania (Zero-impact). System musi tworzyć i aktualizować w czasie rzeczywistym interaktywną mapę topologii sieci SCADA. Identyfikacja atrybutów zasobów: adres IP, adres MAC, producent, model urządzenia, typ urządzenia (PLC, HMI, stacja inżynierska), wersja oprogramowania układowego (firmware). Rozpoznawanie i dekodowanie protokołów wykorzystywanych w MPWiK (np. Modbus TCP, PROFINET, S7, DNP3, IEC 104). Integracje/wyjścia alertów (np. Syslog) do nadrzędnego systemu SIEM;
- 2) Analiza behawioralna i wykrywanie anomalii: tworzenie modelu bazowego (tzw. baseline) normalnego ruchu sieciowego w procesie uczenia maszynowego. Wykrywanie odstępstw od modelu bazowego, w tym: nieznanych połączeń, nowych urządzeń, nietypowych wolumenów ruchu, prób skanowania sieci. Możliwość ręcznego dostrajania modelu bazowego przez administratora (akceptowanie wykrytych zmian jako nowych standardów);
- 3) Monitorowanie logiki i parametrów procesu (DPI): wykrywanie i alertowanie o specyficznych zdarzeniach inżynierskich w sterownikach PLC: zmiana trybu pracy sterownika (np. zmiana ze stanu RUN na STOP/PROGRAM); wgrywanie lub pobieranie programu z/do sterownika (Upload/Download logic), wymuszanie wartości zmiennych i rejestrów krytycznych dla procesu uzdatniania wody, zmiany w konfiguracji sprzętowej;
- 4) Wykrywanie zagrożeń (Threat Detection): wykrywanie znanych wektorów ataków i złośliwego oprogramowania na podstawie bazy sygnatur dedykowanej dla środowisk ICS/OT (np. Industroyer, BlackEnergy, Stuxnet, ransomware). Wykrywanie prób wykorzystania znanych luk bezpieczeństwa (CVE) dla urządzeń automatyki przemysłowej. Baza sygnatur aktualizowana w trybie offline lub poprzez wydzielony, bezpieczny kanał;

- 5) Alertowanie i Integracja: kategoryzacja incydentów według stopnia krytyczności (np. informacyjne, ostrzeżenia, krytyczne). Wbudowane mechanizmy powiadomień e-mail. Możliwość przekazywania logów i zdarzeń bezpieczeństwa do nadrzędnego systemu SIEM za pomocą standardowych protokołów (np. Syslog w formacie CEF lub LEEF);
 - 6) Retencja danych i analiza śledcza (Forensics): przechowywanie metadanych o ruchu sieciowym, logów zdarzeń oraz alertów przez okres minimum 12 miesięcy. Możliwość pobierania zrzutów ruchu (plików PCAP) powiązanych z krytycznymi alertami w celu przeprowadzenia dogłębnej analizy śledczej przez administratorów;
 - 7) Zarządzanie i Administracja: dostęp do konsoli zarządzającej poprzez bezpieczny interfejs webowy (HTTPS/TLS) z weryfikacją tożsamości. Obsługa ról i uprawnień opartych na profilach użytkowników (RBAC – Role-Based Access Control) z podziałem minimum na: Administrator Systemu, Analityk Bezpieczeństwa (Read/Write), Obserwator (Read-Only). Wsparcie dla uwierzytelniania w oparciu o zewnętrzny katalog usług (np. Active Directory / LDAP).
4. **Testy powdrożeniowe, odbiór systemu, szkolenia** - po dokonaniu całości wdrożenia należy przeprowadzić testy poprawności działania całej infrastruktury oraz przeszkolić wskazany personel Zamawiającego (nie więcej niż 5 osób). Ze względu na ciągłość produkcji wody (aplikacje i systemy krytyczne), Wykonawca przeprowadzi testy funkcjonalne oraz testy podatności (bezpieczeństwa) w sposób rygorystycznie dostosowany do specyfiki środowiska OT, gwarantujący brak wpływu na proces technologiczny na obiektach ZUW I, ZUW III i ZUW V.
- 1) Testy funkcjonalne systemu IDS: weryfikacja poprawności mirrorowania ruchu (SPAN) – potwierdzenie, że sondy sprzętowe otrzymują pełną kopię ruchu sieciowego z przełączników bez wprowadzania opóźnień i zakłóceń;
 - 2) Weryfikacja funkcji Asset Discovery – sprawdzenie, czy system centralny prawidłowo wykrył i zmapował urządzenia przemysłowe (sterowniki PLC, stacje HMI, serwery SCADA);
 - 3) Symulacja incydentu (w kontrolowanym środowisku): Wykonawca z wyizolowanego, testowego komputera podłączonego do wydzielonego portu przełącznika wygeneruje ruch przypominający atak (np. nieautoryzowane polecenie zatrzymania dla protokołu Modbus TCP/S7), aby udowodnić, że system IDS poprawnie wykryje anomalię i wygeneruje alert o odpowiednim priorytecie. Log z anomalii powinien być automatycznie przekazany do nadrzędnego systemu SIEM;
 - 4) Testy podatności i bezpieczeństwa sieci (Dostosowane do OT): Wykonawca przeprowadzi testy polegające na weryfikacji podatności wdrożonego systemu IDS oraz urządzeń sieciowych na ataki przeprowadzane z zewnątrz i wewnątrz infrastruktury;
 - 5) Badanie bezpieczeństwa obejmie punkty styku z sieciami obcymi (firewalle IT/OT). Dla systemów operacyjnych pełniących rolę serwerów zarządzających IDS (np. środowisko Linux lub Windows) dopuszcza się klasyczne testy bezpieczeństwa. Dla sieci produkcyjnej OT testy

podatności będą polegały wyłącznie na analizie pasywnej. System IDS zidentyfikuje wersje oprogramowania firmware sterowników na podstawie podsłuchanego ruchu i zestawia je ze znanymi bazami luk (CVE), bez wysyłania do nich jakichkolwiek zapytań skanujących;

- 6) Ponadto Wykonawca przeprowadzi badanie bezpieczeństwa sieci systemów komputerowych, które pozwoli na określenie błędów w konfiguracji skutkujących powstaniem podatności na atak oraz wskazanie nadmiernych uprawnień, niezgodnych z zasadami dobrych praktyk. Skanowanie obejmie urządzenia dedykowane, na przykład routery i przełączniki przemysłowe (w sposób niezakłócający ich pracy);
- 7) Dokumentacja i raportowanie: Wykonawca zobowiązany jest przygotować dokumentację powykonawczą zawierającą listę dostarczonego sprzętu wraz z numerami seryjnymi i opisem konfiguracji poszczególnych elementów systemów. Wykonawca dostarczy certyfikat zgodności zastosowanego wdrożenia z dyrektywą NIS2. Badanie i testy zostaną zakończone zbiorczym raportem. Forma i zakres raportu musi być zaakceptowany przez wskazany personel Zamawiającego przed zakończeniem projektu.

ZAMAWIAJĄCY

WYKONAWCA