**Załącznik nr 6**

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Dotyczy: Zakupu, dostawy i wdrożenia systemu IDS/OT do monitorowania sieci automatyki przemysłowej

# 1. Przedmiot zamówienia

Przedmiotem zamówienia jest kompleksowa dostawa, wdrożenie oraz uruchomienie systemu klasy IDS (Intrusion Detection System) dedykowanego do monitorowania i zabezpieczania sieci przemysłowych OT (Operational Technology). System musi umożliwiać pasywną analizę ruchu sieciowego oraz wykrywanie anomalii, zagrożeń i podatności w sieciach automatyki przemysłowej.

W ramach realizacji należy:

* dostarczyć i skonfigurować 20 zestawów zbierania danych poprzez port SPAN SPAN (Switched Port Analyzer), umożliwiający kopiowanie ruchu sieciowego ze zdalnych lokalizacji poprzez tunel IPSEC do centrali Witomińska 29,
* centralny firewall zagreguje ruch z wszystkich jednostek terenowych i przekaże go na dedykowany port SPAN, podłączony do systemu NDR,
* w 7 wybranych lokalizacjach, gdzie funkcjonują już zestawy do zbierania danych zamawiającego, konieczna jest jedynie konfiguracja portów SPAN oraz przekierowanie kopiowanego ruchu do systemu analizy, z pominięciem potrzeby wymiany sprzętu,
* wsparcie techniczne , dostęp do wszelkich poprawek i aktualizacji systemu przez okres 36 miesięcy.

Obraz zawierający diagram, linia, tekst, Rysunek techniczny

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

# 2. Wymagania ogólne

1. Wymagane jest, aby producent systemu posiadał w Unii Europejskiej autoryzowaną jednostkę wsparcia technicznego i serwisowego.

2. Wykonawca zobowiązany jest zapewnić wsparcie techniczne przez okres 36 miesięcy od momentu podpisania protokołu odbioru końcowego, w ramach którego dostępne będzie:

* + - * prawo do aktualizacji oprogramowania,
      * dostęp do bazy wiedzy i dokumentacji w języku polskim,
      * możliwość zgłoszeń serwisowych w trybie awaryjnym w języku polskim.

1. Całość komunikacji w systemie (sondy–serwer, użytkownik–interfejs) musi być szyfrowana z wykorzystaniem protokołu TLS i/lub PKI.
2. Oprogramowanie systemu musi być dostarczone w wersji umożliwiającej pełne działanie offline, bez konieczności połączenia z Internetem.
3. Wszystkie komponenty sprzętowe muszą być fabrycznie nowe, nieużywane, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostawy.
4. Wykonawca dostarczy oświadczenie o braku zastosowania komponentów wycofanych z eksploatacji (EOL) oraz zawierających znane, nieusunięte podatności (CVE).
5. Wykonawca zobowiązany jest przeprowadzić pełną instalację, uruchomienie oraz konfigurację całego systemu we wskazanych lokalizacjach Zamawiającego.
6. System nie może wprowadzać żadnych zmian w monitorowanym ruchu (całkowicie pasywna praca sond).
7. Wszelkie licencje (na oprogramowanie i sondy) muszą być udzielone w formie wieczystej – bez konieczności odnowień.
8. Rozwiązanie musi być skalowalne – z możliwością łatwej rozbudowy o kolejne sondy i urządzenia monitorowane.
9. Wykonawca zobowiązuje się do przeprowadzenia testów akceptacyjnych zgodnie z zatwierdzonym planem oraz do ich udokumentowania w protokole odbioru.
10. System musi umożliwiać audyt logów administracyjnych i systemowych zgodny z wymaganiami bezpieczeństwa informacji.
11. Wymagane jest wsparcie dla zewnętrznych mechanizmów synchronizacji czasu (NTP).  
    14. Rozwiązanie musi być zgodne z dobrymi praktykami bezpieczeństwa (np. NIST, IEC 62443) oraz wspierać wykrywanie urządzeń i podatności wg słownika CVE/CPE (MITRE/NIST).
12. Wymagana jest zgoda na instalację agenta monitorowania systemu operacyjnego i agenta backupu.

# 3. Minimalny zakres dostawy

1. Fizyczny serwer zoptymalizowany pod kątem wydajności i pojemności (zasób dyskowy przewidziany na 36 miesięcy) w obudowie typu RACK (max 2U) z redundancją zasilania, odpowiednimi interfejsami (LAN 2x10GB/s, FC 32GB/s) i zasobami dyskowymi – RAID 1 dla systemu i danych oraz system zarządzania zdalnego do serwera – IDRAC w wersji Enterprise) wraz z systemem operacyjnym Linux (Red Hat lub Centos w najnowszej wersji ) z gwarancją na 36 miesięcy – Załącznik nr 1.

2. Minimum 20 zestawów do zbierania danych z obiektów zdalnych (zgodny z infrastrukturą zamawiającego) – Załącznik nr 2.

3. Oprogramowanie do analizy i zarządzania ruchem sieciowym OT dla co najmniej 1000 urządzeń.  
4. Licencje wieczyste na cały system wraz z co 36 miesięcznym wsparciem technicznym i aktualizacjami.

# 4. Wymagania funkcjonalne systemu

System powinien zapewniać następujące funkcjonalności:

* pasywną analizę ruchu sieciowego OT,
* wykrywanie anomalii sieciowych i behawioralnych (ML/AI) oraz alarmowania drogą mailową wybranych użytkowników,
* identyfikację urządzeń i protokołów OT (Modbus, DNP3, OPC UA, itp.),
* mapowanie topologii i graficzną prezentację komunikacji,
* możliwość eksportu danych (PCAP lub CSV lub PDF),
* wykonanie pełnej inwentaryzacji urządzeń,
* powinien pozwalać na realizacje DPI – głębokiej analizy pakietów – dla najważniejszych protokołów OT (co najmniej MODBUS oraz DNP3) w warstwie od 2 do 7,
* powinien wyrywać następujące typy zagrożeń:

1. oprogramowanie złośliwe (malware) w tym tzw. „zero-day”,
2. atak DOS/DDOS,
3. atak typu APT,
4. skanowanie sieci, oprogramowanie typu Spyware,
5. zagrożenia typu MitM „Man-in-the-Middle”,

* wykrywanie ataków MITM, DOS, APT, malware oraz innych zagrożeń,
* powinien integrować się z zaporą sieciową FortiGate w celu wysłania komendy blokowania ruchu,
* system musi identyfikować wszystkie urządzenia podłączone do sieci, w tym urządzenia końcowe, serwery, urządzenia IoT itp. Jednocześnie system musi być w stanie zidentyfikować zmiany w sieci - co najmniej:

1. zmiana adresu IP hosta,
2. zduplikowany adres MAC,
3. zmiana sieci VLAN,
4. wykrycie nowej podsieci,
5. podłączenie nowego urządzenia,
6. wykorzystanie lub utworzenie nowej usługi,
7. niedostępność poprzednio dostępnej i komunikującej się usługi lub poprzednio dostępnego i komunikującego się urządzenia,
8. dostęp urządzenia sieciowego do nowej usługi,

* musi mieć możliwość identyfikacji niestandardowego zachowania sieci w oparciu o matematyczny model urządzenia i jego usług, w szczególności odchyleń od normalnego modelu zachowania:

1. odchylenie od modelu transmisji danych, przepływu i pakietów,
2. odchylenie od modelu dla liczby partnerów komunikacyjnych,
3. odchylenie od modelu entropii na portach komunikacyjnych,
4. odchylenie od modelu dla liczby przepływów sieciowych i wykorzystywanych usług sieciowych,
5. odchylenie od modelu wydajności sieci (szybkość transferu) i modelu wydajności aplikacji (czas odpowiedzi).

* integrację z FortiSIEM zamawiającego (Syslog: RFC3164, 5424, 5425),
* zarządzanie uprawnieniami i kontami użytkowników,
* interfejs webowy w języku polskim i angielskim, działający w przeglądarkach Chrome/Edge.

# 5. Testy i odbiory

System podlega testom akceptacyjnym zgodnie z planem testowym. Testy muszą weryfikować zarówno funkcjonalność techniczną (DPI, ML, komunikacja), jak i zgodność z wymaganiami formalnymi. Wyniki testów zostaną ujęte w Protokole Odbioru Systemu, podpisanym przez Zamawiającego i Wykonawcę.

# 6. Szkolenie i dokumentacja

Wykonawca przeprowadzi szkolenie użytkowników końcowych oraz administratorów systemu, w języku polskim, w siedzibie Zamawiającego ( minimum 3 dni robocze). Do obowiązków Wykonawcy należy również przekazanie dokumentacji powdrożeniowej, zawierającej:

* strukturę haseł i dostępów,
* opis działania systemu i komponentów,
* konfigurację i instrukcję instalacji,
* licencje i certyfikaty (w tym CE, RoHS).

Załączniki:

1. Załącznik nr 1\_Specyfikacja funkcjonalna serwera klasy enterprise,
2. Załącznik nr 2\_Opis funkcjonalny zestawu do ochrony i przełączania sieciowego.