

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Dotyczy postępowania pn.:

„Zwiększenie cyberodporności i ciągłości działania Zabrzeńskiego Przedsiębiorstwa Wodociągów i Kanalizacji Sp. z o.o. w Zabrzu poprzez wdrożenie nowoczesnych rozwiązań, modernizację infrastruktury oraz podniesienie kompetencji personelu –

Zadanie 4 Obszar techniczny OT.

Kategoria kosztów: OT3, O12.

Postępowanie: 6”

1. Szczegółowe wymagania techniczne:

- Ochrona natywna: System posiada wbudowaną ochronę dedykowaną bezpośrednio dla środowisk oraz aplikacji OT (Operational Technology).
- Rozpoznawanie certyfikatów: Oprogramowanie zawiera mechanizmy automatycznego rozpoznawania certyfikatów oraz plików wykonawczych. Ochrona plików odbywa się bez konieczności ręcznego budowania list, przy jednoczesnym zachowaniu opcji ręcznego wskazania ścieżek dostępu.
- Wsparcie systemów operacyjnych: Wymagane jest pełne wsparcie zarówno dla nowoczesnych systemów, jak i systemów typu Legacy, w tym Windows 2000, Windows XP oraz Windows 7.
- Tryb Standalone: Agent musi posiadać zdolność do pracy autonomicznej bez stałej komunikacji z konsolą centralną oraz bez konieczności dostępu do sieci Internet.
- Aktualizacja offline: Procedura aktualizacji sygnatur bezpieczeństwa w agencie oraz konsoli musi być realizowana bez wymogu podłączenia do Internetu.
- Wydajność systemu: Maksymalne zużycie pamięci RAM przez agenta nie może przekroczyć 600 MB przy uruchomieniu wszystkich usług.
- Kontrola portów USB: Wbudowana funkcja ochrony portów USB oparta na białej liście dopuszczonych nośników z wykorzystaniem metatagów. System musi pozwalać na jednorazowe dopuszczenie urządzenia spoza listy.
- Zaufane aplikacje: Funkcja ograniczania stacji do listy zaufanych aplikacji.
Po instalacji system skanuje zasoby (rejstry, biblioteki dll) i blokuje każde uruchomienie kodu spoza zweryfikowanej listy, odnotowując zdarzenie w logach.
- Detekcja anomalii: Monitorowanie pracy stanowiska w czasie rzeczywistym poprzez porównywanie procesów z unikalnym wzorcem urządzenia. Kontroli podlegają skrypty, zachowania aplikacji oraz logowania użytkowników.
- Tryby zarządzania: Dostępność trybów pozwalających na wyłączenie funkcji, pracę w trybie samej detekcji lub w trybie pełnej ochrony.
- Tryb serwisowy: Umożliwienie bezpiecznego wykonywania aktualizacji systemu przy zachowaniu aktywnej ochrony w tle.
- Konsola zarządzająca: Centralna aplikacja do zarządzania agentami musi być dostarczona w zestawie wraz z licencjami dla agentów.
- Aktualizacja bez restartu: Aplikacja musi pozwalać na aktualizację agentów, polityk oraz sygnatur bez konieczności ponownego uruchamiania stacji komputerowej.
- Kaskadowanie uprawnień: System nadrzędny umożliwia tworzenie osobnych grup dla lokalizacji oraz indywidualnych polityk (np. osobne hasła administracyjne, listy wyjątków USB czy listy aplikacji wyłączonych ze skanowania). System pozwala na wymuszanie polityk globalnych z zachowaniem lokalnych wyłączeń.

2. Okres wsparcia i gwarancji:

- Okres gwarancji oraz aktualizacji sygnatur dla dostarczonego produktu wynosi 5 lat.

- Wymagane wsparcie techniczne udzielane przez producenta lub oficjalnego dystrybutora w języku polskim, w mowie i piśmie (bez pośrednictwa tłumacza AI lub bota).
- Wymagane przedstawicielstwo producenta w Polsce i/lub terenie Unii Europejskiej.
- Potwierdzenie pochodzenia sprzętu z legalnej dystrybucji w Polsce, nie dopuszcza się dostawy sprzętu nie przeznaczonego przez producenta na rynek polski.

3. Oprogramowanie typu EDR dedykowane sieci OT:

A. Szczegółowe wymagania techniczne:

- Ochrona natywna: System posiada wbudowaną ochronę dedykowaną bezpośrednio dla środowisk oraz aplikacji OT (Operational Technology).
- Rozpoznawanie certyfikatów: Oprogramowanie zawiera mechanizmy automatycznego rozpoznawania certyfikatów oraz plików wykonawczych. Ochrona plików odbywa się bez konieczności ręcznego budowania list, przy jednoczesnym zachowaniu opcji ręcznego wskazania ścieżek dostępu.
- Wsparcie systemów operacyjnych: Wymagane jest pełne wsparcie zarówno dla nowoczesnych systemów, jak i systemów typu Legacy, w tym Windows 2000, Windows XP oraz Windows 7.
- Tryb Standalone: Agent musi posiadać zdolność do pracy autonomicznej bez stałej komunikacji z konsolą centralną oraz bez konieczności dostępu do sieci Internet.
- Aktualizacja offline: Procedura aktualizacji sygnatur bezpieczeństwa w agencie oraz konsoli musi być realizowana bez wymogu podłączenia do Internetu.
- Wydajność systemu: Maksymalne zużycie pamięci RAM przez agenta nie może przekroczyć 600 MB przy uruchomieniu wszystkich usług.
- Kontrola portów USB: Wbudowana funkcja ochrony portów USB oparta na białej liście dopuszczonych nośników z wykorzystaniem metatagów. System musi pozwalać na jednorazowe dopuszczenie urządzenia spoza listy.
- Zaufane aplikacje: Funkcja ograniczania stacji do listy zaufanych aplikacji. Po instalacji system skanuje zasoby (rejstry, biblioteki dll) i blokuje każde uruchomienie kodu spoza zweryfikowanej listy, odnotowując zdarzenie w logach.
- Detekcja anomalii: Monitorowanie pracy stanowiska w czasie rzeczywistym poprzez porównywanie procesów z unikalnym wzorcem urządzenia. Kontroli podlegają skrypty, zachowania aplikacji oraz logowania użytkowników.
- Tryby zarządzania: Dostępność trybów pozwalających na wyłączenie funkcji, pracę w trybie samej detekcji lub w trybie pełnej ochrony.
- Tryb serwisowy: Umożliwienie bezpiecznego wykonywania aktualizacji systemu przy zachowaniu aktywnej ochrony w tle.
- Konsola zarządzająca: Centralna aplikacja do zarządzania agentami musi być dostarczona w zestawie wraz z licencjami dla agentów.
- Aktualizacja bez restartu: Aplikacja musi pozwalać na aktualizację agentów, polityk oraz sygnatur bez konieczności ponownego uruchamiania stacji komputerowej.
- Kaskadowanie uprawnień: System nadrzędny umożliwia tworzenie osobnych grup dla lokalizacji oraz indywidualnych polityk (np. osobne hasła administracyjne, listy wyjątków USB czy listy aplikacji wyłączonych ze skanowania). System pozwala na wymuszanie polityk globalnych z zachowaniem lokalnych wyłączeń.

B. Okres wsparcia i gwarancji:

- Okres gwarancji oraz aktualizacji sygnatur dla dostarczonego produktu wynosi 5 lat.
- Wymagane wsparcie techniczne udzielane przez producenta lub oficjalnego dystrybutora w języku polskim, w mowie i piśmie (bez pośrednictwa tłumacza AI lub bota).
- Wymagane przedstawicielstwo producenta w Polsce i/lub terenie Unii Europejskiej.
- Potwierdzenie pochodzenia sprzętu z legalnej dystrybucji w Polsce, nie dopuszcza się dostawy sprzętu nie przeznaczonego przez producenta na rynek polski.

4. Sprzętowe sondy IDS/IPS dedykowane sieci OT

A. Funkcjonalność ochrony i analizy ruchu OT:

- Natywną ochronę systemów typu Legacy, których modernizacja nie jest możliwa,
- Precyzyjne filtrowanie komend sterujących w trybie Deep Packet Inspection (DPI) dla protokołów Modbus TCP, S7COMM, EtherNet/IP, PROFINET oraz DNP3,
- Identyfikację funkcji protokołu Modbus TCP oraz konkretnych rejestrów (na przykład 0x0F Write Multiple Coils),
- Proaktywne wykrywanie anomalii na podstawie analizy relacji i przepływów ruchu sieciowego,
- Funkcję Virtual Patching pozwalającą na ochronę urządzeń przed znanymi podatnościami ZDI oraz CVE bez konieczności ich fizycznej aktualizacji,
- Możliwość płynnego przejścia między trybem pełnej ochrony (IPS) a trybem monitorowania (IDS).

B. Tryb uczenia i konfiguracji reguł:

- Tryb uczenia bazowego ruchu sieciowego pozwalający na automatyczne generowanie reguł na poziomach L2 (MAC), L3 (IP) oraz L7 (Protokoły),
- Kontrolę administratora nad procesem uczenia (tryb nie może pracować w sposób ciągły, a każda reguła wymaga autoryzacji),
- Mechanizm zapobiegający powielaniu istniejących już reguł oraz możliwość ponownego uruchomienia sesji uczenia po modernizacji sieci.

C. Parametry transmisyjne i niezawodność:

- Tryb Hardware Bypass zapewniający przejrzystość i ciągłość transmisji w przypadku awarii zasilania lub usterki sondy,
- Możliwość konfiguracji zachowania bypassu po przywróceniu zasilania (wznowienie ruchu, blokada lub ruch bez skanowania),
- Minimum dwa interfejsy monitorujące RJ45 1000BaseT, które są całkowicie przeźroczyste dla sieci (brak adresów MAC oraz IP),
- Osobny, fizyczny port RJ45 dedykowany wyłącznie do zarządzania urządzeniem
- w standardzie RJ45 1000BaseT,
- Funkcję LFPT (Link Fault Pass Through) synchronizującą status portów w parze monitorującej,
- Maksymalne opóźnienie wprowadzane do sieci nieprzekraczające 520 mikrosekund.

D. System centralnego zarządzania i raportowania:

- Zdalną konfigurację, grupowanie urządzeń oraz dystrybucję oprogramowania układowego i sygnatur w trybach online oraz offline,
- Interaktywne mapowanie topologii sieci oraz kierunków komunikacji,
- Prowadzenie inwentaryzacji aktywów (IP, MAC, nazwa hosta, producent, wersja firmware, typ systemu operacyjnego),
- Generowanie szczegółowych logów zawierających adresy IP i MAC obu stron zdarzenia, typ protokołu oraz nazwę naruszonej reguły,
- Przesyłanie zdarzeń do systemów klasy SIEM za pomocą standardowego protokołu Syslog.

E. Wymagania konstrukcyjne i formalne:

- Obudowa typu Rugged przystosowana do montażu na szynie DIN35,
- Chłodzenie pasywne (brak wentylatorów) oraz zakres temperatury pracy od -40 do +70 stopni Celsjusza,
- Posiadanie przez producenta certyfikatów IEC 62443 4 1 oraz ISO/IEC 27001 2022,
- Licencja wieczysta (lifetime) na użytkowanie oprogramowania wbudowanego w sondę,
- Gwarancja sprzętowa oraz bieżąca aktualizacja sygnatur przez okres 5 lat (po zakończeniu 5-letniego okresu gwarancyjnego, urządzenie pozostanie w pełni funkcjonalne).

Wymagane wsparcie techniczne udzielane przez producenta lub oficjalnego dystrybutora w języku polskim, w mowie i piśmie (bez pośrednictwa tłumacza AI lub bota).

Wymagane przedstawicielstwo producenta w Polsce i/lub na terenie Unii Europejskiej.

Potwierdzenie pochodzenia sprzętu z legalnej dystrybucji w Polsce, nie dopuszcza się dostawy sprzętu nie przeznaczonego przez producenta na rynek polski.

5. Wymagania dodatkowe:

- Wykonawca zobowiązany jest do realizacji zamówienia zgodnie z zasadą DNSH („Do No Significant Harm”) w rozumieniu Rozporządzenia (UE) 2020/852, w szczególności poprzez ograniczenie wpływu na środowisko, racjonalne gospodarowanie zasobami oraz ograniczenie powstawania odpadów.
- Sprzęt musi być fabrycznie nowy i wolny od substancji z listy REACH/RoHS
- Wdrożenie systemów w 3 wskazanych lokalizacjach Zamawiającego na terenie m. Zabrze, podłączonych do sieci przemysłowej Zamawiającego, bez dostępu do internetu (lokalnie),
- Wykonawca przeprowadzi szkolenie w siedzibie Zamawiającego z działania systemu i jego konfiguracji (np. dodanie nowych agentów, konfigurację dodatkowych sond IPS/IDS, konfiguracja polityk, ich przenoszenie na inne urządzenia),
- Wykonawca prześle niezbędne instrukcje związane z działaniem, uwierzytelnianiem oraz obsługą ww. systemów w formie cyfrowej (w formacie PDF),
- Wykonawca dostarczy wszelkie informacje związane z licencjami dla ww. systemów (np. numery seryjne, konta administratora, loginy, hasła, itp.).