

1.

Dotyczy OPZ, Wymagania funkcjonalne dla obszaru IT (minimalne). Co Zamawiający rozumie pod pojęciem CTI (threat intelligence – bieżąca aktualizacja sygnatur zagrożeń bądź baz reputacyjnych adresów IP) ?

Odpowiedź:

Przez pojęcie CTI (Cyber Threat Intelligence) Zamawiający rozumie mechanizmy zapewniające bieżące dostarczanie oraz automatyczne aktualizowanie informacji o zagrożeniach, wykorzystywane przez system UTM do podnoszenia skuteczności ochrony.

W szczególności obejmuje to:

- aktualizację sygnatur wykorzystywanych przez systemy IPS/IDS,
- aktualizację baz reputacyjnych adresów IP, domen oraz URL,
- automatyczne wykorzystanie powyższych informacji w mechanizmach ochronnych (blokowanie, alertowanie, klasyfikacja ruchu).

Zamawiający wymaga, aby funkcjonalność CTI była integralną częścią oferowanego rozwiązania i była utrzymywana oraz rozwijana przez producenta urządzenia, w ramach dostarczanych aktualizacji bezpieczeństwa.

2.

Dotyczy OPZ, Wymagania funkcjonalne dla obszaru IT (minimalne). Zamawiający wymaga obsługi uwierzytelniania wieloskładnikowego (MFA) dla VPN. Czy Zamawiający zaakceptuje dostarczenie komponentów softwarowych rozwiązania MFA pochodzących z oferty producenta rozwiązania UTM pozwalających na obsługę MFA dla 2 użytkowników przy czym rozwiązanie posiadać będzie możliwość rozbudowy liczby użytkowników mechanizmu MFA poprzez zakup dodatkowych licencji ?

Odpowiedź:

Zamawiający nie wyraża zgody na dostarczenie rozwiązania MFA ograniczonego do 2 użytkowników.

Wymóg obsługi uwierzytelniania wieloskładnikowego (MFA) dla VPN należy rozumieć jako zapewnienie funkcjonalności możliwej do zastosowania dla wszystkich użytkowników korzystających z dostępu zdalnego, zgodnie z potrzebami Zamawiającego.

W szczególności:

- funkcjonalność MFA musi być dostępna dla liczby użytkowników odpowiadającej wymaganej liczbie jednoczesnych tuneli SSL VPN (min. 200),
- mechanizm MFA powinien być integralną częścią oferowanego rozwiązania lub pochodzić z oferty jego producenta i być w pełni z nim zintegrowany,

Celem wymagania jest zapewnienie realnego podniesienia poziomu bezpieczeństwa dostępu zdalnego, a nie jedynie spełnienie warunku formalnego.

3.

Dotyczy OPZ, Wymagania funkcjonalne dla obszaru IT (minimalne). Zamawiający wymaga obsługi na oferowanym urządzeniu UTM co najmniej 6 portów Ethernet w standardzie mGiG o przepustowości 2.5 Gbps. Wdg. najlepszej wiedzy wykonawcy wymaganie to praktycznie eliminuje możliwość oferowania rozwiązania przez wszystkich czołowych producentów rozwiązań NGFW ograniczając się wyłącznie do rozwiązania z oferty Stormshield gdzie najniższym modelem spełniającym te wymagania jest: SNS Series S-320 co potwierdza dokumentacja producenta: <https://www.stormshield.com/wp-content/uploads/SNS-EN-Appliances-Matrix.pdf>

Biorąc poprawkę na minimalną przepustowość wymaganego rozwiązania (5Gbps) 6 portów o przepływności 2.5Gbps pracujących przy pełnej przepustowości i w trybie full-duplex przekroczyło by 6 krotnie przepustowość samego urządzenia UTM i to bez uwzględnienia dodatkowych portów SFP 1Gbps w jakie ma być wyposażone urządzenie. W związku z powyższym zwracamy się z prośbą o zaakceptowanie rozwiązania wyposażonego w min. 6 portów RJ45 o przepustowości 1Gbps.

Odpowiedź:

Zamawiający podtrzymuje wymaganie dotyczące minimalnej liczby portów Ethernet 2.5 GbE.

Wymóg ten wynika z planowanej architektury sieci oraz potrzeby zapewnienia odpowiedniej elastyczności w zakresie segmentacji sieci, separacji stref bezpieczeństwa oraz możliwości rozbudowy infrastruktury w przyszłości.

Jednocześnie Zamawiający wskazuje, iż:

- wymagania dotyczące liczby i typu interfejsów nie są bezpośrednio powiązane z deklarowaną przepustowością firewall,
- porty fizyczne nie muszą pracować jednocześnie z maksymalną przepustowością, a ich liczba i standard determinowane są przez potrzeby topologiczne, a nie wyłącznie przez parametry wydajnościowe urządzenia,
- zastosowanie portów 2.5 GbE pozwala na zachowanie kompatybilności z nowoczesną infrastrukturą sieciową oraz zapewnia większą elastyczność niż porty 1 GbE.

Zamawiający nie ogranicza konkurencji do konkretnego producenta — dopuszczalne są wszystkie rozwiązania spełniające wymagania określone w OPZ.

W związku z powyższym Zamawiający nie wyraża zgody na zmianę wymagania na porty 1 GbE.

4.

Dotyczy OPZ, Wymagania funkcjonalne dla obszaru IT (minimalne). Zamawiający stawia wymaganie w brzmieniu: „centralne zarządzanie (opcjonalne, ale wspierane)” . Prosimy o wyjaśnienie czy Zamawiający wymaga by oferowane rozwiązanie umożliwiało wykorzystanie systemu centralnego zarządzania pochodzącego z oferty producenta rozwiązania UTM przy czym Zamawiający nie wymaga jego dostawy wraz z oferowanymi urządzeniami?

Odpowiedź:

Zamawiający potwierdza, że wymaga, aby oferowane rozwiązanie umożliwiało wykorzystanie systemu centralnego zarządzania pochodzącego z oferty producenta rozwiązania UTM.

Jednocześnie Zamawiający nie wymaga dostawy ani wdrożenia systemu centralnego zarządzania w ramach niniejszego postępowania.

Wymaganie „centralne zarządzanie (opcjonalne, ale wspierane)” należy rozumieć jako:

- zapewnienie kompatybilności oferowanych urządzeń z systemem centralnego zarządzania producenta,
- możliwość późniejszego wdrożenia takiego systemu bez konieczności wymiany urządzeń,
- wsparcie dla centralnego zarządzania konfiguracją, politykami bezpieczeństwa oraz aktualizacjami.

Celem wymagania jest zapewnienie możliwości dalszego rozwoju środowiska bezpieczeństwa Zamawiającego oraz jego centralizacji w przyszłości.

5.

Dotyczy OPZ, Wymagania funkcjonalne dla obszaru IT (minimalne). Czy w przypadku oferowania urządzenia UTM klasy desktop wymagane jest dostarczenie dedykowanego dla niego zestawu rack umożliwiającego jego montaż w szafie rack 19” czy też wystarczy fakt, iż urządzenie będzie posiadało możliwość rozbudowy o taki komponent jednak bez wymagania dostarczenia go wraz z oferowanym urządzeniem ?

Odpowiedź:

Zamawiający nie wymaga dostarczenia zestawu montażowego rack 19” w przypadku oferowania urządzenia klasy desktop.

Wymaganie należy rozumieć w ten sposób, że:

- oferowane urządzenie musi posiadać możliwość montażu w szafie rack 19” przy wykorzystaniu dedykowanego zestawu montażowego dostępnego w ofercie producenta,
- Zamawiający nie wymaga, aby zestaw ten był dostarczony w ramach niniejszego postępowania.

Celem wymagania jest zapewnienie elastyczności w zakresie sposobu instalacji urządzenia, w zależności od przyszłych potrzeb Zamawiającego.

6.

Dotyczy OPZ, Wymagania funkcjonalne dla obszaru IT (minimalne). Zamawiający w wymaganiu „wsparcie i aktualizacje” wymaga subskrypcji na okres min. 12M a aktualizacji firmware na okres 5 lat przy jednoczesnej gwarancji na okres min. 36M. Prosimy o wyjaśnienie czy nie doszło do pomyłki. Typowo okres gwarancji oraz okres ważności subskrypcji jest wspólny przy czym prawo do aktualizacji oprogramowania urządzenia bądź jego firmware dostępne jest zwykle w okresie gwarancji. Prosimy o wyjaśnienie tych rozbieżności.

Odpowiedź:

Zamawiający potwierdza, że wskazane okresy nie są wynikiem pomyłki i pozostają bez zmian.

Wymagania w zakresie subskrypcji bezpieczeństwa, aktualizacji firmware oraz gwarancji odnoszą się do różnych aspektów funkcjonowania systemu i celowo zostały określone odrębnie:

- subskrypcje bezpieczeństwa (IPS, AV, CTI) na okres min. 12 miesięcy – dotyczą dostępu do aktualnych baz zagrożeń i usług ochronnych,
- gwarancja producenta na okres min. 36 miesięcy – dotyczy wsparcia sprzętowego oraz usuwania awarii,
- dostęp do aktualizacji firmware przez okres min. 5 lat – dotyczy zapewnienia długoterminowego utrzymania bezpieczeństwa i możliwości aktualizacji systemu niezależnie od cyklu życia subskrypcji.

Zamawiający dopuszcza model, w którym dostęp do aktualizacji firmware nie jest uzależniony wyłącznie od aktywnej subskrypcji bezpieczeństwa, o ile producent zapewnia ich dostępność w wymaganym okresie.

Celem takiego rozdzielenia jest zapewnienie:

- długoterminowego bezpieczeństwa infrastruktury,
- niezależności od cykli licencyjnych usług subskrypcyjnych,
- możliwości dalszej eksploatacji urządzenia po zakończeniu podstawowego okresu subskrypcji.

W związku z powyższym Zamawiający podtrzymuje wymagania bez zmian.

7.

Dotyczy OPZ, Wymagania funkcjonalne dla obszaru IT (minimalne). Zamawiający w wymaganiach dodatkowych stawia wymagania w brzmieniu: „brak konieczności dokupowania licencji do podstawowych funkcji firewall/VPN”. Prosimy o wyjaśnienie co Zamawiający ma na myśli ? Czy chodzi o funkcjonalności firewall L4 czy L7 (NGFW) ? Czy w odniesieniu do VPN chodzi o to by urządzenie posiadało tę funkcjonalność bez konieczności uruchamiania na urządzeniu dodatkowej, czasowej subskrypcji odpowiedzialnej za usługę VPN?

Odpowiedź:

Zamawiający wyjaśnia, że zapis „brak konieczności dokupowania licencji do podstawowych funkcji firewall/VPN” należy rozumieć jako zapewnienie dostępności tych funkcji w ramach dostarczonego urządzenia, bez konieczności zakupu dodatkowych licencji lub subskrypcji warunkujących ich działanie.

W szczególności:

w zakresie firewall:

- wymagane jest zapewnienie funkcjonalności firewall stanowego (L3/L4) bez dodatkowych licencji,
- funkcjonalności klasy NGFW (L7), takie jak IPS, kontrola aplikacji, filtrowanie treści itp., mogą wymagać subskrypcji bezpieczeństwa, zgodnie z wymaganiami OPZ,

w zakresie VPN:

- wymagane jest zapewnienie funkcjonalności VPN (IPSec oraz SSL VPN) bez konieczności wykupowania dodatkowych licencji aktywujących tę funkcję,
- Zamawiający nie dopuszcza rozwiązań, w których sama możliwość zestawiania tuneli VPN jest uzależniona od aktywnej, dodatkowej licencji lub subskrypcji.

Dopuszczalne są natomiast ograniczenia wynikające z parametrów wydajnościowych urządzenia lub liczby jednoczesnych sesji określonych w OPZ.

Celem wymagania jest zapewnienie pełnej dostępności podstawowych funkcji sieciowych i bezpieczeństwa bez konieczności ponoszenia dodatkowych kosztów licencyjnych na etapie eksploatacji.

8.

Dotyczy OPZ, Wymagania funkcjonalne dla obszaru OT (minimalne). Zamawiający wymaga obsługi na oferowanym urządzeniu UTM co najmniej 3 portów Ethernet w standardzie mGiG o przepustowości 2.5 Gbps. Wdg. najlepszej wiedzy wykonawcy wymaganie to praktycznie eliminuje możliwość oferowania rozwiązania przez wszystkich czołowych producentów rozwiązań NGFW ograniczając się wyłącznie do rozwiązania z oferty Stormshield gdzie najniższym modelem spełniającym te wymagania jest: SNS Series SNI10 (4 porty o tej przepływności) co potwierdza dokumentacja producenta: <https://www.stormshield.com/wp-content/uploads/SNS-EN-Appliances-Matrix.pdf>

Biorąc poprawkę na minimalną przepustowość wymaganego rozwiązania (2Gbps) 3 porty o przepływności 2.5Gbps pracujących przy pełnej przepustowości i w trybie full-duplex przekroczyły by ponad 7 krotnie przepustowość samego urządzenia UTM. W związku z powyższym zwracamy się z prośbą o zaakceptowanie rozwiązania wyposażonego w min. 3 porty RJ45 o przepustowości 1Gbps

Odpowiedź:

Zamawiający podtrzymuje wymaganie dotyczące minimalnej liczby portów Ethernet 2.5 GbE dla urządzeń przeznaczonych do obszaru OT.

Wymóg ten wynika ze specyfiki środowisk przemysłowych oraz planowanej architektury sieci, w szczególności:

- konieczności zapewnienia fizycznej separacji segmentów sieci OT oraz stref bezpieczeństwa,
- potrzeby integracji z nowoczesnymi urządzeniami przemysłowymi i infrastrukturą siecią wykorzystującą interfejsy wielogigabitowe (mGiG),
- zapewnienia odpowiedniej elastyczności w zakresie projektowania topologii sieci oraz przyszłej rozbudowy systemu.

Zamawiający wskazuje, iż liczba i przepustowość interfejsów fizycznych nie jest bezpośrednio powiązana z deklarowaną przepustowością firewall, a porty nie muszą pracować jednocześnie z maksymalną przepustowością.

Zamawiający nie zgadza się ze stwierdzeniem, iż wymaganie to eliminuje wszystkich producentów rozwiązań dostępnych na rynku. Wymagania zostały określone w oparciu o rzeczywiste potrzeby techniczne oraz wymagania środowiska OT.

W związku z powyższym Zamawiający nie wyraża zgody na zmianę wymagania na porty 1 GbE.

9.

Dotyczy OPZ, Wymagania funkcjonalne dla obszaru OT (minimalne). Zamawiający wymaga obsługi na oferowanym urządzeniu UTM wielu różnych protokołów przemysłowych. Czy Zamawiający

zaakceptuje rozwiązanie nie wspierające jednego z wymienionych protokołów tj. protokołu SOFBUS / LACBUS ? Czy Zamawiający posiada infrastrukturę OT komunikującą się w/w protokołem ?

Odpowiedź:

Zamawiający dopuszcza rozwiązania nieposiadające natywnej obsługi protokołu SOFBUS / LACBUS.

Jednocześnie Zamawiający podtrzymuje wymaganie dotyczące natywnej obsługi DPI dla pozostałych wskazanych protokołów przemysłowych.

Wymaganie w zakresie szerokiego katalogu obsługiwanych protokołów wynika z:

- konieczności zapewnienia wysokiego poziomu bezpieczeństwa środowiska OT,
- potrzeby monitorowania i kontroli ruchu w oparciu o specyfikę protokołów przemysłowych,
- zapewnienia kompatybilności z różnorodnymi systemami automatyki przemysłowej.

Zamawiający informuje, iż na dzień przygotowania postępowania nie eksploatuje systemów wykorzystujących protokoły SOFBUS / LACBUS, jednak wymagania zostały określone z uwzględnieniem potencjalnych przyszłych potrzeb oraz ogólnej klasy rozwiązania.

10.

Dotyczy OPZ, Wymagania funkcjonalne dla obszaru OT (minimalne). Zamawiający w warunkach pracy środowiskowej wymaga parametru opisanego jako „wilgotność: 0% – 95% RH przy 60°C (bez kondensacji)”. Sposób opisu w/w parametru wskazuje na jednego z producentów („Relative humidity for storage (without condensation) 0% to 95% @60°C) : <https://www.stormshield.com/wp-content/uploads/SNS-EN-SNi10-Datasheet.pdf> Czy Zamawiający zaakceptuje parametr wilgotności dla oferowanego urządzenia w przedziale : 5% – 95% (bez kondensacji) ?

Odpowiedź:

Zamawiający dopuszcza zmianę zakresu wilgotności pracy do wartości 5% – 95% RH (bez kondensacji).

Jednocześnie Zamawiający podtrzymuje wymaganie dotyczące możliwości pracy urządzenia w warunkach przemysłowych, w tym w podwyższonym zakresie temperatur oraz wilgotności, charakterystycznych dla środowisk OT.

Celem wymagania jest zapewnienie niezawodnej pracy urządzenia w warunkach przemysłowych, a nie odwzorowanie konkretnego sposobu prezentacji parametrów przez producentów.

Zamawiający dopuszcza parametry równoważne w zakresie warunków środowiskowych, o ile zapewniają one nie gorszą funkcjonalność i niezawodność pracy urządzenia.

11.

Dotyczy OPZ, Wymagania funkcjonalne dla obszaru OT (minimalne). Zamawiający w warunkach wymaganych zgodności i certyfikacji oczekuje spełniania wymagania „UKCA”. Czy Zamawiający zaakceptuje rozwiązanie bez w/w certyfikacji ?

Odpowiedź:

Zamawiający dopuszcza rozwiązania nieposiadające certyfikacji UKCA.

Jednocześnie Zamawiający podtrzymuje wymagania w zakresie pozostałych norm i certyfikacji, w szczególności CE oraz innych wskazanych w OPZ, które są istotne z punktu widzenia dopuszczenia urządzeń do obrotu oraz ich eksploatacji w środowisku przemysłowym na terenie Unii Europejskiej.

Wymóg UKCA miał charakter uzupełniający i nie stanowi kluczowego kryterium oceny zgodności oferowanego rozwiązania.

12.

Dotyczy OPZ, Wymagania funkcjonalne dla obszaru OT (minimalne). Zamawiający w warunkach wymaganych zgodności i certyfikacji oczekuje spełniania wymagania: „IEC 61000-4-2 / 4-4 / 4-12”. Czy Zamawiający zaakceptuje również rozwiązanie oferujące alternatywne standardy w zakresie EMC tj. EN 55032:2015 + A11:2020, Class A ;EN 55035:2017 + A11:2020 ; EN IEC 61000-6-4:2019; IEC 61000-4-9; IEC 61000-4-10 ?

Odpowiedź:

Zamawiający podtrzymuje wymaganie zgodności z normami IEC 61000-4-2, IEC 61000-4-4 oraz IEC 61000-4-12.

Normy te dotyczą odporności urządzeń na zakłócenia elektromagnetyczne i mają kluczowe znaczenie dla zapewnienia niezawodnej pracy w środowisku przemysłowym OT.

Jednocześnie Zamawiający dopuszcza rozwiązania równoważne, o ile oferowane urządzenie zapewnia co najmniej taki sam poziom odporności na zakłócenia elektromagnetyczne, potwierdzony odpowiednimi normami lub raportami z badań.

Wymagane normy IEC 61000-4-2, 4-4 oraz 4-12 dotyczą odporności urządzeń na typowe zakłócenia występujące w środowiskach przemysłowych, takie jak wyładowania elektrostatyczne, szybkie zakłócenia impulsowe oraz przepięcia, i mają kluczowe znaczenie dla zapewnienia ciągłości pracy systemów OT.

W związku z powyższym Zamawiający nie wyraża zgody na całkowite zastąpienie wymaganych norm wskazanym zestawem, natomiast dopuszcza rozwiązania równoważne, o ile oferowane urządzenie zapewnia co najmniej taki sam poziom odporności na zakłócenia elektromagnetyczne, potwierdzony odpowiednimi normami lub raportami z badań .

13.

Dotyczy OPZ, Wymagania funkcjonalne dla obszaru OT (minimalne). Zamawiający wymaga gwarancji na okres min. 36M i aktualizacji bezpieczeństwa na okres min. 5 lat. Prosimy o wyjaśnienie czy nie doszło do pomyłki. Typowo okres gwarancji oraz okres ważności subskrypcji jest wspólny przy czym prawo do aktualizacji oprogramowania urządzenia bądź jego firmware dostępne jest zwykle w okresie gwarancji. Prosimy o wyjaśnienie tych rozbieżności.

Odpowiedź:

Zamawiający potwierdza, że wskazane okresy nie są wynikiem pomyłki i pozostają bez zmian.

Wymagania w zakresie gwarancji oraz aktualizacji bezpieczeństwa odnoszą się do różnych aspektów funkcjonowania urządzenia i zostały określone celowo w sposób rozdzielny:

- gwarancja producenta na okres min. 36 miesięcy dotyczy wsparcia sprzętowego oraz usuwania awarii,
- dostęp do aktualizacji bezpieczeństwa i oprogramowania przez okres min. 5 lat dotyczy zapewnienia długoterminowej ochrony systemu oraz utrzymania jego aktualności w zakresie zagrożeń.

W środowiskach OT cykl życia urządzeń jest istotnie dłuższy niż w środowiskach IT, a ich wymiana wiąże się z wysokimi kosztami oraz ryzykiem operacyjnym. W związku z tym Zamawiający wymaga zapewnienia możliwości długoterminowego utrzymania bezpieczeństwa urządzeń, niezależnie od okresu gwarancji.

Zamawiający dopuszcza różne modele licencyjne producentów, pod warunkiem spełnienia powyższych wymagań.

14.

Dotyczy OPZ, Wymagania dodatkowe. Dotyczy wymagania w brzmieniu: „brak konieczności dodatkowych licencji do podstawowych funkcji firewall + IPS + OT DPI”. Czy Zamawiający zaakceptuje rozwiązanie, w którym funkcjonalności IPS bądź OT DPI są pod postacią czasowej subskrypcji (oferowanej na okres wymagany przez Zamawiającego lub tożsamy z okresem gwarancji), która jest dostarczana wraz z urządzeniem UTM? Uprzejmie zwracamy uwagę iż funkcjonalności bezpieczeństwa w rodzaju w/w a często i rozpoznawanie aplikacji w warstwie 7 (NGFW) są prawie zawsze oferowane pod postacią czasowej subskrypcji i nie znajdują się w standardzie tj. z urządzeniem i pakietem gwarancji na urządzenie.

Odpowiedź:

Zamawiający dopuszcza rozwiązania, w których funkcjonalności IPS oraz OT DPI są realizowane w modelu subskrypcyjnym.

Jednocześnie Zamawiający wymaga, aby:

- wszystkie wymagane funkcjonalności bezpieczeństwa (firewall, IPS, OT DPI) były dostępne i aktywne na dostarczonym urządzeniu na moment wdrożenia,
- nie było konieczności dokupowania dodatkowych licencji w celu uruchomienia tych funkcjonalności,
- ewentualne subskrypcje obejmujące IPS oraz OT DPI były dostarczone w ramach oferty na wymagany okres.

Zamawiający podtrzymuje wymaganie, że funkcjonalności te muszą być integralną częścią oferowanego rozwiązania i nie mogą wymagać stosowania dodatkowych urządzeń lub zewnętrznych systemów.

Celem wymagania jest zapewnienie pełnej funkcjonalności bezpieczeństwa od momentu uruchomienia systemu oraz uniknięcie sytuacji, w której kluczowe mechanizmy ochrony wymagają dodatkowych zakupów lub aktywacji po wdrożeniu.

15.

Dotyczy OPZ, Zakres wdrożenia i konfiguracji. Ile tuneli VPN site-2-site w sieci IT i OT posiada aktualnie Zamawiający, które mają zostać zmigrowane na nowe urządzenia w każdym z segmentów ?

Odpowiedź:

Zamawiający informuje, iż obecnie w obszarze IT funkcjonują 3 tunele VPN typu site-to-site, które będą podlegały migracji na nowe urządzenia.

W obszarze OT Zamawiający nie posiada obecnie wdrożonego rozwiązania UTM. Jednocześnie Zamawiający wskazuje, że konfiguracja tuneli VPN w obszarze OT nie stanowi przedmiotu niniejszego zamówienia.

Zamawiający wskazuje, iż konfiguracja urządzeń w obszarze OT będzie obejmowała przygotowanie reguł bezpieczeństwa, zgodnie z wymaganiami określonymi w OPZ.

Wymagania określone w OPZ uwzględniają zarówno aktualne potrzeby, jak i planowany rozwój infrastruktury, w tym możliwość przyszłego wykorzystania funkcjonalności VPN.

16.

Dotyczy OPZ, Zakres wdrożenia i konfiguracji. Prosimy o wyjaśnienie co Zamawiający rozumie pod pojęciem konfiguracji reguł bezpieczeństwa dla środowiska OT. Czy chodzi o zbudowanie polityk ograniczających komunikację urządzeń OT komunikujących się określonymi protokołami przemysłowymi ze wskazanymi hostami w segmencie OT ?

Odpowiedź:

Zamawiający potwierdza, że przez konfigurację reguł bezpieczeństwa dla środowiska OT rozumie przygotowanie i wdrożenie podstawowych polityk bezpieczeństwa ograniczających i kontrolujących komunikację pomiędzy segmentami sieci oraz urządzeniami w środowisku OT.

W szczególności obejmuje to:

- definiowanie reguł komunikacji pomiędzy strefami bezpieczeństwa (np. OT/IT, strefy produkcyjne),
- ograniczenie komunikacji do niezbędnych protokołów i usług, w tym protokołów przemysłowych,
- przypisanie reguł do określonych adresów IP, podsieci lub grup urządzeń,
- zastosowanie zasad „minimalnych uprawnień” (ang. least privilege),
- wykorzystanie mechanizmów inspekcji ruchu (w tym DPI dla protokołów przemysłowych) w zakresie wspieranym przez urządzenie oraz możliwym do bezpiecznego zastosowania w środowisku OT.

Zamawiający wskazuje, iż szczegółowy zakres reguł będzie miał charakter podstawowy i przykładowy (zgodnie z OPZ), a jego celem jest uruchomienie bezpiecznej konfiguracji startowej, która może być dalej rozwijana przez Zamawiającego.