**Załącznik nr B7B – Cyberbezpieczeństwo OT– monitorowanie infrastruktury OT**

**Program Funkcjonalno- Użytkowy**

Spis treści

[1 Wprowadzenie 3](#_Toc163040119)

[1.1 Cel zdefiniowania wymagań. 3](#_Toc163040120)

[2 Założenia 3](#_Toc163040121)

[2.1 Etapy wdrożenia 3](#_Toc163040122)

[2.2 Założenia instalacyjne i wdrożeniowe 3](#_Toc163040123)

[3 Wymagania 4](#_Toc163040124)

[3.1 Legenda do wymagań 4](#_Toc163040125)

[3.2 Narzędzie SAD 4](#_Toc163040126)

[3.3 Konsola zarządzania 7](#_Toc163040127)

[3.4 Interface użytkownika 8](#_Toc163040128)

[3.5 Zarządzanie aktywami (Asset Management) 8](#_Toc163040129)

[3.6 Wykrywanie zagrożeń 10](#_Toc163040130)

[3.7 Raportowanie 11](#_Toc163040131)

[3.8 Integracja z infrastrukturą i systemami funkcjonującymi u Zamawiającego 12](#_Toc163040132)

[3.9 Niefunkcjonalne 12](#_Toc163040133)

[3.10 Zespół/ Dostawca 13](#_Toc163040134)

[3.11 Wdrożenie i instalacja 14](#_Toc163040135)

[3.12 Wdrożenie i instalacja 14](#_Toc163040136)

1. Wprowadzenie

## Cel zdefiniowania wymagań.

1. Wdrożenie narzędzia adekwatnego dla sektora energetycznego działającego w sposób pasywny (bez ingerencji w działanie istniejącej sieci teletechnicznej) oraz posiadającego możliwość uczenia się wzorca działania sieci,
2. Wykrywania zagrożeń w sieci rozpoznawanych jako anomalie (odchylenia) od „nauczonego” wzorca ruchu.
3. Rozwiązanie określane są mianem przemysłowych narzędzi IDS (ang. Intrusion Detection Systems) posiadające funkcję analizy behawioralnej (NBA ang. network behavior analysis) oraz detekcji anomalii w systemach OT SCADA
4. Narzędzie powinno również posiadać możliwość aktywnego odpytywania urządzeń OT oraz ICS, ale czynić to musi w sposób gwarantujący, że zapytanie takie nie będzie miało wpływu na stabilność lub wydajność pracy systemu sterowania.
5. Narzędzie powinno wykorzystywać taki sposób i tryb odpytywania urządzeń, który został zatwierdzony przez ich producentów wprost (poprzez certyfikację) lub dopuszczalnie poprzez domniemanie (jest wykorzystywany w codziennych zapytaniach stosowanych przez stacje SCADA .
6. Założenia

## Etapy wdrożenia

1. Opracowanie projektu technicznego wdrożenia narzędzia do detekcji anomalii w systemach OT. Projekt techniczny obejmuje opracowanie koncepcji i sposobu wdrożenia narzędzia do monitorowania ruchu sieciowego na obiektach energetycznych.
2. Instalacja i konfiguracja narzędzia zgodnie z projektem technicznym w środowisku PGE EC.
3. Zdefiniowanie wzorca bazowego monitorowanego środowiska PGE EC - proces uczenia się narzędzia
4. Uruchomienie pasywnego trybu monitorowania i wsparcie techniczne.

## Założenia instalacyjne i wdrożeniowe

1. Zakłada się, że urządzenie monitorujące (sonda) zostanie umiejscowiona tak aby monitorować ruch sieciowy pomiędzy urządzeniami energetycznymi a centrami danych.
2. Zakłada się również, że krytyczne/priorytetowe urządzenia energetyczne będą wymagały indywidualnego monitorowania ruchu w celu zapewnienia pełnego poziomu szczegółowości i granularności danych monitorowania. Monitoring ten może być realizowany poprzez dodatkowy komponent monitorujący za pośrednictwem funkcjonalności SPAN lub poprzez sensor monitorujący działający w obrębie urządzenia sieciowego, który generuje metadane z ruchu sieciowego i wysyła je do konsoli do dalszej analizy. Metadane te w przeciwieństwie do pełnej kopii ruchu zużywają niewielką ilość pasma a co za tym idzie zwiększają skalowalność rozwiązania i umożliwiają szczegółowy monitoring infrastruktury rozproszonej.
3. Poprzez umieszczenie sond lub zapewnienie innego sposobu monitorowania na urządzeniach sieciowych znajdujących się na granicy sieci punktów centralnych (centrów danych) i/lub w urządzeniach energetycznych (tam gdzie zaistnieje taka potrzeba) monitorowany będzie ruch sieciowy w obrębie poszczególnych urządzeń a także pomiędzy pozostałymi obiektami a centrami danych.
4. Kluczowym założeniem projektu wdrożenia narzędzia detekcji anomalii w systemach OT jest możliwość pasywnego monitorowania ruchu sieciowego oraz możliwość przeprowadzenia inwentaryzacji aktywów znajdujących się w tej samej sieci. Jednym z wymagań dotyczących narzędzia detekcji anomalii w systemach OT jest również możliwość aktywnego, nieinwazyjnego, odpytywania wykrytych urządzeń z wykorzystaniem SNMP (z wyłączeniem PLC) lub zapytań zatwierdzonych przez producenta danego urządzenia, tak aby możliwe było wykrycie szczegółowych informacji np. wersji oprogramowania na urządzeniu sieciowym.
5. Wymagania

## Legenda do wymagań

1. M-musi spełniać
2. P – powinien spełniać

## Narzędzie detekcji anomalii w systemach OT

|  |  |  |
| --- | --- | --- |
| **#** | **Wymaganie** | **Priorytet** |
| Req1.N | Narzędzie do pasywnego monitorowania urządzeń OT i ruchu bazuje na kopii ruchu sieciowego lub metadanych (z obsługiwanego ruchu) generowanych przez urządzenie sieciowe. Jakiekolwiek zakłócenia w działaniu narzędzia do monitorowania (np. brak zasilania) nie mogą zakłócić w żaden sposób ruchu sieciowego – urządzenie staje się nieaktywne. W wypadku uszkodzenia sondy lokalnej system centralny musi w sposób nieinwazyjny odpytać urządzenia w danej lokalizacji w sposób aktywny, tak aby monitorować sytuację w której zachodzi podejrzenie świadomego uszkodzenia sondy (sabotażu). Warunkiem koniecznym jest zgoda producenta urządzenia na pasywne monitorowanie dostarczonej infrastruktury sieciowej urządzenia wytwórczego. | M |
| Req2.N | Urządzenia uzgodnione z Zamawiającym na etapie projektu muszą zapewniać ciągły, on-line monitoring z alarmowaniem w czasie rzeczywistym | M |
| Req3.N | Musi zapewniać sortowanie alarmów względem ich poziomu zagrożenia, ważności, typie i czasie wystąpienia | M |
| Req4.N | Urządzenie umożliwia wysyłanie alarmów do narzędzi klasy SIEM oraz opcjonalnie drogą mailową. | M |
| Req5.N | Rozwiązanie musi identyfikować anomalie oraz incydenty w sieci operacyjnej (OT) | M |
| Req6.N | Mechanizmy alarmujące muszą działać w trakcie budowania modelu sieci OT w celu wykrywania zagrożeń w czasie procesu nauki. | M |
| Req7.N | Możliwość automatycznej identyfikacji urządzeń pracujących w sieci przemysłowej (PLC, HMI, RTU, stacje operatorskie, stacje inżynierskie). Dostawcy wymienionych urządzeń na etapie projektu wykonawczego muszą przekazać Wykonawcy systemu SCADA szczegółowe dane dotyczące typu urządzeń. | M |
| Req8.N | Narzędzie musi zapewniać:   * Pasywne monitorowanie sieci OT, * Aktywne, nieinwazyjne, zbieranie informacji o urządzeniach w sieci OT, * Automatyczne tworzenie graficznej mapy urządzeń, * Rozbudowaną inwentaryzacja wszystkich urządzeń, * Automatyczną adaptację do zmian w sieci (utrata / pojawienie się nowych urządzeń, zmiana komunikacji), * Wykrywanie urządzeń nieznanych: błędnie podłączonych lub wrogich. | M |
| Req9.N | Możliwość implementacji nowych protokołów OT we własnym zakresie bez udziału producenta oprogramowania. Raz dodane protokoły nie mogą przestać działać wraz z aktualizacją wersji oprogramowania do monitorowania, powinny być od tego niezależne. | P |
| Req10.N | Rozwiązanie musi być pasywne, działać na kopii ruchu. Musi mieć również możliwość aktywnego, nieinwazyjnego, odpytywania urządzeń. | M |
| Req11.N | Nie może mieć żadnego wpływu na komunikację urządzeń w sieci OT | M |
| Req12.N | Rozwiązanie umożliwia analizę ruchu sieciowego dostarczanego przez port Mirror / SPAN / tap. | M |
| Req13.N | Rozwiązanie powinno umożliwiać rozszerzoną analizę alarmów na podstawie kopii ruchu sieciowego Packet Capture (pliki PCAP) | P |
| Req14.N | Rozwiązanie umożliwia automatyczne generowanie raportów bezpieczeństwa i podatności sieci przemysłowej (z poziomu interfejsu lub poprzez API) bazując na analizie ruchu sieciowego wraz z rekomendacją w jaki sposób zwiększyć bezpieczeństwo. | P |
| Req15.N | Urządzenie powinno posiadać funkcjonalność przyjmowania ruchu sieciowego do analizy co najmniej na 4 interfejsach sieciowych z łączną wydajnością do 1 Gb/s. Ostateczna liczba wymaganych interfejsów sieciowych zostanie określona na etapie projektowania. | P |
| Req16.N | Urządzenie powinno dysponować co najmniej jednym portem komunikacyjnym przeznaczonym do zarządzania środowiskiem. | P |
| Req17.N | Instalacja sond w segmentach, gdzie nie możliwe jest użycie span-portów. W segmentach, gdzie nie jest możliwe użycie spanportów powinien być zapewniony pomiar bezpieczeństwa z wykorzystaniem odpytywania aktywnego. | M |
| Req18.N | Automatyczne wykrywania urządzeń wpiętych do monitorowanej sieci w czasie rzeczywistym | M |
| Req19.N | Instalacja zarówno na fizycznych jak i wirtualnych serwerach | M |
| Req20.N | Backup i archiwizacje stanu monitorowanej sieci i urządzeń. Tworzenie kopii w celu odtworzenia stanu monitorowanego środowiska offline | M |
| Req21.N | Opis koncepcji realizacji prac wdrożenia narzędzia detekcji anomalii w systemach OT w PGE EC. Opisane funkcjonalności nie będą dotyczyły jednostek gotowych SG, SPC. | M |
| Req22.N | Projekt wykonawczy wdrożenia, który zawiera szczegóły:   * Koncepcji wdrożenia narzędzia detekcji anomalii w systemach OT * Sposób realizacji koncepcji * Harmonogram wdrożenia z podziałem na etapy * Opis ról i odpowiedzialności przy wdrożeniu * Wymagania techniczne/ funkcjonalne/ organizacyjne lub inne w PGE EC w celu realizacji projektu * Opis ryzyk wdrożenia detekcji anomalii w systemach OT w PGE EC z uwzględnieniem sposobu ich zaadresowania | M |
| Req23.N | Zapewnienie wsparcia integratora mającego swoją obecność w Polsce. Instalacja i konfiguracja systemu do pasywnego monitorowania może być przeprowadzona i wykonana przez producenta ale z zastrzeżeniem, że wskaże on firmę która posiada pełną wiedze o wdrożonym rozwiązaniu jest w stanie świadczyć usługi wsparcia zgodne z wymogami PGE EC | M |
| Req23.N | Rozwiązanie musi być skalowane w zależności od wielkości instalacji / miejsca. | M |
| Req24.N | Obsługa instalacji nieinwazyjnej (bez konieczności przeprojektowywania sieci i bez wstawiania ruchu lub opóźnień w sieci procesowej). | M |
| Req25.N | Architektura narzędzia będzie obejmowała serwer centralny w przypadku zakupu centralnego serwera dla wszystkich Spółek i Oddziałów PGE EC. | M |
| Req26.N | Narzędzie zapewni ocenę ryzyka w odniesieniu do każdego składnika aktywów: podatność na zagrożenia NVD (NVD zawiera bazy danych list kontrolnych bezpieczeństwa, bezpieczeństwa związane z wadami oprogramowania, błędów konfiguracji), poziom (w ramach modelu in Purdue), alarmy z białej listy, alarmy z czarnej listy, typ składnika aktywów, proces przemysłowy, najbardziej zagrożone zasoby oraz trendy w zakresie ryzyka. | P |
| Req26.N | Retencja przechowywania danych na serwerze centralnym powinna być wydłużana wraz ze wzrostem dostępnej pamięci. | P |
| Req27.N | Narzędzie zapewni funkcjonalność wirtualnego sensora pozwalającą na uruchomienie monitoringu bez konieczności instalowania dodatkowych sensorów fizycznych (np. w lokalizacjach z ograniczoną przestrzenią montażową oraz w celu ograniczenia kosztów systemu). Funkcjonalność ta może być realizowana również poprzez aktywne, nieinwazyjne, odpytywanie urządzeń. | P |
| Req28.N | Możliwość instalacji wirtualnego sensora (do monitorowania ruchu) bezpośrednio na dedykowanym urządzeniu sieciowym. Funkcjonalność ta może być realizowana również poprzez aktywne, nieinwazyjne, odpytywanie urządzeń. | P |
| Reg29.N | Narzędzie umożliwi wstępną analizę ruchu w obrębie wirtualnego sensora (instalowanego na urządzeniu sieciowym) celem wygenerowania lekkich wolumenowo metadanych które wysyłane są do centralnej konsoli do dalszej analizy | P |
| Req30.N | System detekcji anomalii w systemach OT umożliwi efektywne kosztowo zarządzanie systemem i jego utrzymanie w czasie bez konieczności wymiany sensorów (komponentów monitorujących) wraz ze wzrostem ruchu w środowisku sieciowym. Wymaga się utrzymania rezerwy wystarczającej do prawidłowej pracy po rozbudowie systemu sterowania o urządzenia wytwórcze w ramach wszystkich etapów realizacji projektu Przemysłowego dla EC Kraków. | P |
| Req31.N | System detekcji anomalii w systemach OT umożliwi efektywne kosztowo skalowanie i dalszą rozbudowę poprzez uruchomienie funkcjonalności monitoringu w kolejnych urządzeniach (sensor per urządzenie) bez konieczności instalowania dedykowanych sensorów sprzętowych a poprzez integrację sensora z urządzeniem sieciowym | P |
| Req32.N | System powinien umożliwiać monitorowanie bezpieczeństwa oraz niezmienności kodu źródłowego, co ma zapewnić, że program urządzenia nie został w sposób nieautoryzowany zmodyfikowany, a samo urządzenie realizuje funkcje zaplanowane przez technologa lub automatyka. | M |
| Req33.N | Narzędzie powinno wykrywać zdarzenia związane ze zmianą lub odczytem konfiguracji. Historia zmian musi być przechowywana na serwerze centralnym i tyczyć się całego cyklu życia urządzenia, a nie tylko ostatniej znanej konfiguracji. | M |
| Req34.N | Narzędzie musi potrafić określić stan badanych systemów OT, automatycznie wykrywając co najmniej następujące stany: Running, Stopped, Fault, NoConfig, Backup. | M |

## Konsola zarządzania

|  |  |  |
| --- | --- | --- |
| **#** | **Wymaganie** | **Priorytet** |
| Req1.K | Narzędzie posiada konfigurowalny panel zarządzający, na którym zebrane są co najmniej następujące informacje:   * wysokopoziomowy obraz stanu monitorowanej sieci i urządzeń ze względu na krytyczność poziomu zagrożenia (hygine score) * informacje o wszystkich monitorowanych urządzeniach – statystyki dotyczące aktywów * Kluczowe dla operatora informacje dotyczące liczby i krytyczności alertów generowanych przez narzędzie * Informacje o zdarzeniach, które zaszły na monitorowanych urządzeniach, w tym: zmiana konfiguracji, zmiana nastaw, modyfikacja firmware. | M |
| Req2.K | Narzędzie pozwala na wydzielenie konsoli zarządzającej na osobną maszynę wirtualną lub serwer fizyczny ( w celu umieszczenia w innej strefie sieciowej) | P |
| Req3.N | Centralna konsola do agregacji alarmów i zarządzania wieloma sensorami wdrażanymi zdalnie z jednego interfejsu użytkownika (centralny punkt zarządzania). | M |
| Req4.N | Dostępność – Rozwiązanie oferuje konsolę w postaci webowego/intranetowego interfejsu użytkownika lub Linuks do rozwiązywania problemów technicznych i odzyskiwania danych. | M |
| Req5.N | Dostęp do interfejsu użytkownika do zarządzania w celu zapewnienia różnych widoków dla różnych użytkowników. | P |
| Req6.N | Instalacja aktualizacji oprogramowania narzędzia zarządzana na wielu urządzeniach za pomocą scentralizowanej konsoli. | M |
| Req7.N | Narzędzie udostępnia interfejs typu REST API dający możliwości dalszej integracji oraz automatyzacji | P |

## Interface użytkownika

|  |  |  |
| --- | --- | --- |
| **#** | **Wymaganie** | **Priorytet** |
| Req1.I | Tworzenie graficznej mapy wykrytych urządzeń (strefy, połączenia, charakterystyka, rola, rodzaj połączenia) | M |
| Req2.I | Tworzenie mapy graficznej połączeń sieciowych, na podstawie zebranych informacji z urządzeń sieciowych po SNMP, jako warstwa do mapy połączeń i urządzeń OT. | M |
| Req3.I | Tworzenie własnych reguł przez operatora (użytkownika systemu IDS) dotyczących potencjalnych zagrożeń, którym można przypisać poziom ryzyka i krytyczność. Reguły powinny być konfigurowalne. Przykładowe reguły:   * logowanie się na konta administratora * nieudane próby logowania * restart serwerów * reset hasła użytkownika * instalacja nowego oprogramowania/Firmware * zmiana konfiguracji interfejsów sieciowych * zmiana czasu * skanowanie adresów IP i portów * podłączenie urządzenia USB | M |
| Req4.I | Eksport wszystkich informacji dostępnych w narzędziu monitorowania do plików: lista urządzeń, alerty, pre-definiowane lub stworzone przez administratora raporty | M |
| Req5.I | Definiowanie użytkowników na różnych poziomach dostępu: tylko odczyt, odczyt i możliwość wprowadzania zmian, administrator | M |
| Req6.I | Narzędzie będzie posiadało webowy/intranetowy interfejs użytkownika. Dedykowany klient nie będzie wymagany. | M |
| Req7.I | Graficzna prezentacja węzłów sieciowych i generowanych łączy komunikacyjnych, analizująca komunikację i przydzielająca identyfikację (styl) każdemu elementowi sieci. | M |

## Zarządzanie aktywami (Asset Management)

|  |  |  |
| --- | --- | --- |
| **#** | **Wymaganie** | **Priorytet** |
| Req1.A | Automatyczne wykrywanie urządzeń wpiętych do monitorowanej sieci w czasie rzeczywistym oraz przesłanie takiej informacji do systemu IDS | M |
| Req2.A | Monitorowanie urządzeń wpiętych po Ethernecie | M |
| Req2.B | Monitorowanie urządzeń wpiętych po łączach RS-232 i RS-485 | M |
| Req3.A | Zbieranie informacji o monitorowanych urządzeniach OT   * nazwa * model * typ * funkcja * adresacja * połączenia sieciowe * firmware * stan urządzenia | M |
| Req4.A | Aktywne odpytywanie wybranych urządzeń (w tym urządzeń PLC, SIS oraz infrastruktury sieciowej) w celu szczegółowego zebrania informacji o modelu, wersji Firmware i listy znanych podatności oprogramowania (ICS-CERT database). Odpytywanie nie będzie zakłócało pracy urządzeń. | M |
| Req5.A | Odczytywanie dodatkowych szczegółów o urządzeniach przemysłowych (producent, model, wersja) z referencyjnej bazy danych dostępnej offline. Nie tylko z wykrytego ruchu sieciowego | M |
| Req6.A | Automatyczne generowanie mapy sieci, zasobów i połączeń | M |
| Req7.A | Wizualizacja całej sieci oraz identyfikacja zmiany. | M |
| Req8.A | Śledzenie nieautoryzowanych urządzeń, komunikacji i działań. | M |
| Req9.A | Automatyczne generowanie mapy sieci i zapewnienie pełnej widoczności całej sieci OT. | M |
| Req10.A | Analiza sieci mapuje zarówno IP jak i zasoby szeregowe, wskazuje specyficzne protokoły stosowane pomiędzy urządzeniami, wskazuje na potencjalne zagrożenia i wskazuje na zmiany w sieci. | M |
| Req11.A | Wspiera wykrywanie i analizę protokołów komunikacji sieciowej. | M |
| Req12.A | Wspiera inwentaryzację (wizualizacja) węzłów warstwy 3 i 2 połączonych z sieciami ICS | M |
| Req13.A | Obsługa opcji wyszukiwania obiektów według nazwy, adresu IP, MAC itp. w module mapy sieci. | P |
| Req14.A | Obsługa opcji grupowania obiektów | P |
| Req15.A | Rozwiązanie to będzie obsługiwać moduł zarządzania zasobami co najmniej takimi jak:   * Wizualizacja inwentaryzacji aktywów, * Szczegółowe informacje na temat każdego z aktywów, * Edycja informacji o aktywach, * Przeglądanie podatności z bazy danych NIST/NVD według dostawców, * Przeglądanie alertów dotyczących każdego składnika aktywów, * Informacje o zasobach: nazwa (nazwa DNS lub adres i typ), OS, Wykonawca, Adres, liczba powiadomień związanych z tym zasobem, model, wersja, znane luki w zabezpieczeniach, * Automatyczne wykrywanie wszystkich aktywów, ich nazw, roli/typów (HMI, PLC, bramka, RTU, IED itp.), * Automatyczne wykrywanie wszystkich podatności aktywów w zależności od producenta, modelu i wersji danego składnika aktywów, * Informacja o stanie urządzenia. | M |

## Wykrywanie zagrożeń

|  |  |  |
| --- | --- | --- |
| **#** | **Wymaganie** | **Priorytet** |
| Req1.Z | Analiza próbek ruchu sieciowego zebranych i zapisanych w plikach (pliki PCAP) – analiza offline | M |
| Req2.Z | Identyfikowanie urządzeń, z którymi nastąpiła próba połączenia sieciowego nawet przy braku komunikacji zwrotnej (próby nawiązania komunikacji) | M |
| Req3.Z | Wykrywanie Malware na podstawie prób połącznia ze znanymi adresami złośliwego oprogramowania | M |
| Req4.Z | Wykrywania cyber zagrożeń na podstawie sygnatur podatności. Dostęp do biblioteki sygnatur lub jej aktualizacja nie może odbywać się poprzez łączenie z urządzeniami poza segmentem sieci gdzie zainstalowane jest narzędzie do monitorowania. Rozwiązanie musi być zainstalowane w środowisku zamawiającego bez konieczności komunikacji z Internetem. | M |
| Req5.Z | Wykrywania cyber zagrożeń na podstawie analizy behawioralnej – porównywania stanu bazowego ustalonego w procesie „uczenia się narzędzia” ze stanem faktycznym monitorowanego środowiska. | M |
| Req6.Z | Analiza zdarzeń i nagrywanie ruchu sieciowego w zadanym przedziale czasowym. Ruch sieciowy jest zapisywany do pliku (PCAP) do analizy offline. Ciągła analiza przechwyconego ruchu na serwerze analitycznym. | M |
| Req7.Z | Wsparcie dla wielu rodzajów reguł: Yara, SNORT, CVEs, reguły własne,i analizy zachowań (Behavioral Analysis) | P |
| Req8.Z | Możliwość analizy danych o monitorowanym środowisku tylko dla wybranego odcinku czasu. Zidentyfikowanie zmian w monitorowanym środowisku w zadanym przedziale czasowym | M |
| Req9.Z | Analiza protokołów przemysłowych (deep packet inspection) przy pomocy których komunikować się będą urządzenia dostarczone w ramach Projektu Przemysłowego EC Kraków. Przykładowe protokoły to:   * ICCP, * IEC 61850 (MMS), * IEC 61850 (GOOSE), * IEC 60870-5-103, * IEC 60870-5-104. * MODBUS TCP/IP, RTU, * DNP3, * DLMS/COSEM, * Profibus, * Profinet, * Ethernet IP, * OPC UA. | M |
| Req9.Z | Wsparcie alarmowania zgodnie z zasadami SNORT(Sieciowy System Wykrywania Włamań) . | M |
| Req10.Z | Alerty mogą być wysyłane przez syslog. | M |
| Req11.Z | Zdolność do interpretacji standardowego zachowania i podniesienia alarmu w przypadku wystąpienia anomalii. | M |
| Req12.Z | Narzędzie musi generować alarmy w czasie rzeczywistym | M |
| Req13.Z | Narzędzie musi prezentować Alarmy na mapie sieci | M |
| Req14.Z | Wspieranie agregacji alarmów powielających się | M |
| Req15.Z | Alarm dostarczy informacji na temat zasobów, których dotyczy | M |
| Req16.Z | Podgląd alarmu zostanie wyświetlony w głównym Dashboardzie | M |
| Req17.Z | Alarmy będą łatwo filtrowane co najmniej według typu, dotkliwości, czasu, źródła, miejsca docelowego, liczby. | M |
| Req18.Z | Wpis zawiera informacje o terminie jego pierwszego i ostatniego wystąpienia | P |
| Req19.Z | Funkcjonalność eksportu informacji o inwentaryzacji urządzeń, aktywnościach systemowych, podatnościach i wykrytych lukach w bezpieczeństwie systemów, sterownikach PLC. | M |
| Req20.Z | Alarm będzie miał następujące stany: nowe, rozwiązane | M |
| Req21.Z | Rozwiązanie powinno umożliwiać łączenie podobnych ostrzeżeń | M |
| Req21.Z | System umożliwi generowanie wzorca ruchu tzw. baseline dla sieci w stanie produkcyjnym oraz stanie w którym wykonywane są prace serwisowe (tzw. maintenance) w celu ograniczenia ilości fałszywych alarmów i możliwości efektywnego monitorowania systemu w czasie prac serwisowych | P |

## Raportowanie

|  |  |  |
| --- | --- | --- |
| **#** | **Wymaganie** | **Priorytet** |
| Req1.R | Możliwość automatycznego harmonogramowania generowanych raportów, tj. zadania czasu wykonania raportu i przesłania go automatycznie na podany adres mail (np. poprzez interfejs API). | M |
| Req2.R | Tworzenie własnych i spersonalizowanych raportów (wybrane funkcjonalności, przypisanie do użytkowników, forma udostepnienia np. mail) | P |
| Req3.R | Eksport danych mapy sieci zasobów i połączeń w postaci raportu. | M |

## Integracja z infrastrukturą i systemami funkcjonującymi u Zamawiającego

|  |  |  |
| --- | --- | --- |
| **#** | **Wymaganie** | **Priorytet** |
| Req1.T | Integracja z urządzeniami Firewall:, Juniper, Cisco ASA lub Palo Alto w celu umożliwienia funkcjonalności IPS | M |
| Req2.T | Integracja z Active Directory w celu uwierzytelnienia użytkowników oraz przypisania ról zdefiniowanych w narzędziu monitorowania do grup użytkowników w AD (Active Directory). Automatyczne wykrywanie użytkowników/grup zdefiniowanych w AD (Active Directory). Integracja dotyczy wyniesionej konsoli administracyjnej oraz samego appliancu. | M |

## Niefunkcjonalne

|  |  |  |
| --- | --- | --- |
| **#** | **Wymaganie** | **Priorytet** |
| Req1.F | Zebrania informacji o fizycznej lokalizacji nowo wykrytych urządzeń (switch/port). | M |
| Req2.F | Eksport danych o urządzeniach do formatu Visio lub innego narzędzia pozwalającego na edycję. | P |
| Req3.F | Dostarczenie licencji koniecznych do uruchomienia i użytkowania narzędzia detekcji anomalii w systemach OT. | M |
| Req5.F | Przeprowadzenie jednodniowego warsztatu dla użytkowników narzędzia detekcji anomalii w systemach OT w PGE EC. | M |
| Req6.F | Wdrożenie nie może wymagać od Zamawiającego konieczności zakupu dodatkowych licencji lub wyposażenia, które nie jest bezpośrednio związane z funkcjonalnością samego narzędzia detekcji anomalii w systemach OT. | M |
| Req7.F | W trakcie wdrożenia nie zostaną wyłączone żadne istniejące i działające systemy OT. | M |
| Req8.F | Wdrażane narzędzie powinno być objęte wsparciem/gwarancją producenta w reżimie Next Buisness Day, przez 5 lat. Wsparcie powinno obejmować również możliwość pobierana aktualizacji systemu oraz nowych definicji i sygnatur. | M |

## Zespół/ Dostawca

|  |  |  |
| --- | --- | --- |
| **#** | **Wymaganie** | **Priorytet** |
| Req1.D | Oferent musi przedstawić skład personalny zespołu wdrożeniowego wraz z opisem doświadczenia zawodowego każdego z członków zespołu. | M |
| Req2.D | Oferent musi dysponować odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia a w tym:   * Wykazać dysponowanie minimum dwiema osobami, posiadającymi przynajmniej 3 - letnie doświadczenie w realizacji zadań będących przedmiotem niniejszego zapytania * Wykazać dysponowanie minimum dwiema osobami, posiadającymi przynajmniej 3 - letnie doświadczenie w zakresie bezpieczeństwa systemów informatycznych. | M |
| Req3.D | Oferent musi zapewnić niezmienność zespołu projektowego w trakcie realizacji projektu. | M |
| Req4.D | Każda zmiana składu zespołu projektowego musi być zaakceptowana przez Zamawiającego. | P |
| Req5.D | Dostawca/integrator rozwiązania musi posiadać udokumentowane referencje wdrożenia systemu w Polsce lub w Europie (z wyłączeniem Rosji). | M |
| Req6.D | Producent rozwiązania musi posiadać zaplecze wywiadowcze analizujące zagrożenia, malware oraz CVEs (Mowa o CVE – Common Vulnerabilities and Exposures, czyli słownik identyfikatorów nadanych podatnościom i zagrożeniom. Projekt tworzenia i utrzymywania słownika jest współfinansowany przez biuro Cybersecurity and Communications Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych. W skrócie jest to po prostu baza podatności. | M |
| Req7.D | Dostawca/integrator musi posiadać grupę ludzi wspierającą użytkownika w szczegółowym analizowaniu i zaawansowanych śledztwach. | P |
| Req8.D | Dostawca/integrator rozwiązania musi przedstawić referencje ilustrujące dojrzałość systemu w postaci ilości i skali wdrożeń komercyjnych (minimum jedno wdrożenie o podobnym zakresie prac). | M |

## Wdrożenie i instalacja

|  |  |  |
| --- | --- | --- |
| **#** | **Wymaganie** | **Priorytet** |
| Req1.W | Dedykowany interfejs do przekazywania informacji o alarmach poprzez e-mail/SMS oraz do systemów klasy SIEM. | M |
| Req2.W | Instalacja urządzenia nie zakłóca żadnych aktywności w sieci i może być przeprowadzona „na ruchu” w trakcie pracy systemu automatyki. | M |
| Req3.W | Krótki proces nauki i budowania modelu sieci OT (poniżej 5 dni). | P |
| Req4.W | Aktualizacja systemu oraz bazy zagrożeń off-line | M |
| Req5.W | Platforma zarządzająca lokalnymi instancjami systemu monitorującego, służąca do:   * agregowania zdarzeń i alertów z poszczególnych instancji, * pokazująca na mapie lokalizację poszczególnych instancji, * mająca pełny wgląd do poszczególnych instancji, * pozwalająca na zarządzanie lokalnymi instancjami, * pozwalająca na korelację zdarzeń, raportów itp. z poszczególnych instancji, * umożliwiająca zdalną aktualizacje instancji. | P |

## Szkolenia

|  |  |  |
| --- | --- | --- |
| **#** | **Wymaganie** | **Priorytet** |
| Req1.S | Przeprowadzenie szkoleń certyfikowanych dla co najmniej trzech administratorów | M |
| Req2.S | Przeprowadzenie szkolenia stanowiskowego dla użytkowników końcowych w formie warsztatów do 20 osób grupa | M |