Incydenty cyberbezpieczeństwa okiem praktyka. 3 złote zasady, jak zabezpieczyć infrastrukturę krytyczną.

Marcin Krzemieniewski

GTM Practice Solutions Manager, Intelligent Infrastructure & Cybersecurity

Bezpieczeństwo automatyki przemysłowej - kluczowy obszar zainteresowań dla NTT

Podejście

- 2016 – powołanie globalnej struktury
- Budowa centrów kompetencji

Zespół

- 30+ – Ekspertów ds. Bezpieczeństwa OT – globalnie
- 10 – Ekspertów ds. Bezpieczeństwa OT – Europa
- 3 – Inżynierów ds. Bezpieczeństwa OT – Polska

Technologia

Pasywne monitorowanie OT:
Claroty / Nozomi / Cyber Vision
Aktywna ochrona i segmentacja:
CheckPoint / Cisco / FortiNet / PaloAlto

Nasi klienci

Projekty referencyjne

- **43** projekty referencyjne
- **21** Klientów z branży energetyki i usług użyteczności publicznej
- **14** projektów w Europie
- **3** w Polsce

Poufność

NTT zrealizowało wiele projektów z zakresu cyberbezpieczeństwa w ramach OT Network. Jednak ponieważ chodzi tu o cyberbezpieczeństwo w czystej postaci, bardzo poważnie traktujemy prywatność i poufność klientów.

Z tego powodu nie możemy ujawnić rzeczywistej nazwy klienta ani kontaktu.

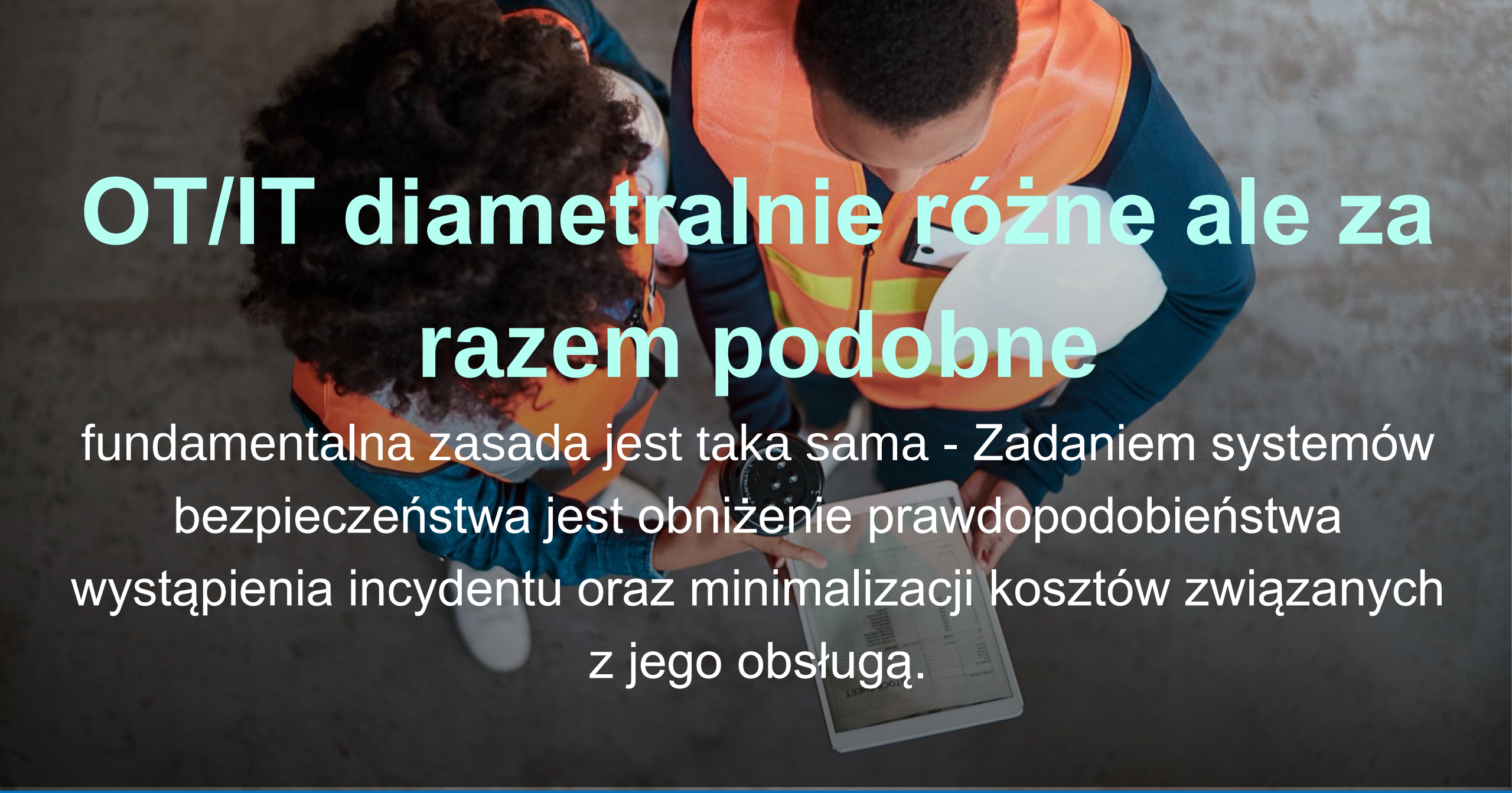
Jeśli chcesz porozmawiać z którymkolwiek z tych klientów, z przyjemnością zaaranżujemy poufną rozmowę bezpośrednią z wybranymi osobami.

Geneza

Projekty bezpieczeństwa w automatyce przemysłowej

Są dwa powody realizacji projektów bezpieczeństwa automatyki przemysłowej:

a. Regulacje
b. Dojrzałość organizacyjna



OT/IT diametralnie różne ale za razem podobne

fundamentalna zasada jest taka sama - Zadaniem systemów bezpieczeństwa jest obniżenie prawdopodobieństwa wystąpienia incydentu oraz minimalizacji kosztów związanych z jego obsługą.

Jak i od czego mamy zacząć?

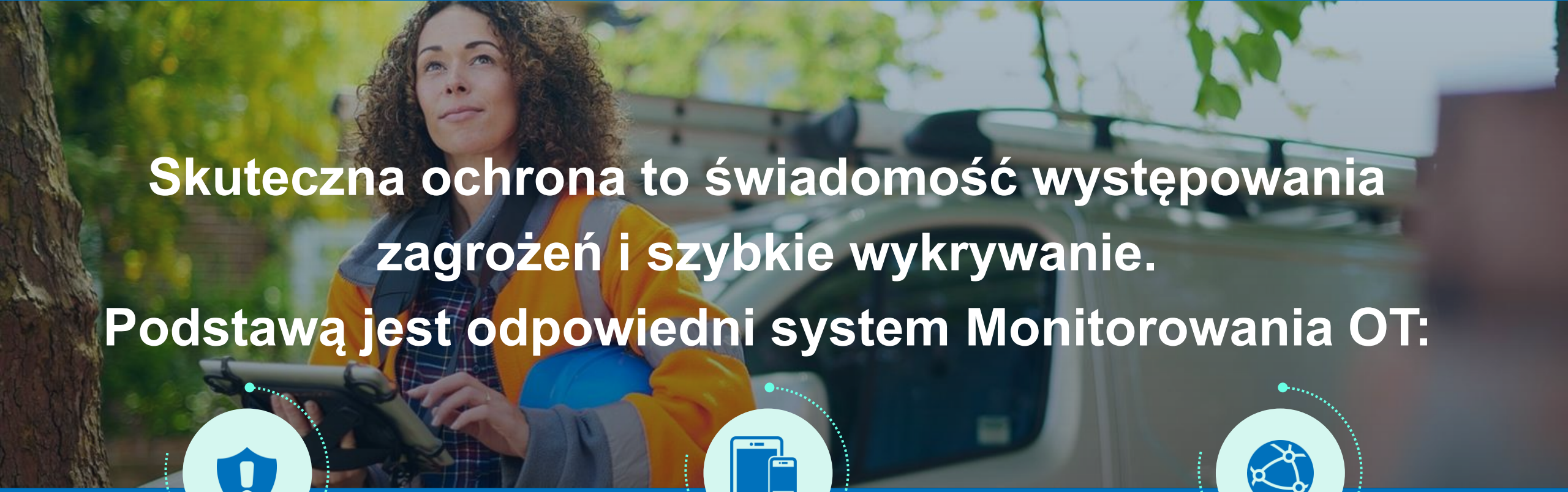
Segmantacja?

Kontrola dostępu?

Patchowanie?

Monitorowanie?

Skąd wiem, że **koncentrujemy się na właściwych obszarach?**



Skuteczna ochrona to świadomość występowania zagrożeń i szybkie wykrywanie.
Podstawą jest odpowiedni system Monitorowania OT:

Taki który nie zakłuci pracy systemu który ma chronić

Taki który zrozumie co się tam w środku dzieje

Taki który wykryje anomalie

Zanim zaczniesz odpowiedz sobie na kilka podstawowych prostych pytań:

Kto będzie na codzień użytkownikiem rozwiązania?

Czy ten ktoś będzie zaangażowany w projekt?

Czy ten ktoś wie jak System ułatwi mu życie?

Czy ten ktoś wie czego system nie zrobi?

Czy ten ktoś jest uczestnikiem czy raczej recenzentem projektu?

Systemy pasywnego monitorowania środowisk ICS/OT

Zasada działania rozwiązań do monitorowania oraz wykrywania anomalii w pracy systemów automatyki przemysłowej

Działa na podstawie **pasywnej** analizy komunikacji z sieci przemysłowej

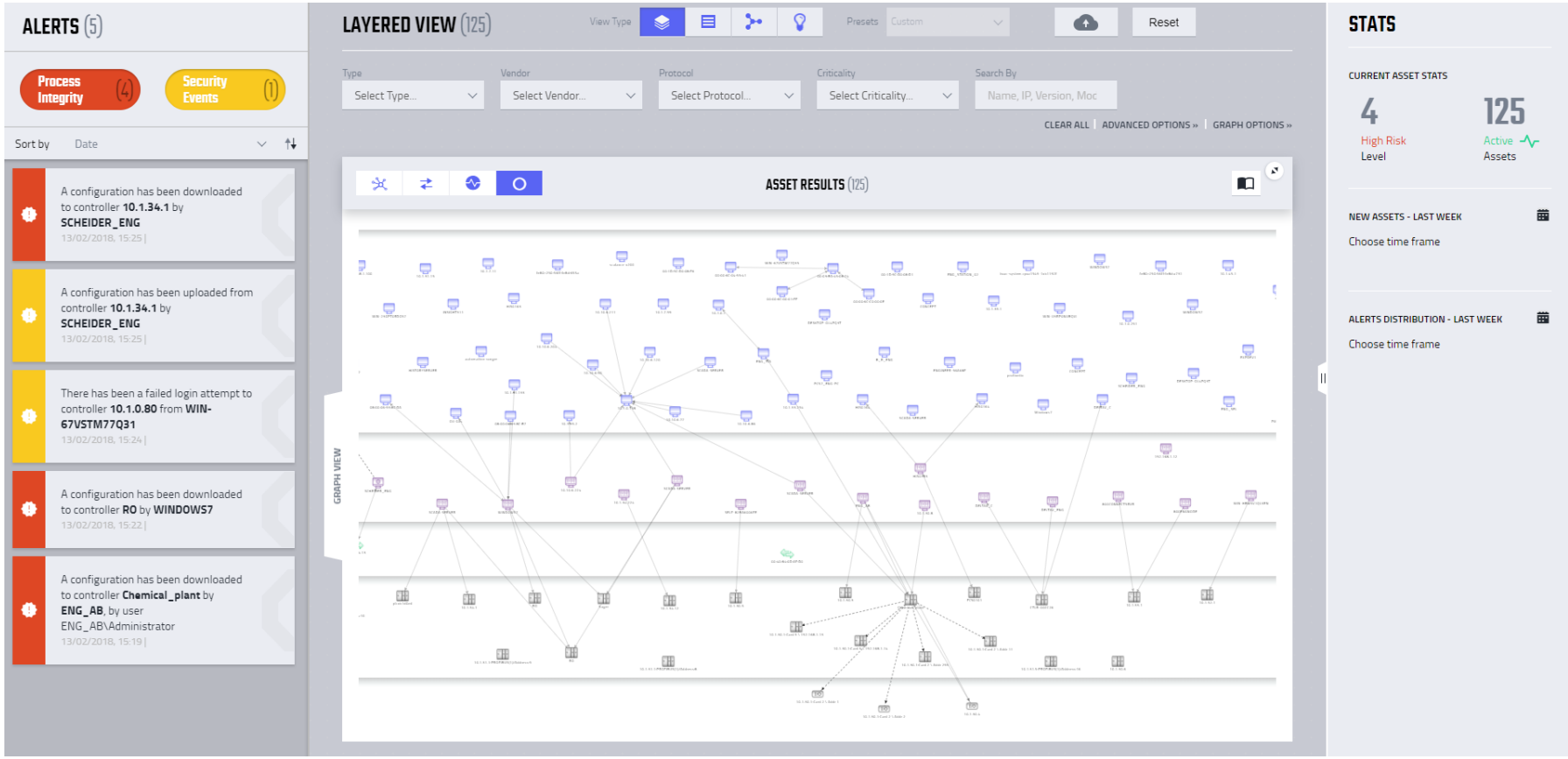
Uczy się wzorca

Informuje o odstępstwach od wzorca, nieautoryzowanych zmianach.

Inwentaryzuje, opisuje i analizuje stan bezpieczeństwa wszystkich wykrytych obiektów

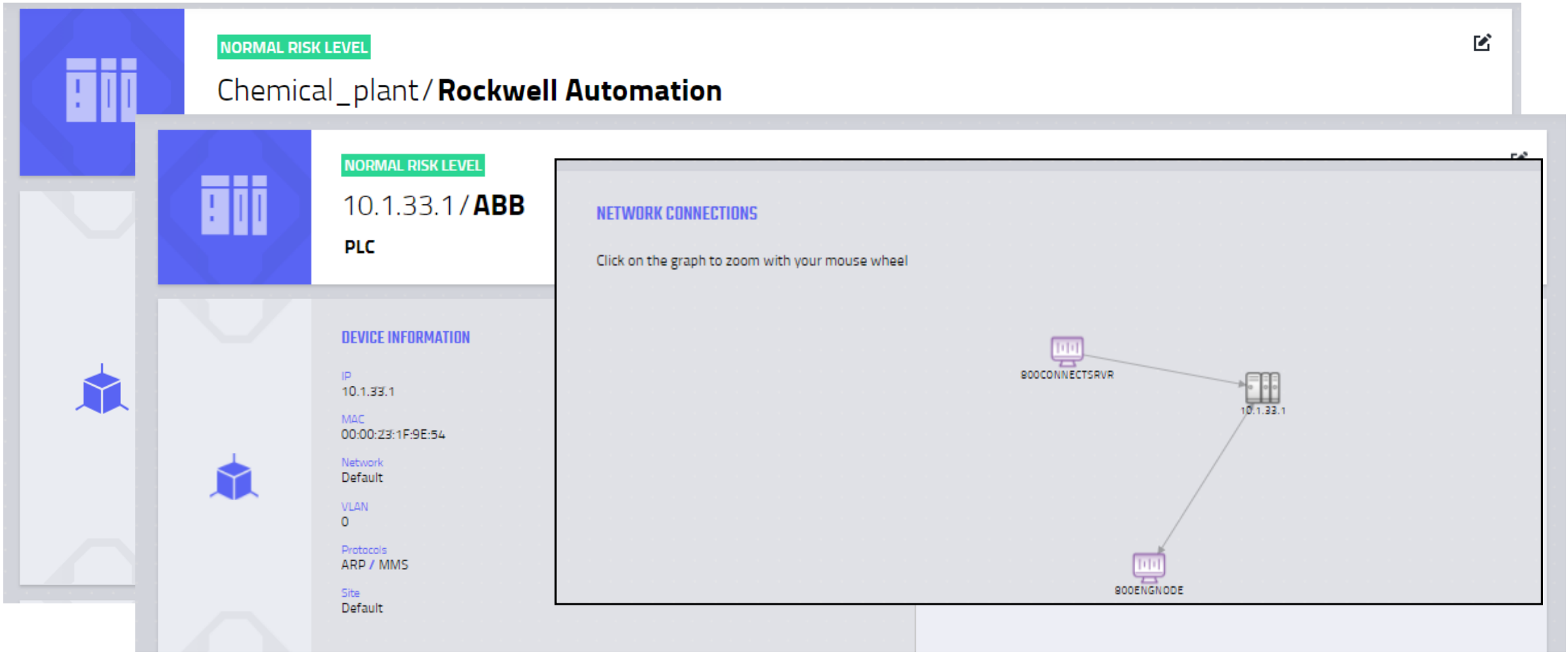
Widok zasobów w podziale na warstwy

Warstwy logiczne (model Perdue) z opcjami grupowania sąsiadów, kierunku komunikacji, modelu ruchu ARP, ukrycia milczących zasobów, komputerów w komunikacji OT ←→ IT



Informacja o zasobach w sieci SCADA (*Assets*)

Typ, producent, wersja oprogramowania, używane protokoły, adresy Ethernet (MAC)



Automatyczne wykrywanie zasobów/analiza protokołów*

„*” robi różnicę

Automatyczne, tak ale dla wspieranych producentów

- Czy wykorzystywane u Ciebie Assety są wspierane przez określone rozwiązanie?

Bogata informacja o zasobach - Typ, producent, wersja oprogramowania, używane protokoły, adresy, tak ale nie dla wszystkich zasobów

- Często konieczne jest uruchomienie „aktywnego odpytywania”, czy jest na to zgoda w Twojej firmie?

Analiza protokołów, tak tych najpopularniejszych

- Jakie protokoły wykorzystuje Twój system OT?
- Czy implementacja jest standardowa, czy może dostosowana specjalnie pod Ciebie?

O czym jeszcze warto pamiętać

Zarządzanie oczekiwaniami

Tuning systemu - rozwiązanie uruchomione i zintegrowane z infrastrukturą Klienta to tylko początek drogi

Odzwierciedlenie rzeczywistego środowiska w systemie to cel

Edukacja w zakresie użytkowania:

- Szkolenia z obszaru utrzymania systemu
- Szkolenia z używania systemu, szkolenia eksploatacyjne

Podsumowanie:

3 złote zasady wdrożenia bezpieczeństwa w OT

Nie daj się rozproszyć

Domena bezpieczeństwa OT jest dzisiaj gorącym tematem, i zapewne wielu dostawców będzie chciało Ci udzielać dobrych rad oraz udowodnić że ich rozwiązania są Ci niezbędne. Doskonały plan nie istnieje i wszystkiego na raz naprawić się nie uda.

Nie komplikuj zbytnio projektu

Wybierz inicjatywę i skoncentruj się na niej. Bezpieczeństwo OT zaczyna się od porządnego monitorowania

Zaangażuj kluczowych odbiorców

Zaangażuj faktycznych użytkowników systemu do wdrożenia od samego początku. To wydaje się oczywiste, ale tematy bezpieczeństwa OT zawsze są realizowanie na styku IT z Automatykami. Zebranie przedstawicieli obu światów jest warunkiem koniecznym dla końcowego sukcesu przedsięwzięcia.

Dalsze kroki

Zrozum swój obecny system cyberbezpieczeństwa i stwórz gotowy plan działania. Umów się na bezpłatne warsztaty online.

Umów się


NTT
Razem robimy
wielkie rzeczy