Public

DYNACON
Connecting Data

Przemysł, komunikacja i cyberbezpieczeństwo

Finanse, korzyści, zagadnienia

Polska odpowiedź na aspekt cyberbezpieczeństwa przemysłowego

Andrzej Cieślak
Prezes Zarządu Dynacon

KORZYŚCI Z PRAWIDŁOWEGO PODEJŚCIA DO CYBERBEZPIECZEŃSTWA

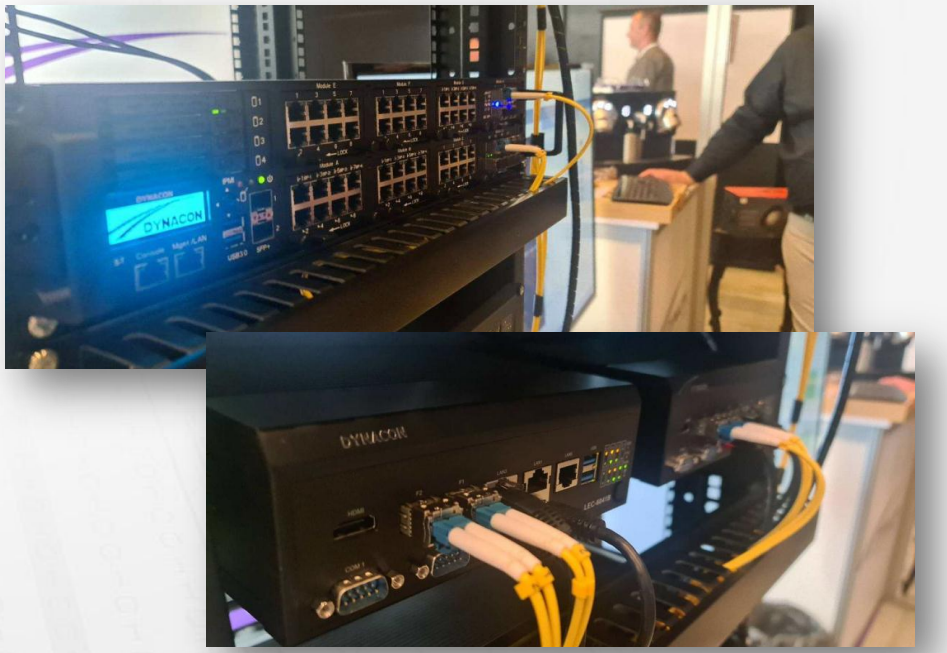
- Pozytywny wpływ na poziom cyberbezpieczeństwa RP
- Wzmocnienie pozycji rynkowej
- Zwiększenie dochodu przy zmniejszaniu kosztów
- Wzmocnienie relacji z dostawcami
- Zgodność prawna
- Minimalizacja ryzyk związanych z ciągłością działania
- Minimalizacja ryzyk związanych z odpowiedzialnością za nieprawidłowości
- Zwiększenie obustronnego zaufania
- Pozytywny komunikat na rynek spowodowany naturalnym rozszerzeniem zakresu
  kompetencyjnego i produktowego o istotne aspekty dla stabilności działania

KORZYŚCI FINANSOWE DLA PRZEMYSŁU

Cyberbezpieczeństwo jako narzędzie minimalizujące koszty produkcji i dystrybucji produktów

Monitoring, widoczność, reakcja, proaktywność

- Mniejsze koszty zakupu oraz eksploatacji przy zachowaniu wysokiego, światowego poziomu jakości, wydajności i stabilności działania systemów OT
- Spełnienie wymogów prawnych, formalnych, normatywnych – NIST, NIS2, ISO 27001, ISO 22301, NERC CIP, Common Criteria
- Spełnienie wymagań branżowych: m.in.: EMC: CE, FCC Class A, Safety: CB, UL, C1D2, IEC 61850-3, IEEE 1613, IEC 62443 a tym samym minimalizacja usterek wynikających z niekompatybilności
- Zmniejszenie kosztów inwestycji, remontów, produkcji, dystrybucji poprzez zmniejszenie usterek i awarii, skrócenie czasu usunięcia awarii, zmniejszenia kosztów utrzymania ruchu
- Zwiększenie cyberodporności i tym samym zwiększenie poziomu utrzymania ciągłości działania – mniejsze koszty pracy firmy
- Wzmocnienie wizerunku firmy
- Uproszczenie otrzymania lub utrzymania certyfikacji: IFS, ISO 27001, ISO 22301, NERC CIP i innych



4

BRANŻE Z SYSTEMAMI PRZEMYSŁOWYMI

GŁÓWNE ZAGADNIENIA

Energetyka, Chemia, Woda, …

ZAGADNIENIA PRODUKCJI i DYSTRYBUCJI PROCESOWEJ

Systemy pracujące, co do zasady, bez przerw. Przerwy technologiczne są realizowane bardzo rzadko. Dla przykładu, dla energetyki występuje ona co kilka miesięcy lub co kilka lat. Podczas eksploatacji produkcyjnej, możliwości zmiany w systemach cyfrowych czy technologicznych jest w zasadzie niemożliwa lub obarczona dużymi kosztami. Wrażliwość na czynniki zewnętrzne, zaburzenia działania komponentów lub materializacji jest bardzo duża. Odporność komponentów stosowanych w systemach przemysłowych, na niestandardowe zastosowanie lub wystawienie na niestandardowe warunki cyfrowe, jest znikoma lub bardzo mała. Sposób przygotowania oprogramowania oraz wdrożenia systemów APKiA czy systemów sterowania procesem technologicznym nie obejmuje (często z powodu niedostosowania samych komponentów jak i wiedzy instalatorów, projektantów, inżynierów) jakiegokolwiek obszaru związanego z odpornością na anomalie. Bezpieczeństwo procesu jest wysokie ale jest oparte o rozwiązania budowlane, mechaniczne, fizyczne, chemiczne, samego procesu technologicznego. Nie wprowadza się technologii cyfrowych do obszaru bezpieczeństwa technologicznego jak i automatyki przemysłowej.

Montażowa lub reakcyjna produkcja liniowa

ZAGADNIENIA PRODUKCJI GNIAZDOWEJ I DYSKRETNEJ

Systemy pracujące, co do zasady, w zakładanych interwałach, w granicach od kilku sekund do kilkunastu godzin. Podejście do części ICS w głębokim OT jest analogiczne jak w systemach procesowych, jednakże większość procesów nadrzędnych jest realizowana z poziomu aplikacji nadrzędnych, administrowanych często przez służby IT. Punkty styku pomiędzy strukturami IT oraz OT wystawiony jest na szereg zagrożeń począwszy od braku poprawnej segmentacji pomiędzy OT a IT oraz OT od przestrzeni publicznej (niezaufanej) do naturalnie szkodliwego wpływu systemów i procedur IT na komponenty i linie produkcyjne OT.

Bezpieczeństwo procesów jest realizowane poprzez wprowadzanie ochrony przed wpływem człowieka na struktury i systemy przemysłowe oraz przyjęte procedury na poszczególnych obiektach. Zagadnienia bezpieczeństwa cyfrowego, w zależności od branży i zespołu jest pomijane lub lekceważone ze względu na brak świadomości wpływu wzajemnego (cyberbezpieczeństwa i produkcji), w wyniku którego wpływa się w sposób zasadniczy na koszty produkcji i rentowność procesów biznesowych.

5

ZASADNICZE ZAGADNIENIA CYBERODPORNOŚCI W OT

Przyczyna pierwotna niskiego poziomu odporności cyfrowej

Od projektu po utylizację – jeden, wielki, niezagospodarowany obszar.

Niestety do chwili obecnej inwestorzy działający w sektorach OT położyli nacisk na zakup sprzętu i oprogramowania, które w większości przypadków nie przynoszą wymiernych efektów. Brak podejścia „Security by Design” w OT, stanowi pośrednią, lecz jedną z największych przyczyn materializowania się zagadnień i zagrożeń.

Wpływ konsekwentnie wywierany na producentów, oraz na dostawców rozwiązań OT już przynosi minimalne ale zauważalne efekty w zakresie cyberodporności.

W roku 2022 w środowiskach OT ARIC NDS zarejestrował ponad 80 milionów alarmów (wartość po eliminacji fałszywych potwierdzeń „false positive”) z czego ponad 90% pochodziło z wewnętrznych systemów OT i ich infrastruktury sieciowej.

- **57% alarmów** jest generowanych ze względu na błędy; architektoniczne systemów OT, oprogramowania, implantacji, instalacji urządzeń oraz systemów operacyjnych.
- **26% alarmów** jest generowanych na styku z siecią IT, gdzie część zawiera styk z siecią Internet
- **17% alarmów** jest generowanych poprzez działania osób wewnątrz struktur i segmentów sieci OT

6 ZASADNICZE ZAGADNIENIA CYBERODPORNOŚCI W OT

Przyczyna pierwotna niskiego poziomu odporności cyfrowej

Od projektu po utylizację – jeden, wielki, niezagospodarowany obszar.

Większość zagadnień, generowanych alarmów i incydentów, jest klasyfikowana jako awarie i usterki, mające swoje podłoże
w nieprawidłowej architekturze sieci i systemów – fizycznej i logicznej.

Nawet przy akceptacji zagadnień i anomalii pierwotnych w komponentach OT, ich uruchamianie z zachowaniem prawidłowego zaprojektowania, implementacji oraz inicjacji w zasadniczy sposób minimalizuje wpływ tych zagadnień na ciągłość działania całości środowiska.

PRZYCZYNY POWSTAWANIA ZAGADNIEŃ ZASADNICZYCH DLA 100% INSTALACJI OT

- Brak segmentacji pionowej i poziomej.
- Brak kontroli ruchu wewnątrz poszczególnych sieci OT.
- Przenoszenie routingu na strefę DMZ lub wręcz DZ (np. na UTM zainstalowany na styku z siecią IT lub wręcz z siecią Internet).
- Nakładające się adresacje pul IP pomiędzy poszczególnymi systemami OT.
- Minimalne użycie zarządzalnych urządzeń aktywnych, pozwalających
  na prawidłową segmentację i kontrolę ruchu wraz z jego kształtowaniem ze zintegrowanym kolekcjonowaniem i analityką danych przepływowych.
- Brak standaryzacji dla sieci OT w zakresie architektury komunikacji.
- Wprowadzanie bezpośrednich połączeń pomiędzy systemami OT.
- Utrzymywanie nieprawidłowej architektury w centralnych systemach sterowania np. DCS.
- Praca niekompatybilnych technologicznie komponentów w jednej sieci.
- Brak utwardzenia źródeł danych (m.in. urządzeń) generujących ruch w sieci.
- Brak sieciowej architektury logicznej w środowiskach zwirtualizowanych.
- Brak lub zasadnicze błędy w synchronizacji czasu.
- Łączenie niekompatybilnych protokołów i charakterystyk ruchu na jednym trakcie komunikacyjnym.
- Łączenie grup funkcyjnych MGMT/MNTS oraz ruchu procesowego
  na jednym interfejsie komunikacyjnym w tym protokołów backbone rodem z IT.
- Szczątkowe środowiska OT z wydzielonymi sieciami MGMT/MNTS.
- Prawidłowego zaprojektowania, implementacji oraz inicjacji w zasadniczy sposób minimalizuje wpływ tych zagadnień na ciągłość działania całości środowiska.

PRZYCZYNY POWSTAWANIA ZAGADNIEŃ ZASADNICZYCH DLA 24% INSTALACJI OT.

Oprogramowanie i jego konfiguracja oraz wdrożenie

- Instalacja rozwiązań aplikacyjnych bez utwardzenia systemu.
- Brak lub szczątkowa kontrola dostępu pomiędzy kontami
  lub kont do obiektów logicznych.
- Obniżanie poziomów bezpieczeństwa, poprzez stosowanie kont z najwyższymi uprawnieniami do realizacji prostych, lokalnych działań.
- Błędy kompatybilności aplikacji ze środowiskiem uruchomieniowym – w szczególności w środowiskach Windows wykorzystujących platformę .Net.
- Niestabilności poszczególnych składowych oprogramowania instalowanego na serwerach centralnych.
- Brak konfiguracji urządzeń aktywnych w urządzeniach typu PLC,
  czy panel HMI zintegrowany ze sterownikiem, falownikach, itd.
- Niekompatybilności implementacyjne stosów protokołów dla urządzeń bezpośrednio sąsiadujących, powodujących niezgodności w wymianie danych.
- Wady produktów OT w zakresie synchronizacji układów active-standby.

9

PRZYCZYNY POWSTAWANIA ZAGADNIEŃ ZASADNICZYCH DLA 12% INSTALACJI OT

Budowa i wdrażanie rozwiązań monitorowania i cyberbezpieczeństwa

- Nieprawidłowe łączenie segmentów sieci OT, które powinny pozostać odseparowane.
- Przenikania ruchu pomiędzy wyspami OT, niegdyś niepołączonymi.
- Wprowadzanie niekompatybilnych protokołów L2 dla enkapsulacji 802.3 i pochodnych.
- Wprowadzanie ruchu monitorowania na tych samym traktach co ruch procesowy.
- Wprowadzanie skanowania komponentów OT bez analizy wpływu i właściwego przygotowania się do konsekwencji skanowania.
- Skanowanie bez dostosowanych narzędzi i ich konfiguracji powodujących bezpośrednie zagrożenie dla działania procesów.
- Brak lub minimalna eliminacja false positive.
- Przekazywanie większości danych do analizy do systemów centralnych.
- Użycie oprogramowania cyberbezpieczeństwa niezgodnie z jego przeznaczeniem.
- Próby implementacji diod danych bez dostosowania aplikacji i systemów do przepływu jednokierunkowego

OBSZAR FINANSOWY, FORMALNY, OPERACYJNY, PRAWNY I KOMPETENCYJNY

Działania prawne, formalne, normatywne

Problemy i ryzyka materializowane już na pierwszych etapach projektów

- Wyciek istotnych danych o procesach produkcji realizowanych na podstawie podpisywanych umów. Należy wymienić także przenoszenie lub próby przenoszenia danych oraz aplikacji funkcyjnych czy obliczeniowych do operatorów chmurowych.
- Wprowadzanie zespołów SOC bez specjalizacji obiektowej, jedynie na podstawie wewnętrznych uwarunkowań, błędów zakupowych, błędów strategicznych.
- Brak budowanych polityk bezpieczeństwa dla OT.
- Brak dedykowanych (rozłącznych w stosunku do IT) budżetów dla cyberbezpieczeństwa OT. W chwili obecnej większość zakupów bazuje na zasadzie dodatkowych, minimalistycznych, środków dla pokrycia wymagań minimalnych, w celu uniknięcia potencjalnych sankcji.
- Łączenie IT i OT na każdym poziomie, gdzie należy to realizować jedynie na poziomie nadrzędnym, bez możliwości komunikacji reaktywnej do obszaru OT.
- Brak blokad dla zakupów i dostaw rozwiązań i usług cyberbezpieczeństwa od firm, które nie są zweryfikowane przez właściwe służby oraz nie są dla nich transparentne.

11

OBSZAR FINANSOWY, FORMALNY, OPERACYJNY, PRAWNY I KOMPETENCYJNY

Działania prawne, formalne, normatywne

Problemy i ryzyka materializowane już na pierwszych etapach projektów

- Spory wewnętrzne w organizacjach (walka IT z OT, nieporozumienia wydziałów prawnych z wydziałami merytorycznymi, brak dostosowania procedur zakupowych
  do faktycznych wymogów cyberbezpieczeństwa).
- Nadal widoczny proceder sterowania zakupami dla uzyskania własnej korzyści (nawet jeśli nie jest to bezpośrednia korzyść majątkowa w kontekście korupcji, a jedynie zapewnienie sobie, lub danej komórce w organizacji, niezbywalnej podstawy do istnienia i utrzymania świadczeń).
- Brak zapewnienia włączenia i stałej obecności ekspertów cyberbezpieczeństwa OT do generowania wymogów dla budowy systemów OT.
- Brak zespołów projektowych włączanych na wstępnych etapach decyzyjnych, mających na celu wprowadzenie istotnych zmian w środowisku OT lub budowy nowej inwestycji.
- Wprowadzanie na stanowiska eksperckie osób bez jakiegokolwiek przygotowania do pełnienia tej funkcji.
- Wprowadzanie do OT rozwiązań oraz procedur przyjętych w IT co jest niezgodne z NIST oraz IEC jak i NERC CIP.

REKOMENDACJE FINANSOWE W KONTEKŚCIE CYBERODPORNOŚCI

- Wydzielić budżet OT względem IT jako niezależny proces i źródło finansowania projektów cyberbezpieczeństwa OT.
- Wzmocnić pozycję cyberbezpieczeństwa poprzez wprowadzenie zespołów ekspertów do najwcześniejszych faz realizacji inwestycji lub istotnych zmian.
- Włączyć zespół cyber do całości obszaru bezpieczeństwa jako stały obszar realizujący zadania utrzymania ciągłości działania w całej fazie eksploatacji jak i życia poszczególnych systemów i infrastruktury OT oraz ich komponentów.
- Wzmocnić nacisk na budowanie właściwych wymagań dla dostawców systemów OT i przestrzeganie normatywów np. IEC 62443, wytycznych NERC CIP czy rekomendacji ENISA, NIST, po dostosowaniu ich do polskich warunków w zakresie cyberbezpieczeństwa OT.
- Wesprzeć polskie zespoły produkcyjne, wdrożeniowe, usługodawcze, które pozostają pod polską kontrolą i nadzorem służb oraz organów właściwych w zakresie bezpieczeństwa kraju.
- Wesprzeć procesy zakupowe oraz inwestycyjne w ramach zamówień publicznych poprzez nadrzędność zapisów merytorycznych nad cenowymi, z uwzględnieniem eliminowania dostawców, produktów i osób, mających sprzeczne interesy z interesem bezpieczeństwa Państwa Polskiego oraz pochodzących z krajów lub dostawców wysokiego ryzyka.

REKOMENDACJE cd.

- Stosować urządzenia zarządzalne sieci wraz z wbudowanymi kolektorami i analizatorami danych.
- Włączyć aspekt cyberbezpieczeństwa do procedur projektowych i odbiorowych jako wymóg podstawowy dla Testów Odbiorowych na Obiekcie (SAT) z kwalifikacją niezgodności cyberbezpieczeństwa jako wada produktu dostarczanego przez Wykonawcę.
- Wprowadzić wymagania projektowe w OT z przestrzeganiem zasad separacji, segmentacji, zarządzania, monitorowania, ekstrakcji i analityki danych z zachowaniem bezpieczeństwa w technikach reaktywnych
- **NIE WYPROWADZAĆ DANYCH PO ZA POLSKĘ**
- **WSPIERAĆ POLSKIE ROZWIĄZANIA KTÓRE MOŻNA NADZOROWAĆ**
- **NIE POZWALAĆ NA BYCIE SĘDZIĄ WE WŁASNEJ SPRAWIE**
- Zachować i promować separację OT oraz IT w całej integracji pionowej
- Umożliwić integrację cyberbezpieczeństwa IT i OT na poziomie, któremu nie wolno wprowadzać taktycznych i operacyjnych zmian bezpośrednio w środowisko OT.
- Promować rozwiązania rozproszone, odporne na atak fizyczny.
- Wydawać rekomendacje dla użycia chmury jedynie w uzasadnionych przypadkach z koniecznością wprowadzania własnych, struktur bezpieczeństwa.
- Wprowadzać specjalistyczne szkolenia i treningi bojowe z obowiązkowymi egzaminami kwalifikującymi do realizacji zadań w zakresie cyberbezpieczeństwa przemysłowego, a w szczególności w obszarze Infrastruktury Krytycznej Kraju.
- **EGZEKWOWAĆ POLSKIE PRAWO**

POLSKA ODPOWIEDŹ
WSPÓŁPRACA ZESPOŁOWA

- Wzajemne wsparcie prawne
- Współprojektowanie umów i zapisów kontraktowych
- Wsparcie technologiczne, techniczne, formalne i proceduralne w trakcie realizacji zadań inwestycyjnych lub remontowych
- Wsparcie prawne na styku biznesu z procedurami OT
- Wsparcie w audytach zgodności z wymaganiami technicznymi prawnymi, formalnymi i normatywnymi
- Wsparcie w reprezentacji firmy przed organami właściwymi
- Wsparcie techniczne w całym cyklu życia infrastruktury OT
- Projektowanie rozwiązań komunikacji i cyberbezpieczeństwa jako niezależny system OT w sekcji AKPiA
- Audyty techniczne w zakresie komunikacji, architektury, zgodności normatywnej, cyberodporności, kompatybilności technologicznej
- Audyty cyberbezpieczeństwa i zgodności z wymaganiami prawnymi, formalnymi i normatywnymi
- Dostosowywanie rozwiązań dla OT na poziomie programistycznym
- Wprowadzanie indywidualnych rozwiązań w systemach cyberbezpieczeństwa
- Stosowanie innowacyjnych rozwiązań
- Wsparcie w identyfikacji i rozumieniu danych generowanych w systemach OT
- Współpraca IT z OT a nie zawłaszczanie

15 OFERTA ZINTEGROWANA

Kierunki, droga, narzędzia, produkty.

- Pełna kompatybilność sprzętu i oprogramowania z większością systemów międzynarodowych
- Integrowanie rozwiązań z lokalnymi systemami, produktami, programami
- Zapewnienie spełnienia lokalnych wymogów: prawnych, technicznych, technologicznych, normatywnych, zwyczajowych, kulturalnych, dobrych praktyk
- Transfer wiedzy
- Krótkie czasu dostaw
- Stock magazynowy dla urządzeń, osprzętu, akcesoriów, części zamiennych
- Szkolenia handlowe i stałe wsparcie handlowe
- Szkolenia techniczne, Egzaminy, Certyfikacje, Treningi bojowe i stres testy

OFERTA MIĘDZYNARODOWA

Sieciowy sprzęt komunikacyjny, cyberbezpieczeństwa, monitorowanie pasywne, platformy reakcyjne,

URZĄDZENIA AKTYWNE SIECI PRZEMYSŁOWYCH ORAZ IT

- Przełączniki Ethernet 802.3, Profinet, EtherNet/IP
- Routery
- Firewalle
- IDS/IPS
- VPN
- MPLS
- BGP
- Sondy Danych
- Diody Danych
- TAPy
- Analizatory
- Preprocesory
- Kolektory danych

Montaż i zasilanie

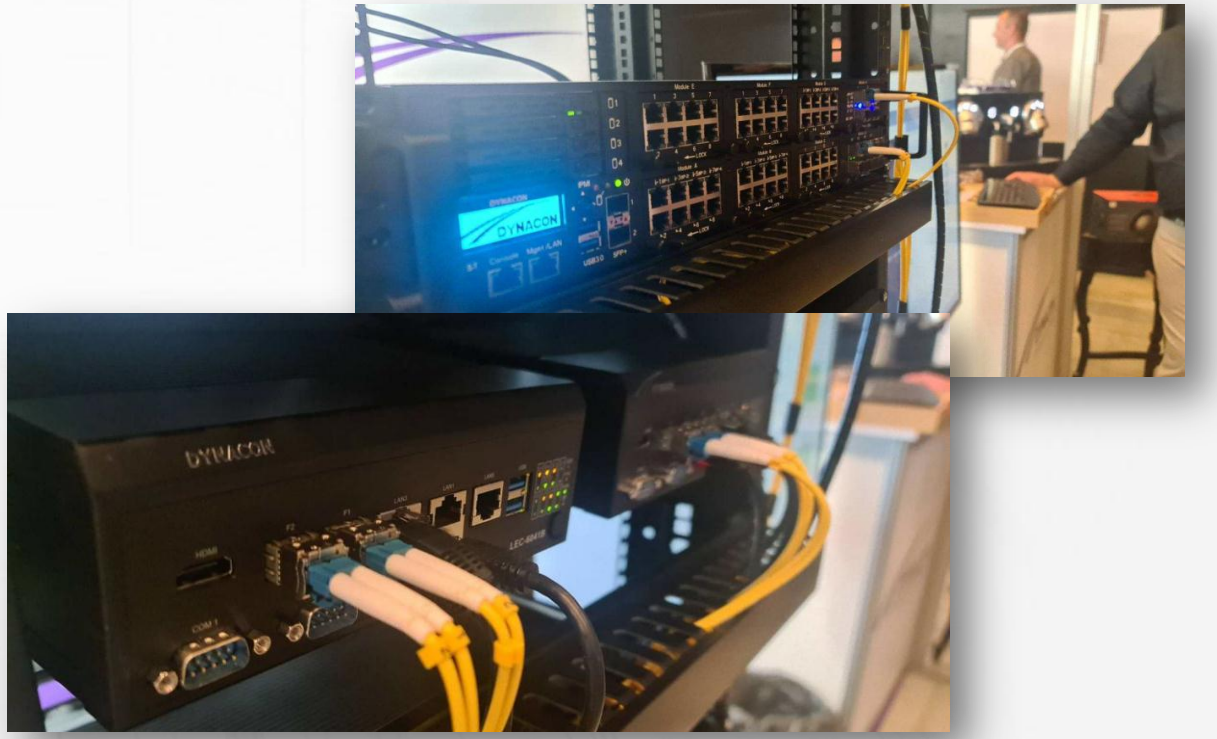
- Przemysłowa Szyna DIN
- Szafa RACK 19”
- Płyta montażowa
- Stand alone
- Redundantne zasilanie DC i AC

OFERTA MIĘDZYNARODOWA w 100 % POLSKIEJ FIRMY DYNACON

Centralne i rozproszone systemy cyberbezpieczeństwa,

Aplikacje monitorowania, wizualizacji, detekcji, reakcji, zarządzania, integracji, forensic, skanowania, oceny bezpieczeństwa, compliance

- SIEM – ARIC Network Defence System
- IDS – Industrial Intrusion Detection System
- SCADA
- Detektory i profiler
- Wizualizacje danych
- DWH
- Platformy administracyjne
- Skanery podatności
- Systemy BPM
- Aplikacje dedykowane
- Automatyka zarządzania dostępem
- CMDB
- Systemy sztucznej inteligencji, DL, ML



OFERTA ZINTEGROWANA

Kierunki, droga, narzędzia, produkty.

- Pełna kompatybilność sprzętu i oprogramowania z większością systemów międzynarodowych
- Integrowanie rozwiązań z lokalnymi systemami, produktami, programami
- Zapewnienie spełnienia lokalnych wymogów: prawnych, technicznych, technologicznych, normatywnych, zwyczajowych, kulturalnych, dobrych praktyk
- Transfer wiedzy
- Krótkie czasu dostaw
- Stock magazynowy dla urządzeń, osprzętu, akcesoriów, części zamiennych
- Szkolenia handlowe i stałe wsparcie handlowe
- Szkolenia techniczne, Egzaminy, Certyfikacje, Treningi bojowe i stres testy

OFERTA ZINTEGROWANA

Kierunki, droga, narzędzia, produkty.

- Projektowanie rozwiązań
- Oceny bezpieczeństwa
- Testy podatności i testy penetracyjne
- Security Operations Center 24/7/365
- Nadzory projektowe
- Wsparcie procesowe, rozwiązywanie sporów
- Audyty techniczne w zakresie komunikacji, architektury, zgodności normatywnej, cyberodporności
- Audyty cyberbezpieczeństwa i zgodności z wymaganiami prawnymi, formalnymi i normatywnymi
- Stałe aktualizacje systemów, sygnatur, paczek bezpieczeństwa,
- Wsparcie inżynierskie przez wysoko-certyfikowane zespoły

20 WSPÓŁPRACA DODATKOWA

Kierunki, droga, narzędzia, produkty.

Materializacja współpracy

- Sympozja i konferencje prasowe
- Budowa centrum kompetencyjnego Dynacon i NCSA na terenie danego kraju
- Opracowania – raporty, artykuły merytoryczne
- Projektowanie umów i zapisów kontraktowych
- Projektowanie wymagań dla procesów inwestycyjnych lub remontowych
- Konsultacje merytoryczne
- Możliwość zapewnienia zespołu posługującego się językiem lokalnym
- Wspólna budowa HUBów kompetencyjnych, show room, sal szkoleniowych i treningowych,

DO KOGO KIERUJEMY OFERTĘ

Rodzaje firm

- Firmy wdrożeniowe automatyki przemysłowej
- Firmy handlowe – branża OT i IT
- Automatyka przemysłowa, BMS, sieci komputerowe, bezpieczeństwo
- Generalni wykonawcy
- Biura projektowe
- Firmy wdrożeniowe systemów cyberbezpieczeństwa
- Zakłady produkcyjne – produkcja procesowa
- Elektrownie, elektrociepłownie, chemia, woda, żywność, petrochemia, gaz
- Zakłady dystrybucyjne – dystrybucja produktu ciągłego
- Zakłady produkcyjne – liniowe, gniazdowe
- Automotive, farmaceutyka, suplementacja, kosmetyka, linie produkcyjne

Sektory i branże przemysłowe

- Elektroenergetka, ciepłownictwo
- Chemia
- Woda
- Odnawialne źródła energii
- Kopalnie
- Automotive
- Farmaceutyka
- Sumplementacja diety
- Produkcja żywności
- Transport – Lotniczy, kolejowy, drogowy
- Produkcja liniowa i gniazdowa
- Kosmetyka
- Rolnictwo zmechanizowane i zautomatyzowane

ZASTOSOWANIE

- Komunikacja sieciowa Ethernet w przemyśle oraz IT
- Strefy EX o podwyższonym ryzyku wybuchu lub zapłonu – strefa 2 – CB, UL, C1D2
- Podstacje energetyczne – IEEE 1613, IEC 61850-3
- Instalacje „safety” – systemy bezpieczeństwa technologicznego, ochrona zdrowia i życia
- Komunikacja, monitorowanie i cyberbezpieczeństwo w systemach PLC, PCS, DCS, PMS, Teletechnika, Bezpieczeństwo techniczne

KORZYŚCI ZE WSPÓŁPRACY

- Pozytywny wpływ na poziom cyberbezpieczeństwa klientów i krajów w których działają
- Wzmocnienie wagi produktów dostarczanych do klientów
- Zwiększenie przychodu dla firm wdrożeniowych i handlowych
- Zmniejszenie kosztów produkcji i dystrybucji
- Wzmocnienie relacji z klientem
- Zwiększenie zaufania klienta
- Pozytywny komunikat na rynek spowodowany naturalnym rozszerzeniem zakresu kompetencyjnego i produktowego o istotne aspekty dla stabilności działania klientów
- Tańsze realizowanie zadań inwestycyjnych, modernizacyjnych wymagających komunikacji sieciowej i cyberbezpieczeństwa

DZIĘKUJEMY ZA UWAGĘ