Cyberbezpieczeństwo Środowiska OT Infrastruktury Kluczowej i Krytycznej

Life Is On | Schneider Electric

www.se.com/pl

DYNACON

Kompleksowe podejście do bezpieczeństwa

Cyberbezpieczeństwo od dłuższego czasu jest koniecznością oraz wymogiem prawnym, które kompleksowo dostarcza Schneider Electric wraz z Dynacon niezależnie od branży przemysłu. W tworzeniu urządzeń i rozwiązań wdrażane są rygorystyczne polityki, metodologia oraz nastawienie.

Usługi takie, jak: audyt inwentaryzacyjny i kwalifikacyjny, szacowanie ryzyka, implementacja systemów cyberbezpieczestwa oraz ich utrzymanie w trybie 24/7, pozwalają w profesjonalny sposób chronić infrastrukturę krytyczną w przemyśle.

Korzyścią dla użytkowników systemów oraz wyróżnikiem wspólnej oferty cyberbezpieczeństwa Schneider Electric i Dynacon jest pełne zrozumiemienie procesów technologicznych, wymagań oraz polityk IT występujących w wielu branżach przemysłu.

Bezpieczne produkty i rozwiązania

Wdrożony **Program Rozwoju Cyberbezpieczeństwa**

2200 Przeszkolonych pracowników

70 Inżynierów z certyfikatami

5 Hubów R&D certyfikowanych IEC 62443

>75 Certyfikowanych produktów

achilles

ISASecure

Usługi Cyberbezpieczeństwa

>100 Ekspertów Usług Cyberbezpieczeństwa

- Audyty oraz Szacowanie Ryzyk
- Konsultacje Cyberbezpieczeństwa
- Projekt oraz wdrożenie systemu
- Szkolenia
- Utrzymanie i serwis
- Security Operation Center

Zalecenia i rozwiązania wypełniają wytyczne Rady Cyberbezpieczeństwa Przemysłowego oraz Rządowego Centrum Bezpieczeństwa.

Cyberbezpieczeństwo w trybie end-to-end z innowacjami na każdym poziomie działania procesów technologicznych.

Produkty IIoT

W sprawie bezpieczeństwa nie ma czasu do namysłu, głównie jeżeli chodzi o komponenty sprzętowe. Bezpieczeństwo uwzględniane jest od systemów automatyki – używając komponetów które spełniają wymagania bezpieczeństwa.

Sterowanie

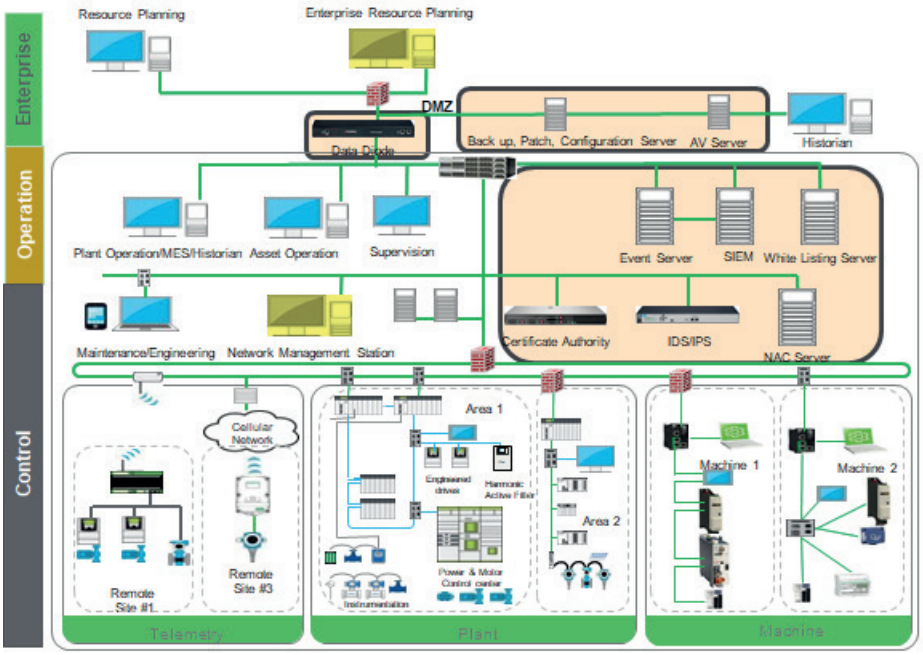
Implementacja bezpieczeństwa podczas budowy oraz procesów rozbudowy systemu, z zastosowaniem rygorystycznych testów i walidacji, w celu zapewnienia odpowiedniej niezawodności systemów sterowania.

Aplikacje, Analiza i Usługi

Bezpieczeństwo musi być częścią budowy aplikacji i jej rozwoju, fundamentalnie wbudowanym w usługi które wspierają pracę i cykl życia systemu przemysłowego.

System bezpieczeństwa A.R.I.C. IDCS AIN® – rewolucja w sieciach przemysłowych

System A.R.I.C. IDCS® z modułem AIN® jest rozwiązaniem uczenia maszynowego sprzężone z systemami klasy SIEM lub ADB czy RAD, dedykowanymi dla cyberbezpieczeństwa i komunikacji OT oraz ICT. Pozwala na znaczącą redukcję kosztów związanych z zarządzaniem siecią przemysłową wraz z jednoczesnym, wysokim poziomem cyberbezpieczeństwa i zachowaniem ciągłości działania procesów technologicznych. System wspiera sieci w czasie rzeczywistym i jest w pełni kompatybilny z takimi protokołami przemysłowymi, jak Modbus TCP, Pofinet RT/IRT czy Ethernet/IP. Warunkiem wdrożenia systemu jest jedynie poprawne przygotowanie sieci (np. zgodnie ze standardami CPwE® i IACS®) i docelowo przekazanie sterowania do IDCS®. Systemy AIN® pracują najbardziej efektywnie dla topologii rozproszonych. Co jest istotne, przygotowanie sieci nie wymaga znaczących inwestycji i rozwiązania AIN® mogą być wdrażane etapowo, co dodatkowo zwiększa bezpieczeństwo i łatwość implementacji w zakładach przemysłowych. Rozwiązanie AIN® może być obsługiwane przez operatorów, którzy nie są administratorami. Ich jedyne zadanie polega na wskazaniu systemów, które muszą wymieniać dane pomiędzy sobą, a system IDCS już samodzielnie dokona odpowiednich konfiguracji urządzeń sieciowych – przełączników, routerów, firewalli, IPS i innych systemów zarządzalnych jak i komponentów systemów sterowania.



Systemy bezpieczeństwa styku ze środowiskiem Enterprise i Operation

Systemy bezpieczeństwa styku ze środowiskiem Enterprise i Operation. Wizualizacja informacji. Systemy reakcyjne, warstwa zarządzania

Kolektory, analityka i reakcja FOG, pasywna analiza strumieni danych deterministycznych, ochrona komunikacji systemów technologicznych, monitorowanie OT, kontrola przepływu sygnałów

Korzyści wynikające z wdrożenia systemu:

- Integracja z istniejącymi urządzeniami oraz systemami
- Redukcja kosztów przez zarządzanie urządzeniami aktywnymi w trybie pełnej autonomii
- Monitorowanie incydentów przez moduł SIEM dla OT – minimalizacja czasu reakcji
- Analityka danych w trybie pasywnym, co nie wpływa na ruch deterministyczny
- Kolekcjonowanie danych
- Zabezpieczanie zebranych danych dla postępowania dowodowego
- Uczenie maszynowe oraz realizacja funkcji poznawczych dla środowisk kognitywnych za pomocą modułu sztucznej inteligencji
- Inteligentne śledzenie oraz profilowanie aktywne obiektów magistrali OT
- Mapowanie dynamicznego ruchu do poziomu sygnałów protokołów deterministycznych
- Redukcja dokumentacji papierowej poprzez automatyczne generowanie dokumentacji przez system
- Szeroka kompatybilność przez magistralę pxGrid
- Możliwość pełnego monitorowania i zgłaszanie incydentów w trybie 24h/dobę za pośrednictwem własnej dyspozytorni (Security Operation Center)
- Spełnienie wymagań Ustawy o Krajowym Systemie Cyberbezpieczeństwa
- Zgodność z wymaganiami Rządowego Centrum Bezpieczeństwa oraz wyśrubowanymi standardami IEC 62443 (ISA99), NIST 800-82, NERC-CIP, CPNI czy ISO 27001/27002/27033 w zakresie komunikacji sieciowej, przepływu i ochrony danych oraz ciągłości działania.

Life Is On | Schneider Electric

Schneider Electric Polska Sp. z o.o.
ul. Konstruktorska 12, 02-673 Warszawa
Centrum Obsługi Klienta:
+48 801 171 500,
+48 22 511 84 64
poland.helpdesk@schneider-electric.com
www.schneider-electric.com

Partner Technologiczny ds. Cyberbezpieczeństwa
Dynacon Sp. z o.o.
ul. Kwiatkowskiego 4
52-326 Wrocław
www.dynacon.pl

DYNACON