

# SCADvanceXP

## NEXT GENERATION IDS DLA PRZEMYSŁU WODNO-KANALIZACYJNEGO



SCADvance XP® pozwala wykryć anomalie oraz cyberzagrożenia w czasie rzeczywistym w sieciach automatyki przemysłowej. Informuje o niepożądanym zdarzeniu, wskazując miejsce wystąpienia zagrożenia, cel ataku i jego prawdopodobną przyczynę.

### MOCNE STRONY

- ≡ PEŁNA PASYWNOŚĆ
- ≡ SKALOWALNOŚĆ SYSTEMU
- ≡ KRÓTKI CZAS WDROŻENIA
- ≡ POLSKA WERSJA JĘZYKOWA
- ≡ POLSKI ZESPÓŁ WSPARCIA
- ≡ ELIMINACJA FAŁSZYWIE POZYTYWNYCH ALARMÓW
- ≡ UNIWERSALNOŚĆ ZASTOSOWANIA (MONITORING I PODŁĄCZENIE DO WSZYSTKICH TYPÓW SIECI AUTOMATYKI PRZEMYSŁOWEJ)

### DLACZEGO SCADvance XP®?

Systemy OT/SCADA zostały zaprojektowane na długo przed rozwojem bezprzewodowego Internetu czy zdalnego dostępu do systemów i sieci. Dynamiczny rozwój technologii nie objął w swoim zakresie bezpieczeństwa sieci OT.

Dzięki rozwiązaniu otrzymasz:

#### ≡ WIEDZĘ

SCADvance XP® pomaga w zarządzaniu ryzykiem biznesowym i operacyjnym

#### ≡ MONITORING W CZASIE RZECZYWISTYM

SCADvance XP® zabezpiecza procesy produkcyjne

#### ≡ OBSŁUGĘ INCYDENTU

SCADvance XP® dostosowuje procedury do wymogów prawnych

### MONITORING SIECI OT/ICS

SCADvance XP® monitoruje sieci przemysłowe nie na ich brzegach, jak robią to standardowe systemy informatyczne, ale zbiera informacje bezpośrednio z ich środka, analizując cały przesyłany ruch pakietów.

Zastosowane interfejsy sprzętowe pozwalają na monitoring i podłączenie do wszystkich typów sieci automatyki przemysłowej, dzięki czemu osoby odpowiedzialne za bezpieczeństwo w organizacji mają wizualizację wszystkich istniejących połączeń oraz urządzeń w czasie rzeczywistym. Tym samym zapewniony jest wgląd w ewentualną niepożądaną komunikację w sieci OT.

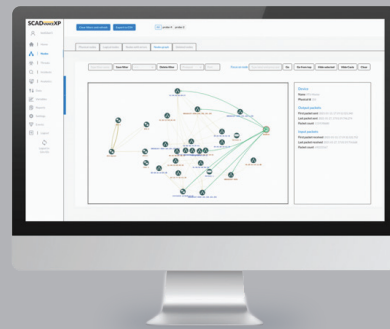
- ≡ ciągłe monitorowanie wraz z raportami na żądanie
- ≡ możliwość nagrywania ruchu
- ≡ monitorowanie działań zewnętrznych dostawców
- ≡ natychmiastowa widoczność mapy sieci, pozyskanie informacji o podłączonych urządzeniach



## PASYWNA I AUTOMATYCZNA INWENTARYZACJA AKTYWÓW

System **SCADvance XP®** wykrywa urządzenia połączone do chronionej sieci na podstawie obserwowanego ruchu. W ten sposób powstaje mapa chronionej sieci w postaci grafu połączeń pomiędzy urządzeniami sieci na poziomie urządzeń logicznych sieci.

- wykrywanie urządzeń połączonych do chronionej sieci na podstawie pasywnej obserwacji ruchu
- analiza ruchu pomiędzy urządzeniami (rodzaj i ilość protokołów, pakietów, portów i wiele innych)

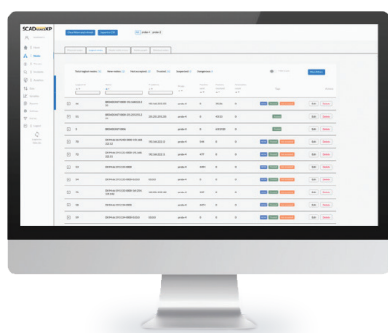


## DETEKCJA ZMIAN W SIECI

**SCADvance XP®**, dzięki analizie anomalii i korelacji wyników pracy modułów AI wykrywa najbardziej niebezpieczne i niezobserwowane nigdzie indziej ataki.

System posiada mechanizmy pozwalające na zbudowanie modeli predykcyjnych dedykowanych indywidualnie dla każdego połączenia logicznego z osobna, co znacząco podnosi jakość predykcji i detekcji anomalii.

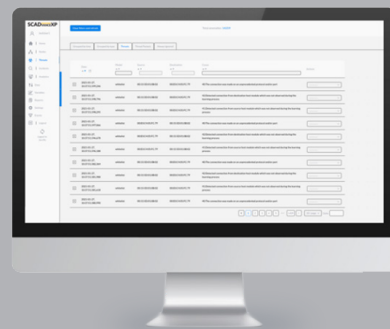
- automatyczne wykrywanie anomalii, ataków i awarii
- automatyczne budowanie dedykowanych modeli predykcyjno-analitycznych



## RAPORTOWANIE

**SCADvance XP®** umożliwia tworzenie i dostosowywanie widoków użytkownika i raportów zgodnie z uprawnieniami oraz preferencjami.

- prezentacja statystyk ruchu w chronionej sieci OT za pomocą wbudowanego i konfigurowalnego dashboardu
- raporty przedstawiające stan sieci (status, scoring)
- raporty z inwentaryzacji urządzeń
- raporty wspierające hardening sieci (podsieci, protokoły, urządzenia)



**ICsec S.A.** jest liderem na rynku zabezpieczeń infrastruktury przemysłowej, w szczególności dla przedsiębiorstw z infrastrukturą krytyczną. ICsec zaprojektował i zbudował system **SCADvance XP®** (system klasy IDS, intrusion detection system), przeznaczony do monitoringu sieci OT. Rozwiązanie adresuje potrzeby związane z monitoringiem sieci automatyki przemysłowej, wykrywaniem potencjalnych zagrożeń i anomalii w ruchu pomiędzy połączonymi do sieci urządzeniami.

ICsec S.A. | ul. Wichrowa 1A, 60-449 Poznań, Polska | tel. +48 506 931 953  
biuro@icsec.pl | www.icsec.pl