

**NEXT GENERATION
IDS
DLA ZAKŁADÓW
PRZEMYSŁOWYCH**

SCADVANCEXP

SECURITY BOOST

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 SCADVANCEXP

- == PEŁNA PASYWNOŚĆ
- == SKALOWALNOŚĆ SYSTEMU
- == KRÓTKI CZAS WDROŻENIA
- == POLSKA WERSJA JĘZYKOWA
- == POLSKI ZESPÓŁ WSPARCIA
- == ODPORNOŚĆ SONDY NA CZYNNIKI ZEWNĘTRZNE
- == INTEGRACJA Z SYSTEMAMI ZEWNĘTRZNYMI
- == PRZEWAGA SONDY NAD KOMPUTERAMI PRZEMYSŁOWYMI

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. Główne wyzwania przed jakimi stoją dziś zakłady przemysłowe to:

Podatność na cyberzagrożenia, która jest spowodowana:

- == brakiem znajomości aktualnej mapy sieci
- == komunikacją sieci przestarzałymi protokołami
- == brakiem całkowitego oddzielenia sieci OT od IT
- == nieprawidłową aktualizacją sterowników

Wypełnienie obowiązków wynikających z Ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz Ustawy o zarządzaniu kryzysowym.

SCADVANCE XP

MONITORING SIECI

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 sieci automatyki przemysłowej, dzięki czemu osoby odpowiedzialne za bezpieczeństwo w organizacji mają wizualizację wszystkich istniejących połączeń oraz urządzeń w czasie rzeczywistym. Tym samym widzą niepożądaną komunikację w sieci OT.



INTERFEJSY

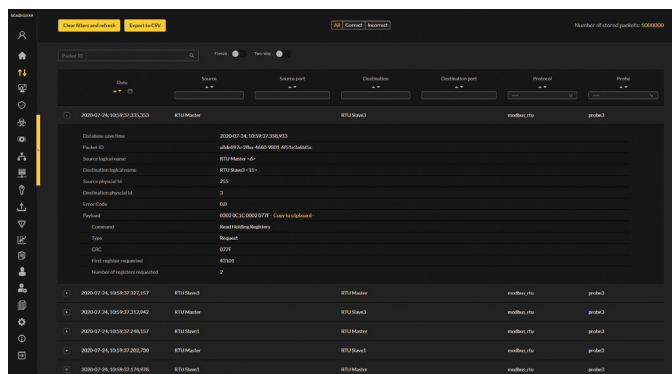
- RS-485
- RS-232
- RS-422
- CAN
- ETHERNET

WYBRANE PROTOKOŁY

- DNP3
- Profibus
- ProfiNET
- Modbus
- CANOpen
- Powerlink

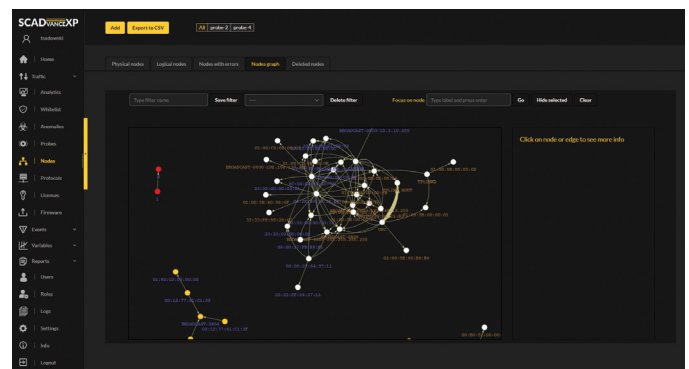
RUCH SIECIOWY

System **SCADVANCE XP** umożliwia wizualizację statystyk ruchu w chronionej sieci OT/IT za pomocą wbudowanego i konfigurowalnego dashboardu.

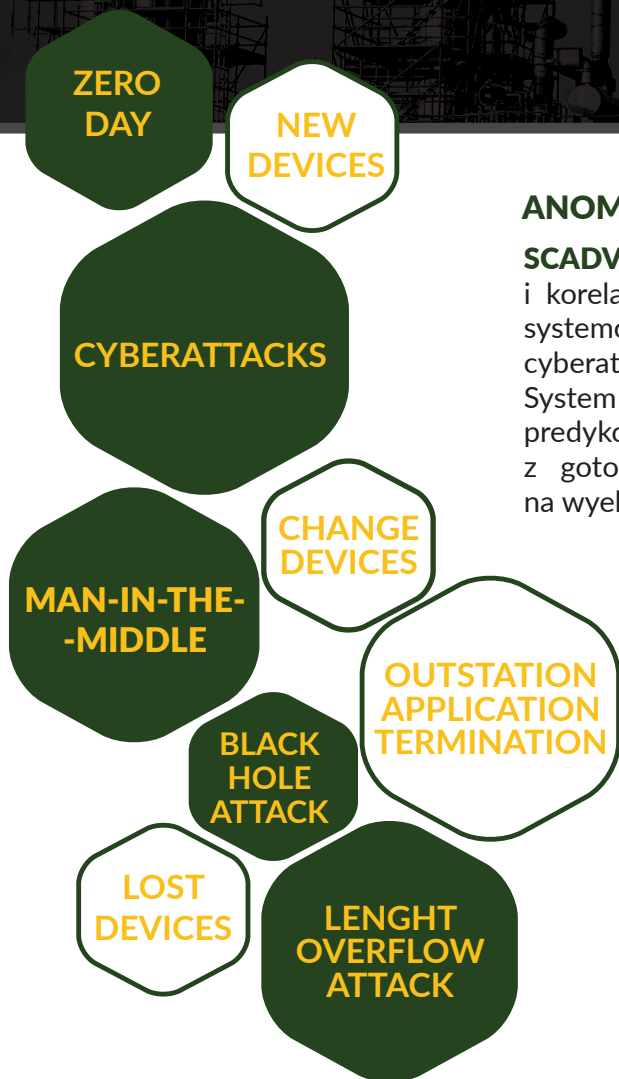


ZARZĄDZANIE AKTYWAMI

System **SCADVANCE XP** wykrywa urządzenia podłączone 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.



SCADVANCEXP



ANOMALIE I CYBERATAKI

SCADVANCE XP - dzięki analizie pakietów, charakterystyk NetFlow i korelacjom - pozwala na wykrycie anomalii, czyli niepożądanego działania systemów sterowania i sieci połączeń, w tym najbardziej niebezpiecznych cyberataków (np.: zero day, man in the middle, black hole attack). System posiada mechanizmy pozwalające na zbudowanie modeli predykcyjnych dedykowanych dla monitorowanej sieci, nie korzystając z gotowych modeli dostarczanych przez producentów, co pozwala na wyeliminowanie błędów false positive.

Machine Learning oraz Artificial Intelligence

System oparty jest o moduły analityczne uczenia maszynowego (ML) odpowiedzialne za wykrywanie sytuacji odbiegających od normy.

MONITORING PROCESÓW

SCADVANCE XP posiada moduł pozwalający na przechwycenie wartości zmiennych fizycznych występujących w procesach rzeczywistych, a także pozwala na śledzenie ich zmian niezależnie od systemu SCADA.

- temperatura
- ciśnienie pary
- napięcie
- stan urządzenia
- stężenie gazów
- wilgotność
- prędkość
- waga

ZASTOSOWANIE SCADVANCE XP W ZAKŁADZIE PRZEMYSŁOWYM

problem

Zaburzenia parametrów procesu produkcyjnego poprzez błędne odczyty czujników. Nieznana pełna lista urządzeń podłączonych do sieci wspólnie ze sterownikami przemysłowymi.



Man in the middle



rozwiązanie

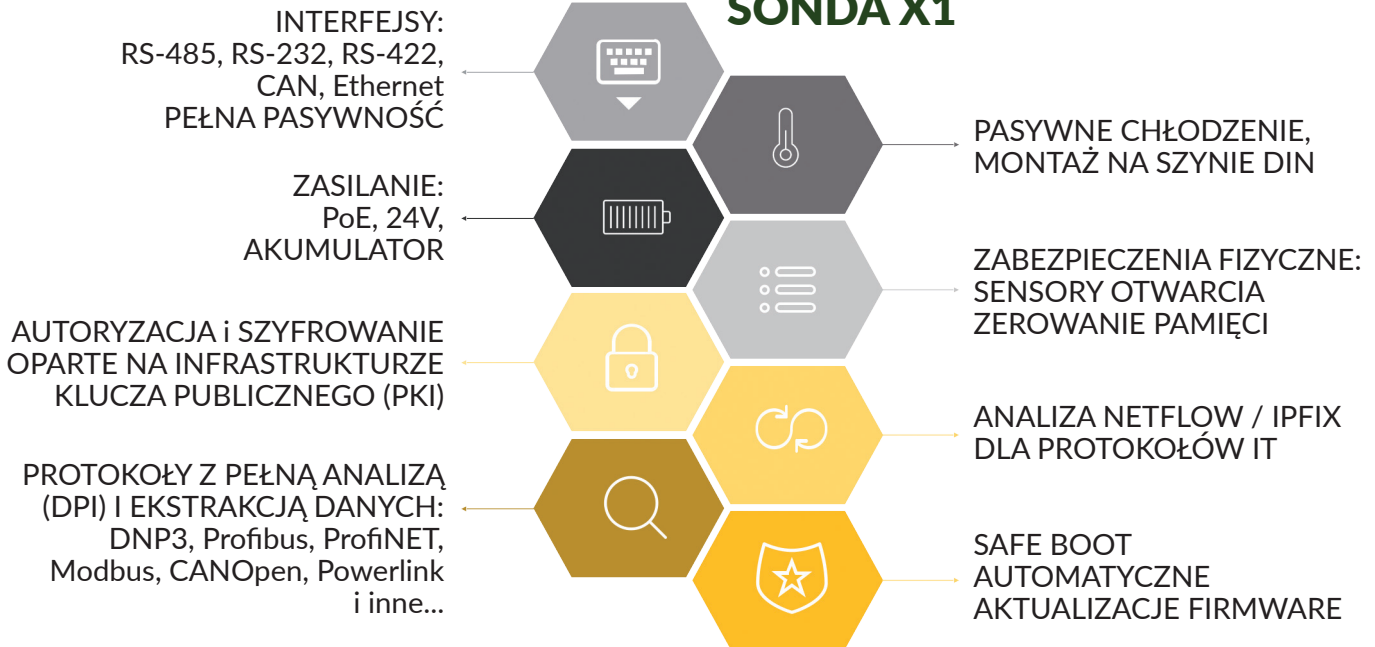
Implementacja **SCADVANCE XP**. Ciągły, pasywny monitoring ruchu sieciowego we wskazanych segmentach sieci automatyki przemysłowej.

**NEXT GENERATION
IDS
DLA ZAKŁADÓW
PRZEMYSŁOWYCH**

SCADVANCEXP

SECURITY BOOST

SONDA X1



SCADVANCE XP



ICsec S.A. jest producentem rozwiązań z obszaru cyberbezpieczeństwa dla przemysłu, 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 podłączonymi do sieci urządzeniami.



www.icsec.pl