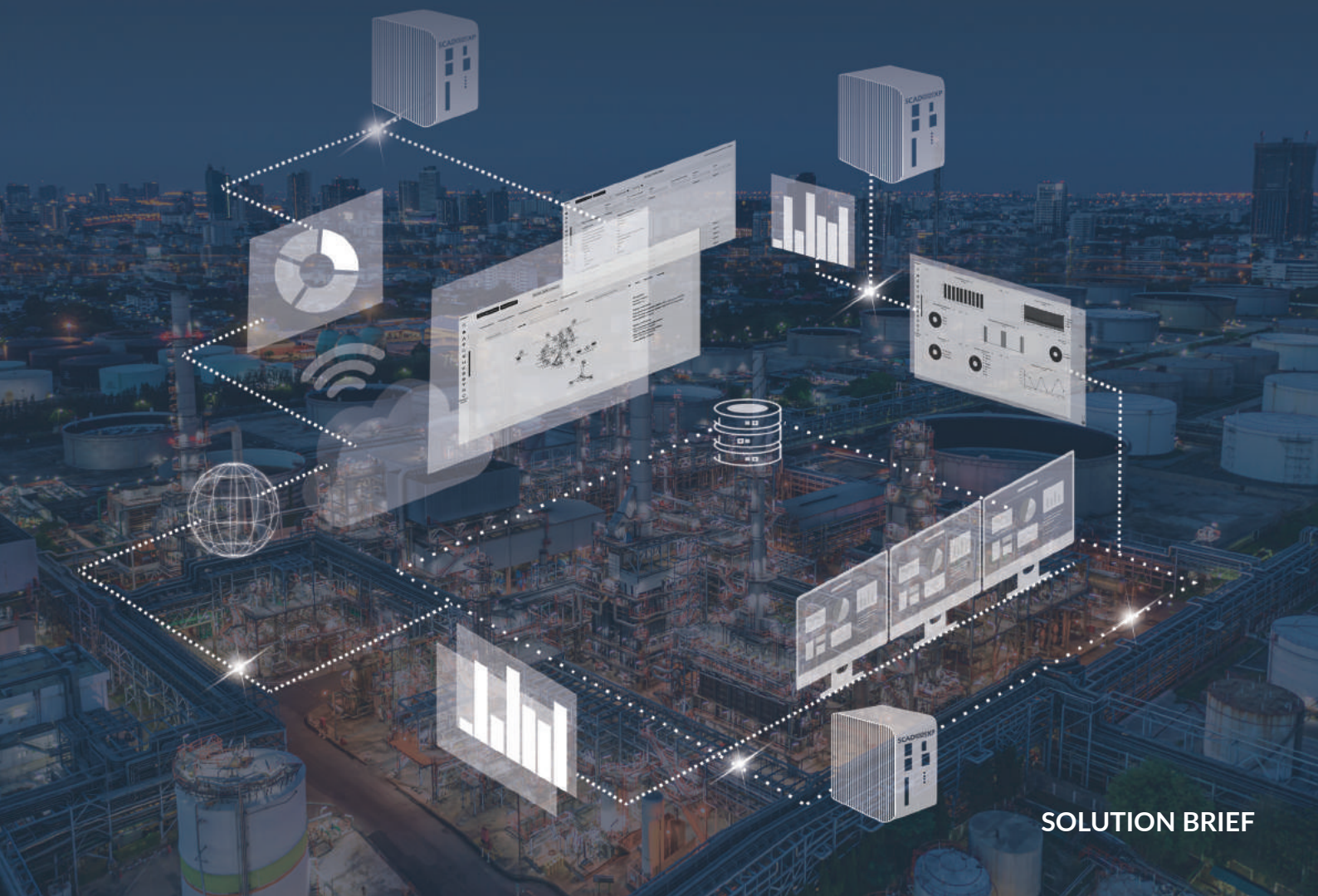
SCADvance XP

SCADvance XP® to innowacyjny system monitorowania sieci przemysłowych zapewniający identyfikację, monitoring oraz bezpieczeństwo posiadanych zasobów w czasie rzeczywistym.

SCADvance XP® jest fundamentem kompleksowego systemu bezpieczeństwa stosowanego w organizacjach wykorzystujących automatykę przemysłową, który równocześnie zapewnia zgodność z wymaganiami regulacji prawnych.

SCADvance XP® wyróżnia się zastosowaniem dedykowanych modeli predykcyjno - analitycznych wykorzystujących algorytmy uczenia maszynowego (ML/AI), które dostosowują się do każdej konfiguracji sieci OT, dzięki czemu system jest w stanie poprawnie wykryć anomalie i zagrożenia w sieci przemysłowej.



SOLUTION BRIEF

WSTĘP

Trwająca konwergencja sieci technologii informacyjnej (IT) i sieci technologii operacyjnej (OT) zwiększa złożoność i podatność na zagrożenia występujące w przemysłowych systemach sterowania (Industrial Control Systems). Problematyka pogłębia się wraz z gwałtownym rozwojem Przemysłu 4.0, cyfrową transformacją oraz wprowadzaniem nowych technologii łączących sieci OT i IT.

Przedsiębiorstwa coraz częściej wykazują zwiększoną świadomość ryzyk związanych z ciągłością działania procesów produkcyjnych oraz cyberbezpieczeństwem występujących już nie tylko w sieciach IT, ale także w sieciach OT. Zarządzający bezpieczeństwem odczuwają potrzebę posiadania narzędzi do monitorowania infrastruktury, które dostarczą pełny wgląd w sieci OT/ICS oraz umożliwią efektywne zarządzanie ryzykiem operacyjnym w czasie rzeczywistym, a także zarządzanie incydentami, w tym odpowiednie ich dokumentowanie.

W wielu sieciach produkcyjnych wciąż występuje problem niepełnej inwentaryzacji infrastruktury i w konsekwencji zakłady przemysłowe nie mają świadomości bieżącej architektury sieci i świadczonych przez nią usług. Efektem tego są luki w zabezpieczeniach systemów, co stanowi wyzwanie nie tylko dla zespołów bezpieczeństwa, ale całej organizacji.

CO NAS WYRÓŻNIA

Autorski algorytm dedykowanych modeli predykcyjno-analitycznych, dla każdej instalacji, z wykorzystaniem metod ML i AI

Używanie metod behawioralnych umożliwia wykrycie nieznanego wcześniej cyberataku (zero-day)

Pasywne monitorowanie (bez zakłócania pracy systemów OT)

Rozpoznawanie urządzeń sieci OT, głęboka analiza protokołów przemysłowych (DPI)

Eliminacja fałszywie pozytywnych alarmów

Niezależność od dostawców automatyki*

Uniwersalność zastosowania (monitoring i podłączenie do wszystkich typów sieci automatyki przemysłowej)

Możliwość monitorowania bezpośrednio z interfejsów Ethernet, RS i CAN

Ciągłe monitorowanie wraz z raportami na żądanie

Integracja z systemami Firewall, SIEM, SOAR, UEBA

Krótki czas wdrożenia (plug & play)

Dostępność wielu wersji językowych

DLACZEGO SCADvance XP®

WIEDZA

SCADvance XP® pomaga w zarządzaniu ryzykiem biznesowym i operacyjnym

System dostarcza wiedzę na temat bieżącej architektury sieci: identyfikuje urządzenia, rysuje mapy sieci, monitoruje krytyczne procesy poprzez analizę ruchu automatyki wspierając proces zarządzania ryzykami oraz ciągłością działania.

Użytkownik ma możliwość monitorowania dostępu zewnętrznych dostawców.

Buduje świadomość sytuacyjną u osób odpowiedzialnych za bezpieczeństwo instalacji automatyki przemysłowej, co stanowi punkt wyjścia i fundament zarządzania bezpieczeństwem. Dostarczone informacje pozwalają na szacowanie i mitygowanie ryzyka oraz na tworzenie strategii bezpieczeństwa systemów.

MONITORING W CZASIE RZECZYWISTYM

SCADvance XP® monitoruje systemy automatyki przemysłowej

Monitoring w czasie rzeczywistym oparty jest zarówno na metodach sztucznej inteligencji, jak i metodach regułowych, whitelistach itp. System monitoruje sieć przemysłową z wykorzystaniem zaawansowanego silnika analitycznego, który z wykorzystaniem modeli sztucznej inteligencji natychmiast identyfikuje zdarzenia odbiegające od standardowego zachowania sieci przemysłowej.

SCADvance XP® nie wpływa na monitorowane sieci i urządzenia OT. Monitorowanie ruchu działa pasywnie i nieinwazyjnie, gdyż sondy są galwanicznie odizolowane od monitorowanej sieci. Sondy sprzętowe wraz z ich oprogramowaniem są projektowane i wytwarzane przez ICsec - zapewnia to pełną kontrolę nad procesem produkcyjnym.

System obsługuje specjalistyczne protokoły, a także jest niezależny od producentów i dostawców systemów sterowania ICS.

OBSŁUGA INCYDENTU

SCADvance XP® dostosowuje procedury do wymogów prawnych

SCADvance XP® gromadzi informacje o zagrożeniach i podatnościach. Dzięki wbudowanemu systemowi workflow, umożliwia kwalifikację zdarzenia w incydent zapisując jednocześnie historię procesu, podjęte działania, osoby odpowiedzialne oraz kopię ruchu, która dokumentuje przebieg incydentu.

Funkcja raportowania pomaga użytkownikowi w zautomatyzowaniu zgłaszania incydentów w ramach własnego systemu bezpieczeństwa (Security Operation Center) lub w ramach wypełniania obowiązków wynikających z Ustawy o KSC.

**

2021 - maj

Colonial Pipeline
Największy w USA operator rurociągów wstrzymał wszystkie swoje operacje

2021 - luty

Stacja uzdatniania wody
na Florydzie - atakujący próbował zwiększyć poziom wodorotlenku sodu

2020

Atak na **Enel Group** przez oprogramowanie ransomwer SNAKE (znane również jako EKANS)

2019

Globalny cyberatak na systemy firmy **PILZ**

2018 **VPNFilter**

Złośliwe oprogramowanie infekuje urządzenia sieciowe i wyszukuje komunikację z systemami sterowania

Rekomendacje prac związanych z zabezpieczeniem infrastruktury OT:

- zarządzaj ryzykiem sieci przemysłowej, monitoruj jej podatności
- monitoruj systemy OT i IT, wykrywaj nieautoryzowane sesje
- audytuj sieć, kontroluj dostępy, stosuj uwierzytelnianie wieloskładnikowe
- segmentuj sieć
- wdróż politykę retencji logów
- świadomie aktualizuj oprogramowanie
- archiwizuj i monitoruj ruch, zarządzaj incydentami

PROAKTYWNE PODEJŚCIE DO CYBERBEZPIECZEŃSTWA W ORGANIZACJI

SCADvance XP® gwarantuje prawidłowe podejście do cyberbezpieczeństwa i skutecznego zarządzania ryzykiem.

IDENTYFIKACJA

Dostarczaj wiedzę i buduj świadomość sytuacyjną w organizacji, aby zarządzać ryzykiem:

- ciągłe monitorowanie wraz z raportami na żądanie
- inwentaryzacja urządzeń i topologii sieci
- wykrywanie protokołów
- scoring sieci

OCHRONA

Opracuj i wdrażaj działania, aby zapewnić ciągłość działania infrastruktury przemysłowej:

- uczenie maszynowe i analiza behawioralna, mechanizmy umożliwiające wykrywanie incydentów
- proaktywne ustalanie priorytetów działań ograniczających ryzyko, mające na celu rozpoznanie i usunięcie z systemu najbardziej narażonych krytycznych podatności
- integracja z wiodącymi systemami zabezpieczającymi, takimi jak zapory sieciowe oraz rozwiązania zapewniające bezpieczny dostęp zdalny (bezpieczeństwo konta uprzywilejowanego)

WYKRYWANIE

Opracuj i wdrażaj działania w celu wykrycia niepożądanego zdarzenia:

- automatyczne wykrywanie anomalii, ataków i awarii
- wykorzystywanie własnych algorytmów AI dedykowanych dla sieci ICS do szybszego wykrywania anomalii i eliminacji fałszywie pozytywnych wyników
- integracja z systemami zewnętrznymi (Syslog, API)
- obsługa zdarzeń i incydentów wraz z zapisem historii procesu i podjętych działań

ZAPOBIEGANIE

Opracuj i wdrażaj działania, aby zapobiec niepożądanym zdarzeniom:

- identyfikacja podatnych elementów sieci w celu zablokowania dostępu do interfejsów, portów i usług
- monitorowanie wartości fizycznych transportowanych protokołami przemysłowymi w celu ochrony procesu biznesowego
- mitygowanie ryzyka oraz budowa własnego systemu bezpieczeństwa

ODZYSKIWANIE

Opracuj i wdrażaj działania w celu zapewnienia odporności systemu oraz szybkiego przywrócenia pracy i usług.

- zabezpieczenie ruchu z ataków i wskazanie wektorów ataków
- odzyskiwanie konfiguracji sieci - archiwum pakietów ruchu sieciowego

FUNKCJONALNOŚCI

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 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.

- wykrywanie urządzeń podłączonych 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 niezaobserwowane 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)

BEHAWIORYSTYKA
Eliminacja alarmów fałszywie dodatnich

System **SCADvance XP®** ma znacząca przewagę nad systemami opartymi tylko o sygnatury. Potrafi adaptować się do zmieniającej się sytuacji w sieci OT. Pozwala to na szybkie wykrycie ataków i zwrócenie uwagi na zmiany zachowania monitorowanego systemu, także w przypadku ataków zero-day.

METODY ML/AI	METODY OPARTE NA REGUŁACH	METODY OPARTE NA SYGNATURACH

SCADvance XP® buduje strukturę parametrów i zaleca odpowiednią symulację ruchu dla każdego kanału komunikacyjnego i dla każdego urządzenia, które jest wykrywane w sieci. Korelacja wyników pracy zapewnia eliminację fałszywie pozytywnych alarmów.

SCADvance XP® jest gotowy na niestandardowe typy sieci przemysłowych i unikalne aplikacje, dzięki wykorzystaniu elastycznych modeli AI/ML.

SCADvance XP® - KOMPONENTY

SONDA X1

- pasywność nasłuchu - brak ingerencji w istniejącą infrastrukturę OT, co oznacza, że system nie wysyła żadnych pakietów do sieci i urządzeń.
- możliwość pracy w trybie pass-through pozwala na zainstalowanie sondy X1 nawet w warunkach, gdy nie jest możliwe monitorowanie na porcie SPAN.
- wewnętrzna architektura sondy zapewnia izolację interfejsów monitorujących od interfejsów sieci zarządzającej, co oznacza brak oddziaływania pomiędzy środowiskiem IT i OT, do którego podłączona jest sonda X1.

System SCADvance XP®

Przetwarza dane przesłane przez sondę X1, analizuje i decyduje o zaklasyfikowaniu danych jako zdarzenia.

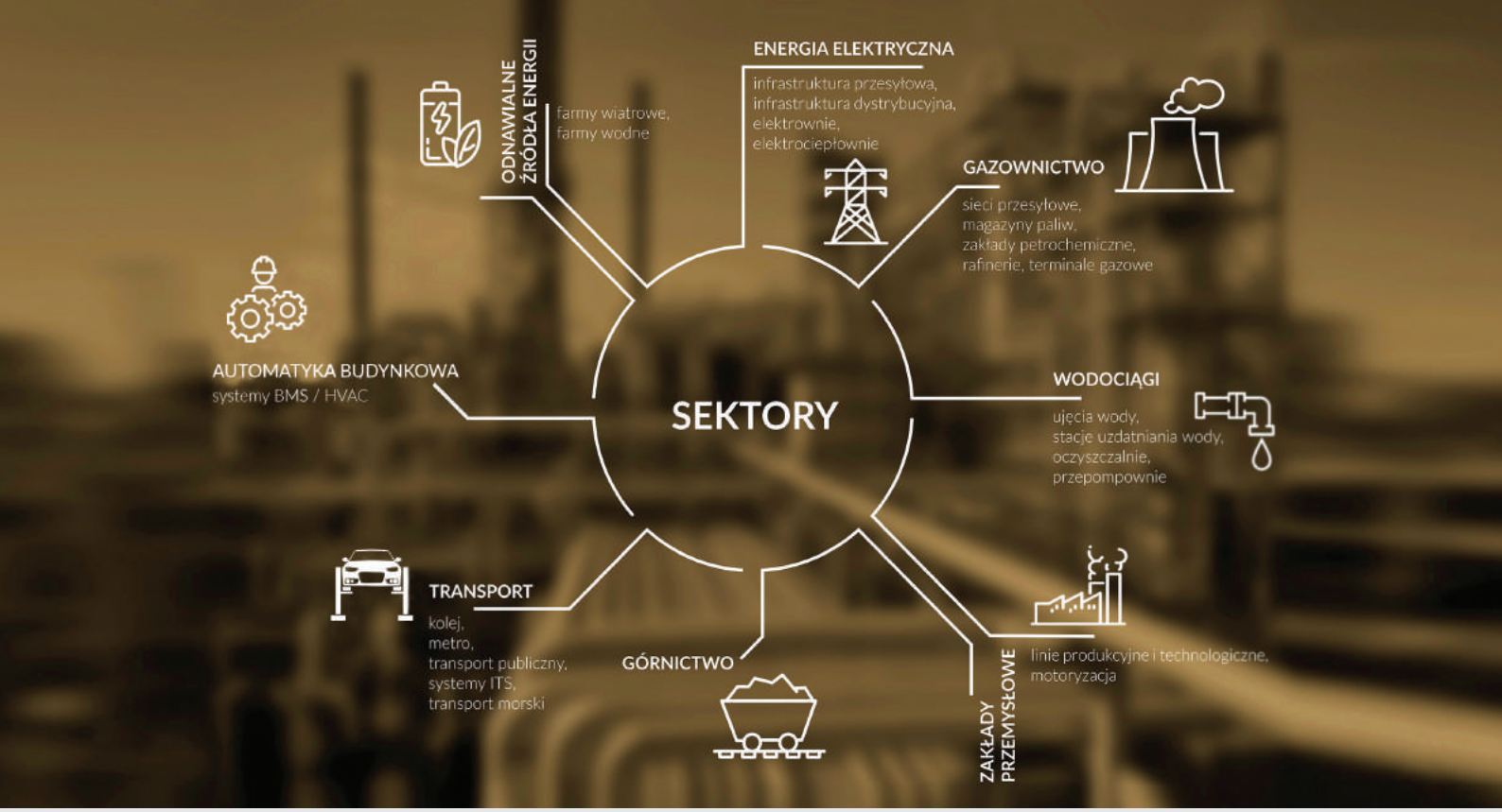
Innowacyjne elementy:

- szyna danych pracująca w czasie rzeczywistym gwarantuje przetwarzanie wszystkich pakietów wysyłanych w sieci i zapisanie ich do późniejszej analizy z wykorzystaniem mechanizmów BIG DATA. Pozwala to na analizę historycznego ruchu, umożliwiając odtworzenie każdego zaobserwowanego pakietu.
- mechanizmy sztucznej inteligencji oparte na algorytmach uczenia maszynowego i sieciach neuronowych.
- mechanizmy CEP (Complex Event Processing), umożliwiają łatwe rozbudowywanie funkcjonalności systemu.

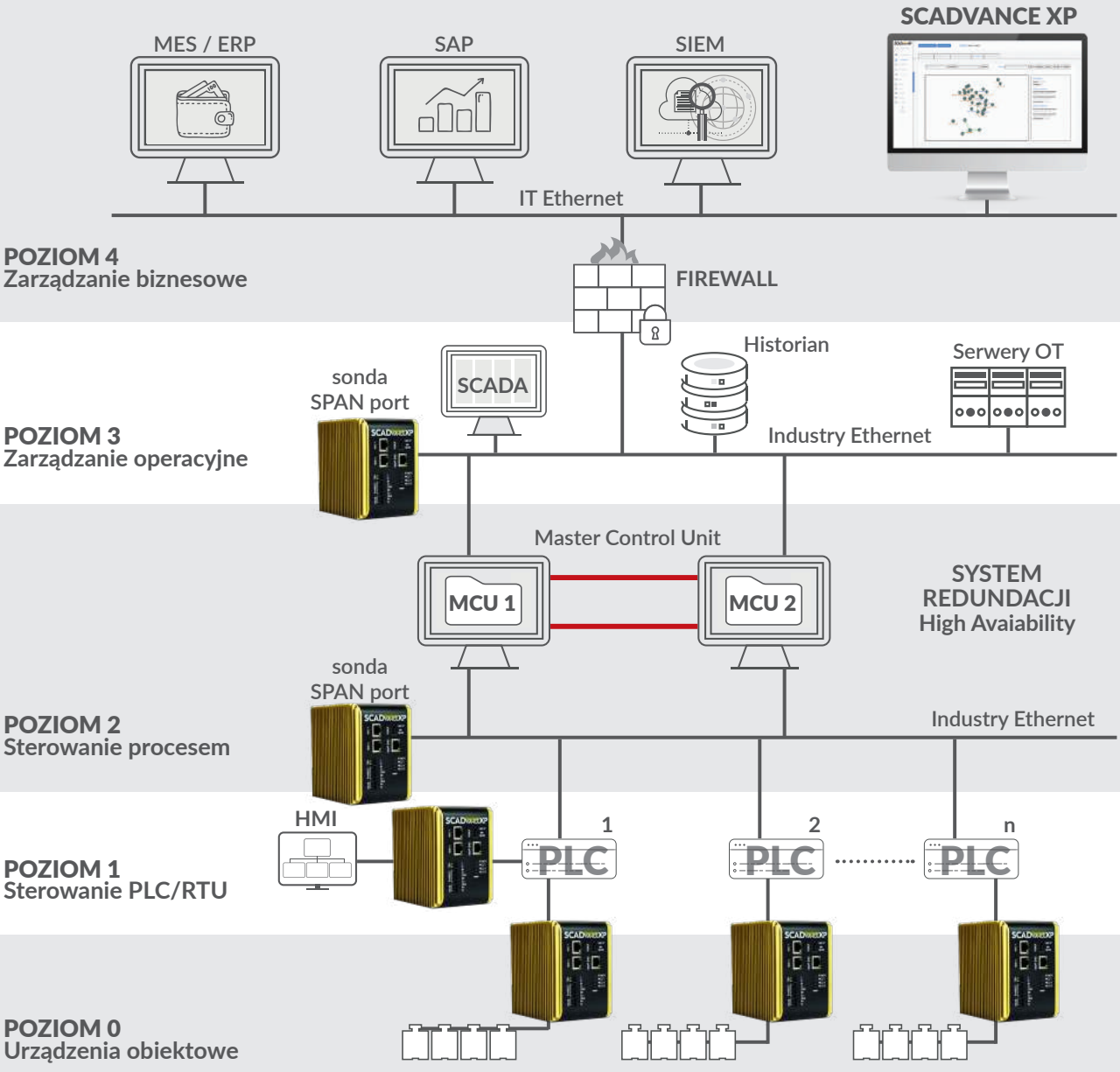
ZALETY

- MAPA SIECI
- INWETARYZACJA ZASOBÓW SIECI
- CIĄGŁE MONITOROWANIE WRAZ Z RAPORTAMI NA ŻĄDANIE
- PULPITY NAWIGACYJNE, WIDGETY I RAPORTY
- MOŻLIWOŚĆ INTEGRACJI Z SIEM, SOAR, UEBA, FW
- ZINTEGROWANY Z PROCESAMI SOC
- MONITORING PROCESÓW PRODUKCYJNYCH
- ARCHIWIZOWANIE PEŁNEGO RUCHU
- WSKAZANIE WEKTORÓW ATAKÓW
- ANALIZA POZDARZENIOWA - FORENSICS

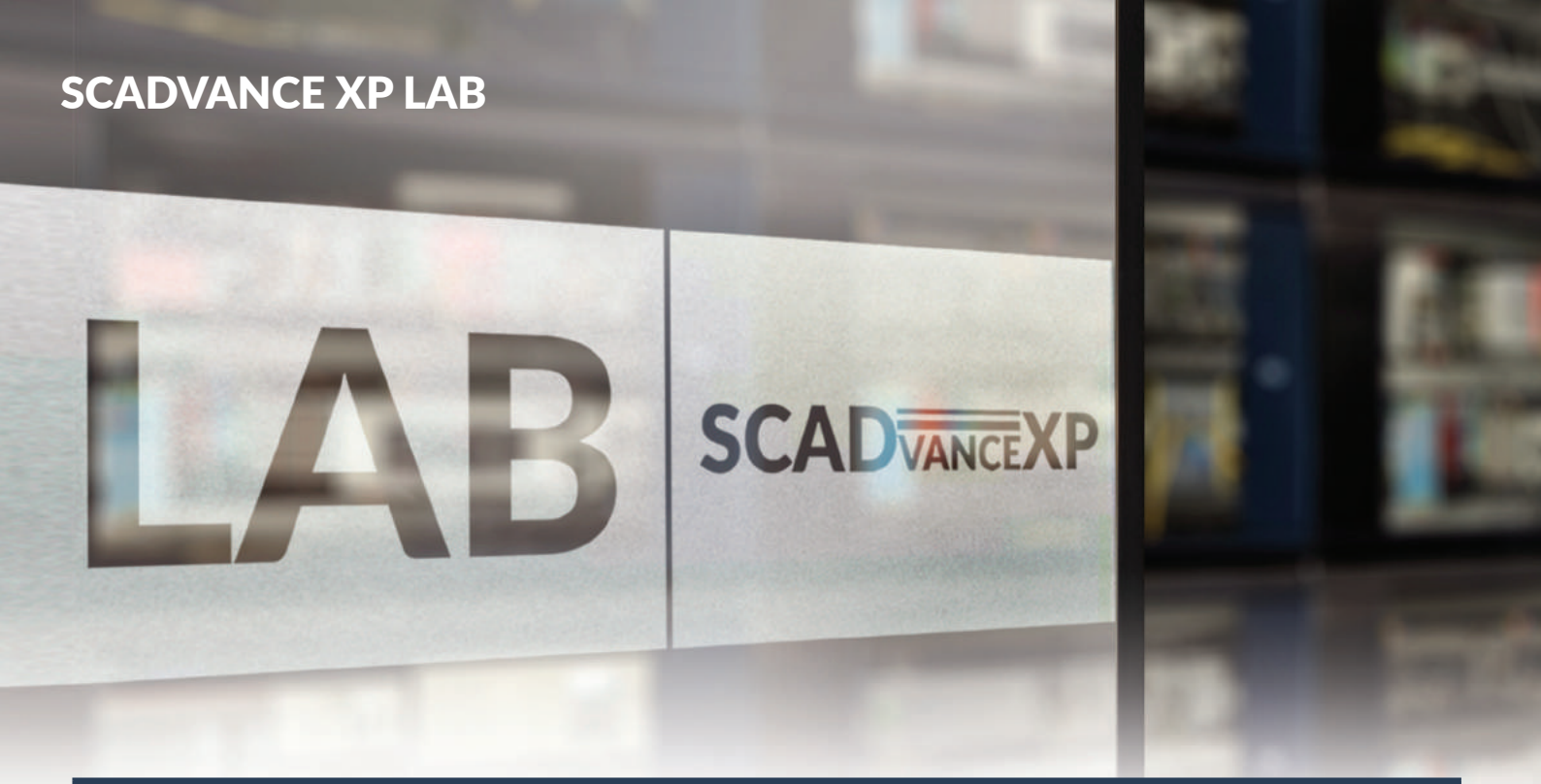
(możliwość przeprowadzenia szczegółowego dochodzenia z zaistniałych zdarzeń w sieci)



Przykład zastosowania systemu SCADvance XP®



SCADVANCE XP LAB



WSPIERANE PROTOKOŁY IP

SNMP, SSH, HTTP/HTTPS, Telnet, FTP, SMB/CIFS, DNS, ICMP, IGMP, FTP, SMB2, CDP, LLDP, DCE/RPC, DHCP V4/V6, ARP, VNC, TFTP, NTP, RDP, SSL

WSPIERANE PROTOKOŁY OT

PROTOKOŁY OT - FUNKCJONALNOŚCI DPI	PROTOKOŁY OT - ANALIZA ML i AI
Modbus RTU, Modbus TCP, Profibus DP,DNP3, CANopen, Powerlink, Profinet	Profinet, Profibus, Powerlink, CANopen, Modbus RTU, Modbus TCP/IP, TASE2, DNP3, OPC UA, OPC, EtherCAT, GE EGD, EtherNet/IP, CIP, IEC-61850, SRTP, BACnet, DDE

* WSPIERANI PRODUCENCI URZĄDZEŃ AUTOMATYKI PRZEMYSŁOWEJ

ABB	BECKHOFF	ROCKWELL AUTOMATION	GENERAL ELECTRIC	HORNER	MIKRONIKA
MITSUBISHI ELECTRIC	OMRON	ELESTER PKP	SIEMENS	SCHNEIDER ELECTRIC	

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 anomaliw ruchu pomiędzy podłączonymi do sieci urządzeniami.

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

© ICsec S.A. Wszystkie prawa zastrzeżone.
Informacje zawarte w niniejszej ulotce nie stanowią oferty w rozumieniu kodeksu cywilnego.