



PREZENTACJA TECHNICZNO- HANDLOWA

ICSEC – SCADVANCE XP

Wrzesień 2025 | Zygmunt Dobosz

TWORZYMYS ROZWIĄZANIA DLA PRZEMYSŁU (OT)

INFORMATION TECHNOLOGY (IT) vs. OPERATIONAL TECHNOLOGY (OT)

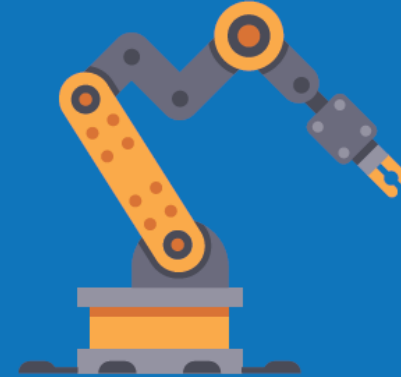
IT

Data and the flow
of digital information



OT

Operation of physical processes
and the machinery used to
carry them out





Stworzyliśmy polski system cybersecurity dla infrastruktury przemysłowej, zbudowany przez polskich inżynierów w oparciu o badania naukowe i współpracę z wiodącymi jednostkami naukowymi oraz ośrodkami obliczeniowymi



HARDWARE
I SOFTWARE



BIG
DATA



SZTUCZNA
INTELIGENCJA

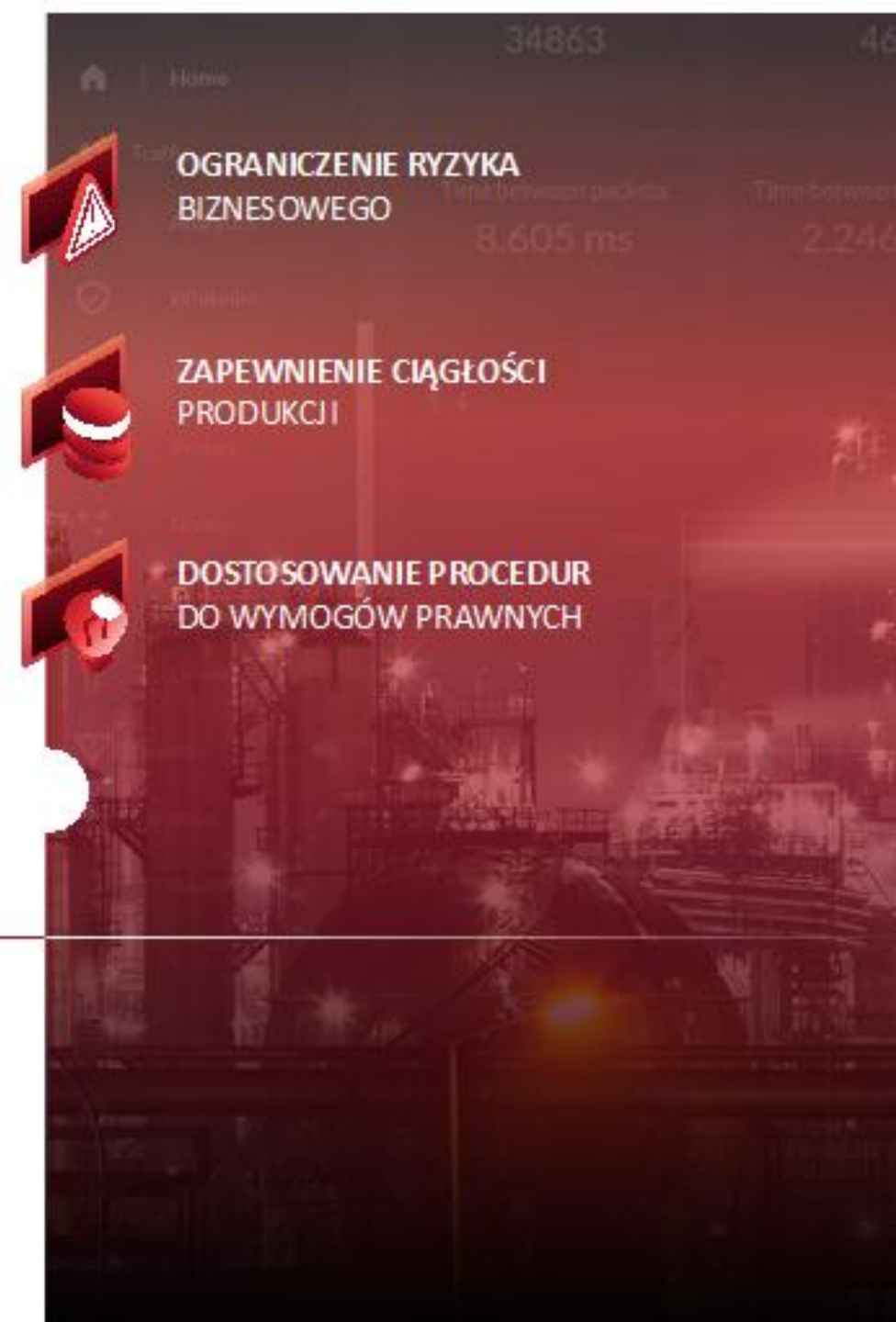


MONITORING
W CZASIE
RZECZYWISTYM



DETEKCJA

Lider rynku zabezpieczeń infrastruktury przemysłowej. Z powodzeniem **tworzymy pierwszy w Polsce ekosystem cyberbezpieczeństwa łącząc przemysł i polską naukę**. Dostarczamy rozwiązania, które pozwalają zmniejszyć ryzyko biznesowe związane z cyberatakami na sieci przemysłowe.



INWESTORZY

PGNiG



CVC



NCBR



PFR



TAURON



POLSKIE GÓRNICTWO
NAFTOWE
I GAZOWNICTWO

EEC MAGENTA

NARODOWE CENTRUM
BADAŃ I ROZWOJU

POLSKI FUNDUSZ ROZWOJU

TAURON
POLSKA ENERGIA

2022

02.06.2022

ORLEN VC z pierwszą polską inwestycją bezpośrednią

Fundusz kapitałowy należący do PKN ORLEN dokonał pierwszej bezpośredniej inwestycji. ORLEN VC samodzielnie objął nową emisję akcji firmy ICsec, polskiego producenta systemów cyberbezpieczeństwa dla przemysłu. Inwestycja jest częścią strategii koncernu, która zakłada inwestycje w spółki z autorskimi rozwiązaniami o potencjale międzynarodowym.

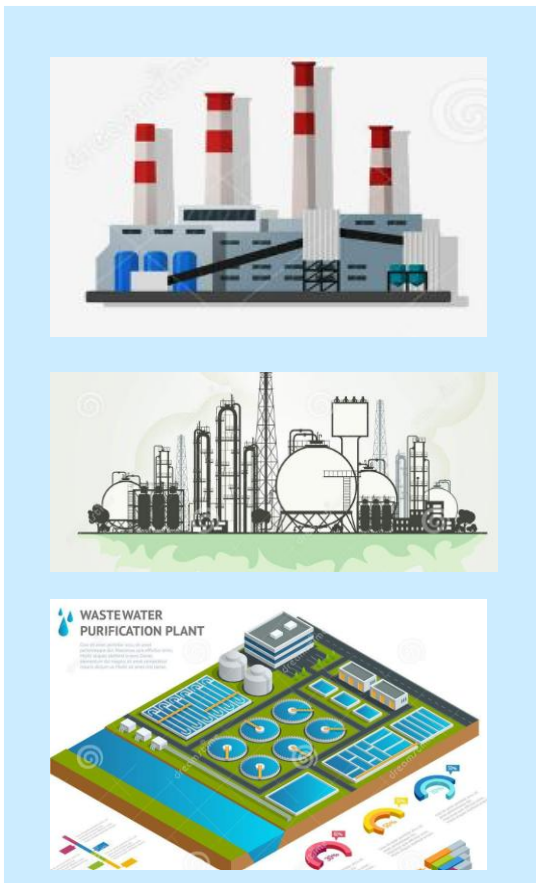
SCADVANCEXP

INTRUSION DETECTION SYSTEM DLA SIECI PRZEMYSŁOWYCH

Pasywna sonda oraz kompletne rozwiązanie
do monitoringu i analizy sieci OT



JAK TO DZIAŁA?



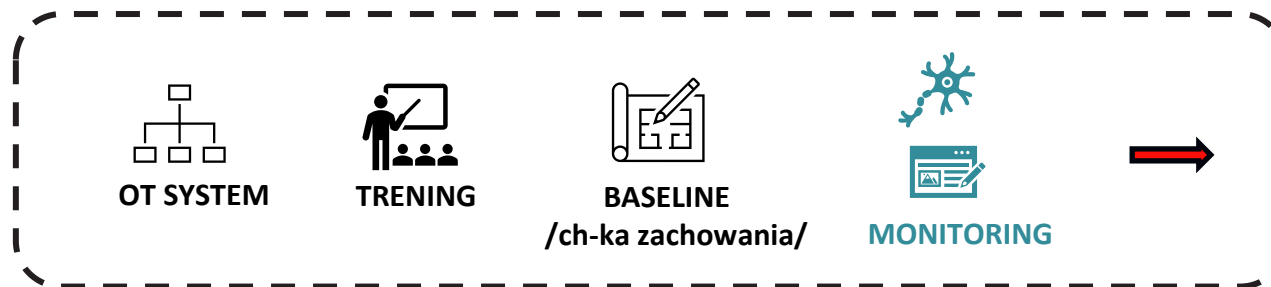
**ZEBRANIE, EKSTRAKCJA I
AGREGACJA DANYCH**

WIZUALIZACJA

TRENOWANIE

SZCZEGÓŁOWA ANALIZA

**OPRACOWANIE I
WYGENEROWANIE
REZULTATÓW**



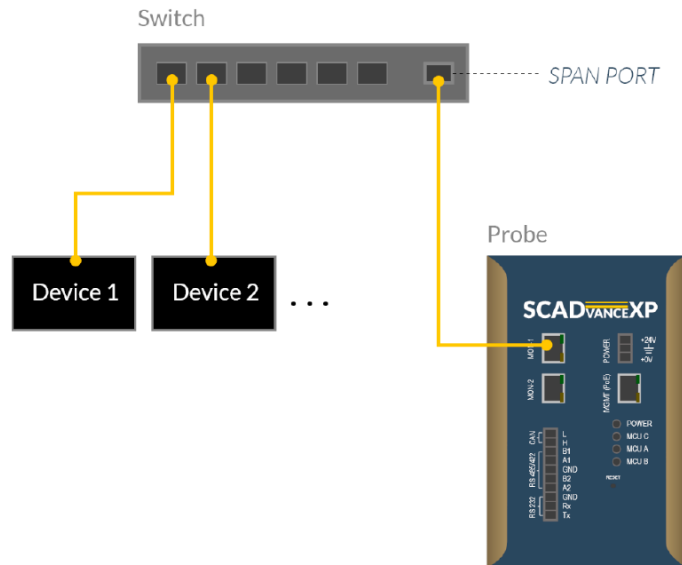
SONDA X1 CECHY



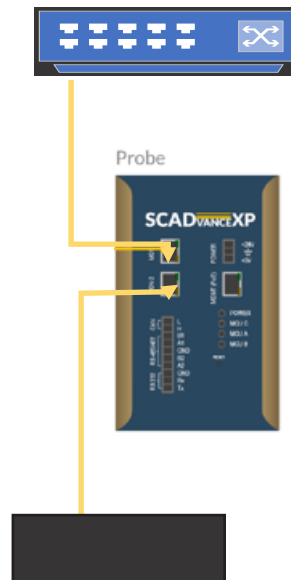
Maksymalna przepustowość: do 100 Mbit/s

- Szyfrowana komunikacja z systemem (AES)
- Certyfikaty bezpieczeństwa
- Porty nasłuchowe: 2 porty Ethernet (RJ45), CAN, RS485/422 i RS232
- Port management (RJ45/PoE)
- Zasilanie 24V DC (+ bateria podtrzymująca do 30 min)
- Zabezpieczenia fizyczne i programowe
- Wyprodukowana w Polsce (dywersyfikacja dostawców)

SONDA X1: SPOSÓB PODŁĄCZENIA (ETHERNET)



Tryb SPAN Port



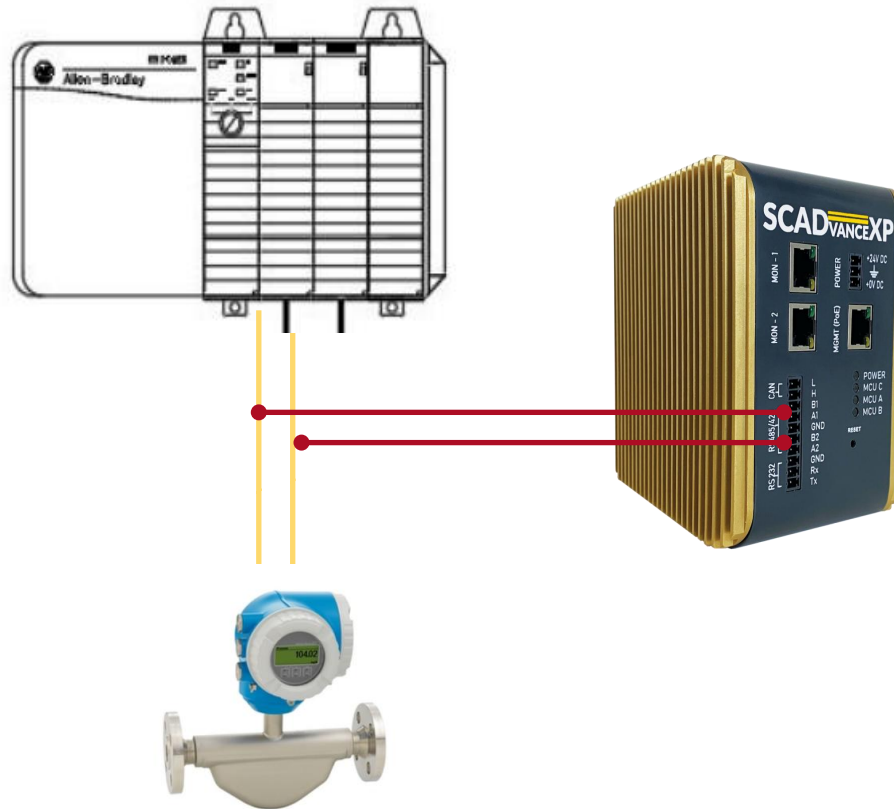
Tryb Pass Through



Sonda wirtualna (emu)

CAŁKOWITA PASYWNOŚĆ – brak ingerencji w infrastrukturę!

SONDA X1: SPOSÓB PODŁĄCZENIA (ŁĄCZA SZEREGOWE)



Podłączamy się do łączy szeregowych dwu- i czteroprzewodowych

Interfejsy RS232, RS485 (422), CAN

Protokoły przemysłowe:

Modbus RTU

DNP 3.0

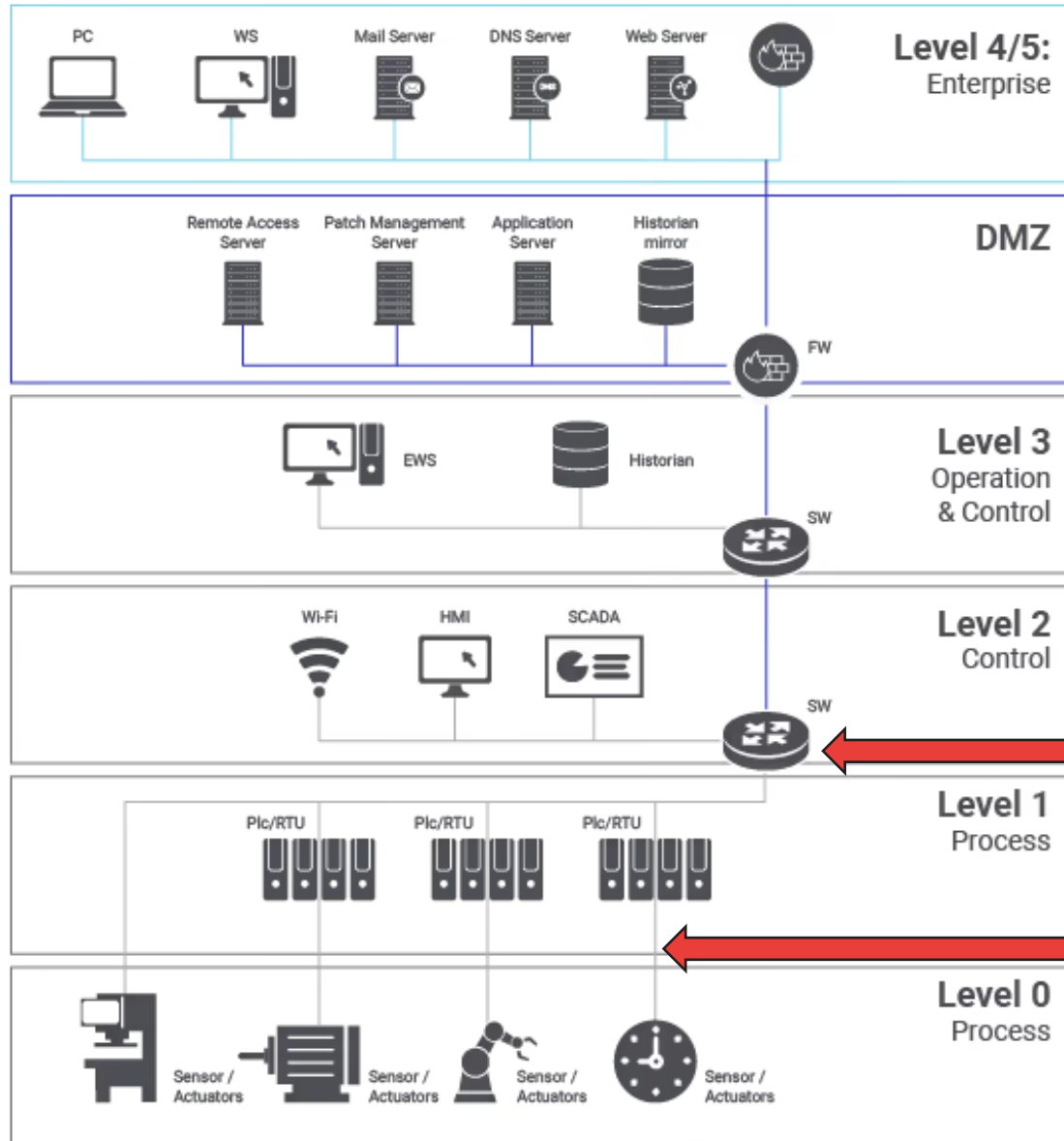
Siemens (S7, Profibus DP)

IEC 60870 (ICCP)

IEC 61850

Implementacja „na życzenie”

BUSZ



PRZYKŁAD ARCHITEKTURY

Operujemy w najniższych warstwach modelu PERA

Wykorzystujemy kopię ruchu udostępnioną przez porty w przełącznikach sieciowych (SPAN/R-SPAN port, TAP lub pass-through).

Oprogramowanie SCADvance XP wg. preferencji klienta (domyślnie warstwa Enterprise).

System on-premise.



PODSTAWOWE FUNKCJONALNOŚCI



ZARZĄDZANIE AKTYWAMI

- Wykrywanie i identyfikowanie urządzeń podłączonych do chronionej sieci
- Możliwość stworzenia mapy połączeń między urządzeniami w sieci



MONITOROWANIE SIECI OT/ICS

- Audyt sieci w czasie rzeczywistym
- Możliwość rejestracji całego obserwowanego ruchu
- **Świadomość sytuacyjna**



DETEKCJA ZMIAN W SIECI

- Automatyczne wykrywanie anomalii, ataków i awarii
- Detekcja występujących podatności
- Budowanie modeli predykcyjno-analitycznych dla monitorowanej sieci



RAPORTOWANIE i INTEGRACJA z SOC

- Prezentacja statystyk ruchu w chronionej sieci OT
- Raporty podsumowujące (predefiniowane i do samodzielnej kompozycji)
- Integracja z innymi systemami (SIEM, SOC)

METODY ANALITYCZNE



Metody
sygnaturowe

- **TTA**, WSO2



Metody behawiorystyczne

- algorytmy ML/AI
- metody statystyczne
- IPFIX (Netflow)



Metody regułowe

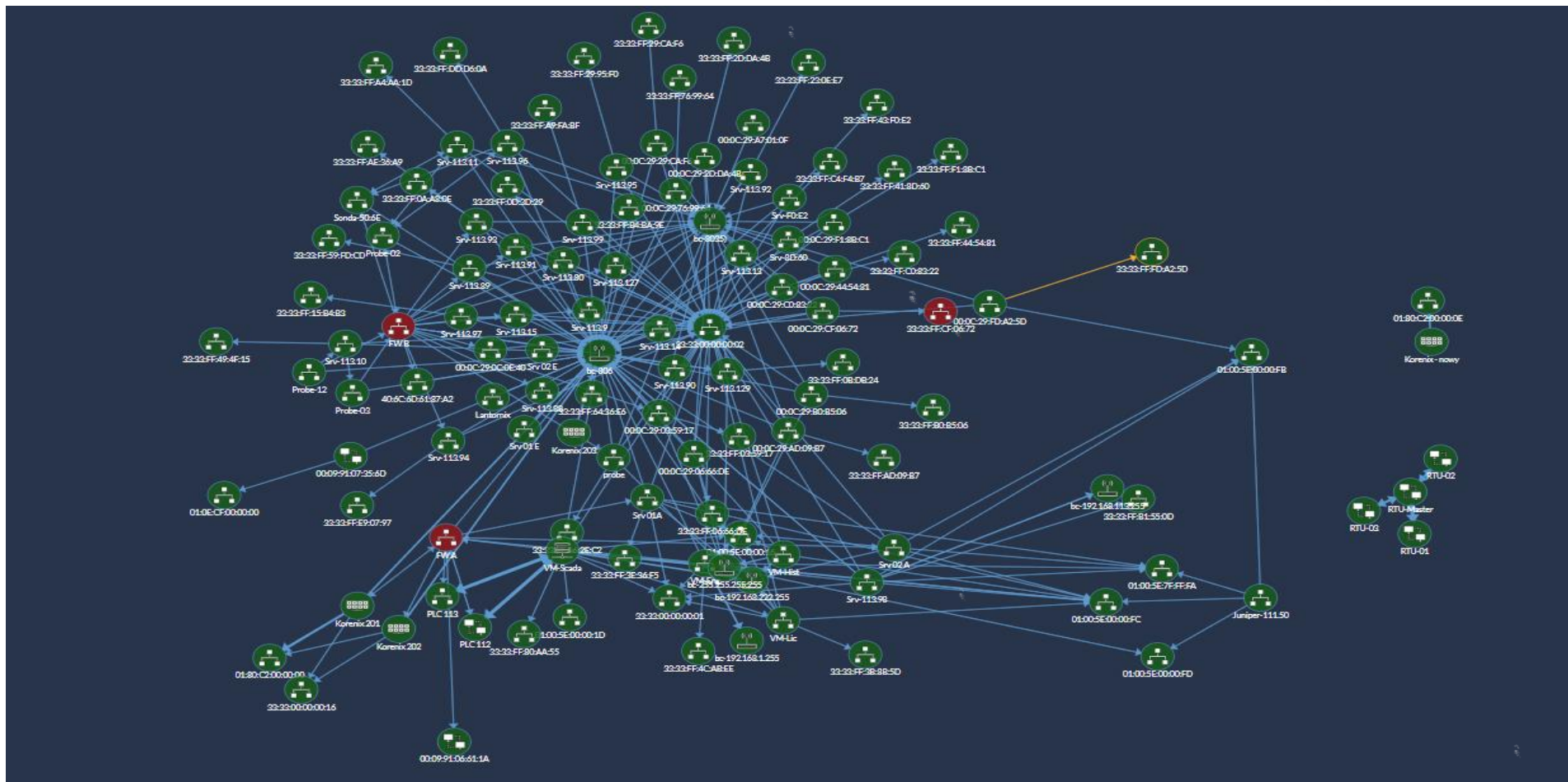
- PVM Process Variable Monitoring
- Reputation List
- Extended Whitelist



Inne

- Vulnerability Checker
- Device Discovery

GRAFICZNY SCHEMAT POŁĄCZEŃ



MONITORING INFRASTRUKTURY OT/ICS

- Urządzenia
- Połączenia sieciowe
- Protokoły
- Porty i usługi
- Statystyki związane z ruchem w sieci, statystyki systemowe
- Anomalie, ataki, błędy i awarie
- Zdarzenia
- Incydenty



WSZECHSTRONNA ANALIZA RUCHU (DPI, IPFIX)

▼

▲

☰

▲▼

▲▼

▲▼

▲▼

▲▼

▲▼

▲▼

▲▼

▲▼

▲▼

2022-08-22 12:40:51.554,209

PLC 112

192.168.222.112

502

0800

VM-Scada

192.168.222.22

50272

0800

modbus_tcp

probe-12

Czas zapisu do bazy

2022-08-22 12:40:51.600,716

ID pakietu

d88a152b-e588-44f8-983a-687f9ca4646c

Logiczna nazwa urządzenia źródłowego

PLC 112-0800-192.168.222.112 <5>

Logiczna nazwa urządzenia docelowego

VM-Scada-0800-192.168.222.22 <6>

Id fizyczne urządzenia źródłowego

00:E0:C4:05:FC:79

Id fizyczne urządzenia docelowego

00:15:5D:01:0B:02

Kod błędu

0,0

Payload info

Pokaż

Skopiuj do schowka

ⓘ

Payload info

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00	15	5D	01	0B	02	00	E0	C4	05	FC	79	08	00	45	02
00	37	73	88	40	00	40	06	89	5E	C0	A8	DE	70	C0	A8
DE	16	01	F6	C4	60	2F	11	96	C8	FA	F8	C8	48	50	18
05	B4	D3	30	00	00	00	82	00	00	00	09	00	03	06	00
07	00	00	00	3C	93	52	89	7C							

ETH

IP

TCP

MBTCP

MODBUS

Skopiuj do schowka

▼ Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface -, id 0

▼ Ethernet II, Src: HornerEI_05:fc:79 (00:e0:c4:05:fc:79), Dst: Microsof_01:0b:02 (00:15:5d:01:0b:02)

▼ Internet Protocol Version 4, Src: 192.168.222.112, Dst: 192.168.222.22

▼ Transmission Control Protocol, Src Port: 502, Dst Port: 50272, Seq: 1, Ack: 1, Len: 15

▼ Modbus/TCP

▼ Modbus

ICSEC | SCADVANCE XP 16

INCYDENTY

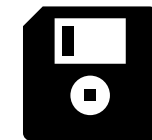
Narzędzie typu WORKFLOW do potrzeb komunikacji zewnętrznej (SOC, audyt, wymogi prawne), jak również do celów inspekcyjnych.

Na podstawie stwierdzonego alertu tworzony jest **Incydent** wraz z historią, opisem, załącznikami (np. pcap)



CERT/CSIRT

SOC

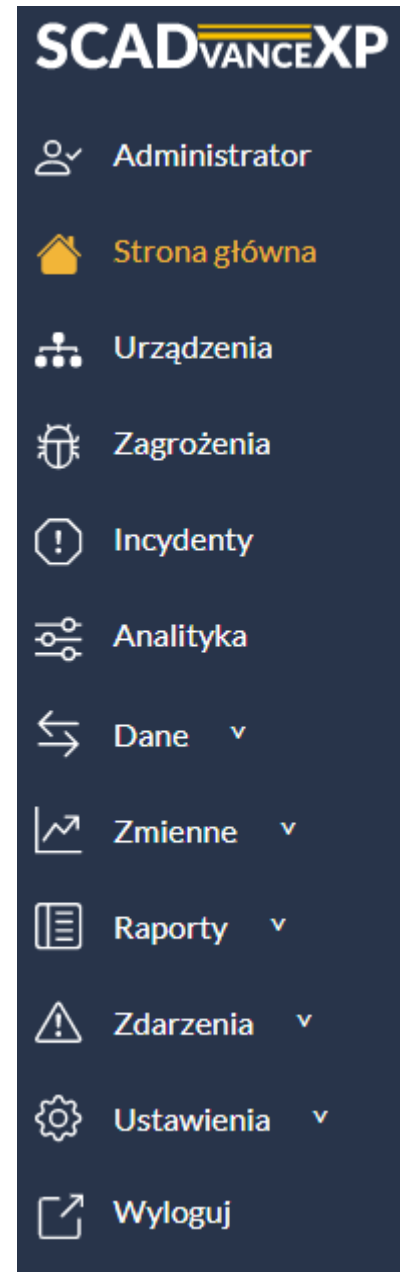


RAPORTOWANIE

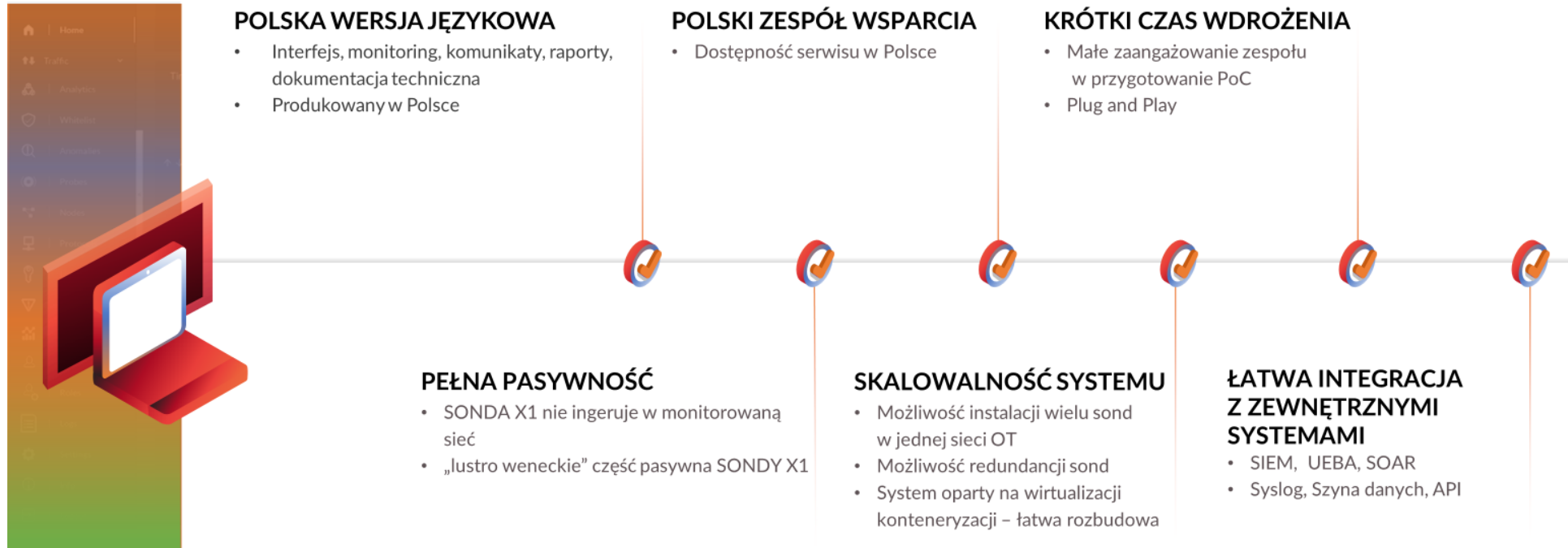
Predefiniowane raporty:

- Podsieci
- Urządzenia
- Protokoły (IP, Ethertype)
- Wektor ataku

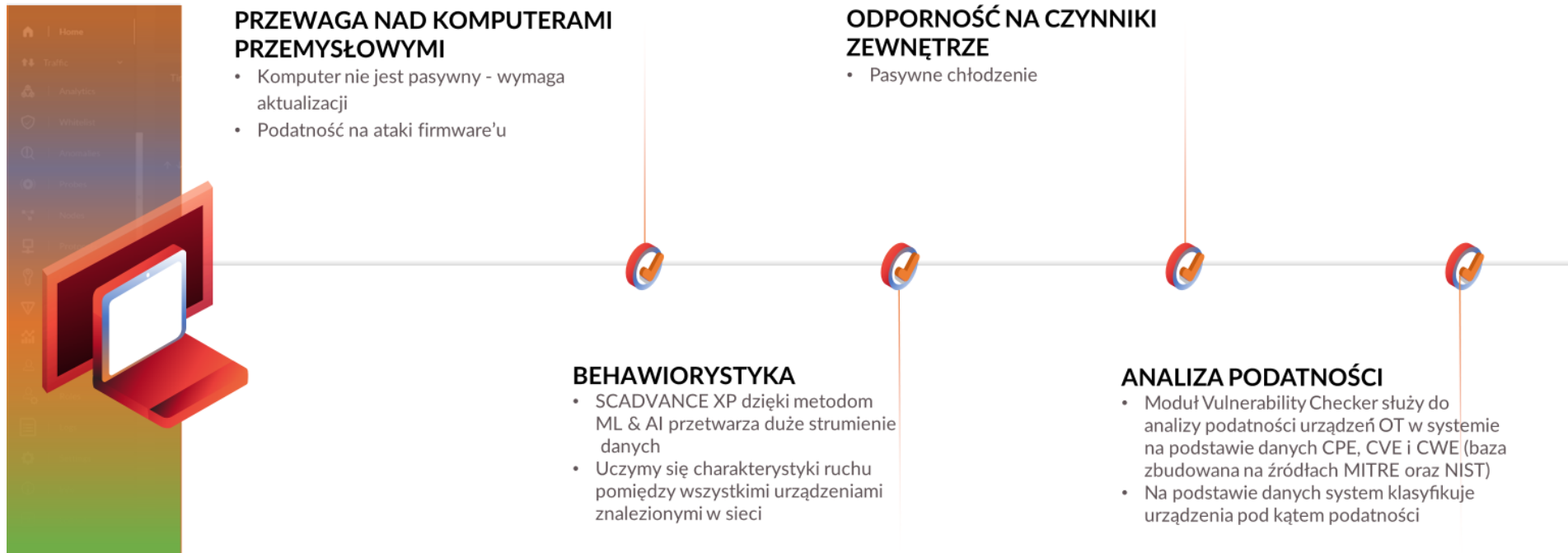
Możliwość definiowania własnych raportów.



Mocne strony Scadvance XP 1/2



Mocne strony Scadvance XP 2/2



CENNIK – PRZYKŁADOWA WYCENA: 300 URZĄDZEŃ, 2 SONDY X1, 3-LETNIE WSPARCIE

Kod	SCADvance XP Manager (oprogramowanie) wraz z rocznym Wsparciem (SERWIS)	Typ	Cena katalogowa jednostkowa	Rabat	Cena jednostkowa po rabacie	Ilość	Wartość łączna katalogowa	Rabat	Wartość łączna po rabacie	Uwagi
SV-S-U	SCADvance XP MANAGER 1 urządzenie.	Licencja	800,00 zł	25%	600,00 zł	300	240 000,00 zł	25%	180 000,00 zł	
							240 000,00 zł	25%	180 000,00 zł	

Kod	Sondy wraz z rocznym Wsparciem (SERWIS)	Typ	Cena katalogowa jednostkowa	Rabat	Cena jednostkowa po rabacie	Ilość	Wartość łączna katalogowa	Rabat	Wartość łączna po rabacie	Uwagi
SV-P-X1	SCADvance Sonda X1 (sprzętowa)	Sprzęt	6 000,00 zł	25%	4 500,00 zł	2	12 000,00 zł	25%	9 000,00 zł	
SV-P-V1	SCADvance Sonda V1 (wirtualna)	Licencja	3 000,00 zł		3 000,00 zł		- zł	0%	- zł	
							12 000,00 zł	25%	9 000,00 zł	

Kod	Wsparcie - Serwis SCADvance XP Manager oraz Sond	Typ	Wartość (%) katalogowa	Rabat	Wartość (%) po rabacie	Lat wsparcia	Wartość katalogowa	Rabat	Wartość po rabacie	Uwagi
SV-PSU-1Y	SERWIS na 1 dodatkowy rok	Serwis	15%	25%	11%	1	37 800,00 zł	25%	28 350,00 zł	
SV-PSU-2Y	SERWIS na 2 dodatkowe lata	Serwis	14%	25%	11%	2	70 560,00 zł	25%	52 920,00 zł	
SV-PSU-3Y	SERWIS na 3 dodatkowe lata	Serwis	13%	25%	10%	3	98 280,00 zł	25%	73 710,00 zł	
SV-PSU-4Y	SERWIS na 4 dodatkowe lata	Serwis	11%	25%	8%	4	110 880,00 zł	25%	83 160,00 zł	
SV-PSU-5Y	SERWIS na 5 dodatkowych lat	Serwis	10%	25%	8%	5	126 000,00 zł	25%	94 500,00 zł	
						pole wyboru ->	SERWIS na 2 dodatkowe lata	70 560,00	25%	52 920,00

RAZEM: 241 920 PLN



Dziękuję za uwagę 😊

Zygmunt Dobosz
ICsec S.A.
+48 504 001 507
zygmunt.dobosz@icsec.pl

ICsec Spółka Akcyjna
Wichrowa 1A, 60-449 Poznań

Biuro w Warszawie
Nowogrodzka 50/54 lok.428
biuro@icsec.pl
www.icsec.pl

