24 KONFERENCJA GAZTERM 2021

Jak wykorzystać możliwości sztucznej inteligencji w celu ochrony cyberbezpieczeństwa automatyki przemysłowej w branży energetycznej?

31.08.2021

Krzysztof Wójtowicz
Head of Sales / ICsec S.A.

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.

CYBERBEZPIECZEŃSTWO DLA POLSKIEGO SEKTORA PRZEMYSŁOWEGO

OGRANICZENIE RYZYKA
BIZNESOWEGO

ZAPEWNIENIE CIĄGŁOŚCI
PRODUKCJI

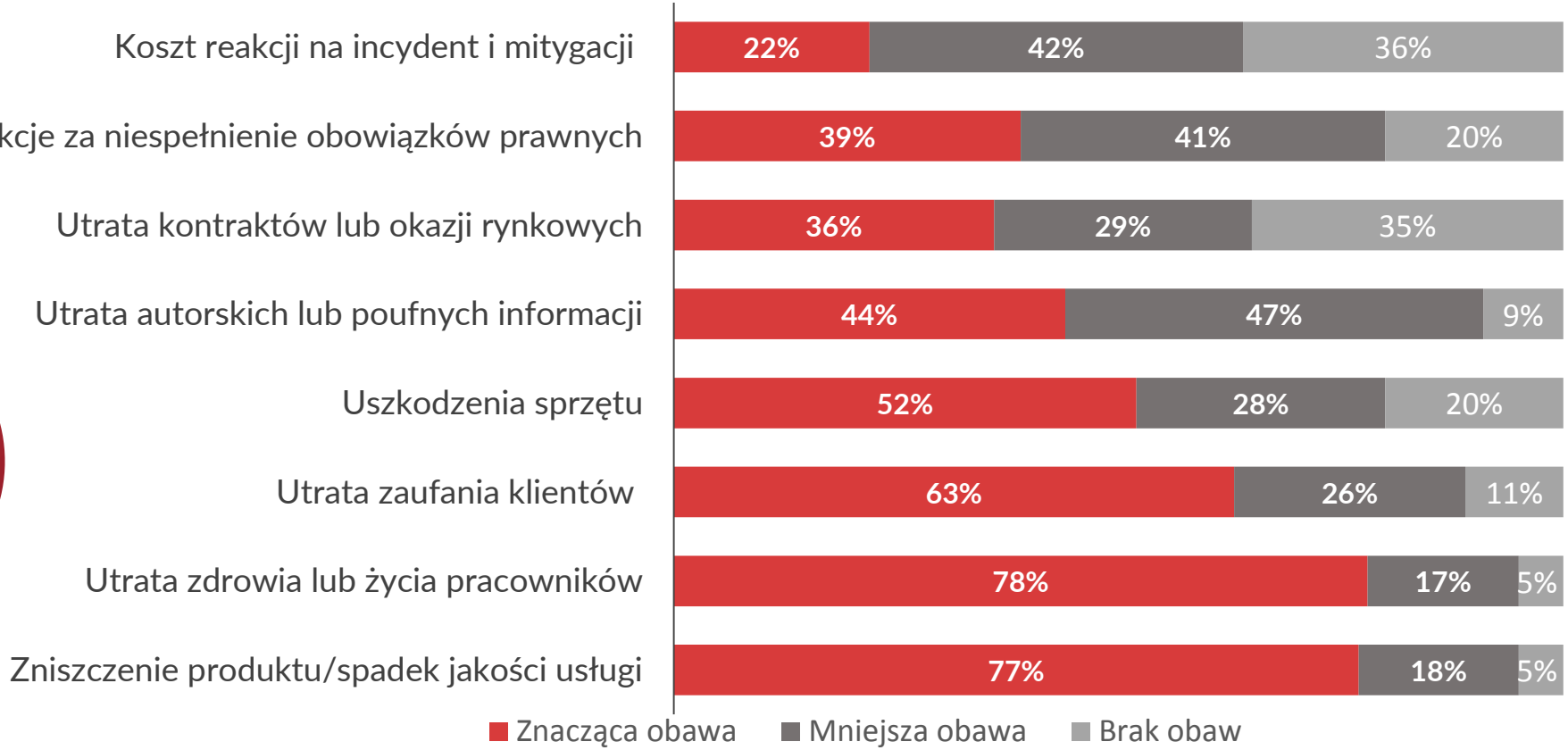
DOSTOSOWANIE PROCEDUR
DO WYMOGÓW PRAWNYCH

INWESTORZY

PGNiG	CVC	NCBR	PFR	TAURON
				
POLSKIE GÓRNICTWO NAFTOWE I GAZOWNICTWO	EEC MAGENTA	NARODOWE CENTRUM BADAŃ I ROZWOJU	POLSKI FUNDUSZ ROZWOJU	TAURON POLSKA ENERGIA

DLACZEGO NALEŻY CHRONIĆ SIECI PRZEMYSŁOWE?

Które ze skutków cyberataku na sieć przemysłową „bolą” najdotkliwiej?



Źródło THE STATE OF INDUSTRIAL CYBERSECURITY, lipiec 2019, raport przygotowany na zlecenie Kaspersky Lab | Przebadano ok.. 300 zakładów przemysłowych na całym świecie

SKALA ATAKÓW JEST OGROMNA

Fragment raportu o stanie bezpieczeństwa technik operacyjnych

- W ciągu 12 miesięcy **90% respondentów doświadczyło co najmniej jednego włamania**, 72% - trzech lub więcej włamań, a 26% - sześciu lub więcej włamań.
- **Ponad połowa badanych (51%) przyznała, że w wyniku ataków ich firma odnotowała spadek wydajności,** 37% stwierdziło, że przestoje operacyjne miały wpływ na osiągane dochody.
- **Według 39% ankietowanych atak miał wpływ na fizyczne bezpieczeństwo**, co stanowi poważny problem, biorąc pod uwagę charakter pracy i strategiczne znaczenie obiektów przemysłowych.

Źródło: firma Fortinet „Raport o stanie bezpieczeństwa technik operacyjnych 2020”

WYZWANIA KLIENTÓW

2009

2014

Dragonfly/Havexy

Złośliwe oprogramowanie atakujące systemy sterowania w USA oraz Europie

2015

Industroyer

Poważne uszkodzenie wielkiego pieca w niemieckiej hucie na skutek cyberataku

2015

Black Energy

Specjalizowany malware powoduje odcięcie od zasilania elektrycznego setek tysięcy osób na Ukrainie

2016

Industroyer

Po raz drugi celem ataku stają się sieci elektroenergetyczne na Ukrainie – skutkiem jest blackout

2017

Ransomware WannaCry oraz NotPetya

Cyberataki na instalacje produkcyjne powodują znaczne zakłócenia pracy zakładów w branżach: motoryzacyjnej, spożywczej i innych

2017

Triton/Trisis

Złośliwe oprogramowanie atakuje układy bezpieczeństwa od Schneider Electric – głównie na Bliskim Wschodzie

2018

VPNFilter

Złośliwe oprogramowanie infekuje urządzenia sieciowe i wyszukuje komunikacje z systemami sterowania

2018

Firma **TSMC** zmuszona do wstrzymania pracy szeregu zakładów po zawirusowaniu systemów komputerowych

2019

Globalny cyberatak na systemy firmy **Pilz**

2019

Ransomware LockerGoga

Globalny cyberatak powoduje wstrzymanie produkcji aluminium w Norsk Hydro

2020

Enel Group została zaatakowana przez oprogramowanie ransomware **SNAKE** (znane również jako **EKANS**)

2021 (luty)

Floryda

Atakujący podłączył się pod kontrolery dozowania substancji chemicznych i próbował zwiększyć poziom wodorotlenku sodu

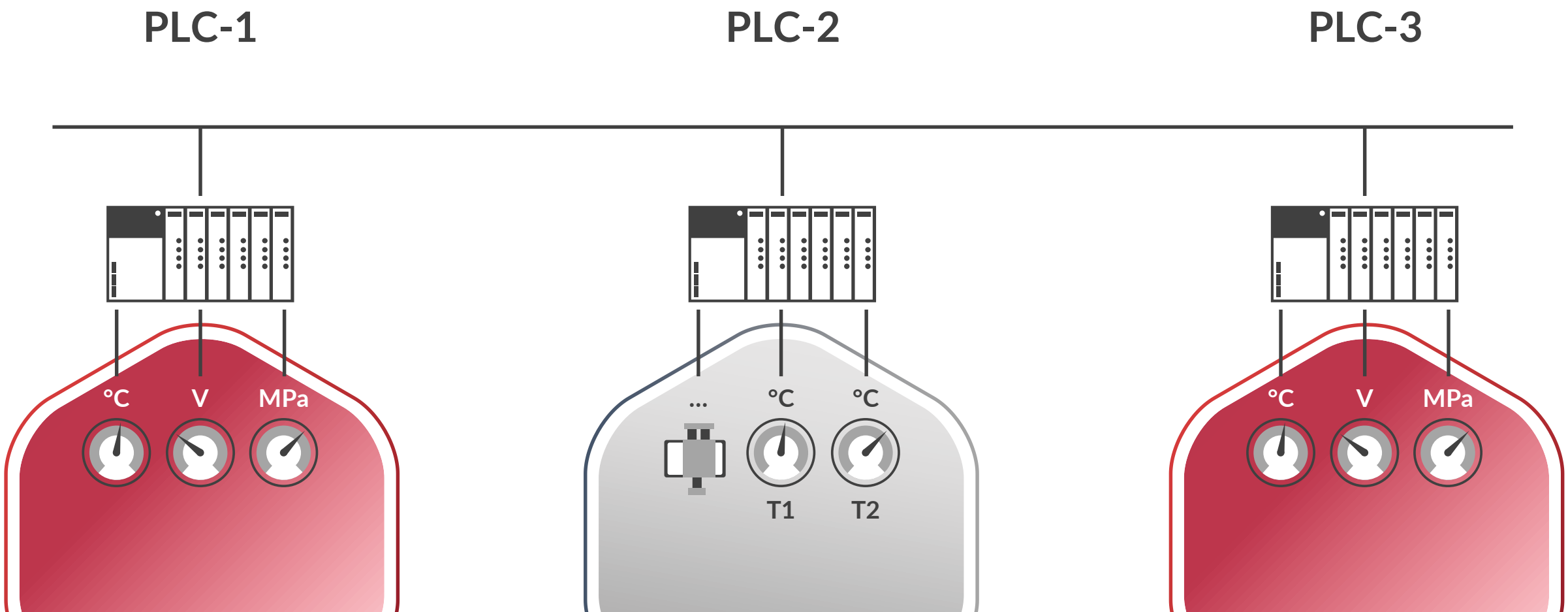
2021 (maj)

Colonial Pipeline

Największy w USA operator rurociągów, wstrzymał wszystkie swoje operacje.

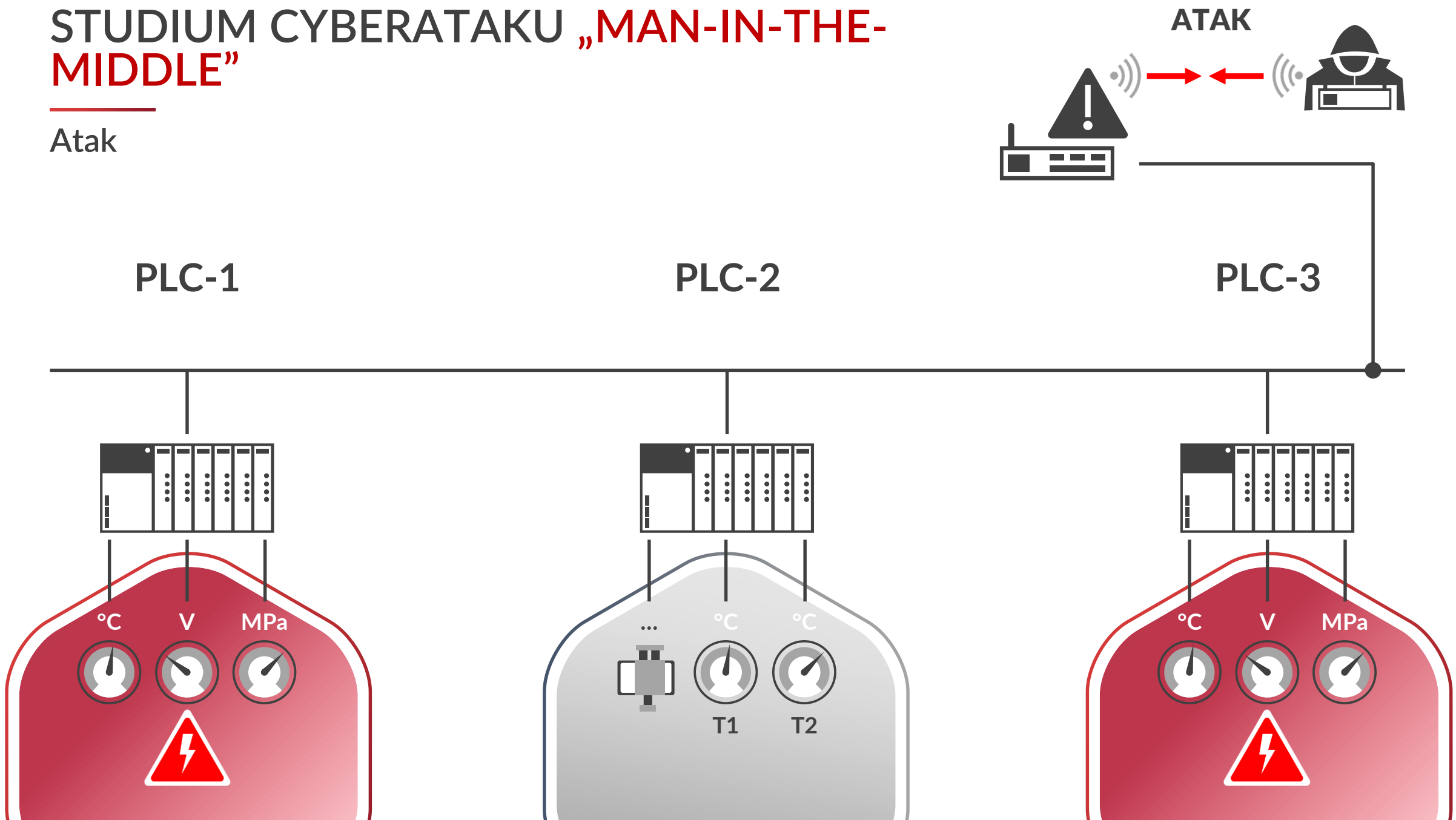
STUDIUM CYBERATAKU

Praca normalna



STUDIUM CYBERATAKU „MAN-IN-THE-MIDDLE”

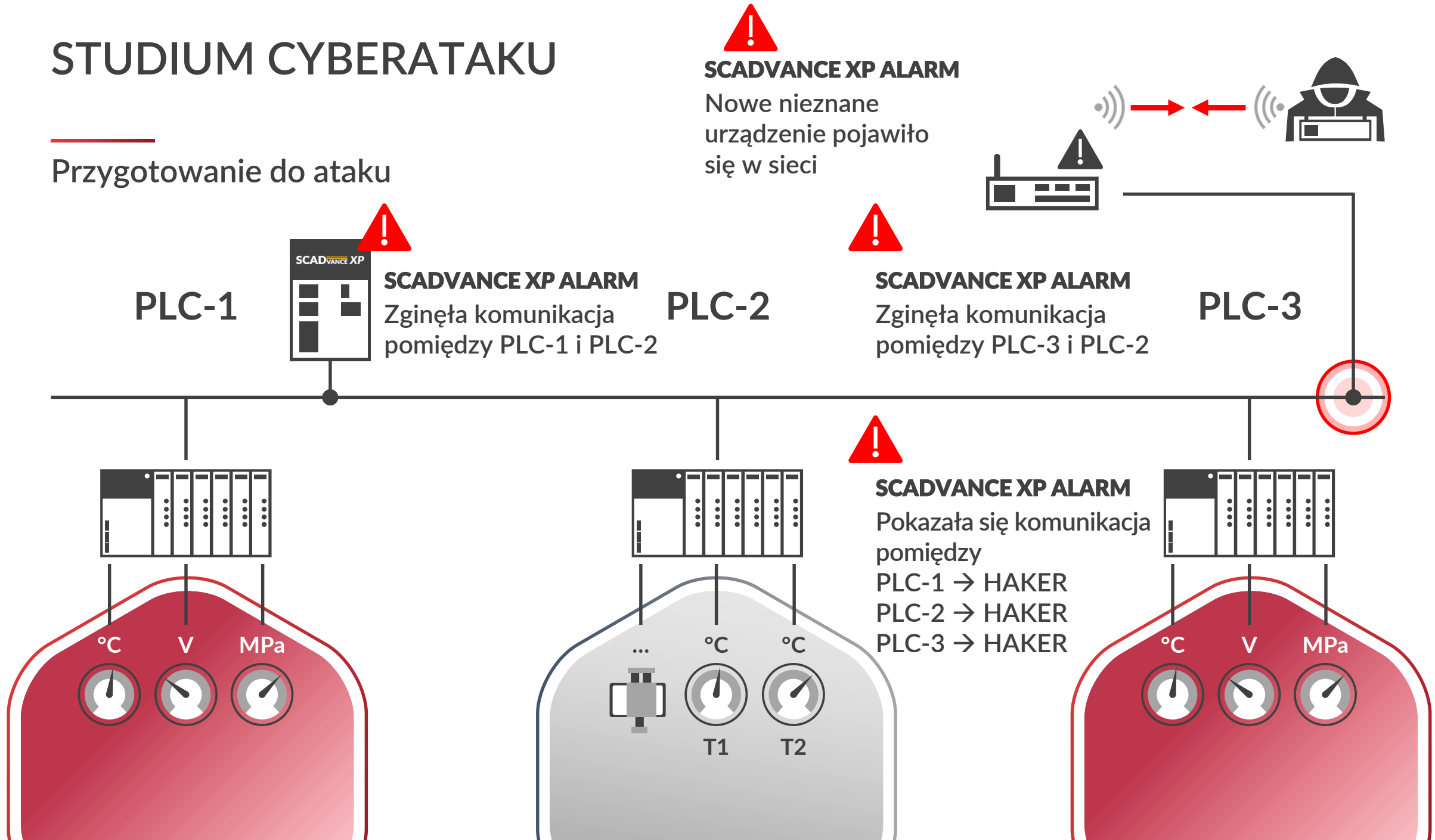
Atak



A CO SIĘ STANIE GDY ZASTOSUJEMY SCADVANCEXP

STUDIUM CYBERATAKU

Przygotowanie do ataku



SCADVANCE XP

INTRUSION DETECTION SYSTEM DLA SIECI PRZEMYSŁOWYCH

Pasywna sonda oraz kompletne rozwiązanie do monitoringu i analizy sieci OT

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

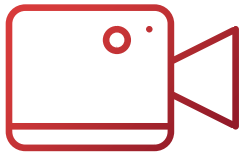
ZALETY WDROŻENIA ROZWIĄZANIA TYPU SCADVANCE XP

CIĄGŁY MONITORING SIECI

Nieprzerwane monitorowanie sieci OT w trybie pasywnym

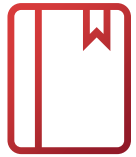
NATYCHMIASTOWY EFEKT

Automatyczne wykrywanie zasobów sieciowych wraz z ich inwentaryzacją



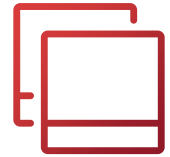
NAGRYWANIE CAŁEGO RUCHU

Nagrywanie i archiwizacja ruchu sieci przemysłowej umożliwia dochodzenie przyczyn ataku



DOSTOSOWANIE DO OBECNEGO PRAWA

Spełnia wszystkie normy nałożone przez dyrektywę NIS oraz KSC



INTEGRACJA Z ISTNIEJĄCYMI ROZWIĄZANIAMI

Integrowane z istniejącymi systemami zarządzania np. SIEM, UEBA

Krzysztof Wójtowicz
ICsec S.A.

Wichrowa 1A, 60-449 Poznań
+48 (61) 82 97 100

Krzysztof.Wojtowicz@icsec.pl