

DZIEŃ 1

IDENTYFIKACJA RYZYKA I WIDOCZNOŚĆ INFRASTRUKTURY KOMUNALNEJ

GODZ.	CZAS	TEMAT / PUNKT PROGRAMU
08:30	00:30	Rejestracja Uczestników
BLOK I — DLACZEGO CYBERBEZPIECZEŃSTWO STAŁO SIĘ ELEMENTEM TRANSFORMACJI INFRASTRUKTURY KOMUNALNEJ		
09:00	00:15	Otwarcie wydarzenia
09:15	00:30	Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa dla JST i spółek komunalnych
09:45	00:30	Cyfryzacja infrastruktury komunalnej a ciągłość świadczenia usług publicznych – dekarbonizacja, nowe technologie i ryzyka cybernetyczne
10:15	00:45	Transformacja przedsiębiorstwa ciepłowniczego i budowa cyberodporności – doświadczenia MPEC Olsztyn
11:00	00:30	<i>Przerwa: kawa, przekąski i networking / TechPlayground</i>
BLOK II — JAK POZNAĆ SVOJĄ INFRASTRUKTURĘ I SYSTEMY AUTOMATYKI		
11:30	00:45	Badanie bezpieczeństwa środowisk OT/ICS – metodyka, narzędzia i typowe podatności wykrywane w środowiskach OT infrastruktury komunalnej
12:15	00:30	Jak zbudować skuteczny monitoring systemów automatyki – architektura, źródła danych i dobre praktyki
12:45	00:30	Warsztat: od wykrycia podatności do reakcji na incydent – praktyczne monitorowanie środowiska OT z wykorzystaniem SIEM i NIDS
13:15	00:45	<i>Przerwa: lunch i networking / TechPlayground</i>
BLOK III — JAK PODEJMOWAĆ DECYZJE W OPARCIU O RYZYKO		
14:00	00:30	Od inwentaryzacji do oceny ryzyka – jak widoczność środowiska OT wspiera podejmowanie decyzji

GODZ.	CZAS	TEMAT / PUNKT PROGRAMU
14:30	00:45	Przykłady architektury ochrony środowiska OT/ICS – segmentacja, UTM/NGFW i kontrola komunikacji przemysłowej
15:15	–	Zakończenie

DZIEŃ 2

ARCHITEKTURA ODPORNEJ INFRASTRUKTURY OT

GODZ.	CZAS	TEMAT / PUNKT PROGRAMU
08:30	00:30	Rejestracja Uczestników
BLOK I — JAK ZAPEWNIĆ ODPORNOŚĆ ŚRODOWISKA OT		
09:00	00:05	Otwarcie 2 dnia wydarzenia – Przemysłowe systemy transmisji danych
09:05	00:30	Odporność środowiska OT – strategia backupu i odzyskiwania danych zgodna z zasadą 3-2-1
09:35	00:15	Live Demo: backup i odzyskiwanie środowiska OT z wykorzystaniem segmentacji i DMZ
09:50	00:30	IEC 62443 jako fundament projektowania cyberodpornej architektury OT
10:20	00:30	<i>Przerwa: Kawa, przekąski i networking / TechPlayground</i>
BLOK II — JAK PROJEKTOWAĆ BEZPIECZNĄ KOMUNIKACJĘ DLA INFRASTRUKTURY KOMUNALNEJ		
10:50	00:30	Nowoczesne architektury transmisji danych w środowiskach OT – niezawodność i bezpieczeństwo komunikacji przemysłowej
11:20	00:45	Bezpieczeństwo przemysłowej sieci Ethernet – mechanizmy ochrony w sieciach transportowych i produkcyjnych
12:05	00:45	Budowanie odpornych sieci przemysłowych – najlepsze praktyki, architektura i podejście wdrożeniowe
12:50	00:45	<i>Przerwa: lunch i networking / TechPlayground</i>
BLOK III — JAK BUDOWAĆ KOMPETENCJE I TESTOWAĆ ROZWIĄZANIA		
13:35	00:30	Cyfrowy bliźniak sieci OT – praktyczne laboratorium cyberbezpieczeństwa i symulacja ataków
14:05	00:25	Ludzie, procesy i kompetencje – fundament cyberodporności infrastruktury komunalnej
14:30	–	Zakończenie

