



* ZAPROSZENIE *

Dołącz do nas w Rzeszowie podczas Network & Security RoadShow

Team Tekniska rusza w trasę!

Wykłady, warsztaty praktyczne z działania licencjonowanych systemów i urządzeń, pokazy rozwiązań typu open source na żywo oraz przegląd nowości wśród wiodących producentów naszego portfolio - to wszystko już **26 i 27 marca w Rzeszowie!**

Dołącz do nas Network & Security RoadShow by Tekniska: [FORMULARZ REJESTRACYJNY](#)

Miejsce spotkania: 🏢 Al. J. Piłsudskiego 44, 35-001 Rzeszów

Start: 📅 2024/03/26 ⌚ 09:00

Koniec: 📅 2024/03/27 ⌚ 16:00

NSR'24 to **dwudniowe wydarzenie**, skierowane zarówno do doświadczonych profesjonalistów z branży cyberbezpieczeństwa i sieci przemysłowych, jak i osób, które dopiero rozpoczynają budowanie swoich kompetencji w tych obszarach.

Skorzystaj z zaproszenia, niezależnie od poziomu doświadczenia – NSR'24 pozwoli Ci poszerzyć wiedzę, nawiązać wartościowe kontakty oraz zdobyć praktyczne umiejętności w dziedzinie cyberbezpieczeństwa i przemysłowej transmisji danych.

WAŻNE: W ramach Network & Security RoadShow przygotowaliśmy dla Ciebie dwie ścieżki tematyczne: OT Network & OT/ICS Security. Możesz wziąć udział w obu dniach wydarzenia lub wybrać dzień z tematyką bardziej interesującą dla Ciebie.

Skupimy się na następujących zagadnieniach:

- ◇ Zapewnienie stabilności działania usług sieciowych – separacja komunikacji i segmentacja sieci.
- ◇ Gwarantowanie wymaganych zasobów sieciowych dla komunikacji krytycznej – specjalne aspekty komunikacji safety.
- ◇ Optymalne wykorzystanie sieci – uporządkowanie w kontekście efektywnego wykorzystania pasma.
- ◇ Ochrona sterownika PLC i sieci ICS – zapobieganie zakłóceniom w komunikacji.
- ◇ Ochrona sieci ICS: IDS vs. Firewall – cechy i różnice oraz wybór odpowiedniej strategii ochrony.
- ◇ Efektywne spożytkowanie budżetu – zwiększanie bezpieczeństwa i niezawodności sieci przy optymalnym wykorzystaniu budżetu.
- ◇ Kompetencje IT/OT w zespole UR – jak budować i rozwijać niezbędne kompetencje.
- ◇ Dostosowanie procesów i konfiguracji sieci do normy IEC62443 – przygotowanie odpowiedniego planu działań.
- ◇ Spełnienie wymagań dyrektywy NIS2 – jakie podjąć kolejne kroki.
- ◇ Badanie Bezpieczeństwa Systemów i Sieci pod kątem:
 - Niezawodności w kluczowych obszarach.
 - Odporności na zakłócenia, zarówno zamierzone, jak i niezamierzone.
 - Monitorowanie połączeń zdalnego serwisu.
 - Wpływ ruchu w sieci IT na sieć OT.
 - Odporność na celowe próby nieautoryzowanego dostępu.

Po części oficjalnej zapraszamy na warsztaty i konsultacje indywidualne przy fizycznych modelach sieci.

Więcej informacji na stronie: [ROADSHOW](#)

Do zobaczenia!

Tekniska Team