

# WOJCIECH SIKORSKI

INŻYNIER ENERGETYK



## KONTAKT

- +48 667 534 399
- wjsikorski@proton.me
- ul. Cicha 65,  
43-178 Ornontowice
- www.hacktrick.pl

## KOMPETENCJE TECHNICZNE

- ICS/OT Security (Purdue Model, MITRE ATT&CK)
- Wireshark, Suricata, Wazuh (podstawy SIEM)
- MES, diagnostyka turbin, analiza parametrów eksploatacyjnych
- Podstawy IEC 62443
- Ubuntu, Windows Server, SCADA/HMI, Kali Linux

## JĘZYKI

- Angielski (Zaawansowany)
- Hiszpański (Podstawowy)

## ZAINTERESOWANIA

- CTF / laby ICS
- Analiza incydentów
- Kryminalistyka i true crime
- Gry strategiczne i łamigłówki
- Rękodzieło
- Numizmatyka



## PROFIL

Inżynier z doświadczeniem w przemyśle ciężkim, chcący rozwijać karierę w cyberbezpieczeństwie systemów ICS/OT. Znam specyfikę środowisk przemysłowych i ich zagrożenia, a także rozumiem kluczowe aspekty bezpieczeństwa operacyjnego. Cechuje mnie myślenie analityczne i szybko się uczę. Moim celem jest ochrona systemów sterowania przed cyberatakami, zapewnienie ich niezawodności oraz rozwój w kierunku roli CISO



## DOŚWIADCZENIE ZAWODOWE

**Przedsiębiorstwo Usług Naukowo-Technicznych Pro Novum** Od 2017  
**Specjalista ds. urządzeń energetycznych**

- Opracowywanie szczegółowych ekspertyz o stanie technicznym urządzeń energetycznych.
- Przeprowadzanie obliczeń strukturalnych dla infrastruktury krytycznej, wykorzystując oprogramowanie MES.
- Analizowanie dużych zbiorów danych eksploatacyjnych.

**Przedsiębiorstwo Usług Naukowo-Technicznych Pro Novum** 2015 - 2017  
**Młodszy specjalista ds. urządzeń energetycznych**

- Współpraca przy implementacji systemów monitorowania i zarządzania infrastrukturą krytyczną.

**PKN Orlen S.A.**

08. 2024 - 09. 2025

**Staż w Wydziale Remontów**

- Zdobycie praktycznej wiedzy na temat systemów sterowania przemysłowego (ICS) oraz procesów konwersji energii.
- Analiza i raportowanie danych operacyjnych dla CHP, identyfikowanie wzorców mogących wskazywać na potencjalne zagrożenia dla systemów sterowania zakładu.



## EDUKACJA

**Politechnika Wrocławska** | Wydział Górnictwa i Geologii | mgr inż.  
Górnictwo podziemne i odkrywkowe | 2014 – 2016

**Instituto Superior Técnico (Lizbona)** | Wydział Mechaniczny |  
Kierunek: Mechanika (stypendium Erasmus) | 2014

**Akademia Górniczo-Hutnicza w Krakowie** | Wydział Energetyki i Paliw  
| mgr inż. Energetyka | 2009 – 2014



## CERTYFIKATY

**Uzyskane:**

- Certified Fundamentals in Cybersecurity - Fortinet
- Certified in Cybersecurity (CC) - ISC2
- Google Cybersecurity Professional Certificate - Google
- Cyber Threat Intelligence Analyst 101 - arcX
- Introduction to Cybersecurity - CISCO

**W trakcie:**

- ISO/IEC 27001 Lead Implementer
- Security + - CompTIA
- CISA - ISACA



## PROJEKTY

- **Hacktrick.pl** - blog o cyberbezpieczeństwie IT/OT (analizy incydentów, własne ramy metodologiczne).
- **Lab OT/ICS Security** - budowa środowiska testowego (Proxmox, PLC simulator, Suricata, Wireshark).
- **Analiza incydentu Colonial Pipeline** - case study w modelu MITRE ATT&CK (portfolio).
- **IT vs OT** - analityczny dokument ukazujący różnice w zapewnieniu bezpieczeństwa w obu przypadkach.
- **ICS Risk Profiler + CIRA** - autorska metodologia oceny ryzyka dla infrastruktury krytycznej.
- **Honeypot OT** - w przygotowaniu



## PUBLIKACJE

- **Autor 150+ artykułów branżowych** (Energetyka, Nowoczesny Przemysł, Energetyka Ciepła i Zawodowa, inne).
- **Tematyka:** cyberbezpieczeństwo systemów ICS/OT, efektywność energetyczna, diagnostyka urządzeń przemysłowych, predictive maintenance, technologie energetyczne
- **Wybrane publikacje:**
  1. „Cyberbezpieczeństwo systemów sterowania przemysłowego (ICS/OT) - specyfika zagrożeń i metody ochrony.” - Nowoczesny Przemysł (2025)
  2. “Cyberzagrożenia dla infrastruktury OZE. Studium rzeczywistych ataków” - Energetyka Ciepła i Zawodowa (2025)
  3. “Rola sztucznej inteligencji w optymalizacji zużycia energii w przemyśle energetycznym” - Nowoczesny Przemysł (2024)
  4. “Automatyzacja procesów utrzymania ruchu w energetyce odnawialnej” - Energetyka Ciepła i Zawodowa (2025)
  5. “Wpływ warunków eksploatacji na żywotność elementów turbozespołu” - Energetyka (2021)



## KOMPETENCJE TECHNICZNE

- **Cybersecurity / ICS-OT:** MITRE ATT&CK for ICS, analiza PCAP (Wireshark), Suricata, podstawy SIEM, segmentacja sieci (Model Purdue).
- **Inżynierskie:** MES (obliczenia strukturalne), analiza przebiegu pracy, określanie przyczyn awarii
- **Normy i standardy:** ISO/IEC 27001, IEC 62443, NIS2 - znajomość podstaw wdrożeniowych.
- **Systemy:** Ubuntu, Windows Server, SCADA/HMI (podstawy), Kali Linux.
- **Narzędzia:** Wireshark, Suricata, Nmap, Wazuh.
- **Wirtualizacja:** Proxmox, VirtualBox, Docker, Cisco Packet Tracer



## KOMPETENCJE MIĘKKIE

- **Zarządzanie ryzykiem w infrastrukturze krytycznej** - podejmowanie decyzji w oparciu o analizę zagrożeń i wpływu biznesowego.
- **Komunikacja kryzysowa** - jasne przekazywanie informacji podczas incydentów, bez eskalowania paniki.
- **Współpraca interdyscyplinarna** - łączenie perspektywy inżynierów, IT, compliance i zarządu.
- **Myślenie strategiczne** - planowanie długoterminowej odporności organizacji na cyberzagrożenia.
- **Mentoring i rozwój zespołu** - wspieranie młodszych specjalistów w rozwoju kompetencji.
- **Myślenie krytyczne** - umiejętność obiektywnej analizy problemów, kwestionowania założeń i podejmowania decyzji opartych na faktach
- **Umiejętność podejmowania decyzji w warunkach presji i niepewności**
- **Rozwiązywanie konfliktów** - mediacja między działami technicznymi i biznesowymi



## CZŁONKOSTWA I NETWORKING

- **ISSA Polska** - członek zwykły od 2025
- **LinkedIn** - profil zawodowy oraz blog