Andrzej Skowroński

01.01.1992 | +48 720 493 633 | andrzejskowronski@proton.me | andrzej.space | github.com/andsko92

Summary

Experienced nuclear safety systems engineer with a strong foundation in risk assessment, safety protocols and regulatory compliance, seeking to transition into the cybersecurity field to apply analytical skills and dedication to safeguarding digital assets.

Education

Gdańsk University of Technology   November 2018
Master of Science in Mechanical Engineering | Spec.: Safety Systems Engineering

Gdańsk University of Technology   February 2017
Bachelor of Science in Power Engineering | Spec.: Fluid-Flow Machinery

Experience

Safety & Governance Power Systems Engineer, GE Power, Poland   Nov 2019 – June 2023
- Designed diagrams and topologies for generator safety and control systems for nuclear power plants
- Supervised design reviews, risk evaluations, incident investigations, and safety assessments
- Positioned as the technical lead for the initiatives involving new products, upgrades and retrofits
- Evaluated designs, updated to comply with the most recent CSA, ASME, and ISO quality and safety standards
- Prepared technical quotes and closely coordinated collaboration with sales and tendering teams
- Negotiated contractual criteria with clients, suppliers and subcontractors

Auxiliary Power Systems Design Engineer, GE Power, Poland   Nov 2018 – Oct 2019
- Designed turbine support systems and steam paths for conventional power plants
- Ensured that engineering safety standards and codes, EHS, and functional safety requirements were met
- Provided technical support for building, commissioning, and startup of turbine auxiliary systems
- Released engineering documentation for piping and arrangement planning of turbine hall

Projects

- Homelab - home network built with Raspberry devices, managed with Ansible, secured with Snort and Splunk
- LAN topologies - simulated networks created in GNS3 and Packet Tracer utilizing Cisco equipment and services
- Honeypot - server used to track and investigate signs of security compromise of common services
- VMware home lab - virtual home lab built with VMware ESXi Server, vCenter and FreeNAS
- Pentest tools suite - tool set for basic penetration tests. (scans, enumerations, password cracking scripts)
- Password verification - script that verifies leaked passwords using haveibeenpwned.com API
- Vending machine - vending machine simulator made in Python
- My website - simple website made in HTML and CSS, hosted on Nginx and running on a private server

Skills

Programming languages: Python, HTML, CSS, C++
Hardware: Raspberry Pi, Arduino, ARM-based microcontrollers
Software: Nmap, Ansible, Wireshark, Splunk, Snort, Burp Suite, Zeek, Metasploit
Certifications: Security+, CCNA, eJPT, AWS CCP, OCI, PCEP/PCAP, CPE, CLE, JSE, PED, ATEX
Languages: Polish, English