RWTH AACHEN UNIVERSITY

E.ON Energy Research Center
ACS | Institute for Automation of Complex Power Systems

Hiwi Position

Software Development Support: Multistep CyberAttack Detection Co-Simulator

Context:
The *Institute for Automation of Complex Power Systems* investigates several circumstances that affect power and Energy systems. While digitization of distribution grids through information and communication technology brings numerous benefits, it also increases the grid's vulnerability to critical cyberattacks. Unlike conventional systems, attacks on many industrial control systems such as power grids often occur in multiple stages, with the attacker taking several steps to achieve the target goal. Detection mechanisms with situational awareness are needed to detect orchestrated attack steps as part of a coherent attack campaign. To provide a foundation for detection and prevention of such attacks, this project addresses the detection of multi-stage cyberattacks with the aid of a graph-based cyber intelligence database (Neo4j) and alert correlation approach [1]. Specifically, we will improve the *technology readiness level* of cosim[1] and adapt to other scenarios.

Tasks:
At the beginning, the candidate will get familiar with the code base in python. Next, based on the starting level, background on graph data modelling is covered and models for new scenarios will be created. More importantly, better methods of packaging and deploying the software solution with detailed documentation will be carried out simultaneously.

Requirements:

- RWTH Bachelor/Master Student in Engineering, computer science or related fields.
- Good knowledge of Python
- Knowledge of DevOps (Docker and Docker-compose in deployment) and Git version control
- Knowledge of graph database (NEO4J) will be beneficial.

[1] https://cyberseas.eu

Notes:

- The project will be coordinated in English
- If you are interested in the advertised position, please send your CV showing relevant experience and current transcript.

Reference

[1] A holistic Multi-Step Cyberattack Detection via a Graph-based Correlation Approach. Omer Sen, Chijioke Eze, Andreas Ulbig, Antonello Monti. https://arxiv.org/abs/2211.10971.

Contact:
Abraham Ezema
Phone: +49 241 80 49749
E-mail: abraham.ezema@eonerc.rwth-aachen.de

Chijioke Eze
Phone: +49 241 80 49738
E-mail: chijioke.eze@eonerc.rwth-aachen.de

ACS | Institute for Automation of Complex Power Systems
ERC | E.ON Energy Research Center
RWTH Aachen University
Mathieustr. 10, 52074 Aachen, Germany