Karlsruhe Institute of Technology

Earliest start: Now!

KASTEL

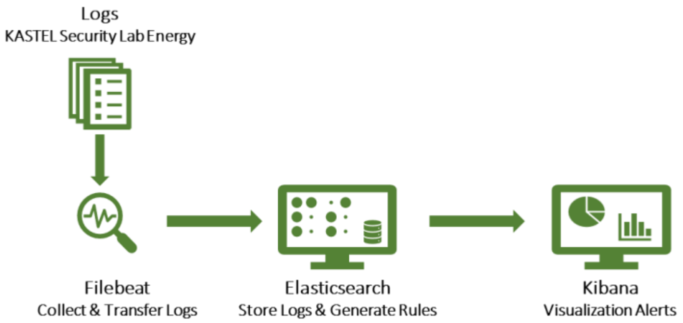
HiWi-Job!
Supporting Alert Generation Through SIEM (Security Information and Event Management) System at the KASTEL Security Lab Energy

Welcome to the Secure Energy Systems (SES) Research Group! The highlighted objective of “Secure Energy Systems (SES)” working group is about the cyber-physical security of energy systems. The working topics cover a broad range from hardware to the communication structure in Smart Grids (SGs).

Discovering the relation between various raised alarms will improve the performance of substation and overall protection of SGs. Security Information and Event Management (SIEM) systems gather and examine data from these various sources to detect and react to potential security incidents such as equipment damage, production downtime, or environmental harm. For this purpose, a SIEM system will be installed and configured at the KASTEL Security Lab Energy that located at the Institute of Automation and Applied Informatics (IAI). Potential future applications are explored for integrating alarm correlation framework into SIEM systems to enhance their existing features such as risk analysis.

We offer:

- Interesting tasks that offer the chance to work with real-world hardware and applications
- Flexible working hours



Requirements:

- Bachelors or Masters in Computer Science
- Familiar (or motivated to work) with network traffic supervision and Elastic Stack
- Familiar (or motivated to work) with Python, Bash/Shell Scripting, YAML, JSON, RESTful API and SQL-based queries in Elasticsearch, Kibana, Filebeat
- Motivated to work independently and as part of a team

Main Tasks:

- Assistance with automation, configuration and deployment tasks for the Elastic Stack
- Support in enhancing current rules and implementing new ones for alert generation in the Elastic Stack
- Data visualization and documentation of the outcomes

We are happy to answer any questions you might have. If you are interested, contact us via email to sine.canbolat@kit.edu including current transcript of records and a resume/CV.

Contact Data

Karlsruher Institut für Technologie (KIT)
Automation and Applied Informatics (IAI)
Location: Campus North

Name Surname: Sine Canbolat
Secure Energy Systems (SES)
Phone: +49 721 608-22913
E-mail: sine.canbolat@kit.edu