Security Information and Event Management for maritime context

Summary

Monitoring systems and SCADA are major components of maritime systems. They detect system status and eventually to indicate issues and alarms to operators. However, failures propagate in interconnected systems and generates correlated alarms that become a nuisance in the operation. The aim of this thesis is to develop SIEMs for the maritime usages

Research field:	Information and Communication Technology
Supervisors:	Prof. Dr. Olaf Manuel Maennel Prof. Dr. Mohammad Reza Kave Salamatian
Availability:	This position is available.
Offered by:	Tallinn University of Technology Estonian Maritime Academy
Application deadline:	Applications are accepted between November 15, 2021 00:00 and December 15, 2021 23:59 (Europe/Zurich)

Description

SIEM are software systems that aggregates and analyzes activity from many different resources across entire IT infrastructures. They collect data from all devices, stores, normalizes, aggregates, and applies analytics to that data to discover trends, correlate them to detect threats, and enable organizations to investigate any alerts.

However, the functionalities of SIEM are also interesting for other domains beyon cybersecurity of classical IT infrastructures. The goal of this thesis is to expand to use of SIEM to SCADA monitoring system in maritime systems. We consider the SIEM as the aggregating component enabling the integrating of classical monitoring of the command-and-control component of maritime systems (SCADA).

The thesis will investigate correlation techniques that helps in filtering a feed of incoming alarm from different devices and to categorize them. This will involve developing root cause analysis techniques leveraging AI. Therefore, the thesis topic seats at the crossing between machine learning, maritime systems and cybersecurity.

The thesis will be done in the context of the European ERA chair on maritime cybersecurity.

Supervisor: Prof. Dr. Mohammad Reza Kave Salamatian
Co-supervisor: Prof. Dr. Olaf Maennel

Applicants should fulfil the following requirements:

The applicant for the position must have a Master’s degree and must fulfil the requirements for doctoral students at the Tallinn University of Technology. In addition, a competitive candidate for this role should demonstrate the following qualifications:

- A degree in computer science, or electrical engineering, or telecommunications, or mathematics another closely-related discipline.
- High level of interest on the topic.
- Good writing and communication skills, in particular in English language.

A lack of experience in the above skills could be compensated by evidence of research potential.

Appropriate training will be provided.

To get more information or to apply online, visit https://taltech.glowbase.com/positions/480 or scan the the code on the left with your smartphone.