TAL
TECH

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 generate 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:	Estonian Maritime Academy
Application deadline:	Applications are accepted between October 01, 2022 00:00 and October 23, 2022 23:59 (Europe/Zurich)

Description

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

However, the functionalities of SIEM are also interesting for other domains beyond cybersecurity of classical IT infrastructure. The goal of this thesis is to expand to use of SIEM to SCADA monitoring systems 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).

Several techniques are currently employed to detect cyber security incidents starting from captured security- related events within networks, computer systems, operation components, but also online contents. However, the large volume of observable events, the continuous sophistication and changes in attack strategies make it challenging to detect and reconstruct effectively cybersecurity incidents and increases the false alert rates. Therefore, it is essential to develop mechanisms and models for fusionning large streams of heterogeneous data, and system's information in meaningful ways to supplying detailed information to IT security management. This thesis should propose such models to correlate detectable suspicious events by combining complementary state-of-the-art methods, which perform correlation along different axes. In particular, the question of causality would have a central role in the thesis as it helps in filtering a feed of incoming alarm from different devices, to categorise them and implement 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.

Bibliography

- Security information management as an outsourced service. Debar, Hervé and Viinikka, Jouni. 2006, Information Management & Computer Security, Vol. 14 No.5, pp. 417-435.
- Kotenko, Igor, Diana Gaifulina, and Igor Zelichenok. "Systematic Literature Review of Security Event Correlation Methods." IEEE Access (2022).
- Sadoddin, Reza, and Ali Ghorbani. "Alert correlation survey: framework and techniques." Proceedings of the 2006 international conference on privacy, security and trust: bridge the gap between PST technologies and business services. 2006.
- By Hector Geffner, Rina Dechter, Joseph Halpern, Probabilistic and Causal Inference: The Works of Judea Pearl
- Temporal and Spatial Distributed Event . Jiang, Guofei and Cybenko, George. Boston : s.n., 2004. American Control Conference. pp. 996-1001.

- Nabil, Moukafih, et al. "SIEM selection criteria for an efficient contextual security." 2017 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, 2017.

Supervisors:

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

Responsibilities and (foreseen) tasks

- Do collaborative, ambitious, and high-level research in a highly international environment
- Publish papers in respectable and highly cite journals and conferences
- Implement systems and prototype to illustrate the research
- Prepare for academic jobs and position by contributing reasonably in the education

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 levels of interest on the topic.
- Good writing and communication skills, in particular in English language.

The candidate should submit a research plan for the topic, The candidate can expand on the listed research questions and tasks and propose theoretical lenses to be used.

We offer:

- 4-year PhD position in one of the largest, most internationalised and leading computer science research centres in Estonia with a large portfolio of ongoing pan-European projects
- The chance to do high-level research in one of the most dynamic cybersecurity contexts globally
- Opportunities for conference visits, research stays and networking with globally leading universities and research centres in the fields of computer science, cybersecurity, and machine learning.

About the research environment

- Excellent opportunities for performing high quality research, as part of a highly competent and motivated team of international researchers and engineers.
- An informal and inclusive international working environment, green campus approach, a flexible schedule and modern office facilities located in Tallinn.
- Opportunities to build international networks, through established collaboration with industry, exchange programs and research visits to other universities, and support to attend research conferences.
- Innovative, ambitious, and multidisciplinary cooperation-oriented research groups in TalTech.
- One of the most compact and sufficient maritime communities in Europe that is surrounded by technology, digitalisation and many high-tech companies and start-ups (Skype, Starship Technologies, Bolt, Pipedrive, etc.).
- To support the high-quality research, it is possible to use the numerous possibilities offered by our state-of-the-art modern laboratories' infrastructure and maritime simulator centre.
- Our digital and small society - everything is doable digitally and on smart ways.
- Individual development and training opportunities.

For further information, please contact

- Kavé Salamatian, ERA Chair Holder kave.salamatian@taltech.ee
- Olaf Maennel, prof. of Computer science, olaf.maennel@taltech.ee

To get more information or to apply online, visit https://taltech.glowbase.com/positions/598 or scan the the code on the left with your smartphone.