Methods and tools for security event processing

Summary

The overall goal of this PhD project is to research methods and develop tools for real-time and offline processing of security events in SOC (security operation center) environments. The PhD project addresses the following research questions – in a production SOC environment, what are the most efficient methods for: (1) the reduction of false positive alerts, (2) the prioritization of alerts, (3) the detection of novel attacks? The purpose of this PhD project is to study the research questions on real-life data, validate research results in a production SOC, and release publicly available tools that implement the research results and advance the security posture of an organization.

Research field:	Information and communication technology
Supervisor:	Dr. Risto Vaarandi
Availability:	This position is available.
Offered by:	School of Information Technologies Department of Software Science
Application deadline:	Applications are accepted between June 01, 2022 00:00 and June 30, 2022 23:59 (Europe/Zurich)

Description

During the last decade, cyber attacks have significantly increased in both complexity and volume. In order to detect these attacks, many institutions have set up organizational SOCs that employ dedicated security monitoring technologies like NIDS (network intrusion detection system). However, existing security monitoring technologies have a number of open issues. First, they tend to generate large volumes of alerts, with many of them being either false positives or having low importance. That will complicate the work of human security analysts who are overwhelmed by irrelevant alerts and unable to focus on high-priority events. Second, many existing security monitoring technologies (for example, most widely used NIDS platforms) are signature-based, where each signature is designed to detect a known attack with a known footprint in network traffic or system logs. Unfortunately, signature-based monitoring technologies are unable to detect novel attacks that are not covered by existing signatures.

For the above reasons, the PhD project focuses on the following areas:

- 1) reduction of false positive alerts in production SOC environments,
- 2) prioritization of alerts in production SOC environments,
- 3) detection of novel attacks in production SOC environments.

Although aforementioned three areas have already received attention and a number of approaches have been proposed in the past research literature, many past approaches have been developed on data sets that are either old or of limited size and thus do not adequately represent real-life environments. Also, these approaches have been seldom validated in production environments over longer periods of time. In addition, the implementations of these approaches are often not publicly available which complicates their evaluation by other researchers.

For this reason, the research of this PhD project will be conducted on real-life data collected from university SOC, with the data including NIDS alerts, Netflow, and other security events. It is expected that the PhD research will not only produce new methods and algorithms as a result, but also tools that implement these methods and algorithms. As a part of the research, the PhD student must evaluate developed tools in the university SOC over longer time frames (e.g., 6-12 months) in order to demonstrate that the developed methods and algorithms are producing expected results in real-life environments. In addition, the tools must be publicly released under open-source licenses (e.g., GPLv2).

Responsibilities and (foreseen) tasks

- Setting up a research environment (e.g., Linux servers) for collecting security data (e.g., NIDS alerts) from live SOC environment
- Feature engineering for turning raw data collected from SOC into structured data sets suitable for use with machine learning algorithms
- Labeling the structured data sets for use with supervised and semi-supervised machine learning methods

- Evaluating existing supervised and unsupervised machine learning and data mining methods (e.g., random forest, SVM, DBSCAN, Apriori, etc.) on structured data sets
- Development of new machine learning and data mining methods (e.g., new stream clustering or stream pattern mining algorithms for textual security event logs)
- Software development in Python, Golang, Perl, C/C++ (or other appropriate programming language) for creating the implementations of new machine learning and data mining methods
- System administration activities (e.g., acting as a Linux administrator) in order to keep the research environment in good order

Applicants should fulfil the following requirements:

- a master's degree in computer science (preferably in a field closely related to computer and network security)
- a clear interest in the topic of the position
- excellent command of English
- strong and demonstrable writing and analytical skills
- capacity to work both as an independent researcher and as part of an international team
- capacity and willingness to provide assistance in organizational tasks relevant to the project
- good understanding of TCP/IP networking and network security
- previous experience with Linux system administration and good understanding of command line tools
- at least 5 years of experience in software development (e.g., using Python, Golang, Perl, C/C++, etc.)
- at least 2 years of experience with machine learning and developing machine learning applications
- good understanding how to employ Python scikit-learn library for developing machine learning applications

The following experience is beneficial:

- Security analyst experience from production SOC
- Developer experience from production SOC
- Administration experience of dedicated security monitoring technologies (e.g., Suricata and Snort)
- Administration experience of firewalls, routers and network switches
- Previously obtained Linux and network administration certificates (e.g., RHCE)
- Previously developed machine learning and data mining tools which have been publicly released
- Research experience in the field of machine learning and previously published academic papers (e.g., in IEEExplore or ACM Digital Library)

The candidate should submit a research plan for the topic, including the overall research and data collection strategy. The candidate can expand on the listed research questions and tasks, and propose theoretical approaches to be used.

We offer:

- 4-year PhD position in one of the largest, most internationalized and leading cyber security research centers in Estonia
- The chance to do high-level research in one of the most digitally advanced country in Europe
- Opportunities for conference visits, research stays and networking with globally leading universities and research centers in the field of cyber security

About the department

TalTech Centre for Digital Forensics and Cyber Security works towards enhancing the competence and ability of Estonian computer security field through education, research and development. We strive towards becoming the best cyber security Master's and Doctoral studies institution in the Baltics and Nordic countries. The centre is a part of TalTech Department of Software Science. The Centre for Digital Forensics and Cyber Security coordinates Cybersecurity MSc programme (IVCM).

The centre focuses on the development of the cyber security field. The goals which stem from this can be elaborated as follows:

- Raising the competence and ability of Estonian digital forensics and cyber security through education, research and development;
- Focusing on the relevant actions in TalTech according to Estonian national cyber security strategy;
- Cooperation and preparation for technological interchange with other relevant fields of research.

TalTech Centre for Digital Forensics and Cyber Security was established in November 2014 at CyberCrime2014 conference. The partnership contract was signed by Tallinn University of Technology, Ministry of the Interior, Ministry of Justice, Ministry of Defence, Ministry of Economic Affairs and Communications, Police and Border Guard Board, Estonian Forensic Science Institute and Information System Authority.

Additional information

For further information, please contact Dr. Risto Vaarandi (risto.vaarandi@taltech.ee) or visit https://taltech.ee/en/centre-for-digital-forensics-cyber-security

To get more information or to apply online, visit https://taltech.glowbase.com/positions/517 or scan the the code on the left with your smartphone.