Project Title

Enterprise Log Analytics

Project Description: This project aims to identify advanced threats targeting enterprise environments through analysis of diverse data sources in order to provide security practitioners with necessary attack intelligence. The work involves fusing and synopsizing vast amounts of data sources, including system logs created by end-hosts, servers, and security devices, to obtain a global view of event level actions performed by users on systems over a long-time duration. The goal of the analysis is to identify sequence of events, dispersed across time and multiple resources, that potentially constitute steps of known attack patterns. The analysis also includes detecting inconsistent and unusual changes in user behavior, in comparison to other users, to identify new attack campaigns. Findings will be presented to specialists in the form of graphs, charts, and other visualizations through a dashboard to allow for effective risk mitigation.

Duties/Activities: The intern will work hand-in-hand with other researchers and support them with one or more of the following tasks

- Mapping system logs to high level security events
- Incorporation of external data sources
- Building a front-end dashboard to visualize developed analytics

Required Skills: Experience with Python and C/C++ programming languages

Preferred Intern Academic Level: Undergraduates at all levels of Computer Science programs

Learning Opportunities: Students will get familiar with system and network security problems in the context of advanced attacks; attain skills and knowledge to process large volumes of data; and acquire hands-on experience of tools and techniques necessary to build cyber defensive capabilities.

Expected Team Size: This work is part of an ongoing project involving various members of the cyber security group at QCRI. We expect 2-3 interns to work on it.

Mentors

Husrev Taha Sencar hsencar@hbku.edu.qa

Ting Yu tyu@hbku.edu.qa