Real-time Event
Analysis and Monitoring
by Hasso-Plattner-Institut

Master project proposal

# Intrusion Detection with Machine Learning

Andrey Sapegin

## Abstract

Intrusion Detection Systems nowadays deal with very big volume of heterogeneous security logs. These logs should be stored and processed as fast as possible to enable security operators to react on the possible attack in a reasonable time. This fact often prevents researchers from using computationally heavy algorithms for log analysis. However, thanks to the in-memory technology used in the SAP HANA database, and also such features as Predictive Analysis Library and R Integration, we are able to process very high amounts of security logs almost in real time.

This master project aims to develop real-time intrusion detection techniques based on machine learning algorithms such as Anomaly Detection, K-means and Online Learning. The developed techniques should be integrated into the prototype of a SIEM system being developed at HPI (REAMS). Based on the results received from machine learning analysis modules, the system should be capable to visualise attacks together with an attacks' paths on the network graph and auto-generate the attack signatures. To achieve it, the system should be integrated with the vulnerability database (HPI-VDB) and network inventory system (GLPI or OCS Inventory NG).

The students will participate in the development of a SIEM system, gather experience with monitoring and inventory systems, learn and further develop algorithms for detection of attacks in the monitored network, create attack signatures and provide solutions for network vulnerability analysis.