Enabling Big Data Security Analytics for Advanced Network Attack Detection

David Jaeger

The monitoring and analysis of log events is a well-known method for the detection of simple and advanced attacks in networks. With the increasing size of networks, however, the amount of log data becomes so overwhelmingly big, that traditional tools and algorithms for attack detection do not work efficiently anymore. In this talk, a prototypical Security Information and Event Management (SIEM) system is presented that addresses the Big Data challenges of event data with common paradigms, such as data normalization, multi-processing, and in-memory storage. The SIEM utilizes a mostly stream-based event processing workflow that collects, normalizes, persists and analyzes events in near real-time. It comes with various contributions, such as a highly parallelized normalization algorithm, the efficient persistence of events into an in-memory database, and the application of advanced analytical algorithms on normalized event information. As a result, multi-step as well as previously unknown attack patterns are detected. Lastly, the integration of cyber threat intelligence (CTI) into the analytical process is presented, for instance, for correlating monitored user accounts with previously collected public identity leaks to identify compromised user accounts. With the presented SIEM, it is shown that even the largest enterprise networks can be monitored for ongoing attacks.