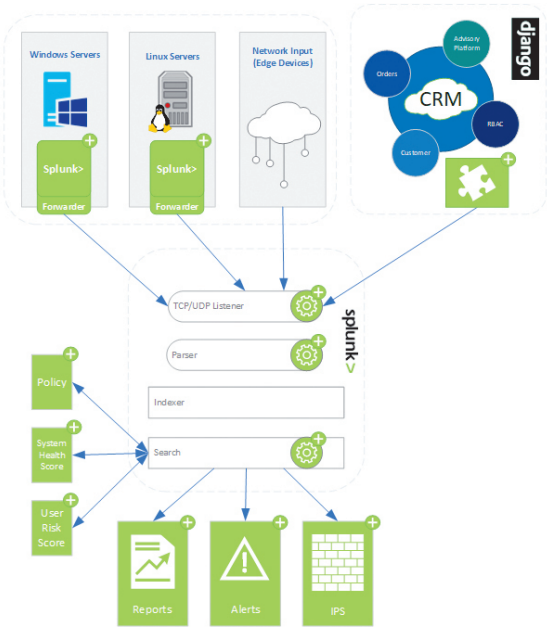
Developing a Behavior Analysis Application for a CRM System using Splunk

Degree programme: BSc in Computer Science | Specialisation: IT-Security
Thesis advisor: Prof. Dr. Ulrich Fiedler
Expert: Prof. Dr. Andreas Spichiger
External project partner: MoneyPark AG, Pfäffikon SZ

About 60% of all security threats come from within an organization. In this Bachelor thesis, we have worked with the industry partner MoneyPark AG who uses Splunk to capture, index and correlate real-time data (e.g. log-events) from various sources. In order to strengthen company IT security, we have set up a system based on Splunk. It addresses internal threats by assessing the health of the system and risks of particular users.

Initial Situation

MoneyPark AG is a FinTech company, providing an advisory in the fields of mortgages, investments, and pension funds using a self-implemented web-based advisory and customer management platforms (CRM). This platform is implemented based on the Django framework. It operates with customer-related personal data and files containing highly sensitive financial information. In the partners' network the Splunk instance is represented as an indexer (the server that captures, indexes and correlated the real-time data) combined with a search head (a server that performs search over indexed data and displays the results).



Overall System Design and Operation

Implementation

The Splunk was used to collect log-event data from all over the partner's computer network to address the issues of insider threats. On the illustration are shown the implemented or configured components marked in green with a plus.

- We have established log-events collection from the network: Windows and Linux servers, email exchange servers, and edge devices (routers, VPN)
- We have designed and developed the module for CRM to fulfill the requirements of extracting the needed data about user's activity from her session
- We have established and adjusted rule-based policy to enable intelligent reaction of a developed system to a potential security threat by triggering alerts and scheduled reports
- The implmented solution evaluates the system health scores and predicts the risk of system failure as well as user risk scores to assess the potential risky users and therefore intelligently react to insider threats
- All implemented functions and configurations have been wrapped into a so called Splunk application

Conclusion

Splunk simplifies the process of collecting and correlating of real-time data from various sources. After we have established log-events collection we started to analyse user behaviors and adjusting the rules in the policy. This has helped us to develop the intelligent reactions to user behaviors.
In comparison with reactive solutions when a user is immediately blocked, our system is able to assess the risk of the user's action and trigger the alert, include the user in a Watchlist or block. This has resulted in a decreasing number of triggered security alerts caused by user mistakes.
In future we plan to extend the current set of features by including the possibility to automatically assessing new user behaviors and improve the descision-taking process by adjusting policy.

Sergii Bilousov