Analytics Bulgaria

CASE STUDY

INSIDER THREAT MANAGEMENT

Insider Threat Management by Analytics Bulgaria

Background

Frequent cases of malpractice and stealing funds from clients of the banks, it was necessary to be found a comprehensive management implementation solution for monitoring and controlling of internal procedures into the administrations. The following aspects and key components had to be covered for implementation of the real project:

- **Insider Threat Library**: Solution's extensive library of out-of-the-box alert rules to cover the most common scenarios of risky user activities, with built-in policy notifications designed to increase the security awareness of users, and reduce overall company risk;
- **File Activity Monitoring**: Track and alert on files that were downloaded or exported using a browser or web-based application, from the internet or intranet. Alert if a tracked file is copied or moved to the default local sync folder of cloud storage services;
- **Policy notification and enforcement**: Define company policies and security regulations and enforce them by posting specific, detailed notification and blocking messages in real-time to any user violating these rules;
- **User Behaviour Analytics and Risk Scoring**: Assess the risk of every user, analyse and score user activity to identify any actions that are out of role, suspicious, or in violation of security policies;
- **Protect employee privacy**: Anonymization of users in the Dashboard and Web Console protects the privacy of recorded users.

The client

Tier-1 Bank in Bulgaria (The Bank).

The challenge

The challenge of the Bank was to identify the risk users, to protect form data loss, and accelerate incident response. The Bank needed to monitor the activities of privileged users by assessing the risk of every user, analyse and score user activity, with the goal of identifying user actions that are out-of-role or in violation of security policies.

The following challenges were faced and had to be mitigated:

- Implementation of **Department level risk management via Active Directory Group-based permissions**: the Bank had to manage the risk of their employees in departments or groups, each owned by a dedicated security team member or manager;
- **Detection of potential data leaks and implementation of Case Management platform.**
- Detection rules, based on severity scoring for risky user activity and out-of-policy behaviour, fully documented and ready for investigation by the compliance department.

The solution

The complete Insider Thread Solution provided the Bank ability to Identify and Eliminate Insider Threat and specifically Data Exfiltration with the following benefits:

- The solution enabled the organization to precisely identify and proactively protect against malicious and negligent behaviour of everyday users, privileged users, and remote vendors, and high-risk employees;
- Optimization of security and risk analysts to track and monitor file activities in order to identify and alert on instances of data exfiltration;
- Provided to the Bank monitoring of both **User Activity** and **File Activity** were critical for detecting Insider Threat and data exfiltration;
- The usage of the **Insider Threat Intelligence** platform increased security awareness by educating employees about out-of-policy behaviour whether malicious or negligent;
- User Risk Dashboard provided Security Analysts and Investigators with an easy way to track users that have experienced any type of policy notification or enforcement as a result of violating company policy or security rules;
- The Insider Thread solution helped the Bank to cover compliance requirements for PCI, SOX, HIPAA, and NISPOM.