SECURONIX™
Security Analytics. Delivered.

CASE STUDY

Preventing Data Exfiltration in the Professional Services Industry

The Challenge: Identify Insider Threats and Prevent Data Exfiltration

More than three years ago the risk team under the chief risk advisor was tasked with starting an insider threat program. The organization handles a lot of sensitive data that is subject to various legal and compliance controls. The group was tasked with identifying insider threats and preventing the exfiltration of sensitive data.

The Solution: Personalized and Customized

Though getting the right tool was important, equally important to the insider threat group was building the processes and techniques around the tool. For them the program was not something just to set up and run, but a process of continuous improvement. Only a security solution that was highly customizable, yet easy to configure to their specific requirements would work.

First, the organization identified the key metrics they needed in order to drive key business decisions. Then, using their security expertise and familiarity with the organizational culture, they were able to take advantage of the ability to customize the risk scores in the Securonix solution to systematically reduce the rate of false positives and surface the top priority threats. In a three year period they were able to increase the percentage of alerts that lead to open cases from 70% to almost 90%. On average they open around 30 cases a week from a population of over 80,000 employees. As they improve their models, they drastically improve their results and their return on investment (ROI).

The Business Impact

Understanding Insiders and Their Motivations

Through identifying and interviewing users who were identified by the insider threat team, the organization has discovered that they have very few actively malicious insiders exfiltrating data. The majority of the incidences they witness are caused by complacency and ignorance. With a deeper understanding of the causes they have been able to craft appropriate detection techniques to identify such users, and in the process they have been able to recommend improvements to several business processes, including changing the hiring policy and introducing focused security training.

Improved Business Processes

Beyond technical considerations, such as identifying a gap in the organization's IT systems where data could be exfiltrated easily and closing it, the insider threat team has also been able to leverage technological and cultural knowledge to effect behavioral changes in the organization. The team of security analysts consists of both analysts with a law enforcement background as well as analysts who come from other departments within the company.

Company Profile

This organization is a global network of member companies providing audit, consulting, financial advisory, risk management, and tax services. They have more than 80,000 employees across America.

Because they are able to combine security expertise with a deep insight into the culture of the company they are able to notice patterns caused by ingrained culture and make recommendations for change. For example, analysts noticed that employees who were off-ramping were causing more alerts. Looking into why, they discovered that employees were not getting clear communications regarding their obligations during that period. After discovering that, the team in charge of off-ramping employees was able to update their process, and the number of violations fell.

Improved Security Training Based on Real Scenarios

Like many companies, the organization also has yearly compliance training that employees are supposed to complete. Instead of using generic hypothetical situations as part of their training, the insider threat team works with the compliance team to create training based on scenarios that the team has been encountering in the organization. Employees are positive about the changes, saying that the new compliance training is relevant, matters, and most importantly, they understand it.

Business Advantage and Marketing

The work of the insider threat team is also something that the organization has been able to promote to their own customers. Because of the industries that they work in, they find their clients are increasingly asking about their security programs to the point that the organization expects clients to ask and have included it in their marketing materials. This has also lead to collaboration from client companies who have surfaced possible issues to their team.

Mitigating Data Breach and Integrity Risks

The organization has also been successful in detecting and preventing sensitive data loss by applying several anomaly detection techniques that succeed where simple rule-based detections fail. In some cases, files have been recovered where the users were able to successfully exfiltrate data, surpassing existing IT controls. As a result, the organization was able to gain insights into correlations between user behavior and data movement. In essence, the organization was able to mitigate potential risks caused by advertent or inadvertent use of technology by users, preventing a breach of confidential data.

About Securonix

Securonix transforms enterprise security with actionable intelligence. Using a purpose-built security analytics platform Securonix quickly and accurately detects high-risk threats to your organization. For more information visit www.securonix.com.