CASE STUDY

Identify and Detect Data Exfiltration in the Professional Services Industry

CASE STUDY

Identify and Detect Data Exfiltration in the Professional Services Industry

Large Professional Services Company

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.

The Challenge: Identifying Insider Threats and Detecting Data Exfiltration

A professional services organization needed a way to assess their security posture and detect unknown threats hiding in their environment. The organization handles a lot of sensitive data that is subject to various legal and compliance controls, but had challenges identifying anomalous user activities and exfiltration of data by their users/employees.

Building an insider threats program was crucial to their security goals. The organization needed a security solution that could be easily customized and configured to meet their unique needs, so the chief risk advisor was tasked with starting an insider threat program.

Key Challenges

- Lack of behavioral analytics to detect insider and advanced threats
- Receive too many false positive security events
- Lack custom use cases to improve the company's business decisions

The Solution: Improved KPIs and Less False Positives With UEBA

When the professional services organization brought in Securonix UEBA, they started by determining the essential KPIs that would be used to guide the program. The security team was able to utilize Securonix to customize risk scores and gradually lower the number of false positives alerts. By prioritizing and investigating the most important threats, the team's KPIs improved.

Before bringing in Securonix, users were able to successfully exfiltrate data, bypassing existing IT controls. With Securonix UEBA, the organization has gained insight into correlations between user behavior and data movement. The professional services organization was able to mitigate potential risks caused by negligent and malicious users.

The Business Impact: Reduce Insider Attacks and Data Breaches

Securonix helped their security team to identify insider threats and the root cause of what caused those incidents. The insider threat team discovered they had very few actively malicious insiders exfiltrating data. The majority of the insider threats they detected were caused by complacency and ignorance. With this deeper insight into their insider threats, the organization recommended improvements to several business processes, including changing the hiring policy and introducing focused security training. Additionally, the organization identified the gap in their IT infrastructure that allowed data exfiltration.

The professional services organization was able to decrease false positives from 30% to only 10% of all alerts. On average the insider threat team performs 30 incident response investigations a week for a population of over 80,000 employees. As they continue to improve their models, they drastically improve their results and their return on investment (ROI) with Securonix.

About Securonix