CASE STUDY

# Financial Services Organization Advances Their Insider Threat and Cloud Security

## The Challenge: Alert Fatigue Left Organization Susceptible to Insider Threats

A large financial services organization suffered from alert fatigue that left them unable to discern which incidents posed a credible threat to their business. Confidence in their previous tool was low, and their analysts were struggling to proactively identify and mitigate risk amidst the noise.

In their search for a new solution, they decided to prioritize strong UEBA capabilities, which made Securonix a top choice. Along with reducing alert fatigue, they needed a tool that could help them understand the behavior of their call center employees and monitor for insider threats. UEBA would help to pinpoint insider threats such as employees sending confidential information to their personal email accounts.

Initially, the company tested a few solutions but soon realized that Splunk was too expensive and LogRhythm would require significant personnel resources to operate effectively. Neither option would bring value to their organization.

## The Solution: Securonix for Insider Threat and Cloud Security

Securonix Next-Gen SIEM was determined to be the right choice due to its superior UEBA capabilities for insider threat detection and response. The organization appreciated Securonix's approach of combining related events together into a timeline view and liked how easy the search function was to navigate.

The organization's security team was able to quickly go through training and began the migration process. First, they focused on setting up analytics to detect and respond to threats across their Microsoft applications. Then, they focused on the important use case of detecting insider threats from employees who were sending confidential information to their personal email accounts.

With Securonix Next-Gen SIEM and UEBA in place, the SOC gained a holistic insight into their AWS cloud environment, versus just reacting to a barrage of false-positive alarms. They onboarded Securonix threat models for more advanced use cases and set up incident management. To ensure the organization's security team had fast issue resolution, they set up regular standing meetings with their Technical Account Manager.

## The Business Impact: One Command Center for Everything Security

The financial organization saw immediate benefits from user-based analytics and greater cloud visibility and security monitoring. When employees changed departments or left the company, the security team now had complete, contextual information around the data the employees were accessing as they moved to their new department, or if they tried to exfiltrate data as they left. The security team also gained greater insight into their AWS environment and behavior for better cloud security monitoring. Now it's easier for them to detect abnormal behavior, such as when new resources such as virtual machines are spun up, so they can confirm if it is a legitimate action or if it is something that warrants investigation, such as unauthorized resource use or abuse.

Even after expanding their operations and adding 3 new acquisitions to their portfolio, their security team feels confident in the value and ease of use Securonix brings. As the acquisitions add more AWS and Snowflake environments to their network, they trust Securonix to detect abnormal behavior and respond to threats.

## Company Profile

This financial services organization offers consulting services to help thousands become more financially independent. Based in the United States, they prioritize insider and cyber threats.

## About Securonix

Securonix has redefined SIEM for today's data-driven enterprise. It reduces noise, prioritizes alerts, and responds to insider and cyber threats. For more information visit www.securonix.com.