SECURONIX™

CASE STUDY

Insurance Provider Uses Open Platform and Behavioral Analytics to Drive Improved Security

The Challenge: Legacy SIEM Restrictions

This organization originally had LogRhythm SIEM, but experienced several challenges:

- Hundreds of new security events per day (with an environment of around 5,000 servers), but only a small team to handle them.
- Limited time to run investigations and ratify normal activity.
- Increased administrative overhead with constant rule tuning.
- Limited ability to create new alerts based on extended baselines that help identify abnormal behavior.
- Limited dashboard creation capabilities to help with threat hunting.

The Solution: Industry-Leading Analytics

The organization needed a solution to monitor privileged account usage, including details such as login times and machines used, as well as typical activity patterns for items such as configuration changes. Their legacy SIEM solution was unable to reliably support this requirement as it did not include robust UEBA capabilities. Therefore, the customer decided to use Securonix for its industry-leading analytical capabilities. The project was done in two stages. First, they layered Securonix UEBA over their existing legacy SIEM. Next, they replaced their existing LogRhythm SIEM with Securonix Next-Gen SIEM.

> “We were concerned about how well it worked and whether they were truly behavioral-based rules or if that was just marketing terminology for the ‘latest greatest system’. But it exceeds what our initial expectations were for being able to detect different cyber threats.”

The Business Impact

Proven Detection of Advanced Threats

Securonix’s rarity-based policies identified anomalous events such as privileged account logins from a machine for the first time, rare time of day logins, and rare/suspicious process runs. These were highlighted in an internal penetration test exercise, which showed off the detection capabilities of the Securonix platform as compared to the organization’s legacy SIEM solution. Of specific interest were the enumeration-type policies that look at increases in the number of files or accounts accessed.

> “We had a recent internal penetration test to try to simulate attacker activity, and Securonix really stood out regarding some of its detection capabilities versus our traditional SIEM, with a lot of the policies that we have for rare process running on a machine.”

The organization also witnessed a live example soon after Securonix was implemented. Securonix detected a threat that would have gone unnoticed using their legacy SIEM solution.

Company Profile

This large mutual insurance provider is based in the United States, with 5,500 employees in offices worldwide. They partner with over one-third of Fortune 1000 companies and have clients in more than 100 countries.

Spend Less Time on Management, More Time on Security

The organization's legacy on-premises SIEM solution required a lot of administration in order to maintain the hardware, perform updates, and operate to solution. The Securonix cloud-based platform, however, allowed the organization to add security capability without increasing headcount.

Securonix enabled the security team to focus on threats rather than on platform configuration. The team was very hands-on, creating new policies specific to their environment, and searching for threats. Securonix helped the team focus on threats and decrease the time required to investigate alerts.

> "One of the things that we really liked about Securonix was that it is very open platform, where we have the ability to tune and tweak and create new policies as needed."

Securonix correlates security alerts in order to identify threat chains. Preconfigured threat models give the security team a high degree of confidence for threats that need attention immediately.

> "Using the threat models has really helped prioritize events of interest for us."

Stable, Scalable, and Supportive

Securonix has been in place for over a year with minimal downtime. Updates are communicated well in advance, allowing for planned maintenance. Additional features and enhancements can also be added without issue.

> "There's been no downtime. Any time there are updates, we're always notified when they will take place, with adequate notice. After the updates, there's very minimal downtime as a result."

Scalability has been solid, with the platform stably handling around 5,000 events per second from over 9,000 servers and nearly 6,000 employees. Support is always on hand to help and close issues as quickly as possible.

> "If we do have any issues, they get addressed in a timely fashion."

About Securonix

Securonix is redefining SIEM using the power of big data and machine learning. Globally, customers use Securonix to address their insider threat, cyber threat, cloud security, and application security monitoring requirements.

For more information visit www.securonix.com.