CASE STUDY

Sub-Zero Reduces Time Spent Investigating Incidents with LogRhythm

LogRhythm
The Security Intelligence Company

Organization
Sub-Zero Group, Inc.

Industry
Manufacturing

Locations
More than 30, including 2 data centers

Key Impacts

- Single platform to consolidate logs and monitoring tools
- Advanced incident notification
- Correlate events coming from different logs
- Streamline investigations and reporting
- Ability to identify and resolve network issues unrelated to security

> *"We have peace of mind knowing if and when we have security issues, we'll be alerted centrally and we don't have to check several separate systems to find the cause. LogRhythm simply notifies us and we can quickly remedy the issue."*
>
> **Tyler Novogoratz,**
> IT Supervisor for Security and Disaster Recovery

Sub-Zero Group, Inc. manufactures the global premium appliance brands Sub-Zero and Wolf. Founded in 1945 and headquartered in Madison, Wis., Sub-Zero, Inc., is the leading manufacturer of American-made luxury refrigeration, freezer and wine storage products. Specializing in food preservation, Sub-Zero pioneered the concept of dual refrigeration and prides itself on being the first company to store frozen foods at ultralow, "sub-zero" temperatures.

In 2000, Wolf Appliance, Inc., the premier maker of ranges, ovens, cooktops and grills, was formed by Sub-Zero, establishing the brands as corporate companions and kitchen soul mates. In its third generation of family ownership, the privately held company operates manufacturing facilities in Fitchburg, Wis., and Goodyear, Ariz. Both brands are continually recognized for the highest achievements in refrigeration and cooking innovation and customer satisfaction.

The Business Challenge

With new products and expanded facilities, Sub-Zero is growing rapidly. Today Sub-Zero has over 30 locations, including multiple manufacturing facilities and numerous showrooms featuring high-end appliances and unique customer experiences. Two data centers support its extensive computer network and array of enterprise applications.

Even as the company grows and the network becomes more complex, the in-house IT security staff remains lean. For the IT security team monitoring the network, it was becoming too cumbersome to work with separate device logs and monitoring tools. They couldn't extract the information on network activity quickly or easily.

"Our leadership and human resources teams were inquiring about user activity on our network. I didn't have a good way to pull that information for them," explains Tyler Novogoratz, IT supervisor for security and disaster recovery.

"We needed a solution that would provide a single point of consolidation for our many sources of logs so that we could easily search and correlate the data. We also wanted to combine all of our monitoring tools into one platform that could alert us when we have security issues. In order to get better at what we do, we needed to consolidate and simplify."

The Solution

Novogoratz and his colleague T.J. Hathaway, systems engineer level III, started their search for a solution with the latest edition of the Gartner Magic Quadrant Report for SIEM. Rather than look at products from just one quadrant, the team took the entire list and considered the top ten. They focused on the solution's ease of use, specifically how easy it is to deploy, to navigate the interface, to apply out-of-the-box reporting and to correlate the data in a meaningful way.

The selection team reviewed the leading SIEM products on Gartner's list and narrowed their focus to four vendors, and then two.

The Wisconsin-based team from the value-added reseller Optiv Security Inc. also played a key support role throughout Sub-Zero's search for a SIEM solution. Optiv Systems Engineer Colin Kappl was familiar with both SIEM products that Sub-Zero tested in the proof of concept stage. He helped to differentiate between the two and identify various features and capabilities, which helped with the selection process.

"We have been working closely with Optiv for a few years," says Novogoratz. "They are our VAR of choice around security. They highly recommended LogRhythm. Ultimately, we purchased the solution through them along with their rapid deployment service. We knew Optiv's expertise would help us get the most value from our SIEM."

> *"LogRhythm was the obvious choice for us. It's easy to set up, the web dashboard is very intuitive and easy to navigate, and the out-of-the-box reporting is very important for us. For me in particular, the drill-down capability is a big selling point. I can investigate incidents quickly, whereas before it could take hours or days to get the information I needed."*
>
> **T.J. Hathaway,** Systems Engineer Level III

Together, Sub-Zero and Optiv spent a week implementing the solution, configuring the logs, and activating the initial layout. "There are threshold settings that we were able to configure to make sure the alert levels met our needs," Hathaway says.

The team started seeing benefits from the solution immediately. Hathaway adds, "On the second day of implementation we learned that one of our switches had a bad power supply and we found a bad fiber link in one of our wiring closets. LogRhythm also alerted us to some

network routing issues and we were able to take a closer look. All in all, LogRhythm has certainly helped us with our server and network health monitoring."

After approximately eight months, the solution has met all the original objectives of the project.

"It's a single place where we can go to view all our logs," Novogratz explains. "When we see an issue on a network appliance and another issue on a server, LogRhythm helps us correlate the events so we can better understand the problem and how to investigate it. We have peace of mind knowing if and when we have security issues, we'll be alerted centrally and we don't have to check several disparate systems to find the cause. LogRhythm simply notifies us and we can quickly remedy the issue."

Hathaway says the reports have simplified his job. For example, he frequently uses a report to know when an administrator has changed their password. He can verify this action with the administrator to be sure the change was legitimate and not initiated by a malicious actor. The report also saves hours of investigation time when an account is locked out and Hathaway needs to know where the administrator was logged in during the password change.

LogRhythm has significantly improved the efficiency of Sub-Zero's security operations. Prior to installing LogRhythm, the workflow for investigating security threats was manual and not well defined. "Now we rely on alerts and reports from LogRhythm to start the process and narrow our search," says Novogoratz.

Looking toward the future, Sub-Zero plans to bring more device logs into the system and to configure and fine-tune alerts.