Healthcare Security Team Proves Strong ROI with LogRhythm

A U.S.-based healthcare organization with a small information security team lacked a centralized way to collect and analyze logs and identify and respond to incidents in an effective manner. The business wanted to find the right solution to enhance its security posture and give the team the tools to build and expand the security program as the healthcare system grew. The organization chose the LogRhythm NextGen SIEM Platform to improve visibility and streamline its security operations into a single solution to help its team detect and respond to threats in real time.

The Business Challenge

SAVE COSTS AND SIMPLIFY THE CENTRALIZED SECURITY SYSTEM

The organization selected LogRhythm for its ease of use with a user-friendly interface, which it knew would simplify operations, as well as for its out-of-the box threat detection content. But as with any investment, the organization had to prove the security program was worth the financial cost and time investment. Because cybersecurity is typically seen as a cost center for the business, the organization's trustees were focused on the security program's impact on the bottom line, as well as the effectiveness of the tool and advancement of the program.

Demonstrating a security program's strong and quantifiable return on investment (ROI) can be a challenge for security teams. This team sought a way to show that the LogRhythm platform was a worthwhile investment.

The Solution

PROVING BENEFITS AND ROI

To show the effectiveness of the LogRhythm NextGen SIEM Platform, the organization created customized dashboards illustrating program data, including the number of logs, alerts, and events it collected and the number of cases that became incidents. As a result of working with LogRhythm, the organization was able to contextualize its data and develop trackable metrics to demonstrate time and cost savings.

Industry

Healthcare

Company

Anonymous

Company Size

39,000 employees

Key Impacts

- Saved costs of $30K- $70K/year by implementing LogRhythm
- Reduced time and work for security team
- Automated repetitive analyst tasks
- Developed trackable metrics to show cost and time savings

"SmartResponse is the most powerful feature LogRhythm has. SmartResponse has really allowed us to step up our game and stay ahead of threats."

– Senior Information Security Engineer

The team also tracked the efficiency of LogRhythm's SmartResponse™ Automation feature to automatically block high-confidence IP addresses from the network whenever attack patterns or otherwise malicious activity emerged. With LogRhythm, the organization estimates it saves between $30,000 to $70,000 a year—roughly most of a firewall engineer's salary—by automatically blocking more than 1,000 IP addresses per month. Now, instead of an engineer having to spend time manually blocking these IPs, LogRhythm's capabilities have helped the organization prove the ROI, and has enabled information security leadership to demonstrate the need for additional staff and better tools to detect and respond more effectively to threats.

Saving Time with Automation

To increase efficiency for Tier 1 analysts, the organization standardized its approach to incident response using LogRhythm's playbooks. The organization used SmartResponse features to automatically attach predetermined playbooks associated with certain alarms, enabling Tier 1 analysts to remediate potential issues quickly and in a repeatable way.

For example, if the organization's anti-malware/advanced threat protection provider detected a possible threat, analysts would perform the same consistent analysis using the playbooks. The team used SmartResponse to further enhance this process by querying its other tools to pull information on the host, file hash, and user into the case management system. This reduced the amount of upfront investigative leg work, and provided analysts with as much information as possible to make an informed decision on how to proceed.

This simple, repetitive task, enhanced with automation, lets analysts spend more time on high-value task—including threat hunting—responding to true incidents, and creating and improving automation.

Conclusion

The organization recognized the value in investing in a security program to mature its security posture and ease the workflow of its security team. Since working with LogRhythm, the organization has dramatically improved its detection and response times and reliably demonstrates the value of the tool and the security program to executive leadership.

"Without LogRhythm's capabilities, there is a very distinct possibility that some of these malware threats would be able to spread more quickly," the organization's security operations analyst said. "It allows us to more quickly get a full view and contextualize what is going on. It has allowed our phishing team to find credential harvesters in real time, instead of waiting for something to happen."

The organization plans to expand its security program and use additional features of the LogRhythm platform.

> "If any part of the information gathering or response processes can be programmed, LogRhythm can automate it."
>
> **– Senior Information Security Engineer**

Contact us to learn how LogRhythm can help solve your organization's security needs.

1.866.384.0713 // info@logrhythm.com // 4780 Pearl East Circle, Boulder CO, 80301

www.logrhythm.com