Global Retailer Achieves Intelligent Infrastructure Defense with LogRhythm's Co-Pilot Service and Security Analytics

Retailers have learned hard lessons in recent years, as organizations like Target and Home Depot have suffered major data breaches. The total cost of these breaches extended far beyond regulatory fines and notifying affected customers. These retailers hired forensic experts to perform incident investigation and response activities, paid for credit monitoring, and suffered lost revenue as a result of a deterioration in customer trust.

The nature of the retail sector makes preventing costly breaches difficult. Retailers generally operate multiple stores, which translate into numerous endpoints, users, and networks spread over a wide geographic area.

To make things more difficult, the types of attacks retailers face take many forms, from distributed denial of service (DDoS) shutdowns of websites, to theft of sensitive company data and internal fraud.

With the number of cyberattacks in the retail sector and the resulting costs having increased by more than 150 percent in just one year, how can retailers protect their businesses, their data, and their customers[1]? This is the story of why one international retailer chose LogRhythm's security intelligence and analytics platform to solve its security challenges.

The Challenge

A Lack of Visibility and Resources

The retailer faced a challenging security landscape. The organization's complex global IT infrastructure included everything from point-of-sale (POS) systems and corporate endpoints to multiple servers housing inventory, customer, and corporate data.

The vast amount and type of data, and the small size of the security team, made manual review of the daily logs and events nearly impossible. Therefore, the company sought a solution that would allow it to centralize all of its logging data, correlate data points, and identify patterns to better detect and respond to security incidents.

The Solution

Security Analytics and LogRhythm's AI Engine

The retailer adopted LogRhythm in 2012 after researching a number of similar options. By the end of the evaluation period, LogRhythm emerged as the most user-friendly and cost-efficient solution available. With LogRhythm, the retailer was able to centralize its logs and begin deploying advanced security analytics to detect threats across its infrastructure.

The company gained immediate value from LogRhythm's AI Engine, which provides automated, continuous analysis and correlation of all activity observed within the environment. With nearly 1,000 rules pre-built into AI Engine, LogRhythm instantly empowered the retailer's security staff to detect unauthorized Telnet login attempts, monitor Active Directory accounts, and perform other security operations activities.

[1] PricewaterhouseCoopers, "Turnaround and Transformation in Cybersecurity: Retail and Consumer: Key findings from The Global State of Information Security Survey 2016." http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/pwc-gsiss-2016-retail-consumer.pdf.

Maximizing Value with Analytics Co-Pilot

After deploying LogRhythm, the company soon realized that it was capable of doing much more. While LogRhythm's core security analytics functionality did much to improve the security and visibility of the company's infrastructure, the security team became eager to go even further by implementing advanced custom rules.

According to the director of IT security, the team wanted to make their rules much more intelligent. They wanted to be able to make multi-level rules that could support use cases such as advanced correlation of different events to identify security incidents, even if each event individually would not trigger an alert.

LogRhythm's Co-Pilot service empowered the team to make substantial gains quickly. By pairing the retailer's IT security staff with Matt Willems, LogRhythm Labs engineer, the year-long Co-Pilot program provided one-on-one guidance that helped the retailer's team to tailor their LogRhythm rules in order to efficiently identify and react to the security threats of greatest priority to the company.

The Best Defense is A Good Offense

Perhaps most importantly, the Co-Pilot program enabled the retailer's security team to migrate from a reactive to a proactive stance in their security operations. Rather than relying solely on rules designed to detect known threats, the team, with the help of LogRhythm's Co-Pilot service, created new rules to identify previously unknown, hypothetical threats. In this way, the company was able to unlock the full functionality of LogRhythm's security analytics to defend against emerging types of threats that have not yet reached its infrastructure, but could in the future.

"We had that experience of 'I had no idea we could do that,'" the retailer's director of IT security said, while describing the way that the Co-Pilot program empowered his team to configure LogRhythm to defend against a wide range of security threats. The capabilities extended far beyond what the team had in mind when it first adopted the platform.

He added that, thanks to the Co-Pilot program, his team went from "treating the AI Engine as a stock tool" that could support only certain types of use cases to a point of "opening our eyes fully to what we were capable of doing" with LogRhythm security analytics.

For Willems, the expert who worked with the retailer's security team, the Co-Pilot program served as a way to help the retail organization realize the full functionality of LogRhythm's feature set. "Co-Pilot was a teach-them-to-fish opportunity," Willems said. He recalled his work with the retailer's team as a partnership that helped the retailer to "recognize what really needed to happen" to improve their security, and use LogRhythm to do it, rather than simply relying on outside resources to do the work for them.

Conclusion

Achieving Advanced Defense with Security Analytics

The retailer's IT security director continues to recognize that complete security is impossible. As a result, he said, "The way we handle security is to rely on many layers."

Since adopting LogRhythm's AI Engine and learning to make the most of it through the Co-Pilot program, security analytics has become an instrumental layer in the retailer's lines of defense against security threats. By helping to find and resolve threats that cannot be addressed by other types of security tools, such as antivirus scanners and firewalls, LogRhythm's security analytics functionality has facilitated a holistic security operation for this company's sprawling global infrastructure.

> **"Through a year-long Co-Pilot Program I was able to provide individualized guidance that helped the retailer's team to tailor their LogRhythm rules. This empowered the team to efficiently identify and react to the security threats of greatest priority."**
>
> - Matt Willems, Threat research engineer LogRhythm Labs