Healthcare Software Company Gains Comprehensive Visibility with LogRhythm Axon

A healthcare identity access provider was looking for a security information and event management (SIEM) platform that could maximize visibility into potential threats and boost analyst efficiency. Due to the nature of their business and the sensitive customer data they handle, they are especially vulnerable to threat actors. With a rapidly expanding hybrid environment due to acquisitions, it was crucial for their small security team to find a scalable platform that provided a single pane of glass across all log sources while keeping pace with the organization's growth. The company chose LogRhythm Axon for its seamless visibility across software as a service (SaaS), self-hosted-cloud, and on-prem log sources and its intuitive workflows to boost team efficiency while investigating threats.

The Challenge

The software company needed a way to reduce the administrative overhead for their their security operations center (SOC). The previous SIEM solution did not provide enough visibility for their small team to effectively mitigate threats across their hybrid environment. The previous solution was also ill-matched with the company's recently acquired Linux systems and infrastructure that created cumbersome workflows and a heavy burden on the SOC.

The company has stringent security requirements and high standards for their security stack due to the sensitive customer information they protect. They needed a security solution that could help alleviate pressure on their SOC, effectively handle their use cases, reduce noise, and enable them to secure their environment.

The Solution

Partnering with LogRhythm, the software company relied on the expertise of an experienced and dedicated team as they outlined the security issues they were trying to solve. Due to their hybrid environment and their primary security concerns, they needed a SIEM that could easily integrate with both cloud services and on-prem applications.

With LogRhythm Axon, the security team was immediately able to surface security gaps and potential threats during their initial log source onboarding and dashboard customizations. Their SIEM dashboard alerted them to operational weaknesses in the business's internal user login automations. This enabled the security team to quickly notify the business and clean up authentication mechanisms and outdated automation processes, securing their environment and further mitigating risk.

LogRhythm Axon's guided and intuitive workflows enabled the team to quickly grow familiar with the platform, reducing ramp up time and bringing faster time to value. The platform's automatic onboarding of new data sources further streamlined analyst workflows, freeing up their time for threat hunting and risk mitigation.

Seamless Visibility, Ease of Use, and Quick Time to Value

Implementing LogRhythm Axon allowed the SOC to monitor systems, appliances, and devices that were not compatible with other tools in their security stack through the lens of a security-focused platform. This provided the company with comprehensive visibility across their network infrastructure. LogRhythm Axon is delivered via SaaS, which reduced the burden of managing the operating infrastructure and enabled the company's security team to prioritize and focus on the work that matters — security.

As they plan the next steps in improving their security maturity, they look forward to bringing more teams across the organization onboard with varying levels of permissions. The security team is confident in cross-functional success with LogRhythm Axon thanks to its easy-to-use interface and assisted search capabilities that negate the need for prior knowledge of the underlying log structure. The SOC is excited to start preventative micro-engagements, using well known open-source threat actor tools to create custom alerts to further automate incident response and investigation workflows.

"I can't say enough how instrumental the teams at LogRhythm have been to our success. It has been wonderful working with a security partner who is truly engaged with their customers. I know they're focused on meeting my needs and value my input as they continue to make bi-weekly releases to LogRhythm Axon." Said the company's Director of IT and Security Operations. "We started seeing value immediately with the visibility from the dashboards and it's been a game changer for our team. The parsing engine capabilities are a personal favorite, and I know we're all looking forward to furthering our security maturity with LogRhythm Axon."

Interested in learning more about LogRhythm Axon?
Request a demo.

info@logrhythm.com // 1.866.384.0713 // +44 (0)1628 918 300 // +65 6222 8110 // +61 2 8019 7185 // +97155 642 2224

www.logrhythm.com