LogRhythm Workshop Uncovers Opportunities to Improve a Team's Security Operations Maturity

The Challenge

Compliance and Security Alignment

A major communications services company in the UK who provides more than 500,000 customers with mobile, fixed line, internet and TV services initially brought on LogRhythm to help their organization address the compliance requirements of the General Data Protection Regulation (GDPR).

The organization's security team knew that, even though they were compliant, they could do more to ensure that their organization is not vulnerable to threats. The organization wanted to strengthen their overall security maturity as they improved their compliance maturity. The problem is, like most security teams, they did not know where to begin in terms of assessing their effectiveness and uncovering areas for improving the alignment of compliance and security processes.

The Solution

Customized Roadmap from LogRhythm SOMM Workshop

LogRhythm's Security Operations Maturity Model (SOMM) was designed to provide security teams with a vendor-agnostic tool to assess their maturity level and plan for a roadmap of improvement over time. LogRhythm realized that security teams benefit the most from the model when they are guided through the initial evaluation and receive assistance with their plans for future improvements, so our engineering team designed an interactive workshop based on the SOMM model.

The LogRhythm SOMM Workshop creates a conversation, sets goals, and provides guidance to help organizations effectively assess their current security posture, develop use cases for meeting their operational and security requirements, identify future security requirements, and build a business case for realizing the value of their investment.

In the case of the communication services company, LogRhythm and the organization's security team scheduled a SOMM Workshop to develop a roadmap for achieving a level of security maturity that aligns with their compliance processes while also being appropriate for the organization's resources, budget, and risk tolerance.

Industry

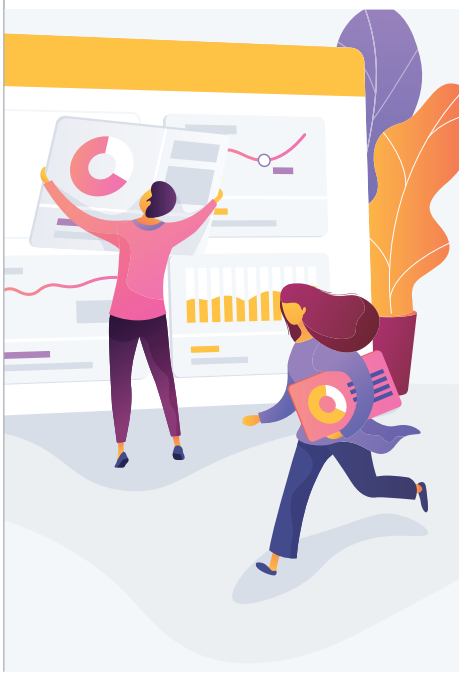
Communication Services

Company Size

1,172 employees

Key Impacts

- Assessment identified current levels of security maturity, and gaps in tools and processes
- Obtained a plan for communicating improvements in investments and reductions in risk to the broader organization
- Aligned compliance requirements with security procedures for greater business efficiencies
- Plan customized to address and prioritize opportunities for greater security maturity



The SOMM Workshop

LogRhythm and members of the organization's security and infrastructure teams met for a half-day guided session to evaluate the teams' current position, where they want to be, and what they can do to get there.

LogRhythm started the workshop with questions that lead to an engaging conversation about the organization's security program. With LogRhythm present, the team was able to learn insights from a third party and discuss their program openly and honestly. The team took a deep dive SOMM assessment, where they use the below five-point scale to rate themselves on the following principal programs in a security operations center (SOC): log management, SIEM, vulnerability intelligence, threat intelligence, user analytics, endpoint analytics, network analytics, holistic analytics, incident management, automation/ orchestration, people and process.

SOMM Five-Point Rating Scale

By comparing the team's current levels with their desired and recommended levels, LogRhythm helped them choose a target level for each program that they could realistically achieve within 12 months. Recommendations for use cases that align to the business and a target mean time to detect and mean time to respond to threats were also provided. This way, the team is given what they need to communicate how improvements in each of the investments can lead to greater reductions in overall risk to the rest of the organization.

LogRhythm took the results from the session to create a SOMM report, with action items that were agreed-upon during the workshop, and an implementation plan that was customized to the organization's security and compliance goals.

Conclusion

The team saw the value in the SOMM workshop experience immediately and believe the delivered output is realistic and will significantly improve their security program. "The SOMM Workshop was a very valuable experience for our team. Working with LogRhythm on a strategic plan for our operation will significantly help our team improve our security capabilities and ability to validate what we have done now and, in the future," a member of the security team said while describing the workshop.

They plan to use the final report to help them make the business cases for several new security projects they are proposing. Following the workshop, the team had a clearer vision for what they can achieve and a roadmap to help execute on that vision.

Contact us to schedule your own SOMM Workshop with the LogRhythm team today.

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

www.logrhythm.com