

CASE STUDY

HOW AN INTERNATIONAL LAW FIRM BUILT THEIR SOC



INTRODUCTION

The international law firm's Head of Information Security joined the team as their very first security manager. At this point, there was no SIEM and no regular team to monitor the firm's environment.

Head of Information Security reports to the CIO and oversees governance, risk management, and compliance, as well as the firm's security technologies and day-to-day operations.

Building a security monitoring capability became a priority as the firm sought to strengthen client data protection and support its business objectives. Establishing an internal team would have required hiring four to five additional people, prompting the need for an alternative approach to security operations.

“With RedLegg, I could shift my focus to planning for future security needs.”

— Head of Information Security

THE PROBLEM

Understaffed yet determined

Head of Information Security was left to manage and monitor the firm's cybersecurity as the firm did not have a managed security services provider to run their SOC, or even intrusion prevention/detection.

Head of Information Security was looking to implement a visibility strategy and building an in-house security team would mean hiring 4-5 people.

Business & Security Goals

Protecting client data became critical to achieve business goals. Both business and security goals aligned in assuring clients that their data is well protected. Due to general fears about data protections and compliance needs that must be met, many clients have implemented vendor management programs that force the law firm to implement the necessary security levels or risk losing business.

Beyond safeguarding the business's current line, the firm also looked to the future, expanding its partner-base and increasing overall business revenue. Cybersecurity became an important component to that plan in order to ensure the business and its operations wouldn't experience a breach and that breach's repercussions.



WHY REDLEGG

The firm needed a cost-effective security partner that could provide consistent analyst support and a flexible approach to SIEM management.

RedLegg's co-managed model offered the expertise and operational support required to establish continuous monitoring while allowing the internal security team to focus on future priorities.

SOLUTION: FUTURE-MINDED SOC FOUNDATIONS

The firm partnered with RedLegg to install and co-manage a SIEM platform, establishing the visibility needed to begin building its SOC.

Logs were ingested into the platform, and RedLegg's content package was deployed to support the firm's visibility strategy.

Through the co-managed model, RedLegg provided 24/7 monitoring and analyst-led event escalation based on procedures established during onboarding.

The firm subsequently expanded the platform through automation, additional security content, and new visibility use cases.

LOG INGESTION

Logs were ingested into the SIEM

REDLEGG CONTENT PACKAGE

The RedLegg content package was installed to align with the visibility strategy.

24/7 MONITORING

RedLegg's co-managed model provided 24/7 monitoring.

EVENT ESCALATION

RedLegg's expert analysts escalated events according to the plan set during onboarding.

ONGOING DEVELOPMENT

The firm built upon the existing platform through automation, additional security content, and visibility use cases.

IMPLEMENTATION

RedLegg and the firm's security team implemented a co-managed SIEM environment using LogRhythm.

The deployment included log ingestion and the installation of RedLegg's content package to support the firm's visibility strategy.

Event escalation procedures were established during onboarding, enabling RedLegg's analysts to provide continuous monitoring and communicate security events according to the agreed plan.

THE BENEFITS

MORE FLEXIBILITY

Starting from scratch with SIEM allowed the firm to choose the most flexible option considering their future growth. Co-managed, legacy tuning.

LOWER COSTS

Most managed security providers begin at a higher cost, but the firm didn't have the budget to entirely outsource their day-to-day security. RedLegg had a cost-effective solution.

CONSISTENT TALENT

Tasked with hiring and staffing, Head of Information Security was relieved to have consistent talent among the provided security analysts.

HOW IT WAS DELIVERED

CO-MANAGED SIEM

Plug-and-play LogRhythm. The firm received correlation tools, timely reports, and security event updates as RedLegg co-managed their day-to-day security.



24/7 VISIBILITY

With RedLegg's co-managed model, the firm provided client's with 24x7 monitoring. RedLegg's expert analysts escalated events according to the plan set during onboarding.



STAFFING & LEGACY TUNING

Safeguarding client data and the business's future. As another member of the firm's team, RedLegg stepped in to fulfill staffing needs and provide custom legacy tuning.

CONCLUSION

RedLegg aided the firm's competitive advantage. Most firms in the industry follow similar security protocols, but this particular firm improvises, grows, and takes their unique environment into account.

The firm can now also respond positively to client concerns and questions about data protection.

With a renewed contract, the security team is supporting business goals long term by safeguarding the firm's future.

"A big concern was man power: staffing and talent consistency. But with RedLegg, I could shift my focus to planning for future security needs"
-Head of Information Security

IMPACT

- **Client assurance:** The firm can respond positively to client concerns and questions about data protection.
- **Future security planning:** The Head of Information Security was able to shift focus toward planning for future security needs.
- **Long-term business support:** With a renewed contract, the security team is supporting business goals long term by safeguarding the firm's future.

"I'm more confident that we made the right choice by working with RedLegg because they are continuously looking to improvise and improve their processes. We have common goals." - Head of Information Security

FOR MORE INFORMATION REACH OUT:



312.757.4941



dotell@redlegg.com



redlegg.com