REDLEGG

"With RedLegg, I could shift my focus to planning for future security needs."
Head of Information Security

CASE STUDY

HOW AN INTERNATIONAL LAW FIRM BUILT THEIR SOC.

Role
Head of Information Security

Industry
Legal

Location
Illinois

RedLegg Client
Since 2016

THE PROBLEM

UNDERSTAFFED YET DETERMINED

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.

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.

FOR MORE INFORMATION, REACH OUT.

Geneva, IL 60134

877.811.5040

dotell@redlegg.com | redlegg.com

CLIENT ASSURANCE
Business and security goals align in wanting to assure current clients that their data is well protected.

BUSINESS CONFIDENCE
Security aims to give business operations confidence needed to move forward with their own goals, for growth within the firm.

BUILD A ROBUST TEAM
Overall, the firm wants to safeguard current lines of business to bring in more partners and increase the firm's revenue.

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.

THE SOLUTION

FUTURE-MINDED SOC FOUNDATIONS

The firm worked with RedLegg to install and co-manage SIEM.

By installing a SIEM, the firm and RedLegg's team gained visibility into their environment as the first step to building their SOC. Logs were ingested and the RedLegg content package was install to align with our visibility strategy.

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. As a partner, RedLegg laid a foundation to build off of; the firm was then able to build upon with existing platform through automation, additional security content, and visibility use cases.

Low costs, plug-and-play flexibility, and consistent talent brought the firm, and their clients, peace of mind.

Now, the firm's security team focuses on the future.

achieved 24x7 visibility into the environment

SOLUTION

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

achieved common business and security goals

SOLUTION

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.

COMPETITIVE ADVANTAGE

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.

THE BENEFITS

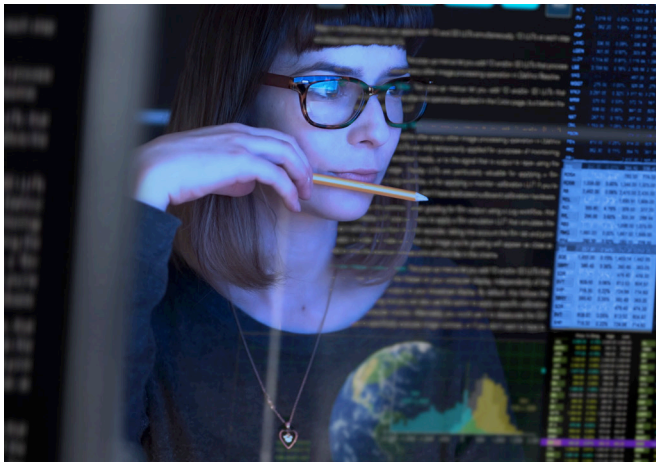
- More flexibility
  Starting from scratch with SIEM allowed the firm to choose the most flexible option considering their future growth. Co-managed, legacy tuning.
- Lower costs
  Most managed security providers begin at a higher cost, but the firm didn't have the budget to entirely outsource their 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.

RESULT

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

"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."

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



REDLEGG