

CASE STUDY

RedLegg and Randa: Enhancing Cybersecurity Through Trusted Partnership



INTRODUCTION

Randa Apparel & Accessories (RAA) is an international powerhouse with over a century of expertise and is a leader in the fashion apparel and lifestyle accessories sector. Operating a diverse portfolio of more than 40 leading global brands, RAA meets the distinct and evolving needs of consumers worldwide.

RAA has faced challenges with security practices, emphasizing the importance of fortifying its operations to match its expansive market presence.

As a company with annual revenues approaching \$1 billion and a workforce of over 1,800 associates, the need for a robust cybersecurity infrastructure was critical.

Upon joining Randa as SVP/CIO, Robert Black, familiar with RedLegg's capabilities from previous collaborations, brought them on board to address these vulnerabilities, leveraging a relationship built on trust and proven success to enhance Randa's cybersecurity and operational efficiency.

THE PROBLEM

Building a security program from the ground up.

Lacking comprehensive SIEM coverage and relying on ad hoc measures in a reactive IT environment, Randa Apparel & Accessories recognized the need to establish a formal security program.

To address this, Randa engaged RedLegg to enhance its cybersecurity infrastructure, aiming to standardize and centralize IT processes across the organization.



SECURITY PROGRAM OBJECTIVES

Randa sought to establish a more structured security program by centralizing IT processes and strengthening security monitoring capabilities. The engagement with RedLegg would support this transition through dedicated expertise, consistent monitoring, and a more coordinated approach to security operations.



“We were much more of a reactive, hair-on-fire, chaotic environment before. Now we’re trying to be more of a proactive, planned, and thoughtful kind of approach.”

— Robert Black

WHY REDLEGG

Randa prioritizes partnerships over typical vendor relationships, aligning well with RedLegg's collaborative approach. The timing was optimal as Randa's existing SIEM/SOC contract was expiring.

Robert Black's past positive experiences with RedLegg and the transparency they provided reinforced the decision to enhance their collaboration. For Randa, RedLegg is more than just a service provider, they are an integral part of their security strategy, deeply embedded in their team's operations.

"I look for partners, I don't just look for vendors."-Robert Black

SOLUTION: SERVICES SCOPE

RedLegg provided Randa MDR with a Managed SIEM solution, significantly strengthening their security monitoring and response capabilities.

This service included deploying a dedicated SIEM platform that ingests and analyzes security data from Randa's IT infrastructure. RedLegg's Cyberfusion Analysts, a team of security experts, offer 24/7 monitoring, threat detection, and incident response services.

Randa and RedLegg collaborate through regular status calls and meetings to ensure seamless integration and proactive security management.

This setup allows RedLegg to be an extension of Randa's internal security team, offering specialized expertise and additional resources.

DATA INGESTION

Dedicated SIEM ingests and analyzes security data from Randa's IT infrastructure.

24/7 MONITORING

Cyberfusion Analysts provide continuous security monitoring.

THREAT DETECTION

Customized detection logic supports coverage of potential risks.

THREAT ANALYSIS & RESPONSE

Playbook-driven threat analysis supports custom investigation and escalation procedures.

REPORTING & INSIGHT

Real-time dashboards and reports provide insight into performance and posture.

IMPLEMENTATION

Both teams efficiently managed the onboarding and implementation processes. Despite his overarching responsibilities as SVP/CIO, Robert Black was relatively hands-off during integration, a testament to the strong collaboration between the teams.

He facilitated connections between RedLegg's Platform Management Team and Randa's internal engineering resources, ensuring a smooth transition.

The implementation was executed so seamlessly that, as Robert Black remarked:

“It was so smooth and went so well, I can't even really outline it for you.”

THE BENEFITS

Randa has significantly enhanced its security operations by partnering with RedLegg for Managed SIEM and SOC services.

By leveraging security automation tools and methodology along with security threat investigation, incident response, and research expertise in the Cyberfusion center, Randa has access to a full-stack cybersecurity practice.

Real-time dashboards and reports by the Cyberfusion Data Analysts provide Randa with key insight into its performance and posture.

HOW IT WAS DELIVERED

CUSTOMIZED DETECTION LOGIC

Customized and confident Detection Logic developed by the Cyber Threat Intelligence team provides full scope coverage of potential risks.



DEDICATED PLATFORM ENGINEERING

Dedicated Platform Engineers who understand both Randa's security platforms as well as security risks have become critical guides to Randa's security operations.



PLAYBOOK-DRIVEN THREAT ANALYSIS

Allows for custom investigation and escalation procedures to provide the best path to lowering both mean time to detection and resolution.

CONCLUSION

RedLegg's partnership with Randa has enhanced their cybersecurity measures and guided their shift from a reactive to a proactive security posture.

A long-standing relationship based on trust, openness, and respect is the foundation for this collaboration's success because it has made it easy for RedLegg to integrate into Randa's strategic vision.

Through Managed SIEM and SOC services, Randa has strengthened its security monitoring and response capabilities while gaining access to dedicated analysts, platform engineering expertise, and security automation. This collaboration has also supported a more structured approach to security operations, with greater visibility into the organization's security environment.

As Randa continues to develop its security program, RedLegg remains an extension of its internal team, providing the expertise and operational support needed to sustain and refine its security capabilities.

IMPACT

- **Security automation:** Implemented along the threat analysis process.
- **Customized detection logic:** Customized high-confidence Detection Logic Lifecycle implemented.
- **Extended security expertise:** Dedicated Cyberfusion subject matter experts function as an extension of the team.
- **Real-Time visibility:** Real-time dashboards and reports provide insight into performance and posture.
- **Investigation and Escalation:** Playbook-driven threat analysis supports custom investigation and escalation procedures.

FOR MORE INFORMATION REACH OUT:



312.757.4941



dotell@redlegg.com



redlegg.com