CASE STUDY

FROM SILOS TO SYNERGY: SIRP'S ROLE IN MODERNIZING A BANK'S SECURITY OPERATIONS

NOV 2024

OVERVIEW

A leading global bank (financial institution) deployed SIRP's SOAR platform to **enhance and streamline its security operations**. With SIRP's integrated solution, the bank connected multiple security tools, including SIEM, EDR, and firewalls, into a unified system designed to automate response workflows across its infrastructure.

By implementing SIRP, the bank was able to **automate use cases** such as threat detection, prevention, and response, resulting in significant operational improvements over their three year tenure with SIRP:

$ 5,330,185
Cost Savings

166,568
Analyst hours saved

This integration enhanced the bank's ability to swiftly address and respond to emerging security threats, **reducing** Mean Time to Respond (MTTR) and Mean Time to Investigate (MTTI) without adding unnecessary complexity or additional personnel.

The deployment of SIRP's automation capabilities empowered the bank to efficiently manage and mitigate security risks, strengthening its overall cybersecurity posture.

ABOUT THE COMPANY

The organization in focus is a major global financial institution with a significant presence in both retail and corporate banking. Serving **millions of customers,** the institution operates more than **1,300 branches** and over **1,500 ATMs** across its regions. With a workforce of over **10,000 employees,** the organization is recognized for its commitment to innovation and delivering secure, customer-centric banking services.

Given the scale and diversity of its operations, managing cybersecurity across a wide range of systems and services is paramount. The institution relies on advanced technologies, including SIEM, EDR, and firewalls, to protect its infrastructure and sensitive customer data. As a result, the need for an integrated security operations solution that can streamline processes, improve response times, and enhance visibility across its security landscape has become essential.

THE CHALLENGE

Before adopting SIRP, the bank's cybersecurity operations were hindered by a **fragmented infrastructure**. Multiple key security systems, such as SIEM, EDR, firewalls, and DNS security, were **working in isolation**. This lack of integration created a major challenge for the bank's security team. The systems couldn't share data smoothly, which meant analysts had to **manually manage and respond to alerts** from different platforms. This slow response time to potential threats was further complicated by the **repetitive and routine tasks** that analysts had to handle.

As a result, the security team found itself spending most of their time on these routine tasks, leaving little room for strategic thinking. This constant **operational pressure** meant they had less time to focus on improving processes, planning ahead, or addressing critical issues. Instead of analyzing data and fine-tuning their security posture, their efforts were consumed by the day-to-day activities that could have been automated. This ultimately made the team **less agile** and less effective in responding to emerging threats.

The financial impact of these challenges was significant, as the financial industry faces escalating threats from cybercriminals. In fact, cybercrime costs for the global financial sector were projected to exceed **$6 trillion** annually by 2023 **(World Economic Forum),** with financial institutions being prime targets for attackers. Delays in responding to emerging threats or operating inefficient security systems could leave the bank exposed to substantial financial losses, reputational harm, and potential regulatory fines. The bank needed a solution that could mitigate these risks by improving the agility and effectiveness of its security operations, ensuring quicker response times and a stronger defense against evolving cyber threats.

THE SOLUTION

To address the challenges the bank was facing, SIRP was deployed to integrate the bank's security stack into **one unified platform**. The goal was to consolidate and harmonize key security controls—SIEM, EDR, firewalls, and DNS security—ensuring smoother workflows and a more efficient, automated approach to responding to threats.

SIRP's onboarding process played a crucial role in ensuring the system's success. Our team worked directly with the bank's Security Operations Center (SOC) team, taking time to fully understand their existing processes and workflows. This collaborative approach allowed SIRP's experts to **design customized playbooks** that addressed the bank's unique needs, automating routine tasks like threat detection and response, and freeing up the SOC team to focus on more strategic activities.

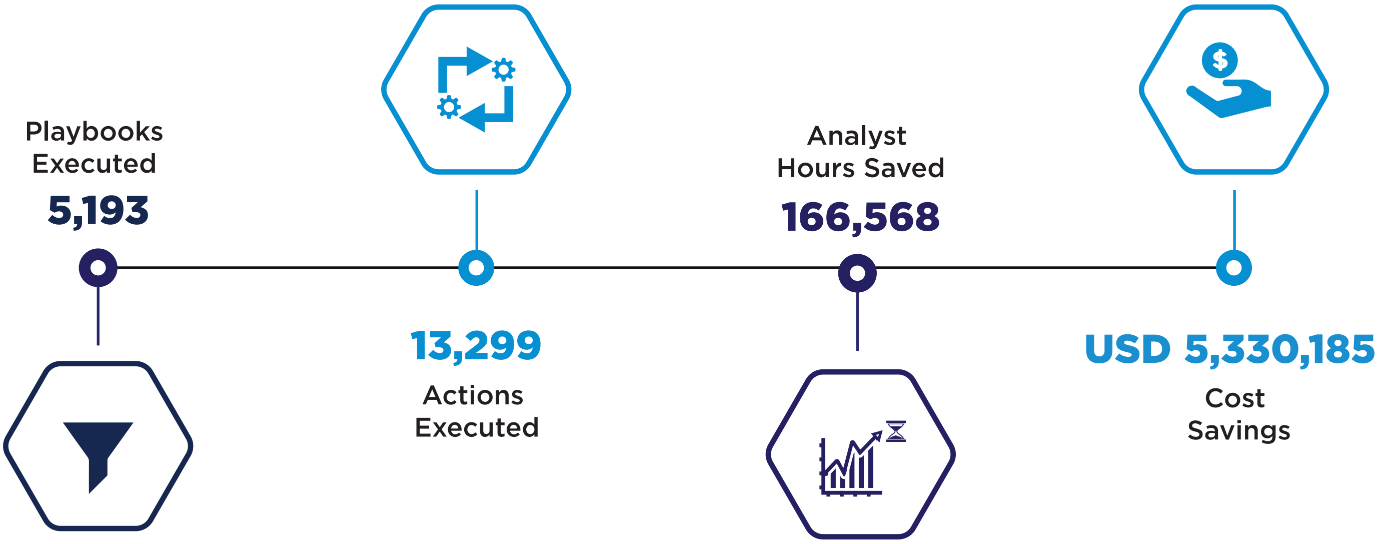
In addition to **automating workflows,** SIRP's integration brought a new level of visibility across the bank's security stack. The previously isolated systems were now able to share **critical data in real-time,** allowing the security team to respond to emerging threats quickly and efficiently. This **centralized visibility** and automation not only reduced the time it took to address threats but also improved overall response time.

Once the playbooks were designed, SIRP's team also provided **hands-on training,** ensuring that the bank's staff was not only familiar with the platform but also empowered to use it efficiently. This was complemented by continuous support from our dedicated Customer Success Managers (CSMs), who worked closely with the bank's team to ensure the **successful adoption** of SIRP's features. The CSMs were pivotal in helping the team unlock the full potential of the platform, providing guidance on how to **optimize workflows,** and encouraging the use of advanced features that further streamlined security operations.

The close collaboration between SIRP's team and the bank's SOC team ensured that the bank was able to leverage the full capabilities of SIRP, from automated playbooks to centralized visibility, resulting in a more efficient, effective, and proactive security operation.

THE RESULTS AND IMPACT

By implementing SIRP's solution, the bank saw **immediate improvements** in both the efficiency and effectiveness of its security operations. Here are the key results since the deployment three years ago:



Playbooks Executed
5,193

13,299
Actions Executed

Analyst Hours Saved
166,568

USD 5,330,185
Cost Savings

These metrics showcase the tangible benefits SIRP delivered to the bank's operations. Automated playbooks and workflows significantly reduced the manual effort involved in handling security incidents. As a result, the bank's security team could focus on more critical, high-value tasks, driving overall operational efficiency.

Beyond just the numbers, SIRP's integration fostered a proactive security environment. By automating the response to threats, such as blocking indicators of compromise (IOCs) and escalating alerts to the appropriate teams, the bank was able to act swiftly before issues escalated, reducing potential damage and minimizing risks.

Additionally, the integration of various security technologies provided the bank with a more cohesive, real-time view of its security landscape. This centralized visibility empowered the bank's SOC to identify threats more accurately and respond faster, further strengthening its defenses.

CHOOSING SIRP: HOW THIS FINANCIAL INSTITUTION GAINED EFFICIENCY, AND HOW YOU CAN TOO

The deployment of SIRP within the bank's Security Operations Center (SOC) demonstrated the transformative potential of a tailored, integrated approach. By unifying previously siloed systems—SIEM, EDR, firewalls, and DNS security—the bank gained centralized visibility, allowing its security team to operate more efficiently and proactively.

The collaboration between the bank's SOC and SIRP's experts ensured the creation of **custom playbooks** that automated repetitive tasks, reducing the burden on analysts and allowing them to focus on critical, strategic threats. Additionally, the bespoke **CISO dashboard** provided real-time visibility into key performance indicators and metrics, empowering leadership with actionable insights.

The bank's CISO highlighted the results:

> *"SIRP has significantly enhanced our security operations. Our analysts can now manage their alert workload with ease, ensuring faster responses to threats. At the executive level, the custom dashboard has been invaluable, offering real-time insights into metrics that are critical for decision-making. This seamless integration has improved efficiency across all levels of our team."*

Through continuous support, tailored training, and a deep understanding of the bank's unique challenges, the solution delivered measurable improvements in threat response time, workload management, and overall operational efficiency.

This case underscores the importance of a personalized approach to security operations. By addressing specific organizational needs, the bank was able to transform its security processes, equipping its team to tackle evolving threats with confidence and agility. For organizations facing similar challenges, this experience serves as a testament to the impact of a thoughtful, customized implementation strategy.