S&J and Macnica Visualize and Centralize a Fragmented Security Operations Framework with Swimlane

Reducing Dependence on Specific Personnel and Enabling Development by Non-Engineer Reducing Dependence on Specific Personnel and Enabling Development by Non-Engineers

CHALLENGES

- Security operations (SecOps) varied from project to project, requiring extensive time and resources for management and maintenance.
- The company's vendor-agnostic policy led to the use of a wide variety of products, making integration complex
- Siloed systems and reliance on individual expertise made it difficult to visualize who had handled which response

OUTCOMES

- Consolidated the fragmented security operations framework into Swimlane, reducing the burden on staff
- Enabled low-code playbook development, improving development speed and quality
- Centralized response logs make it easier to visualize and quantify workloads

> *"We appreciated the extensive integration capabilities with various products and the ability to develop playbooks using low-code."*

Ryuto Otsubo
Tech Lead - Product & Infrastructure, Core Technology R&D Group, Core Technology Division, S&J Corporation

S&J Corporation

- **Head Office:** Hibiya Building 8F, 1-1-1 Shinbashi, Minato-ku, Tokyo
- **Founded**: May 2025
- **Website:** www.sandj.co.jp

Established in November 2008, S&J Corporation is a cybersecurity company with a mission to "always consider the customer's expectations and provide security services that earn their thanks." As a team of cybersecurity experts, the company offers a wide range of services, including MXDR solutions tailored to the needs of Japanese enterprises, hands-on incident response support, impact analysis, and CSIRT formation assistance. S&J aims to serve as a foundational infrastructure for business growth.

S&J Corporation
Koichi Hanzawa
Director
Head of Core Technology Division

S&J Corporation
Takaaki Kuga
Information Security Specialist
Core Technology Division

S&J Corporation
Ryuto Otsubo
Tech Lead – Product & Infrastructure
Core Technology R&D Group, Core Technology Division

Challenges Before Implementation

Increased Workload, Operational Complexity, and Role Dependency in SOC Operations. Exploring Automation Platforms Usable by Non-Engineers

S&J Corporation is a cybersecurity company founded in 2008 by Nobuo Miwa, former president of LAC Co., Ltd. Following a vendor-agnostic approach, the company not only provides security products but also offers end-to-end services from consulting to monitoring and incident response. Known for its strong technical capabilities, S&J has also developed its own domestic managed detection and response (MDR) solution, KeepEye, which integrates managed services with endpoint detection and response (EDR). Regarding the company's mission, Koichi Hanzawa, Director and Head of the Core Technology Division, explains, "We are committed to delivering security services that combine technology with communication, so we can serve even more clients with the solutions they need."

At the time, S&J faced several challenges in operating its Security Operations Center (SOC) services for clients, including increased workload and the growing complexity and personalization of management and maintenance tasks. Ryuto Otsubo, an engineer in the Core Technology R&D Group of the Core Technology Division, recalls, "We had some mechanisms in place, like SOAR (Security Orchestration, Automation, and Response), to help reduce operational burden. However, since each engineer had developed their own solutions using Python, C++, or other languages on a per-project basis, it actually increased the workload required for maintenance and management. While we were initially able to manage with manual processes, as the organization grew, operations became more complex. We felt it was only a matter of time before we hit a limit."

In recent years, the company has maintained a high growth rate of over 20% annually, with a steadily increasing number of clients. Following its vendor-agnostic approach, S&J works with a wide variety of security products tailored to client needs, making system integrations increasingly complex.

With SOAR solutions developed separately for each project, documentation quality was inconsistent, and processes often became dependent on individual engineers. If someone left the company, handing over their responsibilities could be extremely difficult. While our technical expertise allows us to handle such situations through reverse engineering, having to analyze systems each time is a significant burden. That's why we began exploring a platform with strong visualization capabilities and an automation foundation that even non-developer analysts could use to address these challenges," says Otsubo.

Why Swimlane

Proven Integration with a Wide Range of Products and Low-Code Playbook Development. Adopted for Its Flexible Development Framework and Cost Structure

In May 2024, S&J began evaluating automation platforms. The company compiled an extensive list of candidate solutions and conducted a careful comparison and review. "As a company committed to a vendor-agnostic approach, we actively use multiple security products in parallel. For that reason, flexible integration capabilities with other tools were a key requirement. In addition, to eliminate dependence on individual personnel in operations and maintenance, we placed strong emphasis on the ability to develop playbooks—incident analysis and response workflows—as easily as possible using low-code," explains Otsubo.

Benefits of Implementation

Centralized and Visualized Security Operations with Reduced Workload. Eliminated Role Dependency, Improved Development Speed and Quality

The first major benefit of implementing Swimlane was the ability to visualize and centralize security operations, making it clear who handled what tasks.

“Previously, we had a vast number of assets to manage, and it was difficult to gain a centralized view of incident response history. Each analyst maintained their own tracking sheets, so understanding the overall workflow or individual contributions required checking multiple data sources separately. With the introduction of Swimlane, response history has been centralized, and our operational processes are now visualized, allowing us to clearly understand each analyst’s actions and achievements. This has also made it possible to use that data for evaluating the performance of the entire team,” says Otsubo.

Alert management has also been centralized. In the past, analysts had to check multiple tool interfaces simultaneously, sometimes even accessing the customer’s console, which meant having dozens of web browser tabs open at once.

“Swimlane has consolidated all of that into a single, streamlined interface, making management far more efficient. When polling alert information and analyzing logs, we no longer need to search each source individually. In some cases, the entire workflow can be automated through to closure, which has significantly reduced our workload. It has also improved coordination with our CSIRT team,” says Otsubo.

Another major benefit has been the reduction of mental stress on analysts.

“When you have to monitor dozens of screens, there's constant pressure that you might miss something important. Now that everything is consolidated into a single interface, we can manage operations with far less mental strain than before,” says Hanzawa.

The issue of role dependency was also addressed, as the ability to develop playbooks using low-code allowed even non-developer analysts to engage in automation. As a result, both development speed and the overall quality of the playbooks have significantly improved. Takaaki Kuga, an Information Security Specialist in the Core Technology Division, adds, “Another benefit of using low-code is that it has made the development workflow much clearer. Thanks to that, we’ve been able to minimize tasks like writing specifications and documentation, allowing us to allocate those resources to more productive work.”

Future Outlook

Carefully Exploring the Use of Generative AI. Aiming for Security Operations That Combine the Strengths of Humans and AI

Looking ahead, S&J is considering the use of generative AI. However, as a Managed Security Service Provider (MSSP), the company recognizes challenges around detection accuracy and accountability to clients, and for now, believes that relying entirely on AI poses a significant risk. As such, the company is taking a cautious and deliberate approach. “We intend to prioritize human-led management and support while leveraging AI as an assistant within appropriate boundaries. Internally, we’ve already begun using generative AI for tasks like document search and development support.

Going forward, we hope to use accumulated data, such as client-specific escalation details and analysis histories, to generate optimal response recommendations. To achieve that, we plan to take full advantage of Swimlane’s Hero AI functionality and work toward security operations that blend the strengths of both humans and AI,” says Otsubo.