MBSD Automates Security Operations for Faster Threat Hunting and Greater Agility

Key Challenges

MBSD's self-developed security management system worked well for some customers but didn't equip the engineering team with enough support to address all customers' increasingly demanding security operations.

Key Results

By automating workflows and orchestrating security operations with Splunk SOAR, MBSD now has full security visibility for speedy threat hunting and intelligent email filtering.

MBSD®

Industry: Technology

Solutions: Security, IT Operations

When it comes to security, speed is of the essence.

No one understands this urgency more than Japan-based Mitsui Bussan Secure Directions, Inc. (MBSD). Providing security operating solutions for government agencies and global corporations, MBSD covers everything from protection planning, preemptive measures and detection, all the way to post-incident actions.

To deliver these solutions at scale, the company needed to streamline service management for its security incident response team (SIRT), automating daily workflows like handling sensitive information, visualizing security status and responding to security incidents.

Splunk SOAR simplified operations by combining security infrastructure orchestration, playbook automation and case management capabilities. Thanks to the Splunk platform as a whole, MBSD has gained full-stack visibility to improve operational performance and better meet ever-changing customer demands.

Turning Data Into Outcomes

- Faster response to customers' evolving needs
- More advanced threat hunting, better email filtering and stress-free operations through automated workflows
- Unprecedented value for customers with full security visibility

Speedy response to changing needs wins customer trust

"From outsourcing security management to implementing advanced managed XDR, we have to stay abreast of the evolving customer expectations," says Masaru Sekihara, MBSD's chief operating officer of the consulting service department and head of the public projects department. To accomplish this, the MBSD team utilizes Splunk to analyze a wide range of data, including endpoint, authentication, network, application, asset and vulnerability information.

"With its high-speed data collection, search and analytics capabilities, Splunk makes our lives easier when managing all security information and event management (SIEM) systems simultaneously," Sekihara explains. "Without the need to normalize data under a predefined schema, we can support multiple solutions more flexibly and quickly store our data for efficient analysis."

MBSD's security engineers are continuing to perfect their SIEM systems by acting on insights from the Splunk platform and the trove of analysis rules from past projects. With this knowledge, the team now seamlessly handles increasing maintenance requirements while transforming their systems into a flexible, self-service format that customers prefer.

Automating workflows and security responses with full operational visibility

With the advanced security orchestration, automation and response (SOAR) capabilities of Splunk SOAR, MBSD easily manages security events and cases with workbooks and visualizes them as reports. In one case, for example, the company was building a service management system for a customer to consolidate different solutions across various regions. Thanks to Splunk, MBSD achieved a stress-free operation and seamlessly integrated the system with the customer's SOC framework.

"Although the SOAR platform we developed in-house enabled automation to a certain extent, it couldn't take care of all types of operations," Sekihara says. "Human-based management was sometimes required, especially when managing sensitive information since SOC and SIRT operations were not well coordinated with each other."

It wasn't until MBSD deployed Splunk SOAR that manual processes could be visualized on a single pane of glass, allowing security analysts to work more efficiently. To further bolster productivity and security, the company now also tracks time spent on human-to-human contact, such as phone calls and emails, and the amount of information disclosed outside the company.

> Splunk, with its high-speed processing capabilities, is exactly what we are looking for. The automated protection achieved with Splunk SOAR allows us to work much more efficiently."
>
> **Masaru Sekihara,** Chief Operating Officer of the Consulting Service Department and Head of the Public Projects Department, MBSD

In addition to automating data collection, identification, investigation and incident response, MBSD applies threat intelligence to automated processes according to predefined rules, which enhances email filters to guard against suspicious messages and prevent real threats from slipping through the cracks.

"Splunk SOAR works smoothly with our threat intelligence system," Sekihara says. "It reacts immediately once the threat intelligence system detects an invalid domain registration while also helping us record response history and visualize progress toward key performance indicators."

Expanding into new territories

Moving forward, MBSD plans to maximize the potential of the Splunk platform by giving more stakeholders access to insights derived from Splunk. With this data, MBSD management can view the SIRT's operation history in an intuitive way and ultimately provide customers with more valuable information about their operations.

"Customers will be able to understand their security risks in a more comprehensive and quantitative way, such as learning about incidents that were thwarted due to improved security," Sekihara says. "This will encourage them to make further security investments and bring us new business opportunities."

MBSD expects to use Splunk SOAR to empower more aspects of SIRT operations, including service management, incident management and corporate governance. As MBSD looks to the future, Splunk will play a key role in helping the organization expand its service to cover digital transformation support. "With Splunk, our security analysts can capture distinctive characteristics of data and conduct comparative analyses of customers' internal data for digital transformation," says Sekihara, who is eager to explore the use of Splunk beyond security.