splunk> turn data into doing™

CASE STUDY

au Kabucom Securities Brings Dark Data Into the Light to Battle Cyberattacks

Executive Summary

Part of Mitsubishi UFJ Financial Group (MUFG), au Kabucom Securities offers online brokerage services to more than 1.1 million customers across Japan. To achieve its goal to automate DevSecOps, the company needed a way to guard against potentially devastating cybersecurity threats while cost-effectively visualizing and analyzing all its data — including dark data, the unused, unknown and untapped data across the organization. Since turning to the Splunk® Data-to-Everything Platform, au Kabucom Securities has:

- Gained full visibility into its data on a unified analytics platform
- Improved overall efficiency through an agile, automated DevSecOps framework
- Enhanced cybersecurity readiness with a small team of two to three people

Uncovering the Value of Untapped Data

Massive in scale and difficult to monitor without the right tools, machine-generated log data can quickly become overwhelming — and expensive. "In the early days, we engaged a managed SIEM service," says Yoichi Ishikawa, assistant executive to general managing officer of system, system development department and deputy general manager, IT strategy group at au Kabucom Securities. "As log data increased, our costs surged exponentially. Worse still, we couldn't see our log data firsthand. Since data was outsourced for analysis, we only received notifications for identified anomalies. We needed a more proactive approach."

Security was another top priority for the organization. "Although we have a cybersecurity task force to monitor risks, a DDoS outbreak in 2017 revealed the need for stronger defense and greater information transparency across the company," says Ishikawa. "Before we could embrace DevSecOps by incorporating security into development and operation, we had to first analyze the dark data that we'd been generating, but not properly leveraging."

To harness the value of all its data while bolstering security, au Kabucom Securities turned to the Splunk platform.

au カブコム証券

Industry

- Financial Services

Splunk Use Cases

- Log Management
- IT Operations
- Security & Fraud

Challenges

- Lacked effective log management and analysis, which made it difficult to identify emerging anomalies
- Lacked data visualization and actionable insights necessary for successful DevSecOps automation
- Had insufficient manpower to combat threats and ensure cybersecurity readiness

Business Impact

- Gained data visibility and improved incident investigation through a scalable analytics platform
- Heightened cybersecurity by automating DevSecOps
- Simplified and enhanced operation by automating laborious manual processes

Data Sources

- Office 365
- Azure AD
- Active Directory
- DNS forwarder
- Firewalls
- Cyberthreat intelligence
- IT asset management software

Splunk Products

- Splunk Cloud
- Splunk Enterprise Security

Data Drives Competitiveness and Combats Threats

Thanks to Splunk, au Kabucom Securities now consolidates logs from various cloud services into a single console. The team then mines and analyzes this rich data to predict patterns, centralize reporting and gain real-time visibility into the company's security posture. The Splunk platform's ease of use and scalability enable the company to manage its large volume of data in a cost-effective way, while correlation analysis with external threat intelligence helps effectively prevent threats.

With Splunk, the au Kabucom team investigates and responds to critical issues faster. "Our new position as an online trading platform means that data management is more crucial than ever before," says Ishikawa. "Splunk is amazing because it lets us parse, correlate and visualize both structured and unstructured data without a hitch. With an extensive track record in the financial world, Splunk will help us continually drive competitiveness by deriving maximum value from untapped data assets."

Automated DevSecOps Revolutionizes Security

By identifying suspicious behavior, triggering alerts and analyzing logs to automate corrective actions, the Splunk platform has allowed au Kabucom Securities to achieve its goal of fully automating DevSecOps. "Splunk plays an integral role in log data visualization, which begins the entire DevSecOps cycle," Ishikawa explains.

With end-to-end visibility across IT operations and the DevSecOps cycle, the au Kabucom team uses Splunk to visualize granular data in the "Ops" phase and attain new insights for quality improvement and threat mitigation in the "DevSec" phase. By repeating this collaboration cycle, the team effectively fills security gaps in application development and operation, gaining the confidence they need before pushing out new configurations.

"Splunk enables us to get the most out of data to evolve our security initiatives and remain resilient against cybersecurity challenges."

— Yoichi Ishikawa, Assistant Executive to General Managing Officer of System, System Development Department and Deputy General Manager, IT Strategy Group, au Kabucom Securities Co., Ltd.

Increased Cybersecurity Readiness, Reduced Manpower Pressure

Splunk has helped au Kabucom Securities successfully reduce the strain on its resource-strapped team, eliminating workflows like manually searching multiple applications and logs to detect security vulnerabilities. "Recruiting skilled security specialists is difficult," says Ishikawa. "Now, our small Cybersecurity Incident Readiness team of just two to three people can delegate time-intensive security checks to Splunk, allowing them to spend their time on more strategic initiatives."

Today, au Kabucom Securities benefits from streamlined threat investigation and automated response, enhanced visibility and advanced predictive analytics all on Splunk's unified platform. And that's only the beginning. Ishikawa plans to expand use of the Splunk platform to identify illegal financial transactions, improve customer service and revamp workflows through business process mining and visualization.

"Splunk will help us continually drive competitiveness by deriving maximum value from untapped data assets."

— Yoichi Ishikawa, Assistant Executive to General Managing Officer of System, System Development Department and Deputy General Manager, IT Strategy Group, au Kabucom Securities Co., Ltd.

20-13440-Splunk-SEC-au Kabucom-101-CS