GMO Internet Enhances SOC Operations with Advanced Fraud Detection

Key Challenges

Tool sprawl caused inefficient log monitoring and delays in root cause analysis, increasing security risks and negatively impacting anomaly detection, fraud prevention, and service quality.

Key Results

Splunk delivers unified real-time log monitoring and AI-driven fraud detection, reducing false positives, automating threat blocking, and simplifying tool integration for more efficient operations.

GMO INTERNET

Industry: Technology

Solutions: Platform, Security

Products: Splunk Enterprise, Splunk Enterprise Security

Capabilities: SIEM / Security Analytics, Unified Security Operations, Automation and Orchestration, Security Incident Response, Infrastructure Monitoring and Troubleshooting, Incident Response and Automation

Outcomes

- Accelerated log management
- Reduced analyst workload
- Proactive fraud prevention

Advancing security operations center (SOC) workflows with data-driven intelligence

With the mission “Internet for Everyone,” Japan-based GMO Internet Group manages internet infrastructures for global businesses, providing domain registration, cloud hosting, internet connectivity, and security services. Its Kitakyushu office serves as a hub to both ensure 24/7 operations and embrace new technologies like AI.

With security as its highest priority, the company worked with partners to tackle the evolving threat landscape, but found incident management challenging. “Because we used multiple tools to monitor our IT infrastructure, tool sprawl created limited visibility, causing delays in troubleshooting,” says Naoki Hamamoto, SOC team leader, CISO office, systems division, GMO Internet, Inc. “Sometimes we couldn’t even uncover the cause of a system failure.”

The company had a pressing need to upgrade its security operations. “Among all the solutions we evaluated, the combination of Splunk Enterprise and Splunk Enterprise Security stood out as the best SIEM platform,” Hamamoto adds. “Splunk’s well-developed correlation analytics allows us to go beyond performance monitoring and proactively prevent system failures, safeguarding the core value of our service.”

From tool chaos to unified command

GMO Internet stopped the chaos of tool sprawl with Splunk Enterprise, which serves as a unified platform to collect and monitor logs in real time. Soon after, the company began leveraging Splunk Enterprise Security as its complete security information and event management (SIEM) platform.

Together, Splunk Enterprise and Enterprise Security efficiently gather diverse logs from internal and external systems, including web application firewall logs, operating system-level server logs, application logs, and IP address activity logs. Advanced analytics has streamlined log management, enabling the SOC to significantly reduce analyst workload for this critical task. Now, the team can easily set up a workflow for continuous 24/7 monitoring of security alerts.

The highly scalable Splunk platform also allows GMO Internet to expand its use cases in phases. It now covers fraud detection and data mining, IT operation management, and site reliability engineering.

Easing the burden of security analysts through AI and automation

When it comes to fraud prevention, Splunk Enterprise Security offers correlation rules for security analysis, allowing GMO Internet to create custom rules to better detect system anomalies. In addition, Splunk's Application Programming Interfaces can flexibly integrate with other tools, working seamlessly with GMO's own SOC service to capture logs and traces of attacks that bypass the web application firewall (WAF). This enables the automatic addition of IP addresses to a "blacklist" for blocking malicious IPs, which, together with automated alerts and responses, help avoid repeated attacks from the same source.

> Splunk Enterprise Security is very effective at filtering alerts that are more likely to represent genuine issues, so our analysts can focus on what deserves their attention.
>
> **Naoki Hamamoto,** SOC Team Leader, CISO Office of the Systems Division, GMO Internet, Inc.

GMO Internet also integrates the Splunk platform with large language models (LLMs) for early identification of potentially fraudulent activity. "Now we can rely on data science and deep learning to create a robust data analysis foundation," says Hamamoto. "This enables us to analyze complex log patterns and service activities, like user sign-ups and access events, to uncover potential fraud." Analysis results are then compiled into reports and sent out to business divisions, enabling them to take necessary actions.

Splunk has also helped reduce false positives, allowing analysts to take on more incidents. "Splunk Enterprise Security is very effective at filtering alerts that are more likely to represent genuine issues, so our analysts can focus on what deserves their attention," says Hamamoto.

Another advantage of conducting correlation analysis with Splunk Enterprise Security is that the company can organize logs, which come in various formats, into the unified Common Information Model for more efficient operations. "Analysts review a wide variety of logs every day, and with new vulnerabilities and attacks always emerging, Splunk covers the workload and resources that analysts lack," says Hamamoto.

Pushing the boundaries of innovation with Splunk

While GMO Internet currently uses Splunk as a crucial security management tool, it plans to expand its use into three additional areas.

"First, we hope to collect more logs across a wider scope to ensure comprehensive observability of a greater number of systems and service activities," Hamamoto explains. "The second idea is to further leverage AI to boost analysis accuracy, like giving analysts more granular feature values for more precise and proactive fraud detection. Finally, we will continue to automate and streamline security operations through integrations with other tools."

To GMO Internet, Splunk is a great security partner. "Splunk has always been so helpful, even when we presented our conceptual ideas at an early stage. This relationship is crucial for us to implement more complicated use cases in the future," Hamamoto concludes.

Download Splunk for free or get started with the free cloud trial. Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs.

splunk>
a CISCO company

Learn more: www.splunk.com/asksales

www.splunk.com