splunk> turn data into doing™

CASE STUDY

PERSOL Expands Access to Data Through Better Security and Flexibility

Key Challenges

PERSOL's legacy SIEM system lacked customization capabilities and was neither user-friendly nor flexible enough to handle both external and internal threats in the ever-growing IT environment.

Key Results

PERSOL's data-driven decision-making makes security management more efficient and enables the team to respond to evolving threats.

PERSOL

Industry: Technology

Solutions: Security

In the fast-paced, dynamic world of IT, adaptability is the key to success.

That's why Japan's PERSOL Group never stops refreshing its security strategy. Embracing a vision of "Work, and Smile," PERSOL offers a comprehensive array of human resource services such as temporary staffing, IT outsourcing and engineer recruitment. They currently run a total of 133 companies across the globe and operate in over 640 locations.

While protecting such a sheer amount of confidential personal data is never an easy task, PERSOL had been doing a good job fighting external threats with its legacy SIEM system through correlation analyses. When it came to internal fraud prevention, however, the system was inflexible, requiring a predefined set of rules. It was also not scalable enough to combat increasingly sophisticated attacks, and the workflow for normalizing and processing heterogeneous data imported to the system was time-consuming.

PERSOL was also longing for a community where users could exchange valuable experiences and best practices. So, when the old system reached the end of its shelf life, PERSOL decided to make a change.

Turning Data Into Outcomes

- Expanded access to data and improved workflow efficiency with Splunk's user-friendly interface
- Protects customer data more effectively with an ultra-flexible SIEM
- Streamlined operations while enabling proactive threat investigation

A Versatile Tool for the Whole Team

The Data-to-Everything Platform empowers PERSOL to streamline manual workflows and continuously look for potential threats, investigate alerts and relay findings to the security team on a centralized system. "Initially we chose Splunk because of its global track record and superiority over other open source solutions," says Hiroshi Mochida, manager of the cybersecurity office in the group IT security department at PERSOL. "But after using the Splunk platform for a while, we're amazed by the real value it brings us."

With Splunk, PERSOL now detects and prevents data breaches early on via correlation analysis. Anyone at any skill level can easily operate the Splunk platform through a well-localized, intuitive user interface. The schema-free design, in addition to the Splunk Search Processing Language (SPL) — which turns complex investigations into simple searches — take the stress off the IT team by accomplishing daily tasks such as threat hunting, incident investigation and customized analyses. The team no longer has to switch between multiple screens and run various searches just to identify a minor incident.

By joining the Splunk Community, PERSOL also connects with other users from around the globe and taps into a wealth of skill and knowledge about security management, easing the pain of troubleshooting and paving the way for future innovations.

> With Splunk, we easily get what we need today and to build our best future."
>
> **Hiroshi Mochida,** Manager, Cybersecurity Office, Group IT Security Department, PERSOL

Adaptability in a Streamlined Operation

Given the extensive lineup of apps and add-ons Splunk offers, PERSOL now goes the extra mile, facilitating scaling system resources using the Amazon Web Services environment and streamlining remote data collection.

Streamlining manual and repetitive tasks enables the team to spend less time on administrative functions, and more time on investigating potential threats and acquiring new security knowledge. By lessening the burden of threat investigation, PERSOL is also able to cultivate a positive working atmosphere so that employees in the security operation center can be more proactive and creative. The team is now free to come up with more ideas and focus on more valuable, high-impact tasks that help propel their teams, departments and organizations forward.

PERSOL also appreciates the human touch at Splunk, which makes all the difference in customer experiences. "The extensive information and case studies that Splunk shared have given us valuable insights into different ways of using SIEM effectively. We've also enjoyed the seminars and networking opportunities Splunk offers, which enable sharing of skills and expertise among user communities," says Kairi Miyashita, who works in the cybersecurity office of the group IT security department at PERSOL.

> The extensive information and case studies that Splunk shared have given us valuable insights into different ways of using SIEM effectively."
>
> **Kairi Miyashita,** Cybersecurity Office, Group IT Security Department, PERSOL

A More Automated Future

"We have seen more companies automating their operations with Splunk, and that's something we're increasingly interested in," says Mochida, who is considering deploying Splunk Phantom to fully automate the incident management workflow — from incident detection to analysis to response. Another plan is to bring in the Splunk UBA tool to detect various threats, anomalies and suspicious internal activities through behavior analysis powered by machine learning.

Moving forward, PERSOL will bring data to even more decisions and actions across the organization, extending the Data-to-Everything Platform to additional departments and internal systems. Their aim? Maximize benefits from the Splunk platform beyond security management and foster innovation in other business operations.

21-16731-Splunk-Tier2-Persol-101-CS