splunk>

CASE STUDY

ASICS Automates Incident Management and Resolution With Real-Time Log Analysis

Executive summary

ASICS, a Japanese multinational corporation formed by the merger of Onitsuka, GTO and Jelenk, offers a full range of sports supplies and equipment aiming to create a quality lifestyle through intelligent sport technologies. To combat cyberthreats and address incidents at the very moment they occur, ASICS required a central platform to manage, correlate and analyze logs generated from multiple systems. Since deploying Splunk Enterprise, the company has seen benefits including:

- Real-time visibility into incidents and threats through automated log analysis
- Enhanced social accountability due to improved security and visibility
- Boosted efficiency and productivity due to streamlined operations

Why Splunk

ASICS has taken proactive steps to safeguard its business over the years. These include setting up the information security committee and information security office, as well as the computer security incident response team (CSIRT) and security operations center (SOC). After putting the resources in place, however, the company was still unable to centrally manage and analyze the logs generated from internal systems scattered across different locations including firewalls, proxy servers and endpoint detection and response systems, while preserving the trails of evidence for the purpose of social accountability. All of these tasks have been time-consuming, requiring a lot of manual procedures.

Another priority is to accurately detect and provide timely response to every endpoint threat, whether it is an email fraud, a cyberattack or any other issue, through 24/7 monitoring. For crisis prevention, ASICS also needs a reliable mechanism for extracting anomalous patterns and identifying suspicious devices through correlation and historical analysis of log data. Splunk Enterprise not only meets all these requirements but also impresses ASICS with its flexibility to work seamlessly in a small-scale commercial SOC environment and the capability to go live within a short timeframe with a small investment.

Industry

- Manufacturing

Splunk Use Cases

- Log Management
- Security and Fraud

Challenges

- Lack of timely response to incidents and threats
- Inability to centralize log management and analysis
- Inefficient incident response and resolution requiring a lot of manual effort
- Social accountability challenges due to potential data breaches and security risks

Business Impact

- Heightened business security due to real-time visibility into incidents and threats
- Improved operational efficiency due to automated, centralized log management with minimal manual intervention
- Enhanced social accountability with secure and transparent operations
- Sustainable business growth with the potential to go further with Splunk

Data Sources

- Next-generation firewalls
- Cloud proxies
- Proxy servers
- Endpoint detection and response system
- Cloud server event logs

Splunk Products

- Splunk Enterprise

Automating log analysis with real-time visibility and operational insights

Running on a virtual private cloud within ASICS's data center, the Splunk software consolidates log data from all systems and analyzes them on a central platform, generating insights and visibility into the entire operation in real time. It then calculates risk scores based on correlation searches and identifies anomalies and threats in real time. The SOC operators can now access the analysis status anytime and anywhere through an intuitive web console and receive alerts through their smartphones in case of emergency incidents, while the ASICS CSIRT can track post-incident activities easily.

All of these efforts are automated, which allows ASICS to monitor its data center around the clock with minimal manual intervention. By automating log management, ASICS saves valuable manpower and can focus on other high-value business activities.

Achieving social accountability with timely incident tracking and improved security

As a public company, ASICS is obligated to provide its stakeholders a clear picture of the business. For example, it is accountable for how data was captured and how every process was conducted, such as shoe design and manufacturing. With Splunk Enterprise, ASICS can quickly track potential issues, stay ahead of problems and improve security. It also can extract operational insights from logs, identify events and generate reports for top management and stakeholders promptly through a user-friendly interface. Enhanced social accountability enables ASICS to build a better reputation among internal and external stakeholders while attracting talent and motivating employees.

"As an all-around analytics tool, Splunk Enterprise effectively supports our operation and generates great benefits for us. We believe the Splunk solution could be an energizer for the sports industry."

Shigekazu Tanimoto, Global Security Lead
ASICS Corporation

Raising efficiency and productivity with streamlined operations

Now at the center of ASICS's security infrastructure, Splunk Enterprise enables the company with a correlated network of data and streamlines operations in an unprecedented way. Fully compatible with existing applications, it works well with every part of the business environment and enables seamless collaboration between different departments, enhancing operational efficiency and productivity as a result.

Meanwhile, ASICS is exploring more creative ideas with Splunk Enterprise, such as hunting malicious insider threats and data breaches, helping to protect corporate assets and safeguarding employee privacy. Because of this, the company is evaluating Splunk User Behavior Analytics for future use. It also is planning to extend the use of the Splunk solution to a broader geographical coverage by implementing a regional security information and event and management (SIEM) strategy to benefit other countries.

Furthermore, ASICS is trying to capitalize on the Splunk software big data analytics engine for a broader range of business applications. For example, one of its products is a baseball with built-in sensors for measuring pitching data. The big data collected from sensors could provide insights to help athletes break records. With Splunk Enterprise, ASICS believes that the best is yet to come and a sustainable future is just ahead.