

Olympus Achieves Global Security Visibility on a Single Pane of Glass

Key Challenges

Maintaining consistent cybersecurity across global operations proved difficult for Olympus, as fragmented strategies and tool sprawl created visibility gaps that hindered effective threat detection and compliance.

Key Results

Splunk helped Olympus achieve global SIEM integration with unified visibility into its worldwide operations, that significantly accelerated incident investigation and response times while reducing the manual workload for their security analysts.

OLYMPUS

Industry: MedTech

Solutions: [Platform](#), [Security](#)

Products: [Splunk Enterprise Security](#), [Splunk Cloud](#), [Splunk SOAR](#)

Capabilities: SIEM / Security Analytics, Unified Security Operations, Security Incident Response, Incident Response and Automation

Fueling company-wide security transformation through global SIEM integration

As a Japan-headquartered global leader in medical technology, Olympus Corporation provides innovative endoscopes and precision equipment to healthcare providers across 40 countries in EMEA, the US, and APAC. With an unwavering commitment to patient safety, the company prioritizes cybersecurity as the essential foundation for its global business continuity.

However, Olympus faced significant security blind spots because their various managed service providers relied on inconsistent tools across different regions, creating data silos that made it difficult to analyze threats effectively. This fragmentation prevented the team from gaining a clear view of their risk landscape, which ultimately hindered their ability to make informed decisions and delayed their response to potential incidents.

"Without knowing what happens in systems and applications, how could we recognize threats and risks in the network, protect our business assets, and thoroughly enforce security compliance?" says Matthew Stephan, Senior Director, Global Security Operations at Olympus. With the support of Splunk, the company managed to conduct a company-wide security transformation.

Global security posture at a glance on a single platform

Olympus successfully completed its global SIEM integration with Splunk in less than a year, gaining full visibility into its security operations through a single, unified view. "With cyberattacks coming across borders, the ability to visualize the movement of threats across the global network has optimized our security strategy," Stephan emphasizes.

By leveraging [Splunk Enterprise Security](#), Olympus seamlessly ingests and integrates system and application logs from its factories, R&D facilities, and business departments across its entire global footprint. This comprehensive visibility allows the team to establish precise correlation rules for proactive incident detection. Furthermore, by aggregating

Outcomes

- 300 times faster log search time
- Phishing and BEC response improved from days to hours
- Reduce manual workload for analysts with SOAR automation

this data into [Splunk Cloud](#) via AWS collectors and utilizing [Splunk SOAR](#) to automate manual workflows, Olympus has significantly strengthened its ability to respond to threats with greater speed and precision.

Unlike other SIEM providers in the market, Splunk natively integrates, analyzes, and ingests diverse logs, which eliminates the need for complex backend maintenance. Beyond these technical advantages, the Splunk team has earned Olympus' trust by demonstrating consistent professionalism and a deep commitment to the company's success. "They deeply understood our organizational structure, risk posture, and long-term roadmap, gave us the best support during the deployment, and even predicted our future needs," says Stephan. "The sales and [professional services](#) people of Splunk worked as one team and swiftly addressed our complex requirements in any region, significantly speeding up the deployment."

Substantially accelerated incident management and "painless" cybersecurity

For Olympus, the most significant improvement since implementing Splunk has been the dramatic acceleration in response times for phishing attacks and business email compromises (BEC). Tasks that previously required days to detect and resolve are now completed in just a few hours, representing a tenfold increase in speed. Furthermore, log search efficiency has improved significantly, with retrieval times dropping from between three to five hours to now, just seconds — a 300-fold gain in performance.

Splunk SOAR automates complex workflows, which mitigates analyst fatigue and allows the team to focus on high-priority threats. This capability also facilitates real-time collaboration and information sharing, effectively supporting the company's 24/7/365 security operations center.

Security is often viewed as a cost center, making accountability more important than ever. To demonstrate IT's value to the management team, Stephan relies on the integrated Splunk platform to oversee global operations and manage service level agreements and KPIs for his service providers. This unified approach enables him to clearly communicate the specific value provided to each business department. "This is a major achievement!" Stephan says.

Going beyond security to optimize other operations

Following its global security transformation, Olympus plans to extend the use of Splunk to other areas, starting with networking. "We look to share the Splunk instance with our infrastructure team for network and application monitoring," says Stephan. "By bringing the security operations center and network operations center to the same platform, we can better share information as a cohesive group."

Olympus is also considering enhancing its [operational technology](#) (OT) and research and development (R&D) with Splunk. "Splunk already has a rich library of parsers and a strong community in OT and R&D. Creating unique parsers is also easy," Stephan explains.

Reflecting on the journey, Stephan offers this advice to other organizations embarking on transforming global security, "Transformation is difficult, which can take years. The key to success is to obtain support from the top management and proceed at a reasonable pace. This is a question of both technology and people. We have to communicate with business departments, leaders, and teams, involve them, and proceed as one team. Moreover, having an excellent partner is essential. We are lucky that Splunk is a wonderful partner to us."



The partnership with Splunk is essential to our success. Splunk does not just sell products but also predicts our future needs and put forward the best solutions for us to succeed.

Matthew Stephan, Senior Director, Global Security Operations, Olympus Corporation