KELAGROUP sysmex

Case Study

Sysmex, a Leader in the Medical Industry **Enhancing Security Readiness with KELA**

Building a Framework for Proactive Risk Mitigation and Immediate response

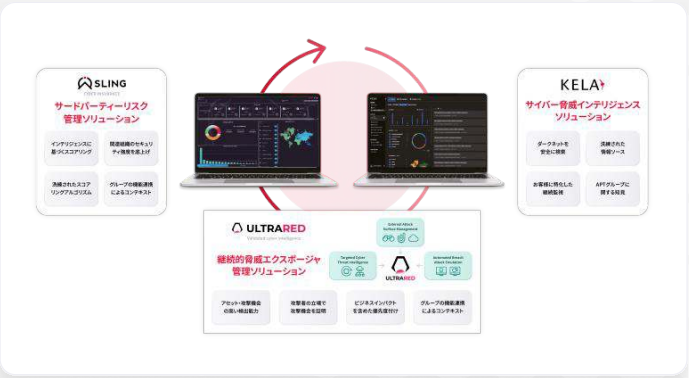
Sysmex Corporation is a global healthcare company engaged in the research and development, manufacturing, sales, and support of medical diagnostic instruments, reagents, and software. In Japan, the company operates through a network that includes its headquarters, 10 sales offices, 1 branch, 7 regional offices, and 13 sales points. Internationally, it has strategic bases in Europe (Germany), the United States, China, and the Asia-Pacific region (Singapore), and conducts business in over 190 countries worldwide.

In response to the growing risks posed by cyber threats— including ransomware-Sysmex established its internal Computer Security Incident Response Team (Sysmex-CSIRT) in 2020. This initiative was aimed at protecting the company' s intellectual property and proprietary know-how, developed over more than 70 years, and at ensuring the continuity and growth of its operations.

Following this, Sysmex implemented three cybersecurity solutions from the KELA Group to strengthen its global defense posture:

- Third Party Risk Management ("SLING SCORE")
- Cyber Threat Intelligence Platform ("KELA Threat Intelligence")
- Attack Surface Management / Continuous Threat Exposure Management Solution ("ULTRA RED")

By deploying these solutions in succession, Sysmex established a global security operation framework capable of close collaboration with regional and local security representatives.

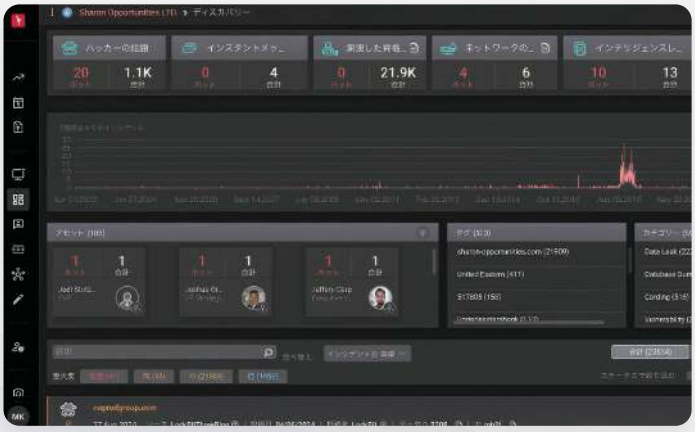


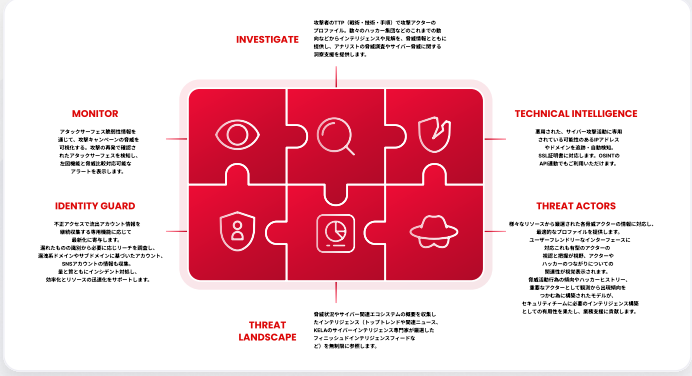
Enhancing the Security Team's Skill and Maturity through the Use of KELA

Background Behind the Establishment of Sysmex-CSIRT

Our company develops, manufactures, and sells core products such as blood analysis equipment. The blood test data of patients forms the basis for diagnosis and is therefore extremely important information. To protect it from unauthorized access and cybercrime, it is essential to establish a robust security tramework.

Previously, our information systems team was responsible for both operations and security. However, in light of the growing importance of cybersecurity, the company decided to establish Sysmex-CSIRT as a dedicated team.





Utilization of Cyber Threat Intelligence: How "KELA Threat Intelligence" Is Applied

KELA Threat Intelligence is a modular solution that requires individual licenses per module. Currently, Sysmex uses two modules Monitor and Identity Guard and has also subscribed to the managed service offering.

KELA provides information typically inaccessible through conventional means, such as data from the dark web and insights into cybercriminal activities. This intelligence enables proactive risk mitigation before threats fully materialize.

The Sysmex-CSIRT team, composed of three members, continuously monitors whether any threat information relates to the company's assets. The intertace provides a list of identihed items, allowing the team to visually grasp the severity and urgency of each case. High-risk Items are tlagged and escalared to the relevant Internal stakenolders Initially, Sysmex lacked internal expertise in threat intelligence.

Howeover, through ongoing monoring and incident handling, the team accumulated experience and improved its skill set. This growth has aligned with one of the original goals or implementing KELA: to develop internal threat intelligence capabilities. The use of KELA has clearly contributed to both skill enhancement and the overall maturity of the team.

Identifying Vulnerabilities Across Unmanaged IT Assets

Application of the ASM/CTEM Solution "ULTRA RED"

Attack Surface Management (ASM) assesses the risk of IT assets that are publicly accessible via the internet. However, because IT environments are constantly evolving-with new websites being deployed at domestic and international locations and increased use of cloud services-there are often unmanaged IT assets whose vulnerabilities remain unaddressed. ULTRA RED helps identity these hidden risks.

When issues are discovered, alerts are generated along with urgency scores, enabling the team to prioritize and respond to high-severity issues first. We believe this contributes to raising the baseline of our security level by allowing prompt action on vulnerabilities.

Previously, selecting which issues to respond to required significant effort and time. With the introduction of KELA, the interface became simpler and easier to use. The platform clearly surfaces the issues reauirina attention. helpina reduce workload across team members.

Concrete Results Achieved with KELA Solutions

Our overseas offices also use the same KELA interface to check the assets they manage within their respective regions.

Previously, our headquarters had to confirm the local situation in each region before communicating, such as when a discovery was made in the U.S. and had to be reported separately to the local U.S. team. This required multiple steps. Now, alerts appear directly on the dashboard, significantly streamlining the process.

In domestic cases, we can now promptly inform relevant departments of issues like account information leaks or exposed assets detected by KELA. We've also been able to take swift action on password resets and deactivation of unauthorized accounts.

Additionally, KELA provides timely and periodic reports on emerging threat trends and common attack techniques, allowing us to take proactive countermeasures. We are now able to reflect these insights into our own defense mechanisms and block attacks in advance.

Interview video now available on YouTube

Expectations for KELA Solutions

There have been cases where malicious third parties acquired domains similar to Sysmex's and used them in phishing schemes to lure users. Monitoring such impersonation domains was not initially covered by tne standard KELA modules, so we contracted tne manaded service to cover this need. We receive alert notifications and reports concerning these threats through that service.

While not everything can be monitored with the standard modules, we hope future enhancements will broaden the coverage area, enabling even more effective and efficient responses.

Future Outlook and Commitment

We plan to continue leveraging threat intelligence going forward. To do so, we must remain capable of responding to threats quickly, and this requires us to further enhance our ability to interpret and act on threat information.

The significance of using threat intelligence lies in how well we can detect and address risks before they become apparent. We aim to further strengthen our team to respond thoroughly to detected threats, which in turn raises the company's overall cybersecurity maturity.

SYSMEX CORPORATION
https://www.sysmex.co.jp/

KELA Threat Intelligence
https://www.kelacyber.com/ja/

ULTRA RED
https://www.ultrared.ai/jp/home

SLING SCORE
https://slingscore.com/