Secureworks
a SOPHOS company

Secureworks Superior Threat Detection Underpins Safe and Secure Services for Sansan

Combining Security and Convenience to Accelerate Customer Innovation

Following its mission of "turning encounters into innovation," Sansan has made its vision "to be the infrastructure for business." Based on this mission and vision, Sansan engages in business activities that support the business innovation of its customers. Sansan offers a wide range of services that include "Sansan," a sales digital transformation (DX) service that allows users to organize over 1 million customer information records for sales activities; "Bill One," an invoice management service that accelerates companywide billing operations; "Contract One," a contract DX service that accurately converts all contracts into data and makes it available throughout a company; and "Eight," a business card app that can be used for business card management and career development.

Through the DX services, the company is entrusted with personal data and other sensitive customer information, and so has taken extensive measures to bolster security. Sansan's Kenta Sato, CSIRT Group and Information Security Management Group, Information Security Department, Sansan Technology Division, explains, "Generally speaking, the main role of a CSIRT is to respond to incidents, but our CSIRT group

sansan

Name: Sansan, Inc.

Capital: 6,633 million yen
(As of August 31, 2023)

Country: Japan

Employees: 1,421

Established: June 11, 2007

Address: 5-52-2 Jingumae, Shibuya-ku, Tokyo

www.sansan.com/en/

SOLUTIONS

Taegis™ XDR
Taegis MDR

PROJECT GOALS

- Enhance threat detection of the defense system
- Reduce the burden on security operations

SYSTEM INTRODUCTION

- June 2023

strives to improve the security of services by working closely with the business units in charge of each product. Our Information Security Management Group also works to improve governance by developing information management guidelines, creating rules, as well as conducting education and awareness activities."

As part of this process, Sansan also takes into account the employee experience. Sato says, "Our company's premise is to provide both security and convenience. Of course, safety and security are central components, but they should not stifle innovation. We believe it is our mission to strike an optimal balance between the two."

Taegis XDR/Taegis MDR Introduced to Enhance Threat Detection

> Sansan is focusing on XDR products, that detect threats using correlation analysis of various source logs.

Sansan is constantly reviewing its security measures to respond to cyberattacks, which become more malicious and sophisticated with each passing year. As part of this effort, Sansan implemented a project to deploy XDR (Extended Detection & Response) products. Sato shed some light on the background, saying, "We conduct penetration tests every year, and one of the issues that came up was the need to improve our threat detection capabilities. In recent years, an unrelenting stream of new attack methods have emerged, and we need to be able to detect them accurately."

Of course, the company has already introduced products such as EDR (Endpoint Detection and Response) and SIEM. However, because it is unrealistic to detect sophisticated cyberattacks solely through category-specific products such as those specialized for endpoints, networks, and the cloud, a holistic view is required. This is why Sansan decided to focus on XDR products, which detect threats using correlation analyses of various source logs.

In selecting a platform, the company required not only excellent threat detection capability, but also a wide range of supported services and solutions, ease of use, and a reasonable cost. These requirements were met by Secureworks' Taegis XDR and the Taegis MDR managed detection and response (MDR) service.

Sato explains why the company chose Taegis XDR: "Although there are existing EDR products with XDR functions, they can only detect threats from one vendor's perspective. We already experienced using Secureworks' managed security services and greatly appreciated its capabilities. Based on that experience, we chose Taegis XDR because we wanted to more comprehensively detect threats using a platform that would allow for multiple data ingests."

> The initial response to incidents was quick and efficient. We had reservations about using a managed service, but in the end, it was the right choice.

Comprehensive Monitoring of Around 3,000 Endpoints and IaaS/SaaS Logs

Integration into the current environment also went smoothly. Sato recalls, "With products like these, it's often difficult to import logs, but Taegis XDR was extremely easy to integrate. It only takes about a week to capture just the logs, and about a month including evaluation and verification. Considering that some products take months just for evaluation, I think it is a very easy product to implement."

Specific monitoring targets include approximately 3,000 endpoints at the company's headquarters and other locations, as well as IaaS/SaaS services such as AWS, Okta, and Azure AD. Many companies using EDR/XDR struggle with oversensitivity and false positives, but because Sansan also uses Taegis MDR, it does not have to deal with these issues.

Sato points out with satisfaction, "If there is no problem with the detected threat, the Secureworks analyst closes it, so we don't have to worry about adding man-hours to manage the situation. Taegis MDR also examines the details of a breach before

reporting it, ensuring that our initial response to an incident is prompt and efficient. We had reservations about using a managed service, but in the end, it was the right choice."

Establishing a Robust Monitoring System for Reliable Response to New Threats

> The number of risks that must be addressed, such as unauthorized use of IDs, continue to grow, however, since the introduction of Taegis XDR, we have been able to detect them.

Sansan is now implementing a hybrid operation that combines Taegis XDR with its existing SIEM platform. By using Taegis XDR for routine monitoring and SIEM for analysis only when conducting special investigations, it has built a cost-effective monitoring system that is also scalable. Despite the increase in monitoring targets, the workload for responding to alerts has not increased.

According to Sato, "SIEM receives logs from a variety of sources, but the data is often difficult to use due to the time and effort required."

However, Taegis XDR performs a correlation analysis on various data and allows us to visualize it in a "single view." For example, for a single alert, it's easy to see which sensors detected it, and the threat can be clearly understood as a chronological sequence of violations. This is a huge advantage."

This demonstrates the impressive progress in improving threat detection, which had been a cause for concern. Sato says, "As cloud computing becomes more widespread, so does the number of risks that must be addressed, such as unauthorized use of IDs. In some cases, the service provider's defenses are incapable of eliminating such risks; however, since the introduction of Taegis XDR, we have been able to detect them."

Another advantage is the ability to leverage Secureworks' extensive global knowledge. The Taegis platform is automatically updated with the latest threat intelligence and detection rules, ensuring that the environment is always focusing on the most up-to-date threats. "It is extremely difficult for user companies to gather information on their own, so being able to tap into the knowledge of experts around the world is a tremendous boon," says Sato with a smile.

Even as the number of services to be monitored increases in the future, Taegis XDR's openness will make it possible to respond effectively.

> **"We have already established a substantial level of security. We needed to ensure that we were adapting our defenses with the threat landscape. That's where we believe Taegis will really help us in the future."**

Kenta Sato

CSIRT Group/Information Security Management Group. Information Security Department Technology Division. **Sansan, Inc.**

Secureworks®
a **SOPHOS** company

Secureworks, a Sophos company, is a global cybersecurity leader that protects customer progress with Taegis™, an AI-native security analytics platform built on more than 20 years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist.
secureworks.com