CASE STUDY

NTT DATA

NTT DATA Global Solutions Improves Security Operations Productivity with Stellar Cyber Open XDR Platform

NTT DATA Global Solutions Corporation, the core company of NTT DATA's SAP business within the NTT DATA group of companies in Japan, has significantly improved the productivity of its security operations by utilizing the Stellar Cyber Open XDR platform. The company was looking for an NDR solution that could analyze data from its mission-critical network, and decided to trial Stellar Cyber in order to send log data from the various products it uses into the platform to see what it could analyze. After deciding to implement the Stellar Cyber platform, NTT data could detect far more cybersecurity issues throughout its infrastructure and its analysts became far more productive.

"We can easily see how many detections occur in a day, and we can see the overall picture," said Junichiro Baba, Manager, IT Strategy & Management Group, Business Strategy Promotion Department, NTT Data Global Solutions, Inc.

NTT DATA

> "Stellar Cyber collects network, PC operation, antivirus, and EDR logs in one place, allowing us to detect and understand signs and trends in real time that something might be wrong or about to happen."
>
> *– Junichiro Baba, Manager, IT Strategy & Management Group, Business Strategy Promotion Department, NTT Data Global Solutions, Inc.*

Before:

Lack of Visibility

It was nearly impossible to see where and how threats were affecting the environment.

Expertise

Threat identification requires the skills and experience of experts, and learning how to use and manage it has not been easy.

With **Stellar Cyber**:

Open XDR

Information from multiple threat vectors can now be aggregated on a single screen for quick threat recognition.

Automation

Improved efficiency by enabling automated threat hunting and application of response actions.

Ease of Use

Stellar Cyber is intuitive and easy to use, allowing even inexperienced personnel to respond quickly.

> "We can easily see how many detections have occurred in a day, and we can see the overall picture. It is also nice to be able to see activity at a glance."

> “Stellar Cyber integrates with so many products that when companies are looking to implement a new third-party product, they can likely choose from the list of integrated products that Stellar Cyber supports.

NTT DATA Global Solutions began operating Stellar Cyber in March 2022, and in March 2023, it expanded the amount of data on Stellar Cyber, thereby expanding the scope of its use.

The company is using the Stellar Cyber Open XDR platform for the security operations of its mission critical systems. Stellar Cyber analyzes packet information flowing on the mission-critical network, collecting operation information from clients and log information running on various servers.

The current deployment configuration deploys Stellar Cyber on Microsoft Azure and sends log data from integrated NW-F/W; NG-SW analysis is performed.

Before implementing Stellar Cyber, the company was looking for an NDR that could analyze the extremely large amount of data between IaaS and SaaS in its mission-critical network. After considering other network monitoring products, the company decided to implement the Stellar Cyber Open XDR platform because it could collect log data from various products, analyze the data, and show what to do next.

Stellar Cyber's ability to analyze multiple products across the enterprise in real time, to monitor with only a few people, and to meet real-time, 24/7 requirements were key factors in the decision to implement the system.

"The fact that Stellar Cyber could analyze multiple products across the board in real time, could be monitored by just a few people, and met our requirements for real-time, 24/7 response was a major deciding factor in our decision to implement the system," said Baba. "The real-time capability was also very important to the company from the standpoint of minimizing the risk of contamination in the event of an incident."

The benefits of Stellar Cyber are as follows, Baba stated: "Firewalls and other products can generate alerts based on human-determined thresholds, but it is difficult to determine when something might be suspicious. Stellar Cyber collects network, PC operation, anti-virus, and EDR logs in one place, giving us the real-time ability to detect and understand signs and trends that show something might be fishy or about to happen."

Baba added, "We use a terminal asset management tool to obtain PC operation logs. We used to look at the logs of the terminal asset management tool whenever something happened. After installing Stellar Cyber, real-time detection was achieved and the number of false positives decreased. The overall picture, including how many detections occur in a day, is easy to see at a glance. The system is also very easy to use and required minimal training before analysts became more productive."

The company is also actively using Stellar Cyber's dashboard, Baba mentioned. "The Stellar Cyber dashboard is very easy to understand. I can see at a glance where it is coming from, where it is going to, and what is going on. The information (IP address, device name, domain name, path, protocol, etc.) is presented in an easy-to-understand visual manner. It also automatically calculates a risk score that indicates the degree of danger and the reason for the detection. I can quickly get the information I need by just looking at the dashboard."

The company is also considering opening its dashboard to the general public as an educational activity to raise security awareness.

Stellar Cyber Open XDR platform delivers comprehensive, unified security without complexity, empowering lean security teams of any skill to successfully secure their environments. With Stellar Cyber, organizations reduce risk with early and precise identification and remediation of threats while slashing costs, retaining investments in existing tools, and improving analyst productivity, delivering an 8X improvement in MTTD and a 20X improvement in MTTR. The company is based in Silicon Valley. For more information, visit https://stellarcyber.ai.