splunk> a CISCO company

CUSTOMER STORY

NEC Revamps Security Culture and Cuts Ransomware Risks by Over 80%

Key Challenges

To accelerate digital transformation in concert with its management plan, NEC had to raise employee cybersecurity awareness and give everyone, not just experts, visibility into the security posture.

Key Results

Splunk dashboards visualize cyber threats and drive cultural change, which not only boosts employee engagement and third-party evaluation scores, but also effectively mitigates ransomware risks.

Orchestrating a brighter world

NEC

Industry: Manufacturing

Solutions: Security

Product: Splunk Enterprise Platform

Boosting security culture with authentic visibility for everyone.

NEC, a multinational information technology and electronics corporation that is headquartered in Japan, is continuing to innovate for the future especially through its NEC's 2025 mid-term management plan. To achieve the goals outlined in this plan, NEC needed to foster a data-driven transformation of security culture with speed and agility.

At NEC, more than 270,000 endpoints generate 1TB logs per day. "Our business targets the aerospace and defense industries, which are prime targets for cyberattacks," says Takeo Tagami, head of the General CISO Office, Corporate IT and Digital Department at NEC. "Therefore, we need an environment where logs are collected and analyzed swiftly to detect and address potential attacks."

NEC needed a way for all managers and staff to have full visibility into the massive volumes of security logs, so everyone could monitor security risks. "We look to raise the awareness of individuals so that they can take proper actions, obtain advanced intelligence to safeguard against cyberattacks, and bolster resilience to enable early detection, action, and recovery," Takeo explains. "We were looking for a way to create dashboards that everybody can view." It turned out that Splunk fits its needs exactly.

Outcomes

120K
internal users are now able to monitor security risks and posture

80%
reduction in ransomware risks

2 awards
won by NEC through innovating with Splunk

Embracing enterprise-wide observability through data-driven transformation

After centralizing log management on Splunk Enterprise, NEC can flexibly turn log data into actionable insights for sharing across the group. The constantly updated information is visualized on two types of Splunk dashboards, which target security threats and risks, respectively. Within Splunk Enterprise, the Dashboard Studio feature adds extra value, which lets NEC customize dashboard layouts to allow all internal and external stakeholders, tech-savvy or not, to view security-related information at a glance.

As security log analysis is no longer limited to a small number of security experts, NEC can now raise security awareness among all 120,000 employees – from new hires to top management, and outside directors and stockholders, while improving security management through a plan-do-check-act cycle. External information like third-party evaluations, threat intelligence, attack diagnoses, and urgent risk investigation are also available through application programming interfaces. The dashboards even display security-related news summarized with generative artificial intelligence and allows the management to get first-hand information before talking to the media.

"Before using Splunk, we tried to raise security awareness through web-based training, but cyber risks were invisible to the naked eye," says Tagami. "We chose Splunk not only because it has served us for a decade, but also because Splunk Enterprise offers full security visibility and optimizes our security culture." In only a year's time, NEC has extended the use of Splunk Dashboards to support 76 functions at 25 sites, covering Asia-Pacific and other regions, as well as research labs in Europe.

> Splunk Enterprise dashboards visualize risks and threats and transform our security culture, which largely improves our third-party evaluation scores and reduces our ransomware risks to one sixth-of the previous levels."
>
> **Takeo Tagami,** Head of General CISO Office, Corporate IT and Digital Department, NEC

Maximizing engagement and third-party scores, minimizing ransomware risks

Splunk Enterprise has created many quantifiable benefits for NEC. In a group-wide survey, 96 percent of participants responded that they have improved their security awareness. The stronger security culture even generates real gains in cybersecurity, with NEC's ransomware risks dropping to one-sixth of the original level, representing a more than 80% reduction. There are also significant boosts in third-party evaluation scores. Moreover, the engagement score of NEC's General CISO Office is now double, and already close to 50% of the target set in its midterm management plan 2025.

With Splunk, NEC is also able to optimize user experience. "User interface design was a challenge to us," says Tagami. "By using Splunk Enterprise and Splunk Dashboard Studio, and teaming up with excellent designers, we now create dashboards highly acclaimed by top management."

The project was recognized internally and has received the NEC Best Value Award (President's Award). Externally, it won an award of IT excellence at the Information Technology Awards organized by the Japan Institute of Information Technology.

Enhanced digital agility brings new opportunities

What Splunk offers NEC is not only a solution, but also true digital agility that opens up a world of unlimited possibilities. For example, the combined use of the Dashboard Studio and Classic Dashboards in Splunk Enterprise, and the versatile set of Splunk tools, allows NEC to tailor the dashboard design. Splunk Community has also provided a wealth of knowledge that helps NEC derive maximum value from its Splunk Enterprise deployment.

Moving forward, NEC plans to further sharpen its attack diagnosis capabilities by working with the Cyber Defense Institute. They plan to use AI automation to develop labor-efficient ways for risk assessment while enhancing non-rule-based detection. Apart from risk evaluation, cybersecurity management governance will also be a focus.

"We are building a framework for comprehensive scoring at the management level, on how well different companies, including overseas ones, are managing cyber risks," says Tagami. "We need a new dashboard to visualize the unique performance of each company and its KPIs."

24-576649 -Splunk-NEC-CS-106