VECTRA

CASE STUDY

Ricoh Co. Ltd. Achieves Real-time monitoring of 100,000 units to detect threats in advance

The need for network visibility after WannaCry

These days, ransomware and other types of malicious threats are always top-of-mind for security teams—especially after seeing the attack challenge organizations face, including WannaCry in 2017. Of course, the words "WannaCry ransomware attack" are etched into the memories of security professionals worldwide, which is certainly the case for the Ricoh Group, located in Japan, where the attack hit a little too close to home.

So close in fact that this leading provider of print and imaging solutions found themselves up against the clock as WannaCry was trying to go to work on Ricoh's systems. It was then that the Computer Security Incident Response Team (CSIRT) knew they needed to act quickly in their approach to ensure customers wouldn't be impacted by the attack. Atsushi Sato, a member of the company's CSIRT team, explains the situation during the time of the attack.

"The ransomware attack was detected on the endpoint, but over time, the number of alerts informing us about the attack increased rapidly. Therefore, when we analyzed the logs of security devices installed on the network boundary, we found that the amount of traffic going out to the internet was increasing rapidly," he said.

> "The ransomware attack was detected on the endpoint, but over time, the number of alerts informing us about the attack increased rapidly."
>
> **Atsushi Sato**
> *CSIRT Team Member*
> *Ricoh*

RICOH

Organization

Ricoh Co. Ltd.

Industry

Manufacturing

Challenge

Lack of visibility in internal network and early detection of threats

Results

- Threat intelligence to detect previously unknown threats
- Moved from a reaction approach to a proactive security process
- Now has visibility into the use of these cloud services and virtual PCs in their network

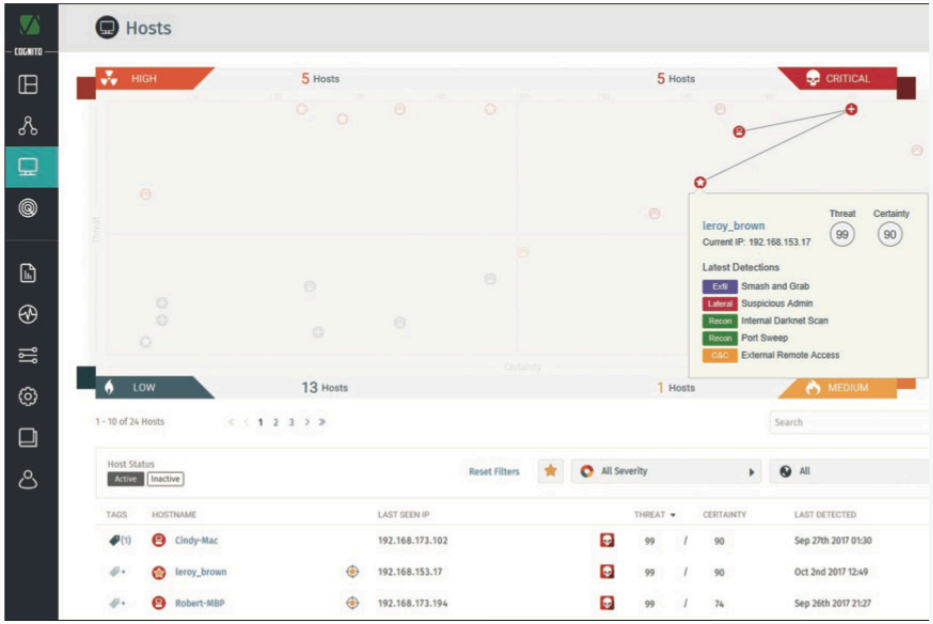
In order to find out what was happening, CSIRT members matched the endpoint information with the network boundary log and analyzed it. “I tried, but I couldn’t figure out what was happening inside the network from these two pieces of information. Therefore, it took a lot of time to realize what was happening. From this experience, I reaffirmed the importance of visibility in the internal network,” Sato recalls.

Prioritized alerts and easy reporting lead the way

After the incident, The Ricoh Group was provided help from the security experts at Nissho Electronics, who proposed Vectra, the leading AI-driven threat detection and response platform. Vectra would be able to help capture data across Ricoh’s workloads and then surface and prioritize any threats that exist.

“Detected events are plotted on two axes, certainty and threat level, and when they are detected, their priorities are clear. It works for several analysts.”

Kazuki Ohara
Security Strategy Group and Security Management Department Ricoh



“My first impression was that my reporting capabilities were excellent,” said Mr. Sato, who was able to prioritize threats without creating rules. “Especially reconnaissance after the invasion of malware. I also highly appreciated the ability to detect and visualize movements in each attack phase, specifically internal expansion.”

Kazuki Ohara, Security Strategy Group and Security Management Department also noted, “I found the dashboard to be very clear and straightforward. Detected events are plotted on two axes, certainty and threat level, and when they are detected, their priorities are clear. It works for several analysts.”

After a three-month trial period, The Ricoh Group selected Vectra AI as their network detection and response solution. “Over the course of about half a year, we have built a system that allows us to supervise the network, which is connected to about 20,000 terminals centered on the five major bases, in real time,” Ohara notes.

A Proactive approach to In-house IT threats, CSIRT activities and Shadow IT / virtual PC

With the Vectra platform deployed, activities of the CSIRT that were previously hidden, were now easily visible in the company network. This is because Vectra is able to capture the right data with the right context, creating a view of activity across the entire enterprise.

Mr. Sato explains that "in the past, there were many post-incident responses, but now that the internal network is visible, we are now proactive when detecting signs that lead to incidents at an early stage and consider countermeasures." Some unexpected issues began to emerge, including Shadow IT and virtual PCs.

An important detail as the Ricoh Group prohibits the use of cloud services for individual contracts. To address virtual PCs, multiple virtual PCs are created in The Ricoh Group development department, which are then used on physical PCs for verification of the software being developed. Without the Vectra platform, the use of these cloud services and virtual PCs would have never surfaced.

In response to these issues, Mr. Ohara said, "currently, we are clarifying the actual conditions of shadow IT and virtual PCs and are considering countermeasures such as detailed CASB settings and reorganization of internal rules."

Strengthening security with Vectra AI

"Cybersecurity teams want to focus on activities that aggregate and accumulate information on incidents that have occurred inside and outside the organization and want to implement comprehensive measures, so efficient detection and response is important for the future. For that reason," said Sato.

After a successful deployment, Mr. Ohara has the next steps in order. He said, "we are also considering creating our own dashboard by linking multiple solutions using the API provided in Vectra. Events detected by each security product such as IPS and Endpoint are associated with each other. We are thinking of conducting a multifaceted analysis of threats."

Now with the effective functionality, visibility, and AI-driven threat detection in place to stop threats like ransomware before they start, The Ricoh Group is well setup to remain resilient against today's attacks now and in the future.

> "We are now proactive when detecting signs that lead to incidents at an early stage and consider countermeasures."
>
> **Atsushi Sato**
> *CSIRT Team Member*
> *Ricoh*

For more information please contact us:
Email: info@vectra.ai | vectra.ai