Maebashi Red Cross Hospital

Harnessing the Power of AI for Analysis, Detection, Scoring, and Automated Response to Ensure Uninterrupted Healthcare

As cyberattacks increasingly disrupted hospital operations, Maebashi Red Cross Hospital has worked to strengthen its cybersecurity. The hospital implemented Cisco XDR, a solution that correlates diverse data and detects behavioral anomalies. While dealing with the limitations of medical systems and organizational challenges, the hospital achieved robust security through AI-based advanced threat detection and automation.

Maebashi Red Cross Hospital

Location
389-1 Asakura-machi, Maebashi City, Gunma Prefecture

Establishment
23 March 1913

Number of beds
555 (527 General Beds, 6 Class 2 Infectious Disease Beds, 22 Psychiatric Beds)

The Maebashi Red Cross Hospital was built with the philosophy of "becoming a caring and reliable hospital for all." It is the only designated Advanced Critical Care Center in Gunma Prefecture and serves as a central emergency hub in the event of major disasters in the Kanto Region. The hospital has an exceptional emergency care capacity, including 72 beds for critical patients, of which 24 are in the ICU, and its entire facility is designed to function as an emergency ward during crises.

Challenges

- Increasing incidents of medical operations being halted by cyberattacks
- Medical systems and equipment often have limitations on having security software installed
- Need to strengthen cybersecurity measures with limited staff

Solution

- Implemented Cisco XDR to monitor and detect abnormal behavior in real time
- Enables behavior detection without modifying endpoints
- Expectation of AI to support and automate security operations

Results

- Achieved uninterrupted healthcare through a new security system focused on early incident detection
- Staff can focus on high-priority incidents based on AI-driven scoring
- Automatically generated backup data provides both operational and psychological support for staff

The Future

- Plan to include endpoints in monitoring for more integrated observation and correlation analysis
- Intend to share insights with other hospitals to help strengthen cybersecurity across the medical industry

"If we get compromised after all of this, it would be hard to prevent with any other measure. That is our wholehearted perspective."

Minoru Nakano
Maebashi Red Cross Hospital
Hospital

Challenges

Constraints of Medical Systems and Equipment, in Addition to Limited Resources, Present Challenges

For Maebashi Red Cross Hospital, which carries significant social responsibility, ensuring that medical services never stop is a crucial mission. The hospital has implemented multiple initiatives toward that goal, one of which is strengthening cybersecurity. "While we knew the risk of cyberattacks was present for hospitals before, around 2020, a series of hospital shutdown caused by cyberattacks highlighted just how serious this risk truly is," says Minoru Nakano from Maebashi Red Cross Hospital.

In response, the hospital undertook a major review of its security systems. The hospital focused particularly on ransomware countermeasures and on securing the remote maintenance connections used by vendors when servicing systems and equipment.

However, several challenges came to light during the overhaul. The first issue was the restrictions inherent to medical systems and equipment. "As is widely known, due to legal and warranty restraints, we cannot install security software on medical systems and equipment," explains Eiji Ichinei of Maebashi Red Cross Hospital. "We also face challenges with remote maintenance connections. We require vendors to submit advance requests and device information, and to use lines prepared by the hospital. however, for some systems and equipment, operational constraints force us to allow exceptions," says Ichinei.

There were also organizational challenges. Security talent is said to be scarce nationwide, and because systems and devices have long run on closed networks, the medical field has considered security risk low, which has delayed the development of talent and organizational structures. "Our IT department has seven members, of whom three handle networks and security. Compared to other hospitals of similar size, this may be relatively robust, but as Ransomware as a Service (RaaS) shows, attacks are organized and increasingly sophisticated. With this staffing alone, it is extremely difficult to track exploited vulnerabilities and understand the function of each countermeasure and handle daily security monitoring, alert response, log analysis and root-cause identification during incidents, and remediation smoothly," says Ichinei. He continues, "I have some experience in networks and applications myself, but I still feel I lack the skills to analyze logs from a security perspective."

Behavior-based detection that works even in hospitals with system and device constraints

Solution

Expectations for AI-Driven Security and Automation

What is the most optimal way to strengthen security while addressing these challenges? The hospital conducted research and compared multiple approaches. Ultimately, they decided to implement Cisco XDR (Extended Detection and Response).

Ransomware can steal admin privileges to attack from within, spawn many variants, and abuse legitimate OS functions, which makes signature-based or perimeter-only defenses insufficient. Measures that monitor and detect abnormal behavior in real time are effective.

Cisco XDR centrally collects diverse data from networks, endpoints, cloud, email, IDs, and applications, then visualizes and correlates it to detect abnormal behavior. "There is also Endpoint Detection and Response (EDR), but it often requires installing agents on PCs and servers, which is difficult to apply to medical systems and devices. By contrast, Cisco XDR has Network Detection and Response (NDR) capabilities that detect spikes in traffic, internal scans, and unknown C2 communications through network flows without altering endpoints," says Ichinei. He adds, "We judged it optimal for behavior detection in a hospital environment."

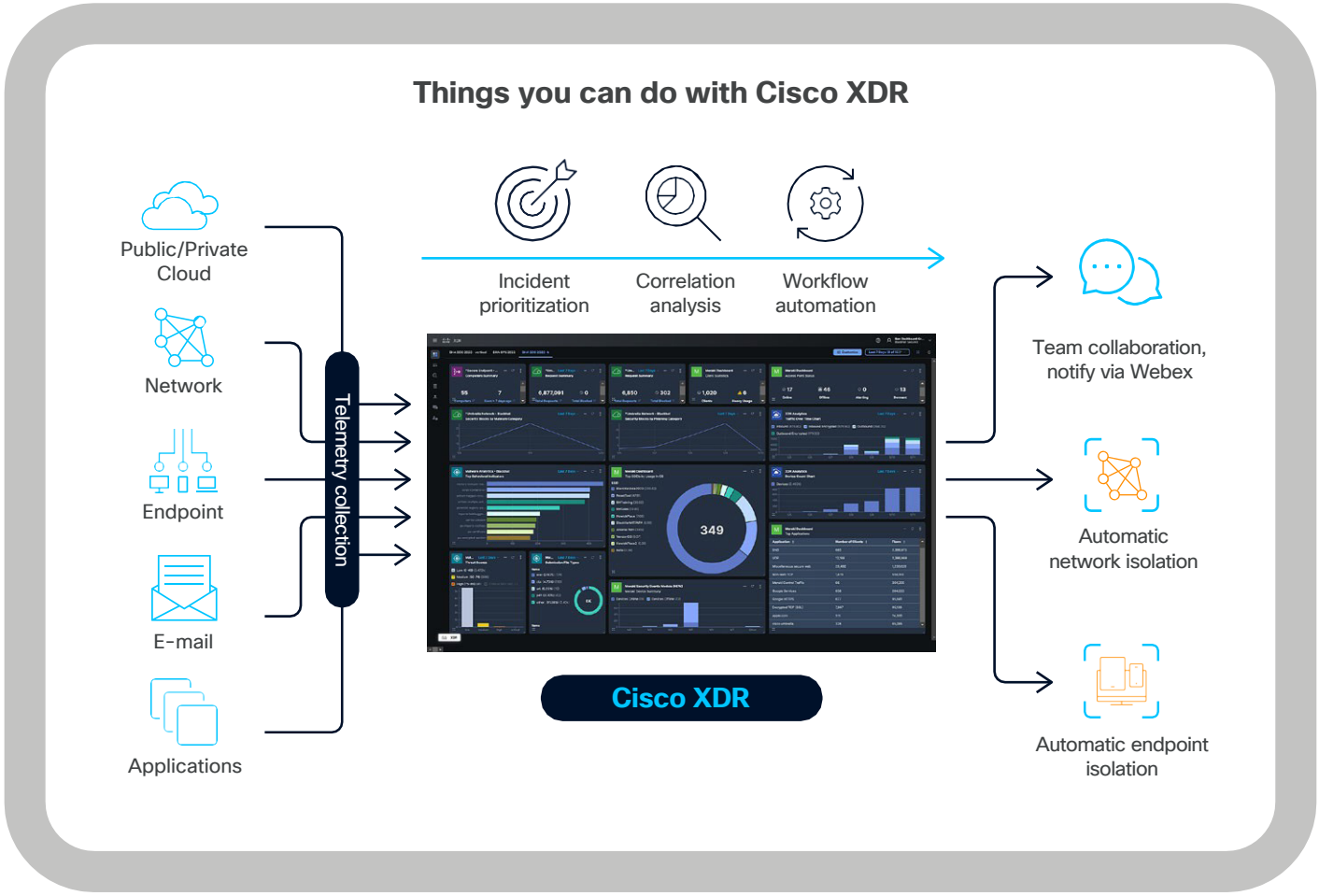
Cisco XDR also offered a solution to organizational limitations.

Although the team and skills are still developing, the hospital plans to eventually operate its own Security Operation Center (SOC). Even if part of the operation is outsourced, the hospital intends to retain control and issue clear directives. In doing so, they expect Cisco XDR's automation and AI-driven security management to provide key support.

Specifically, Cisco XDR uses AI infused with insights from Cisco's threat intelligence team, Talos, to automatically perform investigations such as log analysis, validation, risk scoring, and proposing appropriate responses, supporting security staff. "Incidents are scored between 1 and 1,000 based on their level of risk. This prevents staff from being overwhelmed by alerts, allowing them to focus on the most urgent incidents," says Ichinei.

Using the playbook feature called automation, it is also possible to automate actions such as endpoint isolation, IP blocking, and account deactivation. Moreover, automated actions can integrate not only with Cisco products but also with third-party systems.

"We valued not only integration among Cisco products, such as automatically notifying staff via Webex when an incident is detected, but also the ability to integrate with third-party products. During our research, many vendors advised that 'multilayer defense using multiple products is important,' yet when we continued the discussion they proposed adopting multiple products from their own line and said they could not integrate with other vendors' products. That would severely narrow our choices. By contrast, Cisco XDR does not confine us to Cisco products, gives us broader options, and helps us leverage existing assets," says Ichinei.



Results and the Future

Automatic Backup Generation upon Incident Detection

Physically, the hospital's network is unified, while the medical network centered on electronic medical records and the internet-facing network are logically segmented with VLANs. Currently, Cisco XDR collects NetFlow information from about 150 network switches that make up this network and performs incident visualization and correlation analysis. "Even if a remote maintenance connection were misused, early detection through behavioral analysis allows us to act quickly to minimize damage. Due to the aforementioned constraints of medical systems and devices, we are not doing this now, but once the environment is ready, we are considering aggregating endpoint information to Cisco XDR for more integrated monitoring and correlation analysis," elaborates Ichinei.

The hospital also makes active use of automation for response handling. For example, the hospital implemented automation linking Cohesity DataProtect, Cisco's immutable backup system used for ransomware countermeasures, with Cisco XDR. When Cisco XDR detects an incident, Cohesity DataProtect immediately generates a backup.

"If a backup is automatically created at the time of an incident, staff can immediately begin assessing the scope and identifying the cause. Having that backup serves as a safety net, allowing them to respond calmly. We believe the automation of Cisco XDR and Cohesity DataProtect benefits not just speed but also the team's peace of mind," says Ichinei.

After introducing Cisco XDR, the hospital revised its IT business continuity plan (IT-BCP) to emphasize training for immediate post-detection response rather than recovery after a system shutdown. They have also organized their CSIRT into a Small CSIRT, which activates at incident detection, and a Large CSIRT , which handles response when major damage actually occurs. "There is no doubt that cybersecurity enhancement is essential to prevent medical disruptions.

But it is equally true that our core mission is to provide care," says Minoru Nakano. "We cannot assign too many people to security alone. Achieving advanced security without greatly increasing the staff's workload is a major achievement. If we were to fall victim to ransomware even after this, it would be difficult to avoid it with any other product. That is our evaluation, shared by leadership," emphasizes Nakano.

Going forward, Maebashi Red Cross Hospital will continue to base its security operations on Cisco XDR as it strives to deliver uninterrupted healthcare. They also view the challenges of medical systems and devices, staffing, and organizational structure as common across many hospitals and intend to contribute to raising security across the industry by sharing their experience and insights.

Maebashi Red Cross Hospital
Hospital Director
Minoru Nakano

Maebashi Red Cross Hospital
Administration Department
Information Systems Section Chief
Eiji Ichinei

前橋赤十字病院
Japanese Red Cross Maebashi Hospital

Since its opening in 1913, the hospital has continually evolved and changed to meet the needs of the times. Presently, it contributes to medicine in the region as an AIDS treatment center, a core disaster medical hospital, an advanced critical care center, a regional medical care support hospital, a regional cancer treatment center, a hospital with an air ambulance heliport, a higher brain dysfunction support organization and a regional perinatal medical center. URL: https://www.maebashi.jrc.or.jp/

Products and services

- Cisco XDR

2509-1-HC