NOZOMI NETWORKS | KONKUK UNIVERSITY MEDICAL CENTER

CASE STUDY

Konkuk University Hospital Strengthens Their Security and Collaboration

About the Customer

Konkuk University Hospital

Konkuk University Hospital is committed to high-level treatment, education, and research in accordance with the founding spirit of 'Guryojemin (救療濟民)', which means 'saving and benefiting people through treatment'. It is faithfully fulfilling its role as a representative general hospital in Korea whose top priority is the health of the community and the safety and happiness of patients and their families. In addition, it is leading the way in providing reliable medical services through advanced medical information technology and medical security.

The Challenge

How Can a Top Korean Hospital Protect Itself from the Rise in Cyber Threats?

Konkuk University Hospital has the best medical staff in Korea, cutting-edge medical equipment, a top-notch medical computerization system, and contributes to the development of personalized and precision medicine research by fostering excellent medical personnel. With the rise in cyber threats on medical institutions that hold large amounts of sensitive personal and medical information, Konkuk University Hospital needed to improve its level of security and ability to detect and respond to cyber threats.

Han Ki-tae, CIO and Head of the Medical Information Team at Konkuk University Hospital said, “It is easy to think that medical systems are safe because they are connected to an internal network that is not connected to the outside, but there are still various threats that could be introduced.” He continued, “For example, PCs that manage medical devices can be connected to the outside, and many of these PCs are equipped with OSs that are no longer supported. In addition, unidentified assets and vulnerabilities can cause damage at any time.”

Company Profile

Industry: Healthcare

Employees: <1,000

Location: Korea

Challenges

1. Identifying assets and analyzing traffic
2. Detecting and responding to cyber threats
3. The need for an integrated IT-OT security control system

Results

1. Enhanced security
2. Seamless collaboration across multiple organizations
3. Accurate threat detection and response

The Need for IT-OT Integrated Security in the Healthcare Industry

The Search for the Right Solution

Konkuk University Hospital began with a hospital-wide network security diagnosis, which resulted in the medical information team concluding that it was urgent to introduce an OT security solution that could identify and analyze medical devices and CCTV packets that could not be analyzed by network and security organizations and detect abnormal behavior.

“Since healthcare security requires expertise from both IT and OT, IT-OT integrated security is essential” says Ki-tae. Konkuk University Hospital set out to find an IT-OT integrated security control system that met all their needs.

The most important thing that Konkuk University Hospital needed in a solution was the ability to identify assets used in the hospital environment and analyze traffic. It was also important that the solution provided an easy-to-manage environment so that the medical information team and the biomedical engineering team could collaborate smoothly.

The medical information team began comparing solutions and conducting POCs. Some solutions did not have information about connected devices, making it impossible to know which device generated the malicious traffic and to identify the root cause. Other solutions had limitations in terms of ease of management. In the end, Konkuk University Hospital found that the Nozomi Networks platform met all their needs.

Using Nozomi Networks Vantage, a cloud-based OT security solution, Konkuk University Hospital can determine the devices connected to the network, create zones by role, and easily apply protection and management policies. Its excellent visualization function makes it easy for IT organizations without OT security expertise to manage it.

> “To prevent threats that may arise while providing advanced medical services, a solution that provides real-time protection through the cloud is necessary. Nozomi Networks Vantage uses global intelligence to respond to attacks targeting medical institutions in near real-time.”
>
> **Han Ki-tae**
>
> ***CIO and Head of the Medical Information Team, Konkuk University Hospital***

Introducing an OT Security Solution Optimized for Medical Institutions

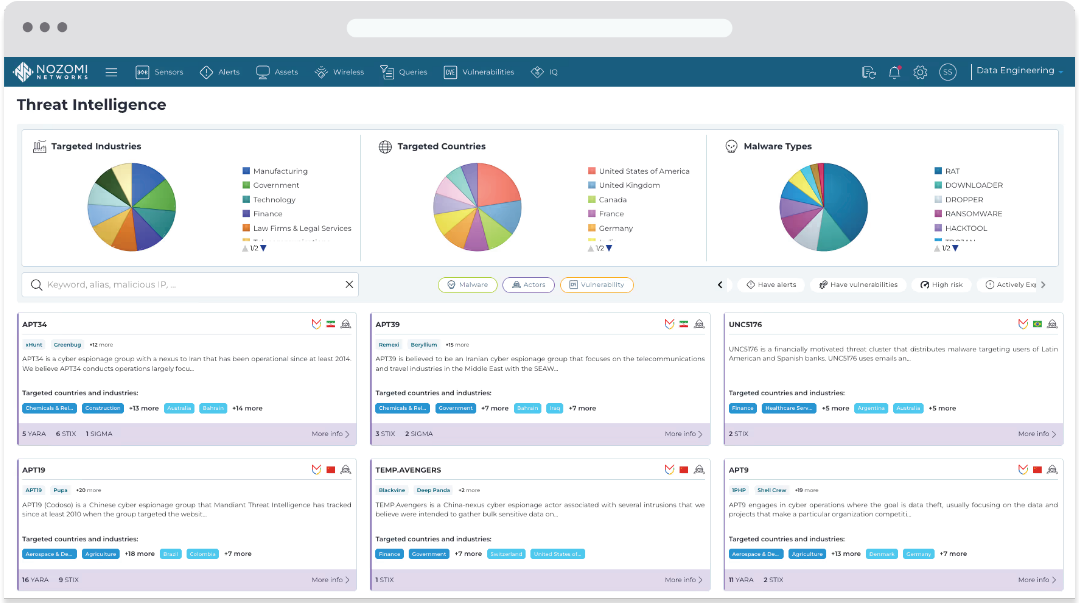
Responding Quickly to the Latest Threats Through the Cloud

Konkuk University Hospital is the first security-sensitive general hospital in Korea to implement a cloud-based OT security solution. Typically, medical institutions are cloud-adverse, but the medical information team at Konkuk University Hospital decided that in order to be able to respond to threats immediately, a cloud-based security solution is necessary.

OT security solutions that are built with external connections disconnected cannot update the latest threats in real time. They download what they learn from the cloud to a separate medium and apply it to the OT security solution, increasing the workload of administrators and management complexity, which has many limitations in the process of identifying and responding to sophisticated and intelligent threats.

Nozomi Networks Vantage is purpose-built to help customers overcome these challenges by running on Amazon Web Services (AWS). By leveraging key AWS services such as Elastic Kubernetes Service, EC2, and Amazon RDS, Vantage provides the scalability and simplicity required to manage the complex security environment faced by hospital systems.

“To prevent threats that may arise while providing advanced medical services, a solution that provides real-time protection through the cloud is necessary” says Ki-tae. He continues, “Nozomi Networks Vantage uses global intelligence to respond to attacks targeting medical institutions in near real-time. Vantage only processes traffic for analysis in the cloud and does not take any data, so there is no concern about data leakage, you can use it with confidence.”



APT34

xHunt Greenbug +12 more

APT34 is a cyber espionage group with a nexus to Iran that has been operational since at least 2014. We believe APT34 conducts operations largely focu...

Targeted countries and industries:

Chemicals & Rel... Construction +13 more Australia Bahrain +14 more

5 YARA 6 STIX 1 SIGMA More info

APT39

Remexi Beryllium +15 more

APT39 is believed to be an Iranian cyber espionage group that focuses on the telecommunications and travel industries in the Middle East with the SEAW...

Targeted countries and industries:

Chemicals & Rel... Government +7 more Bahrain Iraq +7 more

3 STIX 2 SIGMA More info

UNC5176

UNC5176 is a financially motivated threat cluster that distributes malware targeting users of Latin American and Spanish banks. UNC5176 uses emails an...

Targeted countries and industries:

Finance Healthcare Serv... +5 more Argentina Australia +5 more

2 STIX More info

APT19

APT19 Pupa +20 more

APT19 (Codoso) is a Chinese cyber espionage group that Mandiant Threat Intelligence has tracked since at least 2010 when the group targeted the websit...

Targeted countries and industries:

Aerospace & De... Agriculture +18 more Brazil Colombia +7 more

16 YARA 9 STIX More info

TEMP.AVENGERS

Blackvine Deep Panda +2 more

TEMP.Avengers is a China-nexus cyber espionage actor associated with several intrusions that we believe were intended to gather bulk sensitive data on...

Targeted countries and industries:

Finance Government +7 more Switzerland United States of...

1 STIX More info

APT9

1PHP Shell Crew +19 more

APT9 engages in cyber operations where the goal is data theft, usually focusing on the data and projects that make a particular organization competiti...

Targeted countries and industries:

Aerospace & De... Agriculture +13 more Denmark Germany +7 more

11 YARA 2 STIX More info

Within Vantage, Nozomi Networks users are able to quickly identify threats to their OT and IoT environments.

Strengthening Medical Security with IT-OT Integrated Security Control

Accurate Threat Detection and Response

With Vantage and its use of industry-specific and regional intelligence, Konkuk University Hospital is able to accurately assess threats and respond without false or misleading detections. Even network and security teams without OT expertise are able to identify the type and impact of threats and take action.

"When an alert is triggered in Vantage, the medical information team and biomedical engineering team can immediately check and resolve it," said Ki-tae. "The Vantage management environment uses intuitive visualization technology to enable seamless collaboration across multiple organizations. Even non-expert managers can take immediate action."

Reducing the Workload of the IT Organization

He added, "Konkuk University Hospital is investing heavily in IT and security, but it is difficult to be confident that we have enough dedicated personnel. That is why it is important that we have a solution that can accurately report breaches and abnormal behavior without noise and guide necessary actions while reducing the workload of the IT organization. Vantage is excellent in this regard."

The Medical Information Team of Konkuk University Hospital plans to actively promote cloud-based OT security solutions, introduce the strengths of Konkuk University Hospital's reliable medical services, and help attract security investments from other medical institutions.

> "The Vantage management environment uses intuitive visualization technology to enable seamless collaboration across multiple organizations. Even non-expert managers can take immediate action."
>
> **Han Ki-tae**
>
> ***CIO and Head of the Medical Information Team, Konkuk University Hospital***

Nozomi Networks protects the world's critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI powered analysis for faster, more effective incident response. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NOZOMI NETWORKS

nozominetworks.com