Using Cisco security services for IoT open platform development

FANUC Corporation is a leading company that provides factory automation (CNC, robots, and robomachines) to the global market. This time, they will be utilizing Cisco® security consulting services while developing the Internet of Things (IoT) platform FANUC Intelligent Edge Link and Drive (FIELD) system and providing services. In addition to verifying and establishing the robustness of these products and services, they have also formulated security guidelines for implementing companies.

Business Challenge:
• Safe and secure IoT open platforms must be provided to customers.

Network Solution:
• FANUC Corporation tested the vulnerabilities of the products and services and then established robustness and formulated security guidelines through support from the Cisco security consulting services team.

Business Results:
• FANUC Corporation strengthened their cooperation with Cisco to continue improving services and providing them globally.

Customer name
FANUC Corporation

Industry
Manufacturing factory automation (FA) and research, development, manufacturing, distribution, and maintenance services for robots and robomachine products

Location
Oshino-Mura, Yamanashi Prefecture

Number of employees
6,738 people (as of late March 2017)
FANUC Corporation, whose headquarters are located at the base of Mt. Fuji, is the world’s most innovative manufacturer of the CNCs, robots, and robomachines needed for factory automation. It is a global leader. As per its slogan “Service First,” it has been providing world-class service and support to customers in 107 countries from over 260 service locations since its launch in 1972.

The FIELD system, whose service operations began in Japan on October 2, 2017, is an IoT platform that provides CNC machine tools, robots, industrial machinery, peripheral devices, and advanced analytics for sensors, all of which are used with automation systems. By introducing the FIELD system, end users can improve the overall equipment efficiency and rate of return by improving machine productivity, reliability, quality, flexibility, and speed. Sensors and peripheral device manufacturers as well as system integrators can provide solutions to improve equipment efficiency, output, and quality. Our company collaborated with several domestic and international manufacturers, including Cisco, in order to provide complete solutions, including network and computing infrastructures, applications, and middleware platforms during FIELD system development.

As FANUC Corporation Senior Managing Executive Director and FIELD Headquarters Director Shunsuke Matsubara said, “Ever since our company’s founding, we have continued to make efforts towards the automation and rationalization of the machines utilized at manufacturing sites. In addition, IoT, such as the German industry 4.0, is receiving a lot of attention in various countries around the world, but we began planning and development for the FIELD system about 3 years ago and began service operations in Japan in October 2017. The responses from market have been huge, and we are receiving a large number of inquiries.”

FANUC Corporation
Senior Managing Executive Director
Research General Headquarters
FIELD Headquarters Director
Shunsuke Matsubara

“The IoT platform requires good reliability so that the production line never stops. Through collaboration with Cisco, our knowledge of networks and security deepened, allowing us to provide safe and secure services.”

Shunsuke Matsubara
FANUC Corporation
Senior Managing Executive Director and FIELD Headquarters Director
Business Challenge: Our company positioned the FIELD system with the IoT open platform and aimed not only to connect our company’s machines across generations, but also to be able to integrally manage other companies’ production equipment within customers’ factories. During that time, measures related to networks and security became an issue. As Matsubara said, “Due to increases in the number of cybersecurity attacks targeting the manufacturing industry, there have actually been incidents where production lines within Japan were stopped as well. The FIELD system connects to various devices through a network. It not only reads and analyzes data, but also controls devices. The fact that it controls is the biggest difference compared to other IoT solutions. Having a production line stop due to a security incident is something we definitely cannot allow. So, we started a project with Cisco in order to increase our knowledge of networks and security and to provide robust products and services. In the past, FANUC and Cisco have successfully collaborated to provide IoT solutions to large corporations in the North American market. FANUC regards Cisco as a global leader that promotes digitalization through IT usage. Even its own IT infrastructure utilizes many Cisco devices, so it is considered reliable. The project has two main goals. The first is to improve the safety and toughness of the FIELD system itself. The other is to formulate security guidelines in order for customers to safely introduce the FIELD system.”

We look forward to Cisco’s network and security knowledge and global support system.

Network Solution: To establish service safety and robustness through vulnerability tests, Cisco implemented vulnerability tests on the FIELD system during the development stage. Their contents were presented in detail to the company and were useful in verifying and improving robustness. As FIELD Headquarters Platform Development Division Director Koji Nishi said, “Luckily there were no fatal defects during the vulnerability test at the development stage. We learned an approach that uses a multilayered defense incorporating multiple security measures at various levels. We learned concrete defensive measures such as using double- or triple-layered protection like a castle wall against foes who penetrate and attack us through various means.” As FIELD Headquarters Platform Development Division Chief Yoshihito Miyazaki said, “The Cisco security consulting team, including Cisco Talos™, had a high level of knowledge, which helped us understand the latest security incidents. This was extremely beneficial. They were even able to comprehend parts that news reports did not understand. They knew which approaches and ways of thinking were good to use during development.”

Along with efforts to improve the robustness of the FIELD system, we also formulated security guidelines that show the security requirements for customer equipment. As Nishi said, “As for the guidelines, the volume was quite lacking in concreteness, and a lot of the content was difficult to understand. However, we wanted the FIELD system security guidelines to be clearly distinct from the old guidelines. As such, we aimed to make it 100 pages or less, which was an amount customers could finish reading. In addition, we asked Cisco to make the content so customers could clearly understand in detail what they must do.” The security guidelines, which were created based on the idea of “an image in which various items accumulate little by little” (Miyazaki), exhaustively organize the security risks in factory systems and systematically list the security measures customers should implement when installing the FIELD system.

These projects were implemented over the course of about 6 months, and many global members of Cisco also participated via video conference.

Construction of an open platform in IoT is uncharted territory, so the most important thing is mutual understanding. As Matsubara said, “We value the cultures at both FANUC, a Japanese company that promotes OT (operation technology) at manufacturing sites, and Cisco, a global IT (information technology) company. We spent a lot of time building a mutual understanding of the value provided to the market. FANUC has made exhaustive efforts to never stop the production process at factories and manufacturing sites and to ensure that things do not break, inform someone before they break, and fix them immediately if they do break. It has placed great importance on these efforts. In the beginning, there was a disconnect when even one word was missing, but after they came to inspect
The FIELD system is an open platform geared towards the manufacturing industry that aims to further improve production and efficiency at manufacturing companies. Third-party developers can also freely develop and distribute applications and computers for devices. By enabling various devices at manufacturing sites to connect across generations and manufacturers, this platform promotes the unified management and data sharing of manufacturing equipment and data.

**Connects everything:**
- It can connect not only to the latest FANUC products (CNC, robots, robomachines), but also to existing models in factories.
- It supports OPC UA and MTConnect, which are universal communication standards.
- An open development environment will be provided. Production equipment manufacturers can create and provide computers for their production equipment.

**Multilayered defense security:**
The FIELD system security is composed of multilayered defenses that have incorporated multiple security countermeasure techniques in all layers of servers, networks, and the FIELD system.
- Access to the respective data for (1) users, (2) applications, and (3) production equipment can be configured via the access control of the FIELD system installed at factories. In the event there is a malfunction in an application, everything other than the data access determined beforehand will be shut off.
- Unnecessary access between production equipment will be restricted. The network switch separates networks within factories and control paths and identifies production equipment.
- Several security techniques, such as integrated threat management and security measure software, are used in the FIELD system manager and store.
our factory and we spent time communicating, we gradually deepened our mutual understanding and grasped IoT together.”

FANUC Corporation
Research General Headquarters
FIELD Headquarters
Platform Development Division Director
Koji Nishi

**Business Results:** Through projects, FANUC has been assessed as having great results. Security guidelines based on the latest security requirements can be provided, and systems can be safely constructed when introducing the FIELD system. This is very advantageous, not only to customers in the manufacturing industry who have little knowledge about networks and security, but also to partner companies in charge of construction.

Regarding future expansion and the expectations facing Cisco, Nishi said, “In the future, our services will develop, and we will continue to update the guidelines.

Meanwhile, Cisco, who exchanges information on global trends and shows us solutions regarding technical issues we cannot solve on our own, will be our partner who will help us improve the FIELD system.”

As Miyazaki said, “We want to create services with which customers will definitely feel at ease because the services are from FANUC and Cisco. We want to show robust measures, not measures that promote a vague anxiety. We want to work together to globally cultivate an IoT market in which customers can properly enjoy these merits.”

Finally, Matsubara had this to say about the project summary and the future. “Though there was a limited amount of time, the Cisco team proactively and positively made efforts through these projects. I saw their technical skills and felt their passion as engineers working towards our goal, which was to establish a new market. The FIELD system has just begun. As we provide functions like advanced machine learning and deep learning and...
Improve services that connect to apps and the cloud, we will continue to make improvements so it will be easy to use onsite, will last a long time, and will not betray the trust placed in us. FANUC will strengthen cooperation with Cisco as a business partner so it can expand its services globally.

FANUC Corporation
Research General Headquarters
FIELD Headquarters
Platform Development Division Chief
Yoshihito Miyazaki

For More Information:
For details on Cisco’s security consulting services, please visit
www.cisco.jp/go/securityservice.