Shortening threat response and recovery times

35K
.global IT assets visible
company-wide

30%
operational efficiency
 gains

1 minute
from threat detection
to response

“ServiceNow ITOM and Security Operations provide visibility of global IT asset management statuses. We are fully satisfied with the ServiceNow solution.”

Tetsuo Shiozaki, Deputy Head of Digital Strategy Headquarters,
Yokogawa Electric Corporation

Global IT security monitoring system

Yokogawa Electric develops and manufactures measurement and control equipment for the oil, gas, and chemical industries, amongst others. Since its establishment in 1915, the company has provided equipment that is indispensable for the operation of plants in Japan and worldwide. Currently, control systems account for approximately 90% of its sales, with overseas business accounting for around 70% of total sales.
Yokogawa Electric is expanding globally; however, office locations worldwide have been installing different IT equipment and software, and monitoring security based on their own policies. The resulting inconsistent IT security management has posed a challenge to the business's global operations.

The company has established the Yokogawa Security Operation Center (Y-SOC) to monitor security centrally and improve global operations. As of June 2020, the center covers 15 locations around the world.

“We have built a system that compiles events and security logs from some 35,000 IT infrastructure configuration items, comprising PCs, servers, and gateways used in each location. It automatically detects and analyzes suspicious communications and events, and issues alerts. Y-SOC security analysts use the system to monitor IT security centrally. If an alert is issued, on-site engineers are prompted to take action,” says Tetsuo Shiozaki, Deputy Head of Digital Strategy Headquarters, Yokogawa Electric Corporation.

Linking ITOM and ServiceNow Security Operations with Y-SOC through our APIs, I can better understand the impact of any incident.

Tetsuo Shiozaki, Deputy Head of Digital Strategy Headquarters, Yokogawa Electric Corporation

Visibility of IT asset statuses across all locations
It is important to be aware of all the IT infrastructure configurations used by each location to create an automated detection and analysis system.

In January 2020, Yokogawa Electric implemented ServiceNow IT Operations Management (ITOM) with an IT asset management feature. This has facilitated overall management and provided full visibility of the IT infrastructure assets to the company. At the same time, the scope of Y-SOC security monitoring has expanded from six to 15 locations globally, covering most parts of the world.

“I’m grateful to have visibility of IT asset statuses for locations in countries with strict overseas access restrictions, such as China and Russia,” says Shiozaki.

Having a good understanding of IT asset installation statuses for all 35,000 locations eliminates gaps in security monitoring. It also enables good governance, helps optimize vendor selection and applications, and simplifies global IT investment plans.
Building an incident response workflow

Yokogawa Electric has also deployed ServiceNow Security Operations to optimize its incident response workflow.

ServiceNow Security Operations offers various applications that streamline security response measures. This includes Threat Intelligence, which carries out efficient searches and collates reports from multiple intelligence sources. One application is ServiceNow Security Incident Response, which manages the lifecycles of security incidents, covering all aspects from incident analysis to containment, elimination, recovery, and review.

An inventory of target IT asset information is indispensable for security monitoring. By linking ITOM and Security Operations, Yokogawa Electric has created a central system to determine the impact of incidents and appropriate responses based on asset information from all locations.

Connecting to the various Y-SOC tools allows Configuration Management Database (CMDB) to prioritize when security incidents occur. This shortens response times and streamlines response actions by 30%.

“In the past, it was often difficult to understand profile information such as the devices, users, and operating systems that were potentially targeted by an attack,” says Shiozaki. "Linking ITOM and ServiceNow Security Operations with Y-SOC through our APIs has simplified the identification process, and now I can better understand the impact of any incident.”

“I’m grateful to have visibility of IT asset statuses for locations in countries with strict overseas access restrictions, such as China and Russia.”

– Tetsuo Shiozaki, Deputy Head of Digital Strategy Headquarters
Yokogawa Electric Corporation

35K
locations covered, providing IT asset visibility across 15 countries.
Automated threat protection

More serious security breaches can be automatically prevented by linking Security Operations with the automated detection and analysis system developed by the company. Specifically, whenever real-time alert notifications are sent to Security Operations from the automated detection and analysis system, multiple sources of cyber threat intelligence data are aggregated for reference. IP addresses, URLs, and domain names with high threat levels are identified, and communications are automatically blocked by this mechanism. As a result, workflows such as regular incident reviews can be carried out. Where the period between threat incidence and blocking was once up to three weeks, this workflow has reduced it to around a minute.

In addition, vulnerability diagnoses are incorporated into the Security Operations Vulnerability Response module. Prioritization is based on the presence or absence of vulnerabilities in the target system, and risk assessment with reference to the IT asset management log in ITOM. A vulnerability response workflow is also established.

"I am delighted with the ServiceNow solution," says Shiozaki. "In the future, we aim to provide IT and OT security solutions to our clients based on our experience and know-how to help with their global expansion."