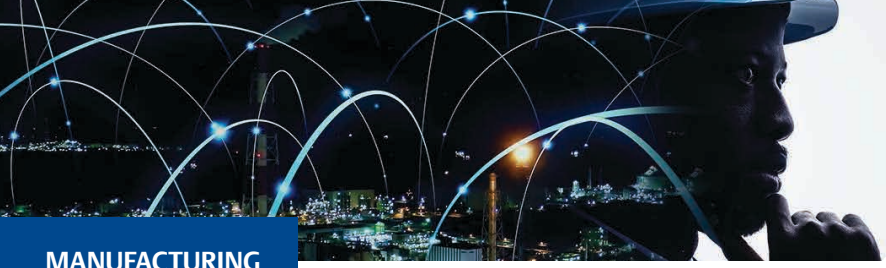

MANUFACTURING

Secure Every Site: OT Cybersecurity Solution To Mitigate Risk

Manufacturer increases layers of protection across industrial control system network.

- **Assessed and analyzed the level of cyber risk and vulnerabilities across the operation**
- **Optimized Industrial Control System (ICS) network architecture with the proper defense-in-depth strategy and protection controls**
- **Enhanced organizational posture and resiliency through proactive planning for a more cyber secure future**

APPLICATION
Industrial Control System - Distributed Control System

CUSTOMER
Food and Beverage Manufacturer in the Upper Midwest

CHALLENGE

A large multi-site food and beverage manufacturer in the upper Midwest had a large DCS infrastructure with limited OT/IT security standards. Increasing concerns stemming from alarming reports of the severe impact cyber attacks could have on industrial control systems availability, manufacturing production levels, data confidentiality, the environment, and personnel safety, led to an initial discussion with Novaspect to explore capabilities.

Recognizing that traditional security measures were not enough to contend with today's sophisticated threats, the customer selected Novaspect to analyze, architect, engineer, and deploy a comprehensive OT cybersecurity solution to safeguard the company's five manufacturing plants.

SOLUTION

Novaspect's cybersecurity engineering team conducted a formal cyber assessment to analyze the current state and potential vulnerabilities to the industrial control system for the customer's operational facilities.

From there, Novaspect presented the findings of its Front End Engineering Design (FEED) study along with critical cybersecurity recommendations tailored to the customer's unique operating environment and in alignment with ISA/IEC 62443 standards.

The proposed solution included the hardware, software, and services to provide the following:

- Secure DMZ/hardware and software layer
- Endpoint protection
- Application whitelisting
- Backup and recovery

With the preliminary engineering completed, and the project scope, system architecture, and functional requirements defined and documented, the project was officially kicked off and successfully deployed.

OUTCOME

The customer was able to take a proactive next step in their OT cybersecurity journey by trusting Novaspect to recommend and install a robust industrial control system cybersecurity solution across their operation.

Tackling other projects in their pipeline can now take precedence knowing that the appropriate safeguards are in place to protect, detect, and defend against cyber attacks over time.

VIEW THE ONLINE CASE STUDY
and connect with an expert