MANUFACTURING

NOVASPECT

OT Cybersecurity Risk Management Plan

Leading ethanol manufacturer fortifies their Industrial Control System (ICS) network and reduces cyber insurance premiums.

Deployed proper defense-in-depth strategy and protection controls to safeguard against cyber threats

Enhanced organizational posture and resiliency through proactive planning for a more cyber secure future

Established compliance with stringent industry standards to meet insurance requirements and reduce cyber policy premium

CUSTOMER

A large biorefinery operated by a leading North American ethanol manufacturing company.

CHALLENGE

Following the directive of the company's board of directors and their business insurance carrier's requirements to underwrite the organization's cyber insurance policy, plant management needed to provide assurance that the proper safeguards were in place to ensure system reliability, uptime, and security.

While the biorefinery already had formal security measures being used to protect its critical infrastructure, much of the policies, procedures, hardware, software, and documentation were out of date, so it was certain that the entire OT network needed to be fully revamped and brought current with industry standards.

Realizing that the successful deployment of this project in a timely manner would require a level of expertise beyond the capabilities of the plant's existing staff and resources, the customer sought professional assistance from the OT Cybersecurity team at Novaspect, an Emerson Impact Partner.

SOLUTION

Novaspect's OT Cybersecurity specialists worked in conjunction with the biorefinery to analyze, architect, engineer, and deploy a robust, vendor-supported OT Cybersecurity Management Plan, to include:

- Control system network security risk assessment and vulnerability scanning report.
- Cybersecurity solution for the entire plant to include all control elements (PLC/DCS) from multiple vendors including Emerson, Rockwell, and Trident.
- Centralized policy management structure.
- Integrated Factory Acceptance Testing (FAT) and Site Acceptance Testing (SAT).
- Network scans of the area control network (ACN) and both wired and wireless devices.
- Endpoint & Whitelisting, OT System Hardening, Controller Firewall, DMZ Firewall, User Access Management, Drawings, and Policy Creation.
- Detailed Design Document (DDD).
- Training and implementing new standards and policies with assigned stakeholders at the plant.
- Ongoing maintenance and support.

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