CASE STUDY

Refiner improves OT cyber risk measurement & managment

Octave Cyber Integrity provides visibility into OT cyber security policy compliance

Key facts:

Industry: Cyber Integrity

Octave products used: Cyber Integrity *(PAS Cyber Integrity)*

Key benefits:

- Provides a comprehensive, unified enterprise view of OT cyber risks
- Identifies potential impact cyber vulnerabilities may have on OT assets
- Improves production safety and reliability through improved configuration management
- Reduces inventory, vulnerability and compliance documentation efforts by 70 percent or more

About the Company

This U.S.-based Fortune 50 company is an independent petroleum refiner focused on enabling safe, reliable and environmentally responsible operations while delivering solid financial results. It manages numerous facilities in the United States, Canada and the United Kingdom.

Challenge

Energy companies today are integrating connected technology to make operations faster and more efficient. However, process automation advances for refineries and petrochemical plants that improve efficiencies and increase output can also increase cybersecurity risks. Devices that monitor pressure, control valves and initiate safety procedures are linked to computer networks and — sometimes — even the Internet. Increasingly sophisticated threat actors now view refineries as alluring targets, regularly scanning their systems for vulnerabilities and weaknesses to exploit.

In 2014, this refiner decided to implement a more rigorous, programmatic OT cybersecurity approach to address increasing threats to their operating infrastructure. First, they designated a small internal team to improve control system security. Next, they researched IT and automation industry security standards and best practices to develop internal OT cybersecurity control standards and policies. They then sought a solution that would provide better visibility into their existing OT security risk and help track compliance with these new OT cybersecurity policies and standards. They also wanted to reduce or eliminate existing, high-effort manual OT asset inventory data collection processes, speed up risk assessment of control system vulnerabilities and reduce production and safety risks through improved control system configuration and change management.

Solution

The refiner selected Cyber Integrity as the foundation for their new OT cybersecurity program. Since you can't secure what you can't see, they first used Cyber Integrity to create an automated, comprehensive, evergreen OT asset inventory — one that provided deep visibility into all installed hardware, software, I/O cards, firmware, configuration and control strategies across their multi-vendor control system assets running on the process control networks (PCNs).

It then deployed Cyber Integrity vulnerability assessment capabilities. Prior to Cyber Integrity, determining if OT assets were at risk from a "critical" or "high" vulnerability published by ICS-CERT could take months. Vulnerability identification and remediation were time-consuming and often inaccurate or incomplete. After Cyber Integrity, the team can assess the potential impact of a vulnerability across all refineries in minutes.

Cyber Integrity ultimately has enabled the team to not only improve cybersecurity and reduce OT cyber risk but also save millions of dollars in program costs over the last five years. These savings have come through the reduction or elimination of manual processes for inventory, vulnerability assessment, and compliance audit data collection.

About Octave

Octave is a leader in enterprise software, turning data into decisive action and intelligence into your edge. Our software solves for and simplifies complexity, from the design and build to operations and protection of people, property, and assets– for any scope, at any scale. For decades, we've partnered with customers to sharpen performance, elevate efficiency, and amplify results. From factory floors to entire cities, our solutions are tuned to scale up what's possible from day one onward.