CASE STUDY

Balancing Cybersecurity and Production in the Oil and Gas Industry

Cyberattacks are often successful due to security lapses caused by internal shortcuts. In order to find vulnerabilities and offer remedies, 1898 & Co. analyzed the systemwide architecture and field deployments of a global energy company determined to shore up its cybersecurity.

Challenge

A global energy company with a portfolio of oil and gas, petrochemicals and green energy resources needed help making its global operations more secure against cyberattacks.

At the time, there was an uptick in geopolitical tensions and cyber-related espionage through both ransomware and malware deployments. The energy sector was regularly targeted for attacks, and because of global connectivity and an ever-expanding attack surface in the field, this company's critical infrastructure was vulnerable.

At risk was the potential for compromising operations and disrupting the company's global supply chain. Low-level security and increased connectivity, as well as online unverified trust relationships with vendors and original equipment manufacturers (OEM), made the company particularly susceptible to a broad spectrum of threats. There were as many as 15 different OEMs that had different systems and security practices that contributed significantly to the risk equation for the client.

Project Stats

Client
Oil and gas company

Location
Confidential

Impacted by hacktivism and other cybersecurity breaches in the past, the client needed a comprehensive review of its assets to determine potential for exposure. The company's project team recognized that as it expanded and modernized, it would be using even more intelligent electronic devices in the field and incorporating more Industrial Internet of Things (IIoT) sensors in their systems, making it easier to collect data and operate. But as the number of digital monitoring components continued to grow, so too would the potential for attacks.

Recognizing it's never too late to question security stability, the company's project team sought to fully comprehend how its operational technology (OT) and industrial automation control systems (IACS) were linked and safeguarded. The team also sought to get a clearer understanding of how OEM systems and networks communicated with the company's assets and what vulnerabilities and challenges existed as a result.

Solution

The company engaged 1898 & Co., part of Burns & McDonnell, to conduct a full IACS cybersecurity assessment based on global standards and the operation's engineering standards specific to OT. The goal was to identify potential threats and prioritize fixing them. Without guidance, the project owners knew continued attacks would result in costly unplanned outages, operational challenges that threatened demand and the loss of public confidence.

While there are hundreds of cybersecurity operations in the enterprise information security space, 1898 & Co. was uniquely positioned for this project because it has cyber professionals working alongside designers and engineers. Our team was chosen for its experience with cybersecurity, control systems, industrial networking, field instrumentation and OT/IT-security. Additionally, there are team members who have extensive knowledge of design, engineering and construction processes.

Using as guides the ISA/IEC 62443 industrial automation and control system cybersecurity standards and the National Institute of Standards and Technology cybersecurity framework categories of identify, detect, protect, respond and recover, the goal was to create a plan that would leave the client more cybersecure and better prepared for more complex and frequent attacks.

The 1898 & Co. team implemented a five-step process to conduct a vulnerability analysis of the client's assets, including industrial control systems. Cybersecurity specialists did an asset inventory by going into the field and identifying what equipment security state the systems were in, how they were configured and the communication to and from the systems within their zones and conduits. The team used noninvasive vulnerability tools, data gathering and more to identify cyberthreats and take a deep dive into data flows and determining what access and administrative controls were in place.

Examining in-field culture and looking at how employees executed their jobs was also a part of the analysis, especially when it came to shortcuts and processes instituted by staff to help with access, speed and convenience.

An important step in the assessment was identifying the highest impact cyberevents that could occur and providing recommendations for remediation. As part of the asset inventory, team members combined what they discovered on-site with what the industry was citing as vulnerabilities specific to vendors and equipment. The team utilized information sharing resources such as the National Vulnerability Database hosted by the National Institute of Standards and Technology, the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team, and other information-sharing resources to help with vulnerability identification and remediation recommendations.

Using the resulting assessment data, the team focused on developing a system to address issues and prioritize threats. One key finding was that equipment from OEMs deemed secure — and sold as safe and reliable — was not. Much of this equipment had connectivity through the internet to domains that were undocumented. Another finding was that staff had created shortcuts and extra access points for convenience's sake that made control systems highly vulnerable. These threats to safety were high on the list for remediating. Hardening security systems, keeping legacy systems as current as possible, and deploying security at the front end of new systems are other key factors that were examined closely.

1898 & Co. was able to effectively identify and develop strategies that will lock down areas of risk. Awareness and technical training that helps better manage staff and contractor access will be provided on an ongoing basis. Other strategies include working with OEMs to implement a more streamlined approach to securing industrial control systems and critical networks. Specifically, the project team secured the client's perimeter, forcing OEMs to go through a secure entrance point and demarcation. This forces a defense-in-depth approach and secure-by-design access and patching to the integrated administration and control system.

The approach taken during this assessment has allowed the client to efficiently analyze its entire service territory and provided the information needed to begin fine-tuning the security of its operation. After the analysis, cybersecurity operators at the company now have the resources needed to enhance monitoring and detection capabilities both physically and remotely. Additionally, the client is better able to secure its devices and networks, including the supervisory control and data acquisition systems used to manage operations.

About 1898 & Co.

1898 & Co. is a business, technology and cybersecurity consulting firm serving the industries that keep our world in motion. As part of Burns & McDonnell, our consultants leverage global experience in critical infrastructure assets to innovate practical solutions grounded in your operational realities. For more information, visit **1898andCo.com**.