Midland Cogeneration Venture Strengthens Security Posture by Employing Emerson Cybersecurity Solutions

RESULTS

- Decreased patch deployment time from approximately 45 to 15 days using automated tools; nearly 30 days faster than the manual process
- Expanded team's scope of responsibility beyond DCS network to encompass 50% more assets without adding manpower
- Mitigated initial high-priority vulnerability assessment findings within 12 months
- Streamlined cybersecurity program management by working with a single vendor

APPLICATION

1,633-MW combined cycle cogeneration power plant that produces process steam at a rate of up to 1.5 million pounds per hour. The plant is equipped 12 ABB GT11N gas turbines, 12 CE heat recovery steam generators, two GE condensing steam turbines and one ABB Stahl non-condensing steam turbine.

CUSTOMER

Midland Cogeneration Venture located in Midland, Michigan

CHALLENGE

As the largest natural gas-fired combined electrical energy and steam energy generating plant in the U.S., Midland Cogeneration Venture (MCV) has always taken cybersecurity protection measures seriously, even in the absence of formal regulatory obligations. MCV, a major supplier of electricity to customers in Michigan and the midcontinent as well as a supplier of bulk process steam energy to nearby chemical production companies, makes safe and reliable plant operation a top priority. As cyber threats continue to intensify and become more sophisticated in nature, protecting the plant from vulnerabilities has become increasingly burdensome.

Under the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards Version 6, which went into effect on July 1, 2016, MCV would be officially classified as a medium-impact bulk generating asset. Having had no previous NERC CIP obligations, the plant would now have to comply with NERC CIP standards 2 through 11, which meant that a formal, documented process for patch management, configuration management, security event monitoring and more was needed.

With a two-man team (out of a staff of 120) responsible for the control systems at a 12-plus unit facility, meeting those obligations would be challenging.

"With the help of Emerson and the cooperation of our internal team, we developed a solid cybersecurity program that not only enables us to meet our compliance obligations but also focuses on best practices to ensure reliable plant operation - all without the need for additional staff."

Scott Woodby
Manager of Engineering
Midland Cogeneration Venture

EMERSON

SOLUTION

In early 2015, MCV looked to establish a formal security program performed by an in-house staff of two using a combination of homegrown tools and tracking sheets. Manually patching 70 control system-related workstations proved unmanageable, taking about 45 days to complete what was supposed to be a "monthly" task. This effort did not include patching workstations on other plant networks nor the team's responsibility to manage malware protection, annual vulnerability assessments, configuration management and daily DCS operation.

In seeking outside assistance, MCV met with independent security consultants and IT-focused businesses which would have required them to work with four different companies to install four different systems that would each address a specific aspect of their security program. Not only was this going to be costly, but the resource burden was still going to be significant.

MCV's DCS supplier, Emerson, offered a comprehensive and proven program consisting of cybersecurity suite modules and services, not only for the Ovation™ control system, but for control systems supplied by other vendors. Emerson's patch management module was installed in November 2015 to push patches out to Windows workstations and servers once a month. A centralized, automated patch management process proved significantly more manageable, taking roughly 1-1.5 weeks to complete – nearly 30 days faster than the previous manual process. Additional cybersecurity modules were also deployed including security incident and event management, backup and restore, configuration management and malware prevention.

"After reviewing several options, the most comprehensive cybersecurity program came from our DCS supplier, Emerson.

Unlike other vendors, Emerson not only knew us, our plant and our system quite well, but also had been developing and deploying full-featured cybersecurity solutions for years.

Their customizable cybersecurity suite integrates hardware and virtualized software modules to provide a variety of security management functions not only for their own Ovation system, but also for control systems supplied by other vendors."

Scott Woodby
Manager of Engineering
Midland Cogeneration Venture

After successful implementation of the cybersecurity modules, the responsibilities of MCV's two-man team expanded beyond managing the security of the primary DCS system to include all plant networks and equipment affiliated with plant operations including turbines, CEMS and plant LAN assets; nearly doubling their scope of responsibility to 140 workstations and servers.

NERC CIP regulations require medium-impact assets to conduct a vulnerability assessment once every 15 months. In early 2016, Emerson was contracted to perform a comprehensive cybersecurity evaluation which included scanning the entire system, verifying asset inventory, looking for vulnerabilities and identifying mitigating options. The resulting assessment report contained specific recommendations separated into immediate, short-term and long-term actions geared towards improving the plant's security posture and meeting NERC CIP obligations. Emerson recommendations were further segregated into nine categories, where each finding within those categories were ranked by severity level representing the relative security, compliance and reliability risks to MCV's systems. About 52% of the findings fell into the critical/high-priority categories and the remaining 48% into the medium or low-priority categories. Within12 months, MCV resolved all the initial, high-priority findings while proactively budgeting for and scheduling implementation of the remaining, lower-priority findings.

MCV overcame the challenges of having to secure a large system with very limited resources by implementing a custom approach with the help of Emerson. MCV now has a solid cybersecurity program that not only helps them meet compliance obligations but also focuses on best practices to ensure reliable plant operation — all without the need for additional staff.

OVATION™ For more information:
www.Emerson.com/Ovation

EMERSON™