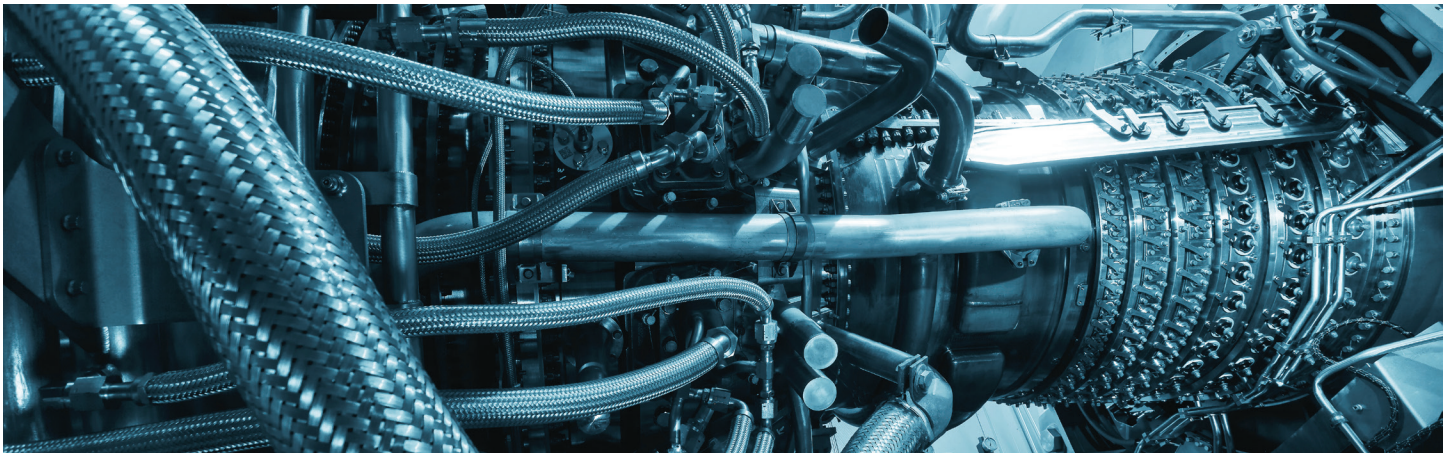
1898 & CO.
PART OF BURNS McDONNELL

CASE STUDY

Defending a Large Power Producer Against Cyberthreats Means Anticipating the Intentional and Unintentional

The main principle guiding cybersecurity strategy development is to recognize that not every threat will be from an advanced persistent threat or other known adversary. There are many incidents that were simply the result of an unintended action. A comprehensive cybersecurity plan for a large power producer accounts for both intentional and unintentional events that could disrupt vital operations.



Challenge

A one-gigawatt natural gas power facility owned and operated by a multinational energy corporation was facing an escalating risk of cyberattacks from malicious actors. Located in Pennsylvania, this combined-cycle independent power facility provides power to approximately 1 million homes and businesses, making it an essential resource for the regional power grid.

The plant is similar to many power generation facilities that face threats of service disruptions or damage to sensitive pieces of expensive equipment if attackers gain access to operational technology that runs the equipment.

The operator needed a cybersecurity partner that could provide year-round, 24/7 monitoring for threats and anomalies, along with the resources and know-how to develop a multi-layered response strategy that would instantly kick in should an attack occur. This power corporation contracted with 1898 & Co., along with Armis to provide its proprietary sensor-based monitoring for the operational technology (OT) system, and CrowdStrike to provide endpoint detection and response for monitoring of the organization's information technology (IT) system.

Solution

A layered defense-in-depth strategy was determined to be the most effective strategy to protect the sensitive controls that run the mission-critical turbines and other components of the power generation unit.

Using proprietary sensor-based technology developed by Armis, information feeding into the OT network is passively monitored. This part of the managed security strategy is designed to account for the fact that some events or anomalies are actually false positives, meaning they warrant an investigation before shutting down systems. A false alarm that shuts down power operations could disrupt power service and cost multiple millions of dollars.

Meanwhile, a more aggressive protection scheme is viable for the IT system. Because more than 90% of external attacks hit the IT network first through phishing or another form of attempted intrusion, the actively-managed CrowdStrike protection strategy is designed to prevent intruders from traversing across data silos while attempting to find a vulnerable point that would provide access to the OT network controlling the physical components of the business. This system utilizes detection devices deployed at multiple endpoints on the network servers, enabling quick detection and quarantine of an infected segment of the network.

Prework is Vital

The incident response (IR) plan was developed in collaboration with system operators to account for lines of communications and business continuity. The IR plan includes precise definitions of what such an event might look like and sets up specific lines of responsibility with identification of individuals who have accountability for actions that would contain a threat.

As the cybersecurity contractor, 1898 & Co., does not take responsibility for turning off critical systems, even during an attack, so the plan includes a collaborative agreement to work side-by-side with plant engineers in a coordinated incident response.

In most plan scenarios, the first step is aimed at containment, but the actual mechanism used for IR varies by the type of threat that is occurring. In many cases, a threat could be contained within the network communications interfaces, avoiding the need to shut down overall operations.

Industry Best Practices

Best-in-class cybersecurity plans are typically built around recognized industry standards. In this case, response plans comply with the North American Electric Reliability Corporation (NERC) critical infrastructure protection (CIP) standards.

The plan also establishes a virtual chief information security officer (CISO) to assist in long-term budget management and business continuity planning to accommodate the evolving nature of the threat landscape. The virtual CISO is a function that recognizes that cybersecurity methods have costs associated and that certain investments should rank as higher priorities because of the benefits they bring.

The IR plan also incorporates proactive tabletop training exercises to simulate different attack vectors and allow the team to fine tune response steps.

With the right sensors and protection systems deployed, and proactive training and alignment of the organization, this power facility is gaining the insight needed to quickly counter cyberthreats that could pose devastating impacts to ongoing power generation 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**.

349390-0623