CASE STUDY

Gaining Operational Resiliency and Reliability Through the Management of Cybersecurity Threats

Critical infrastructure companies often struggle to keep their operations protected from cybersecurity attacks. Unlike other firms that focus mostly on information technology cybersecurity, 1898 & Co. is one of the first firms to support operational technology through managed threat services.

Challenge

With only a few exceptions, critical infrastructure companies rarely have the resources necessary to meet basic cybersecurity needs.

Cybersecurity threats are an ever-present challenge that companies of all sizes must defend against and mitigate. If undetected, cyberattacks on critical infrastructure assets like the power grid and water systems can result in service disruptions, data theft, infrastructure damage and negative impacts to public health and the environment.

Solution

Realizing just how vulnerable it was, a utility client was determined to better secure its systems and networks so that the operation would be safer and more resilient. Without its systems and networks being properly secured, the company's program team understood the potential for cyberattacks could increase, resulting in unplanned outages, operational challenges and a loss of public confidence. 1898 & Co. was chosen to enhance cybersecurity and meet increasing threats by delivering managed

Project Stats

Client
Confidential water utility

Location
Confidential

threat services for the company's operational technology. 1898 & Co. is one of the first companies dedicated to offering managed security services for critical infrastructure.

Our team managed all aspects of the program from deployment and integration through around-the-clock detection. This began with the deployment and integration of requisite hardware and software sensors within the company's environment. The team configured and tested the sensors to validate proper data capture and then established the secure transmission of data to the 1898 & Co. Advanced Threat Protection Center (ATPC). Once sensors and the cybersecurity monitoring infrastructure were in place, 24/7 monitoring began. In particular, the team implemented a cybersecurity program that consisted of asset identification, asset mapping, protocol and IT statistics, identifying and configuring baselines, vulnerability identification, and threat landscape monitoring.

Tuning is a critical part of this program. 1898 & Co. conducted tuning during client onboarding and will continue to do so throughout the partnership. Tuning provides the backdrop of effective analysis and detection. The tuning part of the program called for working with the client to establish legitimate activity including normal maintenance periods, standard system messaging, update schedules and the like. Tuning can be broken down into four phases: learning mode, high priority event review, platform specific detection tuning and global tuning.

Knowing the assets of the organization's network was key to baselining normal behavior and detecting malicious anomalies. Assets were identified via IP addresses, MAC addresses and protocols that enable navigating within the network. This baselining behavior was critical for mapping potential threats. Data gathered from the asset sensors was visually mapped by the program team into a network diagram. This step is crucial for future threat hunting and incident response.

All behavior and interaction between devices and protocols was baselined by the program team. Having these defined baselines for the company's network will increase the visibility of potential OT cyberthreats and malicious activity. For instance, if a threat actor is in the network and starts making unauthorized changes to devices, that will trigger a notification that alerts cybersecurity operators to determine if the changes are part of a normal process. If not, an incident response will take place.

For this program, sensors observed assets, protocols, communications, configurations, behavior, IP address segmentation, routers, switches and programmable logic controllers (PLC). The 1898 & Co. team deemed activity was consistent with standard industrial control systems operations.

The team also identified some possible vulnerabilities, which are being mitigated. Around-the-clock monitoring, detection and incident escalation services will continue and regular threat reports will be issued. The team will act, where appropriate, whenever client activities trigger events requiring investigation.

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**.