CASE STUDY

Electric & Water Utility Secures OT with Dragos Platform & Services

INTRODUCTION

While many in modern society take utilities for granted, we all rely on them to provide essential resources like electricity, natural gas, and water each and every day. Any downtime or disruption in service could have a significant impact on our daily life and even the economy. Unfortunately, this dependency often makes utility companies an appealing target for cyber attacks. As evidenced by the recent news, the industry is a focus on many fronts motivated by both financial and political reasons. The risk of a disruptive attack on the core business operations of electric and water utilities has increased significantly.

Most utilities today have two or more unique operational environments, providing different services such as electricity, natural gas, and water/wastewater treatment. This leads to a mix of specialized industrial control systems (ICS) such as Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), Energy Management Systems (EMS), Human-Machine Interfaces (HMI), Remote Terminal Units (RTU), and Programmable Logic Controllers (PLC), which manage and control the operation of valves, transducers, system protection relays, and other key components of the physical processes in an electric or water operations environment. All of these control systems are becoming increasingly connected to enterprise networks, and in some cases even the internet, through digital transformation, in an effort to improve asset utilization,

OUC The *Reliable* One®

BUSINESS OVERVIEW

The Orlando Utilities Commission (OUC) is a municipally-owned public utility providing water and electric service to more than 250,000 customers, with over 400,000 unique service connections, in Orlando, St. Cloud and unincorporated areas of Orange and Osceola counties. Established in 1923, OUC ("The *Reliable* One") is the second largest municipal utility in the state and is fully committed to providing world-class customer service and energy and water innovation.
www.ouc.com

CHALLENGE

OUC has always prided itself on its track record of success in providing reliable water and electric service to its customers each and every day. This means OUC is dedicated to minimizing systems downtime or any disruption of service—no matter how brief—in order to exceed its customers' expectations.

The risk of hurricanes and other powerful storms is a real and ongoing threat, requiring OUC to constantly assess its disaster preparation and recovery systems and look for opportunities to improve. However, the Stuxnet event and rise in industrial malware caused OUC's operational technology (OT) and cybersecurity teams to wonder if they were as protected and prepared as they should be for the new threats posed by sophisticated cyber adversaries.


Stanton Energy Center

process efficiency, and business forecasting. The entire utility industry now views the intersection of these OT and IT systems to be the prime candidate for cyber attacks—and one that is difficult to defend using traditional enterprise cybersecurity tools and methods.

Making things even more challenging, electric utilities such as OUC must ensure that their EMS complies with the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) Reliability Standards. Any business that owns, operates, and uses any type of bulk electric power system must comply with all NERC-approved Reliability Standards, including its cybersecurity framework that requires the identification and security of critical cyber assets. However, many utilities focused solely on compliance often find it difficult to achieve the level of security required to truly protect their core operational systems.

CHOOSING DRAGOS

All of these factors led OUC to objectively evaluate its existing internal systems and controls, and ultimately, decide that it needed a new approach, including an OT-specific cybersecurity platform to address the challenges it was facing. Specifically, OUC was looking for a solution that could help identify and eliminate cybersecurity blind spots to develop a comprehensive approach to monitoring, threat detection, and remediation. It was also looking to partner with a proven team of industrial cybersecurity experts capable of providing specialized skills and services.

OUC started the process by conducting extensive research and evaluating many vendors, yet the initial findings were disappointing. Joe Reilly, OUC's Director of Operational Technology, noticed that many vendors were too narrowly focused on a particular type of attack and didn't address the right audience within the organization. "We met with one vendor who only wanted to talk about ransomware. Their approach only spoke to a C-level audience and was more externally focused related to communications and damage control," he said. "We were looking for a cybersecurity partner who could deliver a wider range of cybersecurity services and one who could work

OUC AT-A-GLANCE

250,000+
customers

400,000+
service connections

closely with our technical team members and really investigate the critical controls needed on the infrastructure side. This is what led us to Dragos."

Reilly met with Dragos team members who were leading an ICS cybersecurity training course. The result of this discussion resulted in Reilly hiring Dragos to perform an assessment of OUC's exposure to an attack on its OT environment. As a municipal entity, OUC is required to publish certain information to their constituents. However, as the Dragos analysts discovered, some of the information posted online went beyond the required reporting and could potentially have been used by an adversary to initiate a cyber attack. From there, the Dragos team conducted an in-depth workshop, known as a tabletop exercise, with OUC's IT and OT teams to simulate the steps an adversary would take as it moved through the systems on their ICS network.

This discussion highlighted the fact that OUC did have a number of blind spots related to its cybersecurity efforts. "For example, our IT department has a dedicated SOC, but our discovery meeting with Dragos showed that it didn't do enough to monitor everything on the network, especially our OT assets," Reilly explained. This was the information OUC needed to make the decision to go with the Dragos Platform, but also to purchase a retainer for professional services that Reilly could foresee needing in the future.

> We were looking for a cybersecurity partner who could deliver a wider range of cybersecurity services and one who could work closely with our technical team members and really investigate the critical controls needed on the infrastructure side. This is what led us to Dragos.
>
> **JOE REILLY**
> **OUC Director of Operational Technology**

IMPLEMENTATION HIGHLIGHTS

Once the decision was made, Reilly's team wanted to do all they could to help with the implementation and adoption of the Dragos Platform. Multiple staff members, ranging from SCADA technicians to network engineers, attended Dragos training, an important distinction since these team members represented the two different lines of OUC's business. "Dragos did a great job with training because they cross-trained our employees on cybersecurity


Ken P. Ksionek Community Solar Farm


OUC Southwest Water Plant

implications specific to each division by talking about relays (electric) but also PLCs (water), for example," said Reilly. "It was a great experience."

When it came time to implement the Dragos Platform, OUC decided to start with its water operations. Water was perceived as the ideal proving ground because this part of the business didn't have to comply with NERC CIP standards. This would allow OUC to roll out the Dragos Platform and then apply lessons learned and best practices to its implementation on the electric side of the business. "At that time, there was no real industry guidance related to network architecture and how to best ensure compliance with NERC CIP," explained Reilly. "It was great to have Dragos experts working with us because they were able to clarify guidelines and make recommendations to help us improve our compliance effort when we deployed the Dragos Platform within our Energy Management System."

SOLUTION BENEFITS

The Dragos Platform's in-depth, automated passive asset discovery capabilities, coupled with its mapping and zoning functions, were well-suited to the OT environment at OUC rather than some alternatives that did IT-style active scanning. It provided key visibility into important activities, such as when IT deploys or upgrades computers, servers, and other assets in the field, or when 3rd party contractors connect to the OT network. Activities like these, while necessary to support automated operations, can easily introduce new vulnerabilities and risk to the OT environment if not monitored closely.

However, like many asset owners in critical infrastructure, OUC's cybersecurity staff was stretched thin and did not have the specialized ICS security-specific knowledge to perform advanced hunting tasks for the presence of cyber threats within their industrial networks. To address those concerns, Reilly elected to enlist the help of the Dragos team on an on-going basis to remotely monitor their Dragos Platform via a secure connection with the OT Watch solultion. In this arrangement, a Dragos analyst performs regular asset tuning, zoning, alert triage, and performs proactive intel-driven threat hunts for adversaries in OUC's OT environment. Reilly's team receives

DRAGOS SOLUTIONS UTILIZED

- Dragos Platform
- Dragos OT Watch
- Dragos WorldView
- Dragos 5-Day ICS/OT Cybersecurity Training
- Dragos Professional Services with Incident Response Retainer

"It was great to have Dragos experts working with us because they were able to clarify guidelines and make recommendations to help us improve our compliance effort when we deployed the Dragos Platform within our Energy Management System"

JOE REILLY
OUC Director of Operational Technology

regular reporting and communications from the Dragos team, who were themselves once control system engineers with an appreciation for the day-to-day challenges a utility operator faces. In one case, a Dragos analyst noticed communications between the OT network and a third party vendor outside of planned maintenance windows. These insecure practices were highlighted to OUC security and operations leadership so that they could understand and correct the issues.

ADDITIONAL BENEFITS

OUC also utilizes Dragos WorldView, an actionable ICS threat intelligence subscription service managed by Dragos's dedicated threat intelligence and adversary hunting teams. The timely reports and threat feed gave OUC's teams in-depth visibility into the threats facing other utilities and critical infrastructure companies, so they could better prepare for, detect, and respond to potential attacks.

Reilly explained the difference in what his team experienced with other threat intelligence sources with this anecdote: "We did receive notices from the sector-specific information sharing services, but it was like someone telling us that a person (threat) was about to enter America somewhere along the U.S.-Canada border," he said. "Unfortunately, this information wasn't as specific or as actionable as we needed. These types of alerts even led to confusion and panic. The combination of Dragos WorldView and the Dragos Platform gives us much better information." With the Dragos reports, the security team are able to automate the blacklisting of malicious industrial-themed domains, as well as ensure that their OT network is configured to better defend against the tactics and techniques of determined adversaries.

At this point, Reilly is confident that Dragos has given his team a critical edge when it comes to cybersecurity, and one that he looks to continue in the future. "As we proceed, we have solid plans to make Dragos the de facto standard for any cybersecurity processes we need to manage," he said. "We are continuing to roll out the use of Dragos sensors so we can fully monitor all assets and traffic," he said. "We are also evaluating other Dragos solutions, such as Neighborhood Keeper, but for now, we are convinced that Dragos has significantly helped us increase our overall security posture—as well as our ability to provide the best service possible to our customers. We couldn't ask for anything better."

OUTCOMES

- Complete visibility into electric and water OT environments
- Actionable OT threat intelligence
- Enhanced OT cybersecurity skills among staffers
- A trusted ally for OT security

To learn more about Dragos Platform, Threat Intelligence, and Professional Services, please contact **sales@dragos.com** or visit **dragos.com**