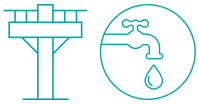
CASE STUDY

Electric & Water Utility Partners with Dragos to Improve OT Visibility & Reduce Risk



BUSINESS OVERVIEW

This leading U.S. utility has delivered on its commitment to provide reliable and affordable water and power for more than a century. By providing these essential resources, it has helped a major metropolitan area develop and thrive. The utility has a mission to continue to lead the way by applying a forward-thinking approach and new technology to address water and energy supply challenges.

CHALLENGE

After the series of high-profile cyberattacks against Ukrainian utilities, a leading U.S. electric utility wondered if it could be vulnerable to a similar attack. The assessment led the company to select the Dragos Platform to improve OT visibility—and overall cybersecurity—for all of its sites.

INTRODUCTION

The utility's search for a better operations technology (OT) monitoring solution started shortly after the infamous cyberattacks that targeted key industrial control systems (ICS) and crippled three Ukrainian power distribution companies in 2015. In response, the company's executive team wanted to know if the organization, including many different sites and assets, might be vulnerable to a similar type of attack.

The utility's project team determined that the quickest and most effective way to identify potential vulnerabilities and assess the organization's overall security posture was to conduct a red team exercise. This security assessment technique used simulated cyberattacks to determine the overall strength of the utility's existing capabilities and identify areas for improvement.

When the project team presented its findings to the executive team, they were surprised by some of the executives' perceptions of their company's cybersecurity capabilities at the time. Many of the utility's executives had experience in the Security Operations Center (SOC) and other parts of security operations. Yet some executives misunderstood exactly what the utility's

previous cybersecurity infrastructure could do. For example, they believed that the security team could quickly drill down into an alert, immediately find the threat, and prevent cyberattacks. There was also a misperception about the cybersecurity capabilities within the OT environments.

Despite these misunderstandings, the meeting was still valuable since it allowed the project team to pitch the idea of overhauling the existing architecture and implementing a comprehensive ICS/OT cybersecurity solution. Their request was met with full and immediate approval: the utility's executive committee quickly created a new mandate that would require the team to find the industry's best ICS/OT cybersecurity platform and deploy it organization-wide to drastically improve the utility's security posture.

THE DECISION TO GO WITH DRAGOS

The cybersecurity team was somewhat familiar with Dragos, but it initially focused on anomaly detection software, thinking the utility would benefit from the ability to see and react to alerts. But the project team soon realized that the majority of those solutions weren't as mature yet. This awareness led them to consider OT-specific visibility platforms in general, and Dragos in particular.

After a thorough evaluation of many of the industry's leading vendors and products, the team became convinced that the Dragos Platform was the right choice for them, specifically for its ability to provide complete visibility into critical ICS and OT assets. A key use case the utility wanted to achieve was to monitor for adversary behaviors and actions that are commonly seen against energy systems such as generation distributed control systems (DCS) and energy management systems (EMS).

The utility also selected additional Dragos products and services, including Worldview Threat Intelligence for better situational awareness, Neighborhood Keeper for visibility of real-world threats that their peers see in their environments, and an IR retainer that enabled them to request help from Dragos Industrial Incident Responders if the need arose.

UTILITY AT-A-GLANCE

1 million+
customers

GENERATION PORTFOLIO

- Hydro
- Natural Gas
- Geothermal
- Coal
- Biomass
- Solar
- Wind
- Nuclear

LESSONS LEARNED IN THE DEPLOYMENT PROCESS

When it came to implementing the Dragos Platform, the project team realized that their infrastructure was inconsistent due to legacy systems, security employees with limited OT skills, and a lack of complete visibility.

As they began, they were able to achieve a few significant quick wins, such as asset verification, identification of misconfigurations, and the successful monitoring of remote access. Early in the process they were able to see and validate a vendor's recent activity on the network. This behavior might have gone unnoticed before the use of Dragos and served as proof positive that they were on the right track.

These early successes translated into valuable lessons learned—best practices that the utility would recommend to any organization looking to implement a continuous network monitoring solution in a challenging industrial setting.

First up: securing top-down support from executives and even the board. In this case, the project team had the good fortune of starting with this support because of the original mandate. Yet it was critical to the project's success because it helped address issues that could arise later, such as budget questions, change management directives, risk management, and even issue mediation and resolution.

The project team engaged with a wide variety of employees, representing a cross-functional swath of the workforce, including engineers, technical staff,

> We were initially focused on anomaly detection software and originally thought that we would benefit from the ability to see and react to alerts. But we quickly realized that the majority of those solutions just weren't as mature as we needed. This awareness led us to consider OT visibility platforms in general, and the conversation pretty much started and stopped with Dragos.

plant managers, security professionals, and even equipment operators. These employees all have different perspectives, requirements, and use cases related to any cybersecurity solution. The project team discovered it was in their best interests to find early adopters of the Dragos Platform and give them access to the solution. This helped them identify potential challenges and overcome them much faster than they could have without their support.

AVOIDING MISTAKES

The most important lesson learned is the importance of avoiding mistakes in the operations environment. This means considering virtually every implication they could think of—and then reacting to many that they never could have predicted—to ensure that the security monitoring system installation does not cause or increase the likelihood of operational upsets. The Dragos architecture allows passive monitoring of all industrial control systems at the utility and can be implemented without adding to risk of failure or compliance risk.

This organization is not unlike many other utilities and industrial organizations where its architecture was comprised of legacy applications, systems, and equipment—some of which were decades old. One of the tenets in making changes to an OT network is that there can be no impacts to production processes, which meant they had to carefully consider issues such as ports, switches, and implications related to architecture deployment options such as spanning.

Above all else, the project team recommends a proactive mindset when it comes to jumping in and doing everything possible to gather information, prepare documentation, assess infrastructure maturity levels, and virtually anything else that could help make the deployment process as smooth as possible. This also includes working with vendors, who are often very willing to help asset owners and operators who are interested in implementing ICS/OT network monitoring and visibility solutions.

DRAGOS SOLUTIONS UTILIZED

- Dragos Platform
- Dragos Worldview
- Dragos Neighborhood Keeper
- Dragos Incident Response Retainer

CONCLUSION

After an extensive deployment process, the team is confident they've benefited from their experience and valuable lessons learned along the way. Yet even more importantly, they can now point to the success deploying the Dragos Platform, a critical advantage when it comes to helping their company improve OT visibility, detect cyberattacks, and keep its valuable services up and running for the citizens it serves.

OUTCOMES

- Complete visibility into electric and water OT environments
- Actionable OT threat intelligence
- Successful buy-in across operations, engineering, and cybersecurity teams
- A trusted ally for OT security

If you're interested in learning more about Dragos Platform, Neighborhood Keeper, Worldview Threat Intelligence, and ICS/OT Professional Services, please contact **sales@dragos.com** or visit **dragos.com**