

DRAGOS PLATFORM & NEIGHBORHOOD WATCH

CASE STUDY TRINITY RIVER AUTHORITY

THE CHALLENGE

Water utilities provide one of society's most essential services and are an integral component of our everyday lives. As such, they present unique targets for adversaries who aim to disrupt their operations and the lives of people who depend on them. Many water utilities are moving down the path of digital transformation, enabling new efficiencies, better customer support, and enhanced safety, responsiveness and productivity of their operations. However, with all of these benefits comes additional risk to their operations, including cyber attacks that may originate in IT networks and pivot into the ICS/OT environment leading to operational disruptions and safety issues.

BUSINESS OVERVIEW



Trinity River Authority (TRA), a Texas water utility, owns and operates six water treatment and distribution facilities, as well as five wastewater treatment facilities serving millions of residents in more than sixty cities in the state of Texas.

Like most critical infrastructure utilities, they face challenges driving enhanced ICS/OT security in their industrial operations environment.

INTRODUCTION

Drinking Water systems, at a high level, can be categorized into three functions: the **source** of the raw water supply, **treatment** systems that disinfect and treat the water, and **distribution** systems that convey the water to consumers. Source and distribution systems can be geographically dispersed and include networks of aqueducts and pipes, as well as many small facilities such as pump stations, valve vaults, and storage tanks. Treatment systems, by contrast, are typically contained within one or a few sites but have much more equipment and systems to monitor and control. Many water systems are cross connected between adjacent systems in either support or producer-consumer configurations.

Many technical challenges for detecting and responding to cybersecurity events within the industrial control systems of water utilities are driven by the geographic dispersion and interconnection to neighboring systems. Trinity River Authority is confronted with those

same hurdles, as well, despite its commitment and dedication to securing its industrial controls.

The Dragos Platform's in-depth, automated passive asset discovery capabilities, coupled with unique mapping and zoning abilities, allow an asset owner or analyst to gain a comprehensive understanding of their assets. This understanding transcends a simple knowledge of the protocols transmitted since assets are represented in an easy-to-categorize map view. Analysts can quickly and automatically organize their different assets by custom zones, as well as view a particular device's history, the last time seen, and the protocols used. They can also conduct deep packet inspection of ICS protocols and create alerts for any new device seen on the network.

The Authority could, in fact, be considered a leader among their peers when it comes to their awareness of the problem and commitment to addressing it. They have been working over the last decade at building a defensible ICS system architecture and instilling a culture of cybersecurity vigilance; however, they also realize the scope of the challenges they face and understand where they can most effectively utilize help from external partners.



CHALLENGE 1 - LACK OF VISIBILITY INTO THE ICS ENVIRONMENT AND ASSET MANAGEMENT

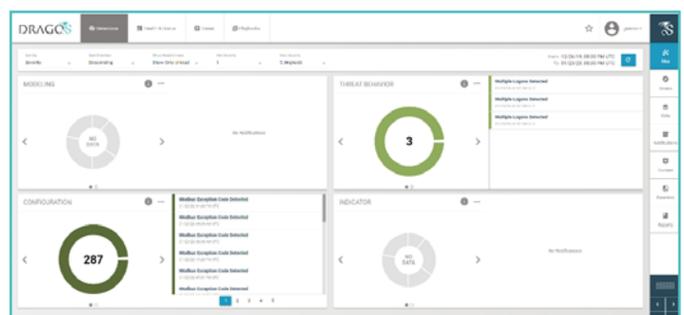
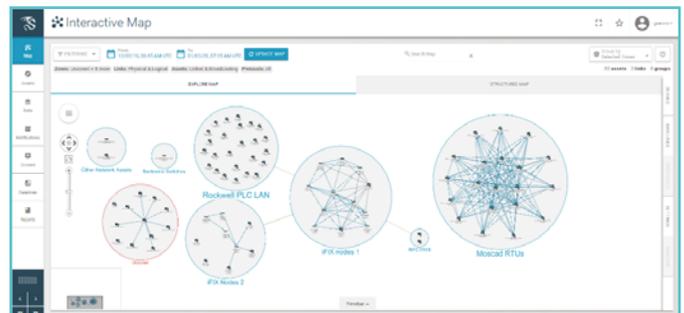
Prior to partnering with Dragos, TRA relied on maintaining fully segregated ICS networks as the backbone of their security. While providing a security barrier, they lacked sufficient visibility into communications occurring in the ICS network and were forced to rely on logs and alerts from perimeter security devices to detect malicious activities. Additionally, assets were tracked in spreadsheets and Microsoft Visio drawings, requiring manpower-intensive updates every time a change was made to one of the assets.



SOLUTION - THE DRAGOS PLATFORM + NEIGHBORHOOD WATCH

The Dragos Platform's in-depth, automated passive asset discovery capabilities, coupled with unique mapping and zoning abilities, allow an asset owner or analyst to gain a comprehensive understanding of their assets. This understanding transcends a simple knowledge of the protocols transmitted since assets are represented in an easy-to-categorize map view. Analysts can quickly and automatically organize their different assets by custom zones, as well as view a particular device's history, the last time seen, and the protocols used. They can also conduct deep packet inspection of ICS protocols and create alerts for any new device seen on the network.

TRA uses this capability as a force multiplier for their limited staff. With their subscription to the Dragos Neighborhood Watch service, these asset identification reports are generated and presented to TRA management on a regular basis, allowing them to focus their attention on alerts rather than producing mundane reports.





CHALLENGE 2 - LACK OF PERSONNEL TO MONITOR AND HUNT FOR THE EVIDENCE OF THREATS AND VULNERABILITIES

Like many asset owners in critical infrastructure, TRA's cybersecurity staff is stretched thin and does not have the specialized ICS security-specific knowledge to perform advanced hunting tasks for the presence of cyber threats within their industrial networks.



SOLUTION - THE DRAGOS PLATFORM + NEIGHBORHOOD WATCH

To address those concerns, the Authority elected to enroll in the Dragos Neighborhood Watch service. With Neighborhood Watch, Trinity is assigned a dedicated Dragos team to remotely monitor their Dragos Platform via a secure cloud connection, triage and add context to any alerts present, and proactively hunt for adversaries. This team has deep expertise in ICS security and is backed by the best ICS security threat intelligence information available.

In addition to monitoring for ICS-specific cyber threats, the Dragos Neighborhood Watch team has an appreciation for the many tools used by control system engineers and administrators, and a solid understanding of many vulnerable ICS tools and practices.

With this knowledge, the Authority's Operations and Security teams can benefit from better situational awareness that Dragos provides before undetected issues become realized as operational problems. In one case, a Neighborhood Watch analyst utilized the Dragos Platform to identify an ICS-specific communications protocol error between the HMI and an endpoint device. In another case, the Dragos team noted that TRA were using a vulnerable web application within their ICS environment. On a routine call, these insecure practices were highlighted to Trinity security leadership so that they could understand and correct the issues.



CHALLENGE 3 - LACK OF INSIGHTS INTO OT-SPECIFIC THREATS AND HOW TO RESPOND TO INCIDENTS

Without specialized OT security analysts and incident responders, TRA was at risk of severe operational, financial and safety impacts in the event of a sophisticated cyberattack. While there were OT/ICS-specific threat intelligence feeds available, translating that information into actionable defensive strategies and effective threat hunts required a very specific skill set the Authority didn't possess in-house. In the event of an incident in the ICS network, the process of reporting the incident and recommended mitigations was in need of improvement.



SOLUTION - THE DRAGOS PLATFORM + NEIGHBORHOOD WATCH

With Dragos Neighborhood Watch, TRA is assured that when new information about an active ICS cybersecurity threat arises, their Dragos Industrial Hunters proactively search for evidence of that behavior in their environment and recommend actions to prevent an incident before it happens.

By receiving tailored incident reports and actionable recommendations in the context

of the ICS network, the OT and Security teams can quickly take decisive action to mitigate any issues. With the Dragos Platform and Neighborhood Watch, the Authority is in a more secure position to deliver on its mission to safeguard the water supply for the citizens of the Trinity River Basin.

DRAGOS PLATFORM & NEIGHBORHOOD WATCH

CASE STUDY TRINITY RIVER AUTHORITY



The **Dragos Neighborhood Watch** team, enabled by **Dragos Platform** technology, provides a level of visibility into our assets and threats that we did not have the expertise nor the bandwidth to do on our own.

DOUG SHORT,
CIO & CISO
TRINITY RIVER AUTHORITY
OF TEXAS

CONCLUSION

The Dragos Platform and Neighborhood Watch provides the visibility and expert analysis that Trinity River Authority needed to give them the assurance that their environment was monitored by experts capable of identifying evidence of malicious activity within their control systems. As an outsourced service, the Neighborhood Watch team alleviated TRA from the burden and expense of maintaining these experts as full-time resources on their own staff. Through their trusted partnership with Dragos, the Authority gets the unique value of Dragos threat intelligence-driven monitoring to look for the latest ICS-focused malicious activity. Finally, the combination of the Dragos Platform and Neighborhood Watch adds further value by identifying insecure practices, vulnerabilities, or configuration errors that would otherwise go unnoticed. This holistic approach ensures TRA is taking appropriate measures to safeguard its water supply facility and the over 240,000 people in its service area that depend on the clean water they provide every day.

LEARN MORE

To learn more about Dragos Platform & Neighborhood Watch, please contact sales@dragos.com or visit dragos.com