CASE STUDY

DRAGOS
SAFEGUARDING CIVILIZATION

Hunting Active Threats in Littleton's Grid with the Dragos Platform and OT Watch

Serving Littleton and Boxborough, Massachusetts, the Littleton Electric Light and Water Departments (LELWD) is a public power utility that grappled with substantial obstacles in safeguarding its operational technology (OT) infrastructure due to its small size and constrained resources. The utility's challenges came to a head when a sophisticated threat group compromised their network to collect data on OT systems, necessitating swift action, expedited implementation of the Dragos Platform, and a rapid response by OT Watch. Dragos worked with the Littleton team to identify, examine, and counteract the persistent breach within their critical systems.

> In collaboration with the American Public Power Association, we were presented with a unique opportunity to engage with various companies that could assist us in achieving our operational goals. We ultimately decided to partner with Dragos because we received numerous positive testimonials from our peers regarding both the quality of their product and the exceptional support provided by their dedicated team.
>
> **David Ketchen, Assistant General Manager at LELWD**

LITTLETON LELWD ELECTRIC LIGHT & WATER DEPARTMENTS

About Littleton Electric Light and Water Departments

Littleton Electric Light and Water Departments (LELWD) is a public power utility serving the communities of Littleton and Boxborough, Massachusetts. The utility was established in 1912 to supply low-cost reliable energy to residents of the town of Littleton. In 1926, the Electric Light Department was granted the franchise rights to service the town of Boxborough. The Littleton Water Department has provided water service to Littleton residents for nearly 100 years and has received national recognition for its aggressive groundwater protection program.

The APPA Grant Program: A Catalyst for Change

LELWD's cybersecurity journey with Dragos began through one of APPA's government-funded programs.

APPA leverages funding to support OT cybersecurity deployments at public power utilities. Through cooperative agreements, APPA members have access to a host of programs and resources, including deployments of monitoring technology like the Dragos Platform. Through its cybersecurity programs to date, APPA has awarded over $14 million to 32 utilities, funding 78 cybersecurity projects.

This context underscores the importance of choosing not just a security vendor, but a true partner in OT cybersecurity. For utilities like LELWD, the decision goes beyond product features; it's about finding a trusted expert who can provide ongoing support, guidance, and cutting-edge solutions tailored to the unique challenges of operational technology environments.

Choosing Dragos as Their OT Security Partner

LELWD went through a careful process to select Dragos as its cybersecurity partner, establishing these criteria to guide decision-making:

Specialized OT Security Expertise
Unlike traditional IT security, OT environments in critical infrastructure require specialized knowledge and tools. Dragos's focus on industrial cybersecurity made it an attractive choice for LELWD, as it could address the unique challenges faced by utilities.

Reputation in the Industry
LELWD's decision was influenced by Dragos's strong reputation, particularly regarding its product quality and support team. This reputation is crucial in the OT security space, where trust and reliability are paramount.

Comprehensive Solution
LELWD was looking for more than just software. It needed a partner that could provide both advanced technology and expert guidance.

Alignment with APPA Goals
APPA's cybersecurity programs aim to enhance cybersecurity for its members. Choosing Dragos aligned with these goals, matching the specific needs of public power utilities.

Long-Term Partnership
LELWD was thinking beyond just implementing a product — it was looking for a long-term partnership with ongoing support and expertise.

Addressing Resource Constraints
As a smaller utility, LELWD faced resource constraints. Choosing a vendor with a strong support team provides access to expertise to augment its internal capabilities.

VOLTZITE Compromise Prompts Rapid Deployment

LELWD's partnership with Dragos was immediately put to the test when it was discovered that a sophisticated threat group, VOLTZITE, had persistent access to LELWD's network. VOLTZITE, a Dragos-identified threat group that overlaps with Volt Typhoon, has been responsible for the widespread compromise of industrial organizations across critical infrastructure sectors since the start of 2023. This development accelerated their cybersecurity journey with Dragos.

To LELWD's credit, the utility had already taken steps to bolster its cybersecurity posture and was implementing the Dragos Platform to gain visibility of its OT assets, secure IT-OT network traffic, and monitor communications between OT devices and systems. Additionally, the utility had initiated the engagement of OT Watch's threat hunting services.

Now prompted to deploy quickly and bypass the planned onboarding timeline, OT Watch identified VOLTZITE actions close to the utility's OT. Specifically, the Dragos Platform confirmed server message block traversal maneuvers and remote desktop protocol lateral movement. OT Watch provided these actionable findings to LELWD, empowering responders to eradicate the adversary and secure the network against additional threats. Further investigation determined that the compromised information did not include any customer-sensitive data, and the utility was able to change their network architecture to remove any advantages for the adversary.

This incident-driven acceleration of Littleton's partnership with Dragos underscored the critical importance of specialized OT security solutions and expert support in the face of unprecedented cyber threats targeting utilities.

Challenges Before Deploying the Dragos Platform

Aside from the VOLTZITE compromise, LELWD faced several other cybersecurity challenges prior to deploying the Dragos Platform:

LIMITED VISIBILITY INTO OT NETWORKS

DIFFICULTY MANAGING VULNERABILITIES EFFECTIVELY

OVERWHELMING VOLUME OF SECURITY ADVISORIES

LACK OF SPECIALIZED OT CYBERSECURITY EXPERTISE

MIXING OF IT AND OT TRAFFIC ON THE SAME NETWORK

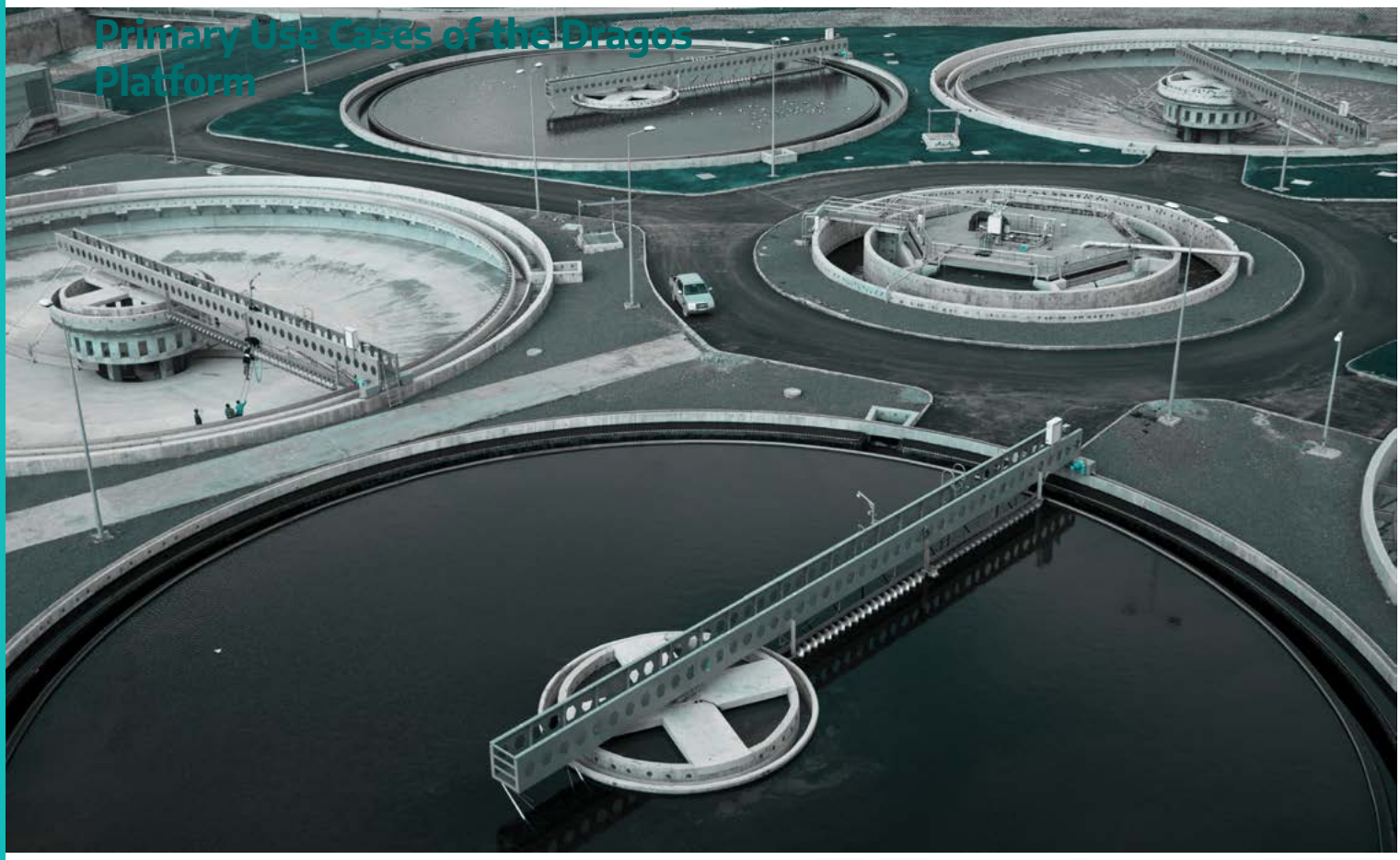
Conor Willard of EvoLab Technology Solutions, a GML Utility Services partner and LELWD's managed service provider, elaborated on previous challenges. "Before implementing the Dragos Platform, there were some visibility gaps when it came to LELWD's OT networks. We were having to manually inventory assets, identify potential security issues, and detect unusual network behavior. This lack of automation meant we were spending a significant amount of time on these tasks. The implementation of Dragos's solution was a very welcomed change, giving us the visibility and control we needed to protect LELWD's critical infrastructure effectively and efficiently."

Primary Use Cases of the Dragos Platform

LELWD leverages the Dragos Platform for several critical use cases.

1. **Asset Visibility and Inventory.** The Dragos Platform utilizes passive network monitoring and deep packet inspection to automatically discover and classify OT assets, providing a comprehensive inventory without disrupting operations.
2. **Threat Detection and Response.** Littleton leverages the platform's advanced analytics and threat intelligence to identify malicious activities, alerting security teams and providing actionable insights for rapid response.
3. **Vulnerability Management.** The Dragos Platform combines asset information with threat intelligence to prioritize vulnerabilities based on actual risk to the OT environment, enabling focused remediation efforts for LELWD's small staff.
4. **Network Segmentation Analysis.** The platform analyzes network traffic patterns to identify potential segmentation issues and recommend improvements to enhance security posture.
5. **Incident Response Guidance.** LELWD is able to see detailed forensic data, threat intelligence, and expert playbooks within the platform to support efficient and effective incident investigation and remediation.

> The improved visibility we gained through the Dragos Platform has been a game-changer for our day-to-day operations.Just being able to see all the IP addressess that we know should or shouldn't be talking to each other, it's huge.
>
> This level of insight allows us to quickly identify and investigate any unusual network communications, potentially catching security breaches or operational issues before they escalate. It's not just about cybersecurity; it's about operational efficiency. We can now optimize our network configurations, troubleshoot issues faster, and ensure that our critical systems are communicating as intended.
>
> This visibility has empowered our team to make data-driven decisions, improve our incident response times, and maintain reliable and secure infrastructure for our community.
>
> **Josh DeTerra,**
> **Supervising Engineer**



Results from Deploying the Dragos Platform and OT Watch

The implementation of the Dragos Platform yielded significant results for LELWD:

1. **Enhanced OT Network Visibility.** The platform provided comprehensive insights into LELWD's OT environment, allowing for better asset management and risk assessment.
2. **Improved Threat Detection.** Dragos's OT Watch team was instrumental in identifying and responding to the VOLTZITE threat activity.
3. **Streamlined Vulnerability Management.** The platform helped prioritize vulnerabilities, making it easier for the small team to manage risks effectively.
4. **Expertise On-Demand.** Access to Dragos's OT security experts provided LELWD with critical support during incidents and for ongoing security improvements.
5. **Efficient Incident Response.** During the VOLTZITE incident, Dragos's rapid response and expertise were crucial in containing and mitigating the threat.

Conclusion

LELWD's partnership with Dragos, facilitated by the APPA cooperative agreement programs, has significantly enhanced the utility's cybersecurity capabilities. From facing a high-profile threat group to developing a proactive security posture, LELWD's journey demonstrates the value of specialized OT security solutions for critical infrastructure providers of all sizes. The combination of advanced technology, expert support, and a commitment to continuous improvement has positioned LELWD to better protect its operations and serve its communities securely in an evolving threat landscape.

> The Dragos team's exceptional response combined calm expertise with strategic insight, contextualizing our situation within the broader threat landscape. Their confident approach reassured us we were in capable hands, providing both technical solutions and the reassurance needed during a critical time.
>
> **David Ketchen, Assistant General Manager**

> Working with Dragos has transformed our approach to cybersecurity, shifting our mindset to see it as an ongoing process requiring constant adaptation. This partnership has empowered us to take ownership of OT security, equipping us to protect critical infrastructure and foster a culture of security awareness throughout our operations.
>
> **Josh DeTerra, Supervising Engineer**

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

Learn more about our technology, services, and threat intelligence offerings:

Request a Demo | Contact Us