

DRAGOS and EMERSON

Protecting Industrial Power and Water Operations from Cyber Threats Together

HIGHLIGHTS

- Emerson has selected and validated the integration of the [Dragos Platform](#) to expand its [Power & Water Cybersecurity Suite](#) (PWCS) for industrial cybersecurity.
- Emerson is augmenting its cybersecurity services for the power and water industries with Dragos' proactive and incident responsive services to help customers detect and respond to threats.
- Emerson and Dragos have co-created targeted protocol dissectors and threat analytics to improve visibility and detection of threats targeting Emerson's Ovation automation technology in power generation and water/wastewater applications.
- Emerson and Dragos offer extensive ICS cybersecurity experience, expertise, and support services to enhance visibility into OT networks and detect threats targeting industrial networks in power plants and water treatment facilities.

THE CHALLENGE

Operations and Management at industrial organizations—including critical infrastructure sectors such as electric utilities water utilities, oil & gas, manufacturing, and others—are tasked with running their plants safely and efficiently. However, increased risks from growing cyber threats (both targeted and untargeted) against Industrial Control System (ICS) and operational technology (OT) networks can jeopardize the primary mission of safe and efficient operations.

In addition, most industrial organizations are moving down the path of digital transformation, enabling innovative new products; better customer support; and, enhanced safety, responsiveness and productivity of their operations. However, this can open operations to additional risk as well, including cyber attacks that may originate in IT networks and pivot into the ICS / OT environment.

Expanded connectivity and a heightened ICS / OT threat landscape bring significant cyber risks to mission critical assets. In order to mitigate these cyber risks and maintain safe, reliable operations, industrial organizations need cybersecurity tools and services that protect production lines or indeed the entire plant.

These cybersecurity tools and services need to work in concert and provide in-depth capabilities to address the gamut of at-risk elements in the environment. This helps ensure the organization is proactively addressing threats, enhancing protection, and reducing risk across their entire ICS / OT environment.

THE SOLUTION

Emerson and Dragos have teamed to help power generation and water/wastewater organizations address cybersecurity concerns:

Product Collaboration: Emerson has validated the integration of the [Dragos Platform](#) into its [Power and Water Cybersecurity Suite](#) (PWCS) for industrial cybersecurity. The Dragos Platform provides passive ICS / OT network monitoring which enables improved asset identification and mapping; proactive anomaly and threat behavior detection; and, better threat response and recovery capabilities. In addition, Dragos is incorporating Ovation platform-specific capabilities into the Dragos platform, including protocol dissectors, asset characterizations, threat behavior analytics, and investigation playbooks to enhance threat detection and response.

Services Collaboration: Emerson and Dragos are jointly supporting customers in the power and water industries by supplementing and expanding Emerson cybersecurity assessment capabilities with the Dragos threat detection and incident response capabilities. To empower cyber defenders, Dragos and Emerson are also collaborating on content to detect threats that specifically target Emerson Ovation automation equipment, including asset characterizations, threat intelligence, and continuously updated response playbooks. In addition, joint Incident Response (IR) engagements from Dragos and Emerson are now available, providing power and water customers with expert threat detection and response across their entire environment. Finally, Dragos and Emerson are also offering proactive tabletop exercises (TTX) and training services to these industries.

These collaborative solutions provide plant managers and cyber defenders with:

- a comprehensive view of all connected assets on the industrial OT network;
- actionable intelligence on threats impacting the network; and
- guided playbooks to mitigate those risks to ensure safety, reliability, and resilience.

BENEFITS and IMPACTS

BENEFIT	IMPACT
Validated Platform	Emerson has tested and validated the Dragos platform for its Power and Water Cybersecurity Suite —enables improved threat detection and response across the entire industrial OT network.
Improved Visibility	Unprecedented visibility into OT environment—allows industrial organizations to assess, monitor and mitigate threats aimed at core ICS networks.
ICS-specific Focus	Continuously updated content packs hyper-focused on ICS networks for Emerson Ovation-specific and other vendors' hardware —provides fast, efficient and effective threat detection, response and mitigation to help maintain safety and uptime.
Expanded Services	A full range of OT cybersecurity services are available throughout Emerson's global services network for power and water customers.
Joint Incident Response (IR)	Holistic incident response that covers entire ICS networks—provides the necessary experience and expertise to respond to any threat efficiently and effectively, thus enabling business operations to continue.
Community Contributions	Joint research and intelligence will be shared with the ICS community through white papers and webinars to enhance education for defenders.



For more information, please visit www.dragos.com or contact us at info@dragos.com.