DRAGOS AND EMERSON

Protecting Industrial Infrastructure from Cyber Threats

HIGHLIGHTS

- Emerson has validated the Dragos Platform into both its Ovation™ automation platform and Power & Water Cybersecurity Suite (PWCS), as well as its DeltaV™ distributed control system (DCS) for industrial cybersecurity.
- Emerson has augmented 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.
- Dragos has incorporated DeltaV™ DCS platform-specific capabilities into the Dragos platform, including protocol dissectors, asset characterizations, threat behavior analytics, and investigation playbooks to expand Emerson's cybersecurity assessment capabilities and enhance threat detection and response for process industries.

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 subsequently open operations to additional risks, 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 throughout 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

Product Collaboration: Emerson has validated the integration of the Dragos Platform into its Ovation™ automation platform and Power and Water Cybersecurity Suite (PWCS), as well as its DeltaV ™ distributed control system (DCS). 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 has incorporated both Ovation™ automation, as well as DeltaV ™ (DCS) platform-specific capabilities into the Dragos Platform, including protocol dissectors, asset characterizations, threat behavior analytics, and investigation playbooks to enhance threat detection and response. This additional layer of protection complements Emerson's robust portfolio of security offerings for industrial control systems.

Protecting critical infrastructure requires a comprehensive approach — not a single vendor or product. In order to provide a complete solution, multiple technologies must operate together without introducing complexity, adversely impacting safety or availability, while helping security teams achieve their goals. Obtaining visibility of events across the enterprise (IT) and ICS (OT) network is essential to operational security and compliance. Understanding and enabling defenders with the ability to react to adversaries that often pivot from enterprise networks to OT is important. Since both IT and OT systems and network technologies, as well as cyber threats, are continually evolving, industrial control system vendors must embrace a lifecycle approach to industrial cybersecurity.

Services Collaboration: Emerson and Dragos are jointly supporting customers within industrial 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 automation equipment, including asset characterizations, threat intelligence, and continuously updated response playbooks. In addition, joint Incident Response (IR) engagements from Dragos and Emerson are available, providing customers with expert threat detection and response across their entire environment. 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 OF EMERSON OVATION

BENEFITS	IMPACTS
Validated Platform	Emerson has tested and validated the Dragos platform for its Power and Water Cybersecurity Suite —enabling 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-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.
Community Contributions	Joint research and intelligence shared with the ICS community through white papers and webinars to enhance education for defenders.

BENEFITS AND IMPACTS OF EMERSON DELTAV

BENEFITS	IMPACTS
Validated Platform	Emerson has validated the Dragos Platform within its DeltaV ™ distributed control system (DCS), providing organizations within the processing and manufacturing industries with greatly enhanced ICS/OT cybersecurity.
Combined Domain Experience	Leverages the industrial and enterprise cybersecurity expertise from Dragos and Emerson to help uncover threats and improve overall security posture.
Intelligence-Driven Threat Detections	Utilizing comprehensive IT and OT threat intelligence as the primary method of detecting threats, which improves detection confidence and reduces alert fatigue.
Enhanced Visibility	Integrating the Dragos Platform with Emerson's DeltaV™ DCS enhances visibility into the DeltaV™ environment, allowing industrial organizations to discover and monitor assets, track and mitigate vulnerabilities, and leverage traffic monitoring information to investigate issues and incidents.
More Efficient Security Operations	Enables defenders with a more comprehensive workflow from initial threat detection through response, improving Mean Time To Recovery.

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