

DRAGOS AND ROCKWELL

Protecting Industrial Operations from Cyber Threats Together

HIGHLIGHTS

- Reduce risk to operations, safety, and intellectual property with the combined ICS cybersecurity experience, expertise, and support services from Rockwell Automation and Dragos.
- Respond to threats confidently with Rockwell Automation's and Dragos's joint proactive and reactive Incident Response services.
- Improve continuity of operations with global insights into threats to your control system environment with proactive threat hunting services and collective defense capabilities from the Dragos Platform and Rockwell Automation advisories.
- Arm your organization with in-depth visibility of threats targeting industrial environments so you can be better prepared to defend with mutually developed OT Threat

THE CHALLENGE

As organizations look to capture operational gains from digital transformation and modernization initiatives there is more interconnectivity between enterprise and industrial networks than ever before. While these interconnections are intended to increase efficiencies in operations, they have also increased the risk of cyber threats.

In operational technology (OT), targeted and untargeted threats that can cause disruptions, lead to loss of intellectual property, cause reputational damage, physical damage, personal injury, or loss of life are expanding in frequency and sophistication.

With the business stakes so high, OT cyber risk management is an organization-wide activity and encompasses different stakeholders than traditional IT security strategies. The CISO plays a pivotal role as a risk advisor, but the risks are owned by each business unit leader and, ultimately, the CEO and board of directors. Therefore, planning and strategy must be done with all the relevant stakeholders and include operations engineers with specialized expertise in keeping OT equipment running and maintaining complex ICS vendor relationships.

THE SOLUTION

Building and maturing an effective OT cybersecurity program requires long-term investments in resources and expertise.

There is no replacement for dedicated OT cybersecurity staffing, but the right technical and professional allies can help you more quickly scale and mature processes.

By combining Rockwell Automation's global industry, application, and industrial cybersecurity domain expertise with Dragos's world-class technology, professional Services, and Threat Intelligence services, customers can accelerate their digital transformation securely while managing risk to protect their core business.

Built by OT cybersecurity practitioners, the Dragos Platform provides teams with visibility into ICS/OT assets and their vulnerabilities, in the context of current threat conditions, with best practices guidance for responding to incidents before they become significant compromises.

With a coalition of OT field service engineering and ICS cybersecurity practitioners, organizations at all stages of maturity can respond to immediate incidents, conduct architecture and vulnerability assessments, hunt for threats, establish technology roadmap and response plans, and conduct tabletop exercises.

Backed by a world-class team of ICS cybersecurity analysts and equipment developer insights, organizations are provided with in-depth visibility to threats targeting industrial environments globally.

Through managed services and collective defense capabilities, customers can improve network visibility and proactively hunt for threats, helping organizations extend existing security operations center (SOC) capabilities without hiring an internal army of security pros with OT expertise, reducing mean time to discovery, and enhanced situational awareness in their ICS.

BENEFITS AND IMPACTS

BENEFITS	IMPACTS
Respond to Threats Confidently	Reduce the cost of cyber incidents and improve operations uptime and availability with the combined global industry, application, and industrial cybersecurity domain expertise of Dragos and Rockwell Automation's joint Incident Response capabilities.
More Efficient Security Operations	Gain in-depth visibility to global threat activity targeting your Rockwell Automation control systems, with specific guidance on how to be better prepared and improve Time to Recovery through joint Threat Intelligence Services.
Improved Visibility into the OT Environments	Reduce alert fatigue with intelligence driven detections based on international industry context, increasing confidence, and reducing mean time to detect. Aligned with common industry frameworks and qualified through global collective defense advisories with Rockwell Automation.
Extend existing SOC capabilities	Reduce mean time to discovery and enhance situational awareness to ICS threats with managed services. Providing proactive threat hunting, triage, fine tuning of tools, and environment specific setup and configuration.

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