

## Data Sheet

# ICS/OT ARCHITECTURE REVIEW

## Evaluate the cybersecurity posture of your ICS/OT environment

### CYBERATTACKS THREATEN TO DERAIL CRITICAL INDUSTRIAL ASSETS

Cyber threats targeting critical industrial assets and infrastructure can be devastating to operations, key industries and communities. It is essential that industrial organizations understand their most critical industrial control systems (ICS) and operational technologies (OT) and the potential consequences of a cyberattack on those systems.

### REVIEW YOUR OPERATIONAL TECHNOLOGIES AND INDUSTRIAL CONTROL SYSTEMS

An ICS/OT architecture review helps you develop a preliminary understanding of your existing network and security posture in relation to your capabilities of protecting against, detecting and responding to a targeted cyberattack. The review evaluates your existing cybersecurity program across your ICS/OT environment to:

- Assess your organization's existing cybersecurity posture, including detection and protection capabilities.
- Analyze network architecture, review documentation and interview staff to improve your overall ICS security program.
- Recommend tactical and strategic steps to mature your organization's ICS security.
- Establish a baseline to institutionalize your current architecture, assets and vulnerabilities, and help develop a better understanding of your unique safety and business continuity risks.

#### KEY BENEFITS:

**Assess risk to critical assets:**  
Understand if your critical assets are at risk of a cyberattack

**Enhance ICS/OT security posture:** Identify and close gaps in your cybersecurity practices and controls

**Prevent industrial cyberattacks:**  
Stop threat actors from exploiting vulnerabilities and disrupting your business operations

**Fortify cybersecurity controls:**  
Get actionable recommendations for improvements based on in-depth intelligence

# KEY SERVICE FEATURES

The ICS/OT architecture review is a partner-delivered service from Dragos that review can be customized depending on your evaluation needs to include:

- **OT Program Assessment:** Dragos' most comprehensive type of Architecture Review evaluates your ICS/OT environment.
- **Program Review:** Review the policies, procedures and organizational structure around your network security. Corporate and site plans may also be evaluated for consistency and completeness.
- **Collection Management Framework (CMF):** Document and institutionalize data sources, outlining what, where, how and how long.
- **Crown Jewel Analysis (CJA):** Identify primary assets and network locations where process disruption would most impact the organization, and analyze the potential consequences of an attack.
- **Topology Review:** Evaluate industrial network segments to identify cybersecurity weaknesses and get recommendations to strengthen architecture and systems.
- **Compromise Assessment:** Analyze your ICS/OT environment's asset maps, indicators of compromise (IOCs), threat behaviors, asset and protocol vulnerabilities, unsecure credentials and more.

# ABOUT DRAGOS

Dragos is the Industrial Cybersecurity expert on a relentless mission to safeguard civilization. In a world of rising cybersecurity incidents, Dragos protects the most critical infrastructure – those that provide us with the tenets of modern civilization – from increasingly capable adversaries who wish to do it harm. Devoted to codifying and sharing our in-depth industry knowledge of ICS/OT systems, Dragos arms industrial defenders around the world with the knowledge and tools to protect their systems as effectively and efficiently as possible.

# CONTACT CROWDSTRIKE

CrowdStrike: **We stop breaches.**

Learn more: [www.crowdstrike.com/services/](http://www.crowdstrike.com/services/)

Email: [services@crowdstrike.com](mailto:services@crowdstrike.com)

Request information: [click here](#)

© 2022 CrowdStrike, Inc. All rights reserved.

## WHY CROWDSTRIKE PARTNERS WITH DRAGOS

CrowdStrike has established an ecosystem of trusted partners to deliver expertise and capacity in key areas of cybersecurity.

**Industrial cybersecurity expertise:** Dragos brings decades of industrial and enterprise cybersecurity expertise to uncover vulnerabilities and threats in your ICS/OT environment.

**Amplified defenses:** Dragos delivers a powerful combination of technology and team expertise to amplify your resources and reinforce your ICS/OT defenses.

**Full-spectrum coverage:** A single Incident Response Retainer (IRR) to engage expert threat detection and response covers the spectrum of IT and OT networks across the converged environment.

