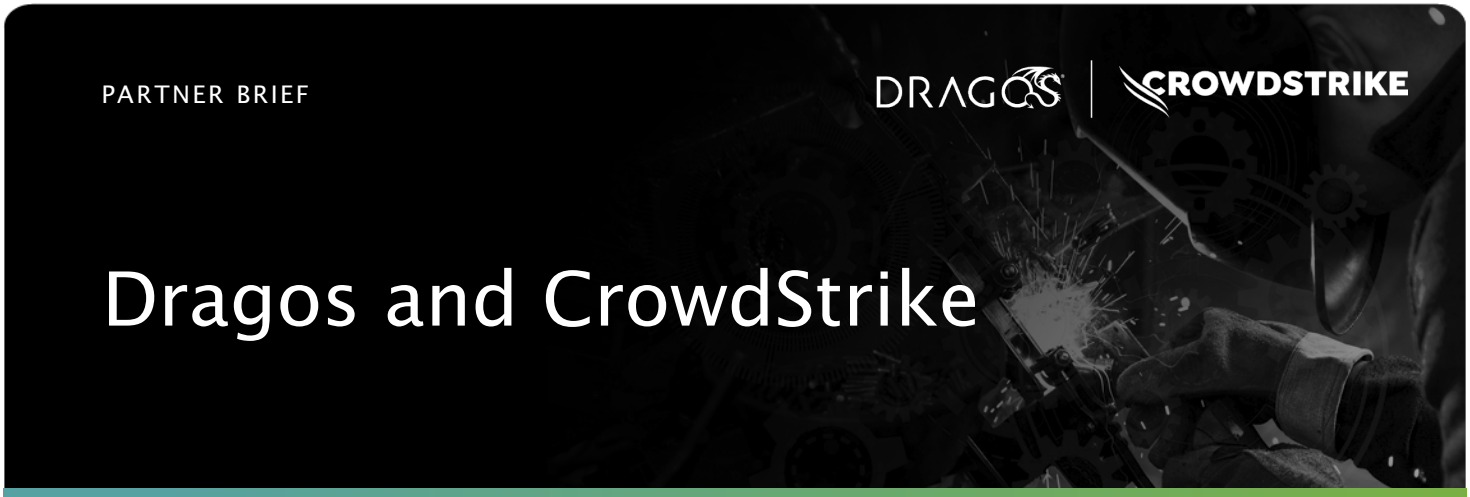
PARTNER BRIEF



Dragos and CrowdStrike

Comprehensive Cybersecurity for IT and OT Networks

HIGHLIGHTS

- Dragos and CrowdStrike® combine to bring an intelligence driven approach to threat detection and response across an industrial organization
- The CrowdStrike Falcon® Insight XDR and the Dragos Platform integration provides EDR enriched asset visibility and detection to enhance cybersecurity across IT and OT networks
- With CrowdStrike Falcon Discover for IOT, customers can leverage asset discovery and vulnerability management details in the Dragos Platform to provide a bilateral flow of information and can also be combined with CrowdStrike's LogScale to centralize log management and gain valuable analysis insights
- The Dragos ICS/OT Threat Detection app provides an early warning system of ICS threat activity in your IT network, leveraging exclusive Dragos ICS threat intelligence indicators of compromise
- CrowdStrike Retainer customers can use their hours to have Dragos evaluate the cybersecurity posture of their OT environment with an ICS/OT Architecture Review

THE CHALLENGE

Industrial infrastructure organizations in electric utilities, oil & gas, and manufacturing, must provide complete cybersecurity coverage for both their information technology (IT) and operational technology (OT) environments.

Despite the growing interconnectivity of the enterprise IT and OT networks, critical challenges remain – cybersecurity ownership is often fragmented across the organization, the IT network and industrial control systems (ICS) are very different and use different technologies, and the teams have different needs, skill sets, and use different tools and processes.

Cybersecurity analysts across organizations strive to bridge this gap with the need to understand and protect against both IT and OT threats. These analysts now look to an aggregated approach for

ingesting, leveraging, and acting on both enterprise IT and OT network data for effective detection across both environments. This data affords them faster identification of known threats and expedites investigation of cyber events.

This deep insight is needed across the entire IT/OT environment to enable cyber defenders to quickly identify and respond to threats and provides them with defense recommendations to better prepare for future cyber incidents.

THE SOLUTION

Dragos and CrowdStrike have partnered together to provide industrial organizations with a holistic cybersecurity offering that covers both IT and OT environments with industry leading technology, IT and OT threat intelligence, and proactive and incident response services.

The Dragos Platform is an ICS cybersecurity technology that provides comprehensive visibility of your ICS/OT assets and the threats you face, with best-practice guidance to respond before a significant compromise.

Backed by the industry's largest and most experienced team of ICS cybersecurity practitioners, Dragos WorldView threat intelligence arms your organization with in-depth visibility of threats targeting industrial environments globally and the tried-and-true defensive recommendations to combat them.

CrowdStrike Falcon® Insight XDR delivers continuous, comprehensive visibility that spans detection, investigation, and response to ensure nothing is missed and potential breaches are stopped.

Detecting, responding to, and mitigating threats across enterprise (IT) and operations (OT) environments requires industry expertise and an in-depth understanding of the tactics, techniques, and procedures (TTPs) by which adversaries exploit gaps that may exist in IT and OT environments. In addition, the highly experienced Dragos and CrowdStrike teams leverage the latest technology and intelligence during an incident response to quickly identify threats, eject them from the environment, and give cyber defenders deep insight into preventing further incidents.

Together, Dragos and CrowdStrike provide unparalleled asset visibility, threat detection, and response coverage of IT/OT environments, with demonstrated synergies across threat detection and response platforms, threat intelligence, and proactive threat prevention services.

COMPREHENSIVE IT/OT CYBERSECURITY

	Dragos (OT)	CrowdStrike (IT)
Platform	In-depth ICS/OT asset visibility, comprehensive vulnerability management and threat detection.	Automates endpoint and network monitoring to enable threat detection, and incident response on both IT and OT networks (with Dragos integration).
Threat Intelligence	In-depth visibility of threats targeting industrial environments globally and defensive recommendations.	Provides security teams with the enterprise threat intelligence tools and insight required to combat cyber threats across their whole network.

Professional Services	ICS/OT services that include Architecture Reviews, Program Assessments, Crown Jewel Analysis, Compromise Assessment, and Incident Response.	Ensures organizations are prepared throughout the entire threat lifecycle across the entire IT/OT environment (with Dragos).

To defend these environments and provide comprehensive IT/OT cybersecurity, industrial organizations need a holistic approach that utilizes a combination of both IT and OT cybersecurity tools and skills.

This is particularly critical when pursuing network security and maintaining interoperability in an environment without disrupting critical services, especially when a cyber event occurs. Having the proper teams and structure in place – including internal expertise and industry-leading partners to address both IT and OT sides of the environment – will help improve recovery time when a cyber event does occur and effectively provide expert threat protection, detection and response to cyber events targeting enterprise IT and industrial OT networks.

BENEFITS AND IMPACTS

BENEFITS	IMPACTS
Combined Domain Experience	Leverages the industrial and enterprise cybersecurity expertise from Dragos and CrowdStrike to help uncover threats and improve overall security posture.
Build Internal Team Expertise	Train industrial cybersecurity teams to ensure knowledge transfer and expertise and develop robust internal defensive capabilities.
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 of IT and OT Networks	Integrating the Dragos Platform with CrowdStrike Falcon® Insight XDR, ensures more effective asset visibility, threat detection, and response in both the IT and OT domains. Integrating the Dragos Platform with CrowdStrike Falcon Discover for IoT allows customers to take advantage of the comprehensive visibility from Dragos and CrowdStrike into a single solution.
More Efficient Security Operations	Integrating the technologies enables defenders with a more comprehensive workflow from initial threat detection through response, improving Mean Time To Recovery.

For more information, please visit dragos.com/partner/crowdstrike or contact us at **info@dragos.com**