DRAGOS and CROWDSTRIKE
Complete Cybersecurity for IT and OT Networks

HIGHLIGHTS

- Customers benefit from extensive cybersecurity experience across both enterprise and industrial networks.
- Dragos and CrowdStrike® combine to bring an intelligence-driven approach to threat detection and response across an entire organization.
- The combination of endpoint and network level detection technologies provides customers with in-depth insights to enhance security across an entire organization.
- Joint Incident Response (IR) retainer package offers expert threat detection and response across the entire environment, covering both enterprise IT and industrial OT networks.
- The ICS/OT Threat Detection app analyzes existing CrowdStrike Falcon® endpoint data and provides early warning of ICS / OT threat activity in IT networks.

THE CHALLENGE

Industrial organizations – including critical infrastructure sectors like electric utilities, oil & gas, water utilities, manufacturing, and others – must provide complete security coverage for both their Information Technology (IT) and Industrial Control System (ICS) environments.

Yet despite the growing interconnectivity of the enterprise IT and Operational Technology (OT) networks, cybersecurity ownership is often fragmented across the organization.

For one, the IT / OT networks in these environments are different – they use different technologies, have different needs, and require different tools and processes. For another, the cybersecurity teams protecting them are different – they have a different focus, leverage different skill sets, and use different tools and processes.

OT & IT ENVIRONMENT EXPERTISE	OT & IT ENVIRONMENT INVESTIGATIONS
Challenge: Security teams are being tasked with comprehensively covering both IT and OT systems at industrial organizations, despite being two fundamentally different missions requiring two different in-depth skill sets that one person or one siloed team typically does not possess.	**Challenge**: Standard IT best practices are ineffective in OT environments; therefore, coverage of both environments needs to be carefully planned and implemented to ensure complete detection capability while maintaining continuous operations and system availability.
Solution: Leverage the expertise and experience of industry-leading Dragos and CrowdStrike platforms, IT & OT threat intelligence, and proactive & responsive services to improve your security posture and make informed decisions on how to better prioritize security focus and resources.	**Solution**: Dragos and CrowdStrike deliver the technology, threat intelligence, and services to discover, respond, and recover from adversaries' threats anywhere in the network, across both enterprise IT and ICS environments.
Benefit: Prepared security teams leverage asset identification & anomaly detection and threat detection & mitigation technology and services to get a deeper insight and better visibility into adversaries across the integrated environment for a proactive stance, reducing adversary dwell time and quickly restoring safe operation.	**Benefit**: Security analysts benefit from extensive OT and IT cybersecurity experience through platform technology and/or via services engagement. Regardless of the approach used, analysts can quickly pivot as needed to handle cyber threats across the entire IT / OT environment.

Therefore, to comprehensively defend these converged environments against cyber threats, cybersecurity teams at industrial organizations must work together using a combination of both IT and OT cybersecurity tools and skills.

This is particularly evident 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.

In order to achieve a better cybersecurity posture, industrial organizations need a holistic approach which quickly and effectively provides expert proactive threat protection, detection and response to cyber events targeting enterprise IT and industrial OT networks.

THE SOLUTION

Dragos and CrowdStrike have teamed together to provide industrial organizations with the most holistic cybersecurity offering that covers both IT and OT environments with industry-leading Dragos and CrowdStrike platforms, IT and OT threat intelligence, and proactive and incident response services.

Customers benefit from improved security postures with proactive assessments, network monitoring, and threat intelligence; faster response times and reduced adversary dwell times; IT and OT-focused technology that empower security teams; as well as expert incident response services.

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.

The Dragos ICS cybersecurity ecosystem provides security defenders with unprecedented situational awareness over their OT environments, with comprehensive asset identification and mapping, threat intelligence, threat detection, and incident response capabilities. Likewise, CrowdStrike provides security technology and services focused on identifying advanced threats and targeted attacks against IT environments.

Together, Dragos and CrowdStrike provide unparalleled 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.

	OT ENVIRONMENT	IT ENVIRONMENT	
Threat Detection and Response Technology	Dragos Industrial Cybersecurity Platform	CrowdStrike Falcon Platform	Automates endpoint and network monitoring to enable threat detection, and incident response on both IT and OT networks.
Threat Intelligence	Dragos WorldView	CrowdStrike Falcon X	Provides security teams with the ICS **and** the enterprise threat intelligence tools and insight required to combat cyber threats across their whole network.
Threat Detection and Incident Response Services	Dragos Professional Services	CrowdStrike Services	Ensures organizations are prepared throughout the entire threat lifecycle across the entire IT / OT environment.

BENEFITS and IMPACT

BENEFITS	IMPACT
Expertise & Commitment	Leverage decades of industrial **and** enterprise cybersecurity expertise to uncover vulnerabilities and threats, and to improve overall security posture.
Build Internal Expertise	Train industrial cybersecurity teams and ensure knowledge transfer and expertise to develop robust internal defensive capabilities.
IT and OT Threat Intelligence	Gain visibility and understanding of threats for both enterprise IT and ICS operations networks to improve detection and response, reducing attacker dwell time.
Platform Technology	Deploy endpoint and network-based tools to enable detection of threats across both IT and OT networks and to provide defenders with step-by-step guides to counter threats.
Joint IR Retainer	Cover the spectrum of IT and OT networks under one Incident Response (IR) retainer agreement to engage expert threat detection and response across the converged environment.
Integrated Technology	The ICS/OT Threat Detection App analyzes event-based telemetry gathered by CrowdStrike to detect OT threats in managed endpoints, to visualize key ICS threat data, and to pivot into Falcon for further investigation and mitigation.

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