CrowdStrike Store

Data Sheet

DRAGOS: ICS/OT THREAT DETECTION

Identify and respond to adversary threats in your industrial networks

CHALLENGES

Security teams at industrial organizations — including those in critical infrastructure sectors such as electric utilities, water utilities, manufacturing, and oil and gas — face many challenges in protecting their industrial control system (ICS) or operational technology (OT) networks, including:

- IT security teams with limited tools and visibility to detect adversaries in their ICS networks
- ICS security teams with no access to endpoint data or other device data in their OT networks

These silos of data and security teams' tools and purview allow adversaries to gain a foothold and remain hidden in your ICS networks. This increases the adversary's dwell time and their likelihood of attaining their goals — reconnaissance, monitoring your network, stealing intellectual property (IP) or worse.

SOLUTION

The Dragos ICS/OT Threat Detection app for CrowdStrike provides needed visibility into ICS threat activity in your IT network, as it is not available via typical IT security tools because of the specialized tactics, techniques and procedures (TTPs) used by ICS adversaries. Because many ICS adversaries initiate their attacks via IT networks, this Dragos-fueled visibility provides valuable early warning to security teams protecting OT networks. Dragos' powerful app allows you to analyze your existing endpoint data collection in the CrowdStrike Falcon® platform for indications of ICS adversary activities and provides visibility into ICS adversary events and impacted devices, enabling further investigation in the Falcon platform.

KEY BENEFITS

Easily import Dragos' repository of over 25,000 industrial indicators of compromise (IOCs) to broaden existing detection capabilities

Gain visibility into ICS threats discovered in your existing Falcon platform data

Get early warning of ICS threat activity in your IT network by leveraging Dragos ICS expertise

Access additional context of ICS threat activity via the Dragos WorldView threat intelligence report (available to WorldView subscribers)

DRAGOS: ICS/OT THREAT DETECTION

BUSINESS VALUE

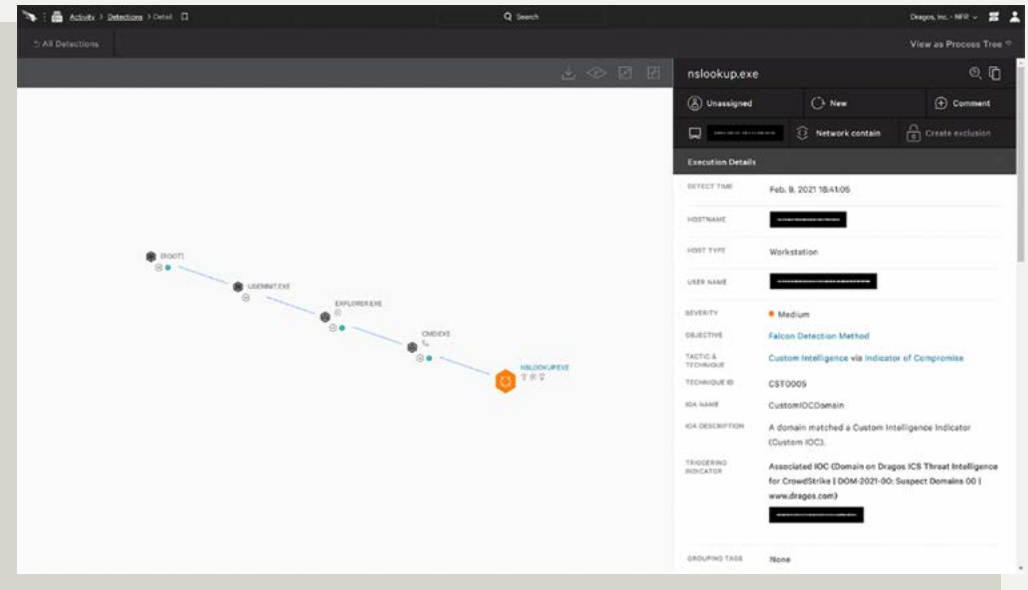
Use Case/Challenge	Solution	Benefits
Visibility into ICS/OT threats found on Falcon endpoints	Use intelligence-driven insights from Dragos' threat intelligence team to improve detection of ICS-focused adversaries operating in enterprise networks	Eliminate blindspots in protecting converged IT/OT networks
Insights into OT threat activity in your IT network sorted by ICS-focused threat activity group, event type and impacted device(s)	Enhance the the Falcon platform's native detection capabilities with Dragos' extensive repository of industrial threat indicators to detect OT threats	Catch ICS threat activity in IT environments for protection beyond your OT network boundaries
Listing of ICS/OT-focused IOCs that impact endpoint assets	Receive early warnings about potential ICS threats before they impact your production systems	Deploy the app via the CrowdStrike Store with no need to deploy additional agents on endpoints

"Together, Dragos and CrowdStrike offer organizations an unparalleled ability to detect and respond to threats across both the enterprise and industrial environments."

Robert M. Lee,
Co-founder and CEO, Dragos

TECHNICAL SOLUTION

The Dragos ICS/OT Threat Detection app uploads the complete Dragos ICS indicator repository to the Falcon platform, further enhancing its detection capabilities. The indicators include file hashes, IP addresses and domain names of threats known to target OT. Once activated, the Dragos detections become a native part of the Falcon detection engine and will automatically notify analysts when a threat has been detected. The analyst can then perform response activities within the Falcon platform.



KEY CAPABILITIES

- **Expanded visibility:** Leverage Dragos ICS threat intelligence within CrowdStrike Falcon.
- **Early warning:** Catch ICS threat activity in IT environments for protection beyond your OT network.
- **Zero implementation:** Deploy the app directly within your existing Falcon environment using the CrowdStrike Store with no additional agent deployments on endpoints.
- **Reduced workload:** Streamline your workflow when investigating industrial IOCs or suspicious events flagged by Dragos directly within the Falcon user interface.

Dragos is a trusted **CrowdStrike Store Partner**, providing a secure application, leveraging rich data from the CrowdStrike Security Cloud and extending the Falcon platform's capabilities with Dragos' industrial cybersecurity capabilities. Visit the **CrowdStrike Store** for a free trial.

ABOUT DRAGOS

Dragos has a global mission: to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The practitioners who founded Dragos were drawn to this mission through decades of government and private sector experience. Dragos codifies the knowledge of our cybersecurity experts into an integrated software platform that provides customers critical visibility into industrial control systems (ICS) and operational technology (OT) networks so that threats are identified and can be addressed before they become significant events. Our solutions protect organizations across a range of industries, including power and water utilities, energy, and manufacturing, and are optimized for emerging applications like the Industrial Internet of Things (IIOT).

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Try the App
in the CrowdStrike Store

Learn more **www.crowdstrike.com**