ICS/OT THREAT DETECTION APP

Detect Industrial Threats in Your Enterprise Networks

HIGHLIGHTS

The Dragos ICS/OT Threat Detection app provides CrowdStrike® customers with:

- Easy importation of Dragos's repository of over 25,000 industrial IOC's to broaden existing detection capabilities.
- Visibility into ICS threats discovered in your existing Falcon platform data.
- Early warning of ICS threat activity in your IT network leveraging Dragos ICS expertise.
- Additional context of ICS threat activity via Dragos WorldView threat intelligence report (available to WorldView subscribers).

The Dragos ICS/OT Threat Detection app is available now via the CrowdStrike Store.

OVERVIEW

In today's threat environment, industrial focused adversaries are known to gain access to control systems by leveraging initial access to enterprise IT networks and then pivoting into production OT (Operational Technology) networks.

The Dragos ICS/OT Threat Detection app provides intelligence driven insights from Dragos's Threat Intelligence team to improve detection of ICS (Industrial Control Systems) focused adversaries operating in Enterprise networks. Utilizing Dragos's extensive repository of industrial threat indicators, CrowdStrike Falcon® platform customers enhance the native detection capabilities of Falcon to detect OT threats. Understanding OT adversaries operating in your IT network serves as an early warning about potential ICS threats before they impact your production systems.

The app is well suited for any industrial company that is developing a more robust ICS cyber security program but might not yet be prepared for more comprehensive technology such as the Dragos Platform.

THE CHALLENGE

Security teams at industrial organizations, including critical infrastructure sectors such as electric utilities, oil & gas, water utilities, manufacturing, and others, face many challenges in protecting their ICS or OT networks, including:

- IT security teams have limited tools and visibility to detect ICS adversaries in their networks.
- ICS security teams generally do not have access to data from endpoints and other devices in the IT network.

These silos of data and security teams' tools and purview allow ICS adversaries to gain a foothold and remain hidden in networks. This increases the adversary's dwell time and the likelihood of them successfully attaining their goals, be it a reconnaissance mission, simply monitoring your network, IP theft, or worse.

THE SOLUTION

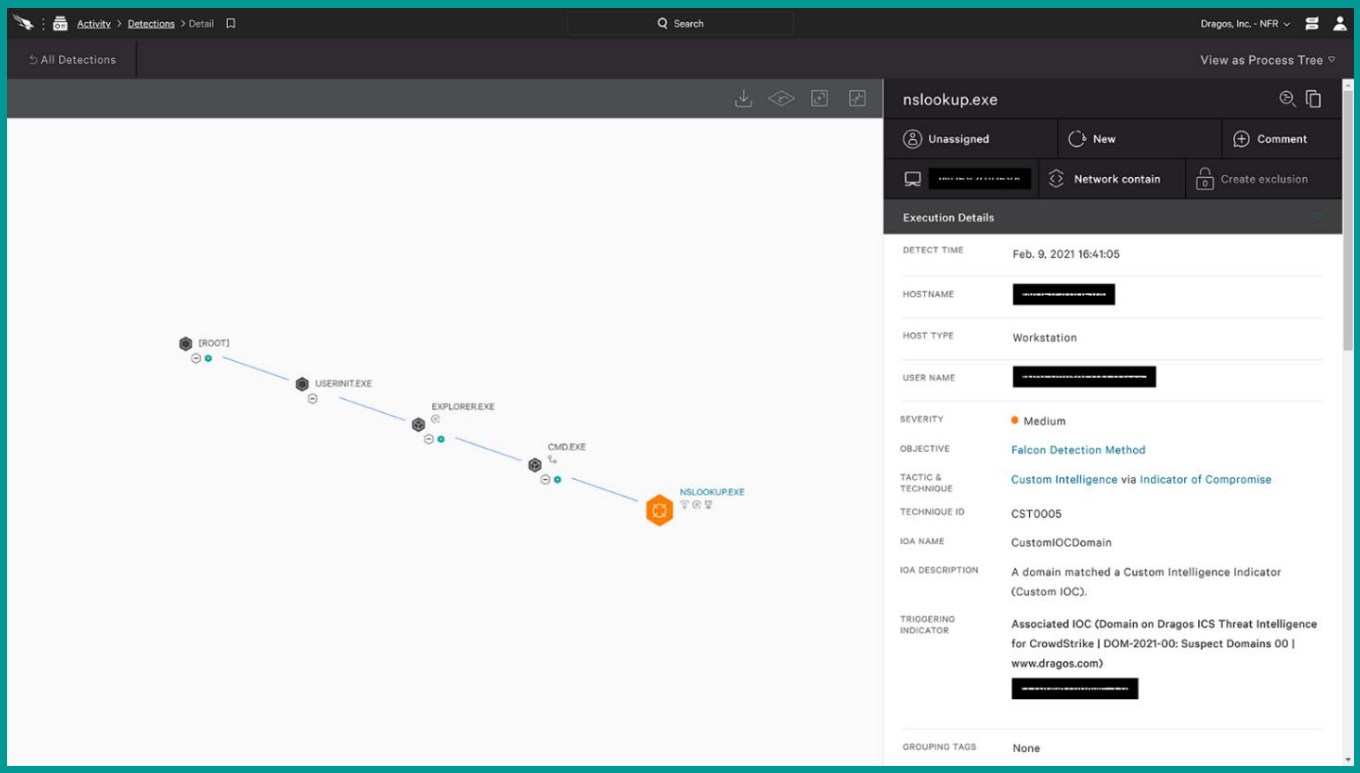
The Dragos ICS/OT Threat Detection app for CrowdStrike provides visibility into ICS threat activity in your IT network, which is not available via typical IT security tools because of the specialized tactics, techniques, and procedures used by ICS adversaries. Since many ICS adversaries initiate their attacks via IT networks, this provides valuable early warning to security teams protecting OT networks.

The Dragos ICS/OT Threat Detection app allows you to analyze your existing endpoint data collection in the Falcon platform for indications of ICS adversary activities and provides you with visibility into ICS adversary events and impacted devices, enabling further investigation in your CrowdStrike Falcon platform. Powered by the highly experienced ICS-focused intelligence team at Dragos that actively investigate adversary tradecraft to provide you with the latest and most relevant ICS threat detection capabilities.

HOW IT WORKS

The Dragos ICS/OT Threat Detection app allows uploads the complete Dragos ICS indicator repository to your CrowdStrike Falcon deployment, further enhancing its detection capabilities. The indicators include file hashes, IP addresses, and domain names of known OT targeting threats. 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 their usual response activities natively within the Falcon user interface.

The screenshot below provides an example of how, after detecting threat activity based on Dragos IOC's, analysts would follow their typical response process. By jumping into the detailed detection, they can gather additional information such as the impacted endpoint, the responsible user, the executing process, surrounding events, and the triggering indicator provided by Dragos.



The app encapsulates Dragos' unique view of the ICS threat landscape and our proven experience and expertise in detecting and mitigating those threats. It leverages Dragos WorldView industrial threat intelligence against endpoint data collected in your CrowdStrike Falcon platform, allowing your security team to visualize key ICS threat data and to pivot into your managed instances for further investigation and mitigation.

The Dragos app is ideal for industrial clients developing an OT cybersecurity program, but when combined with Dragos Platform, customers benefit from more complete threat detection and response capabilities across the IT and OT environments, further reducing adversary dwell time and any associated impact to operations.

BENEFITS AND IMPACT

BENEFITS	IMPACT
Expanded Visibility	Leverage Dragos ICS threat intelligence within the CrowdStrike Falcon platform to eliminate blindspots in protecting converged IT / OT networks protection.
Early Warning	Catch ICS threat activity in IT environments for protection beyond the boundaries of your OT network.
Zero Implementation	Deploy the app directly on existing CrowdStrike Falcon platforms 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 CrowdStrike Falcon user interface.

CrowdStrike customers can download the Dragos ICS/OT Threat Detection app from the CrowdStrike Store at: https://www.crowdstrike.com/endpoint-security-products/crowdstrike-store/

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