DRAGOS

CROWDSTRIKE

SOLUTION BRIEF

DRAGOS: ICS/OT THREAT DETECTION

Detect Industrial Threats in Your Enterprise Networks

CHALLENGES:

Security teams at industrial organizations, including critical infrastructure sectors such as electric utilities, oil and 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 endpoint or other device data 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 your 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.

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. This powerful 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.

KEY BENEFITS

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).

BUSINESS VALUE:

USE CASE / CHALLENGE

- Visibility into industrial (OT) threats found on Falcon endpoints.
- Insights into OT threat activity in IT network by ICS-focused threat activity group, event type and impacted device(s).
- Listing of ICS / OT focused Indicators of Compromise (IOCs) impacting endpoint assets.

SOLUTION DESCRIPTION

- Intelligence driven insights from Dragos's Threat Intelligence team to improve detection of ICS-focused adversaries operating in Enterprise networks
- Dragos's extensive repository of industrial threat indicators enhance the native detection capabilities of Falcon to detect OT threats.
- Early warnings delivered about potential ICS threats before they impact your production systems.

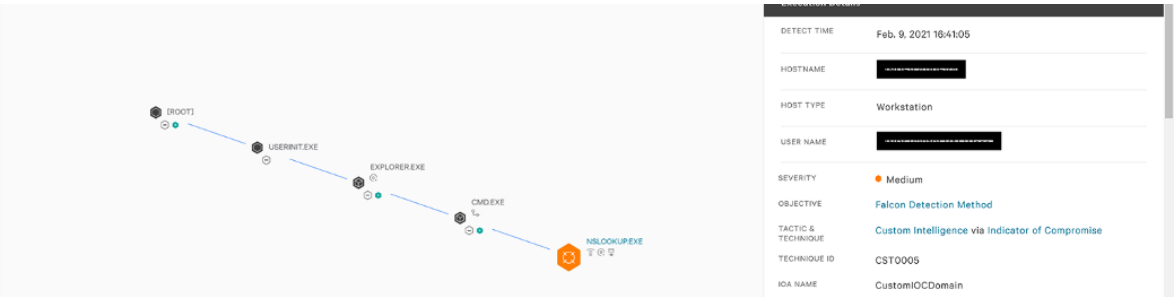
BENEFITS

- Eliminate blindspots in protecting converged IT / OT networks protection.
- Catch ICS threat activity in IT environments for protection beyond the boundaries of your OT network.
- Deploy the app using the CrowdStrike Store with no additional agent deployments on endpoints.

SOLUTION BRIEF

TECHNICAL SOLUTION:

The Dragos ICS/OT Threat Detection app uploads the complete Dragos ICS indicator repository to CrowdStrike Falcon, 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 response activities within Falcon.



KEY SOLUTION 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 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.

"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 Chief Executive Officer

CrowdStrike customers can download the Dragos ICS/OT Threat Detection app from the CrowdStrike Store.

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® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over two trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/