SOLUTION BRIEF

Integrated Cybersecurity Technology from Dragos and CrowdStrike

Endpoint enriched visibility, detection, and response for improved IT/OT cybersecurity

HIGHLIGHTS

- Improve asset visibility and threat detection with enriched endpoint detection and response (EDR) asset information discovered in OT networks
- Enable a coordinated response of industrial control system (ICS) threat activity in your IT network by raising event notifications to a known OT asset
- Leverage the Dragos Platform's visibility of ICS/OT assets and threats, threat behavior analytics, and investigation playbooks with best-practice guidance
- Coordinate response efforts by using the wide range of CrowdStrike Indicators of Compromise (IOC) on known OT assets that could impact edge ICS devices

In today's threat environment, industrial focused adversaries are known to gain access to control systems by leveraging initial access to enterprise information technology (IT) networks and then pivoting into operational technology (OT) networks. Dragos and CrowdStrike are working together to help organizations implement a defensible architecture to protect against cybersecurity threats that impact both IT and OT environments.

THE CHALLENGE

Cybersecurity teams at industrial infrastructure organizations in electric utilities, oil & gas, manufacturing, and others, face many challenges in protecting and assessing risk to their IT and OT networks. Securing today's OT environments comes with various challenges through increased ICS connectivity, unique protocols, legacy systems, and an expanding attack surface as companies embrace digital transformation.

Because of these challenges, there is an increasing demand for cybersecurity teams to have a broader view of the entire network, including IT and OT, which is often limited across endpoints and devices in the IT network.

These silos of data, simplistic cybersecurity tools and limited purview allow ICS adversaries to gain a foothold and remain hidden in networks, increasing the adversary's dwell time and the likelihood of them successfully attaining their goals.

The risk to these organizations is magnified as threats to ICS increase in frequency and sophistication, with potentially significant consequences. Analysts require complete situational awareness to make critical decisions as efficiently as possible.

THE SOLUTION

To address these challenges, Dragos, in collaboration with CrowdStrike, is making it easier for organizations to monitor, detect and respond to threats across their IT and OT environments.

Together, CrowdStrike Falcon® Insight XDR and the Dragos Platform integration allows users to pull EDR asset information from CrowdStrike to enrich device information in the Dragos Platform, improving OT asset visibility and threat detection. The integration also provides early warnings of ICS threat activity in IT networks with event detection that allows users to raise notifications for threat events relating to a known asset.

In addition, CrowdStrike users can leverage the Dragos Platform's comprehensive visibility of ICS/OT assets and threats, including protocol dissectors, asset characterizations, threat behavior analytics, and investigation playbooks with best-practice guidance to respond. Teams are also enabled to rapidly pinpoint malicious behavior on ICS/OT networks, to provide in-depth context of alerts, and reduce false positives for unparalleled threat detection.

Furthermore, the Dragos ICS/OT Threat Detection app in the CrowdStrike Marketplace provides additional detection capabilities with the complete Dragos ICS Indicators of Compromise (IOCs) repository.

HOW IT WORKS

The CrowdStrike Falcon® Insight XDR and the Dragos Platform integration can be configured within the Dragos Platform.

EDR Enriched Visibility and Detection

Enrich your Dragos Platform asset visibility and detection capabilities by taking advantage of Windows based devices already managed by Falcon Insight XDR. The integration enhances your team's ability to quickly understand what is happening in their OT environment and respond faster by passing through device information and detections against known assets.

By pulling EDR asset information from CrowdStrike, you get enriched and enhanced device information of known assets in the Dragos Platform, including IP address, MAC address, endpoint hostname, associated AD Domain, OS data fields and additional custom attributes. This integration also provides additional context on edge devices in OT environments allowing users to forward CrowdStrike Falcon detections on known assets to the Dragos Platform for accelerated remediation.

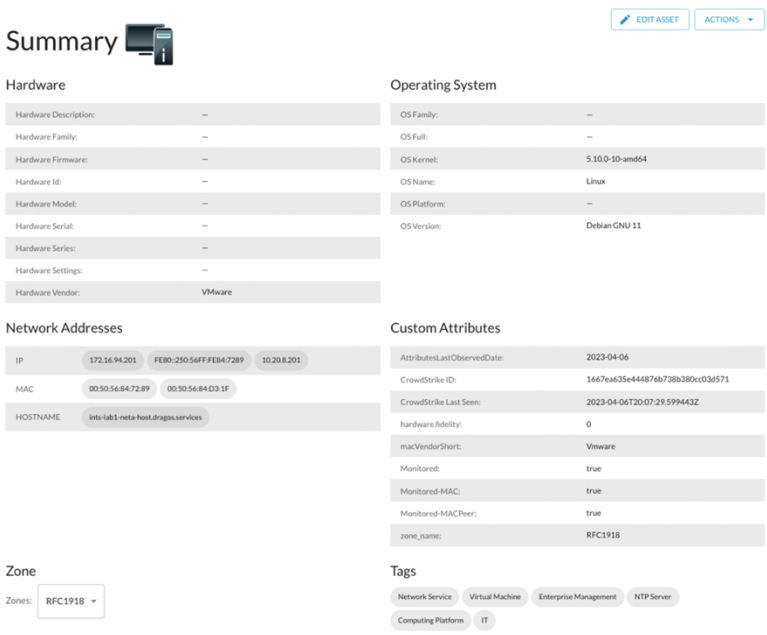

Figure 1. Asset summary with enriched data fields and additional custom attributes.

In addition, the Dragos Platform provides you with the ability to leverage ICS/OT asset visibility and threat detection, that analyzes multiple data sources including protocols, network traffic, data historians, host logs, asset characterizations, and anomalies for rich threat context.

Strengthen IT/OT Collaboration

To help facilitate collaboration between IT and OT security teams and strengthen communication strategies, this integration helps coordinate response efforts on known OT assets leverage the wide range of CrowdStrike Indicators of Compromise (IOCs) that could impact edge ICS devices and forward detections to the Dragos Platform to coordinate activity across response teams.

Additionally, your team can leverage CrowdStrike Falcon Discover for IoT to access the Dragos Platform's repository of OT assets, threat detection, and vulnerability information. Get richer visibility faster, accelerate proactive vulnerability management and, especially when combined with CrowdStrike's Falcon LogScale to centralize log management and gain valuable analysis insights.

The Dragos ICS/OT Threat Detection app

The Dragos ICS/OT Threat Detection app, available in the CrowdStrike Marketplace, enhances CrowdStrike Falcon detection capabilities, allowing users to import the complete Dragos ICS indicator repository (over 25,000 Industrial IOCs). These indicators include file hashes, IP addresses, and domain names of known OT targeting threats.

Once activated, the Dragos detections provides context enrichment directly to Falcon detections, automatically notifying analysts when a threat has been detected for an early warning for ICS threats originating in the IT environments.

The app allows you to accelerate IoT/OT-specific threat detection, investigation and response with deep context and integrated response actions to prevent compromise and lateral movement.

Use Case: After detecting threat activity based on Dragos IOC's, analysts would follow their typical response process. By utilizing these detailed detections, analysts can gather additional information such as the impacted endpoint, IP & MAC addresses, OS, AD domain, the responsible user, the executing process, surrounding events, and the triggering indicator provided by Dragos.

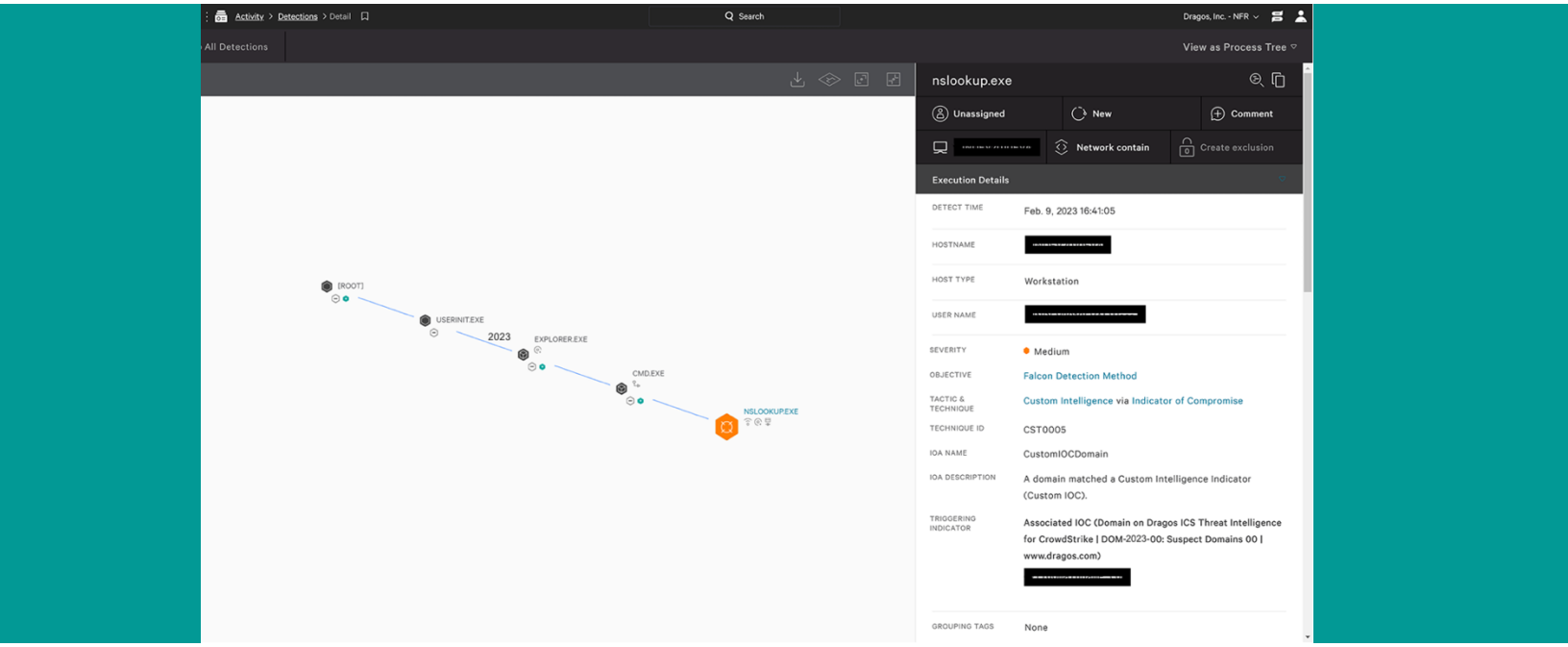

Figure 2. Detecting Dragos IOC threat activity in the CrowdStrike dashboard.

[Download the Dragos ICS/OT Threat Detection app]: Gain rich context immediately without additional infrastructure or deployment.

The Dragos integration with CrowdStrike provides visibility into ICS threat activity across your endpoints and IT network. Since many ICS adversaries initiate their attacks via IT networks, this provides valuable early warning to security teams to ensure they gain complete protection for OT networks.

TECHNICAL BENEFITS OF THE INTEGRATED CROWDSTRIKE AND DRAGOS SOLUTIONS INCLUDE:

- Leverage Dragos ICS asset visibility and threat intelligence to enrich device information discovered in your existing CrowdStrike Falcon data to protect converged IT / OT networks.
- Gain visibility faster by deploying CrowdStrike Falcon sensors integrated with Dragos across your IT/OT environment.
- Perform more thorough investigations and root cause analysis across IT and OT to reduce mean time to detection & recovery.
- Streamline your workflow when investigating industrial IOCs or suspicious events flagged by Dragos directly within the CrowdStrike Falcon user interface.
- Spans the needs of security professionals for both IT and OT networks for improved situational awareness and decision-making.

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