SOLUTION BRIEF

ICS/OT Threat Detection App

Detect Industrial Threats in Your CrowdStrike Falcon Endpoint Data

HIGHLIGHTS

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

- Visibility into ICS threats found in your existing Falcon platform data.
- Early warning of ICS threat activity in your IT network by leveraging Dragos ICS expertise.
- Insight into ICS threat activity in your IT network by adversary group, event type and impacted device(s).

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

OVERVIEW

In today's threat environment, ICS-focused adversaries are known to penetrate industrial organizations via the enterprise IT network and then pivot into the production (OT) network.

The Dragos ICS/OT Threat Detection app provides intelligence-driven insights as threat indicators on your CrowdStrike Falcon® platform so you get an understanding of the adversaries operating in your IT network and an early warning about potential ICS threats against your production systems.

And while the app helps you bridge the IT / OT divide, the Dragos Platform enables you to perform more extensive detection and response to ICS-focused threats in your OT environment.

THE CHALLENGE

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

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

This siloing of data and of security teams' tools and purview allows 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[1], be it a reconnaissance mission, simply monitoring your network, IP theft, or worse.

[1] Learn more: The Industrial Control System Cyber Kill Chain (SANS Institute, Oct-2015)

THE SOLUTION

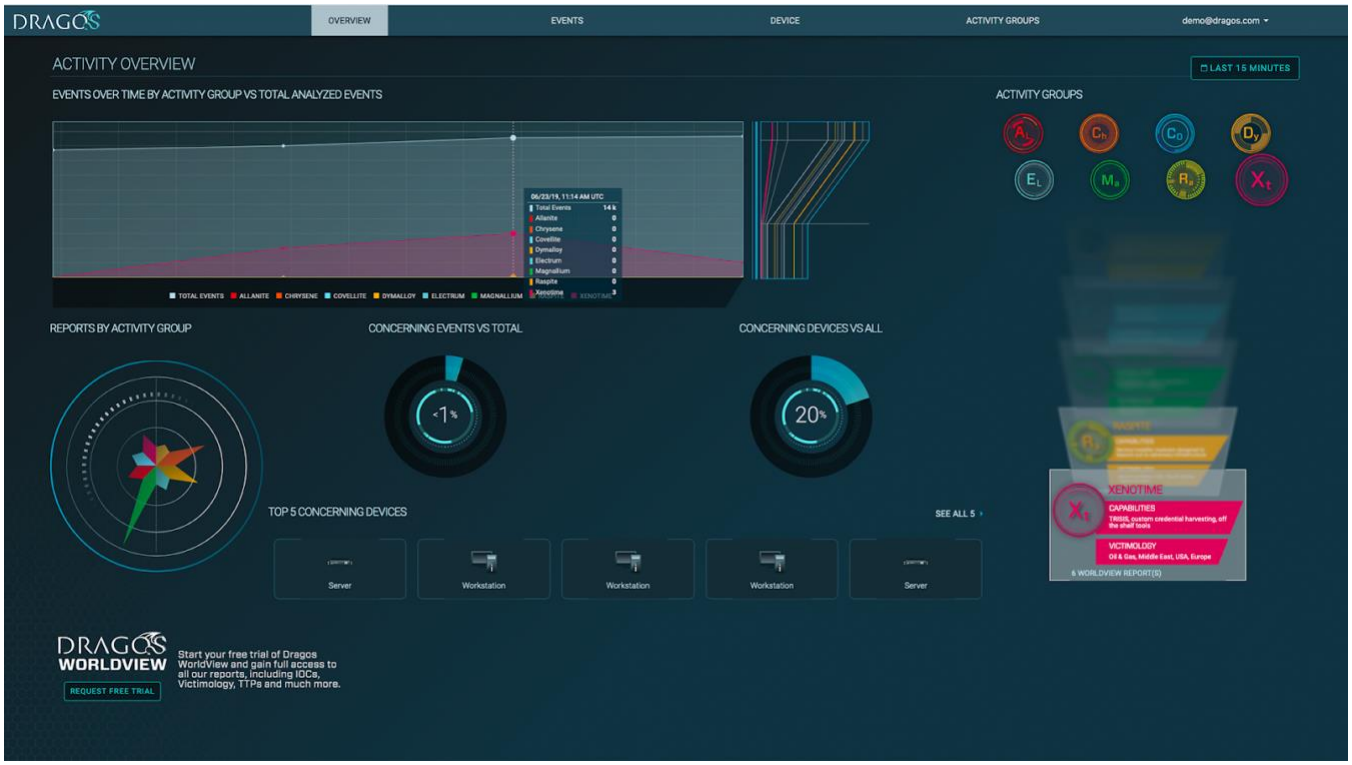
The Dragos ICS/OT Threat Detection app for CrowdStrike provides visibility into ICS threat activity in your IT network, which is not available via typical IT security tools because of the specialized tactics, techniques and procedures used by ICS adversaries. Since many ICS adversaries initiate their 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. And it is powered by the highly experienced ICS-focused intelligence team at Dragos, who actively investigate adversary tradecraft to provide you with the latest and most relevant ICS threat detection capabilities.

THE TECHNOLOGY

The Dragos ICS/OT Threat Detection app allows our ICS indicator feed to be leveraged against your host-based device, network, and event data collection in your CrowdStrike Falcon Insight™ deployment to look for known ICS adversary activity in your IT network.

The dashboard provides a Summary view for quick situational awareness, as well as views focused on Devices, Events, and Activity Groups.



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.

When combined with Dragos Platform, you have the most complete threat detection and response capabilities across your IT and OT environments – reducing adversary dwell time and any associated impact to operations.

BENEFITS and IMPACT

BENEFITS	IMPACT
Expanded Visibility	Leverage Dragos ICS threat intelligence against existing endpoint data from 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 IOCs or suspicious events flagged by Dragos by pivoting directly from the app to your CrowdStrike Falcon dashboard.

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