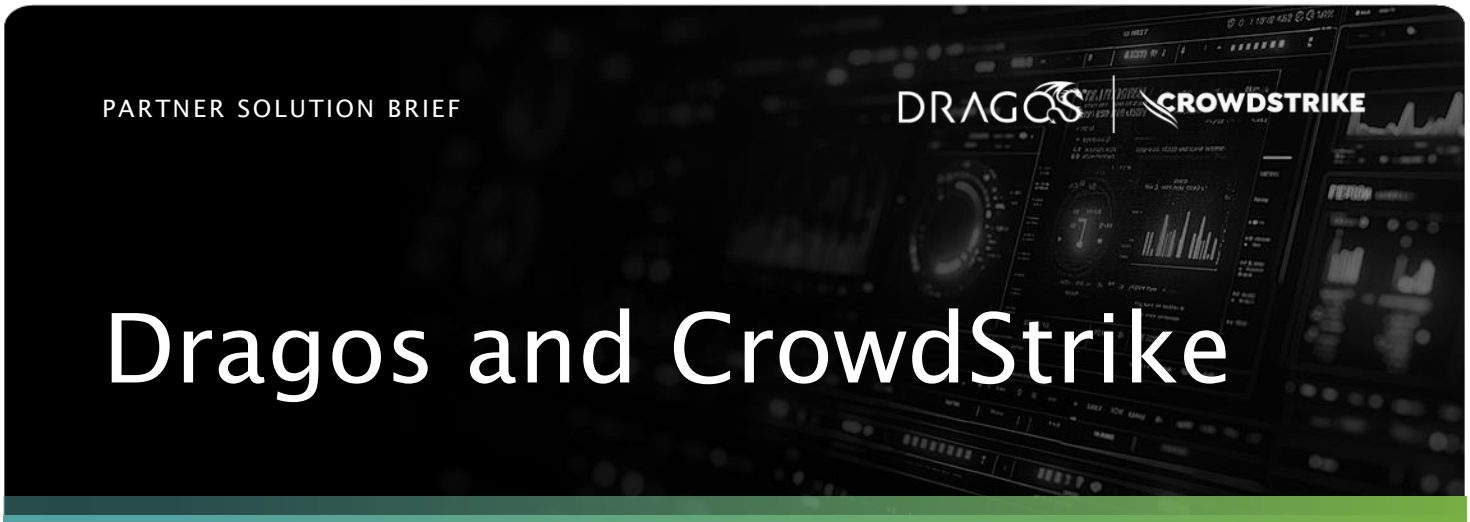
PARTNER SOLUTION BRIEF



Dragos and CrowdStrike

Unified IT/OT SOC with Intelligence-Driven Cybersecurity

HIGHLIGHTS

- Integrate a best-of-breed cybersecurity ecosystem with CrowdStrike Falcon® Insight XDR Endpoint Detection and Response (EDR), CrowdStrike Falcon Next-Gen SIEM, and the Dragos Platform's OT-Native Network Visibility & Security Monitoring.
- Deliver a unified IT/OT view with OT-Native Network Visibility & Monitoring to eliminate blind spots across industrial environments.
- Empower SOC analysts to consolidate workflows across IT and OT by combining the Dragos Platform's asset visibility, vulnerability management, threat detection, and response capabilities with CrowdStrike Falcon® Discover for IoT.
- Enhance Dragos Platform OT asset visibility and intelligence-driven detection capabilities with Endpoint Insight, enabling operations teams to quickly understand activities within their OT environment and respond more rapidly.
- Better coordinate incident response between SOC and operations teams by leveraging CrowdStrike detections on edge ICS devices and Dragos's tailored OT response strategies.

As organizations advance their digital transformation in industrial environments, it's becoming essential that security teams have complete visibility and correlation across both Information Technology (IT) and Operational Technology (OT) networks. Together, Dragos and CrowdStrike unify the IT/OT SOC with intelligence-driven cybersecurity, providing comprehensive visibility into OT assets, enhanced threat detection, and effective vulnerability management.

THE CHALLENGE

In today's threat landscape, cyber adversaries targeting industrial control systems (ICS) often penetrate industrial organizations through the enterprise IT network before they pivot to the operational technology (OT) network.

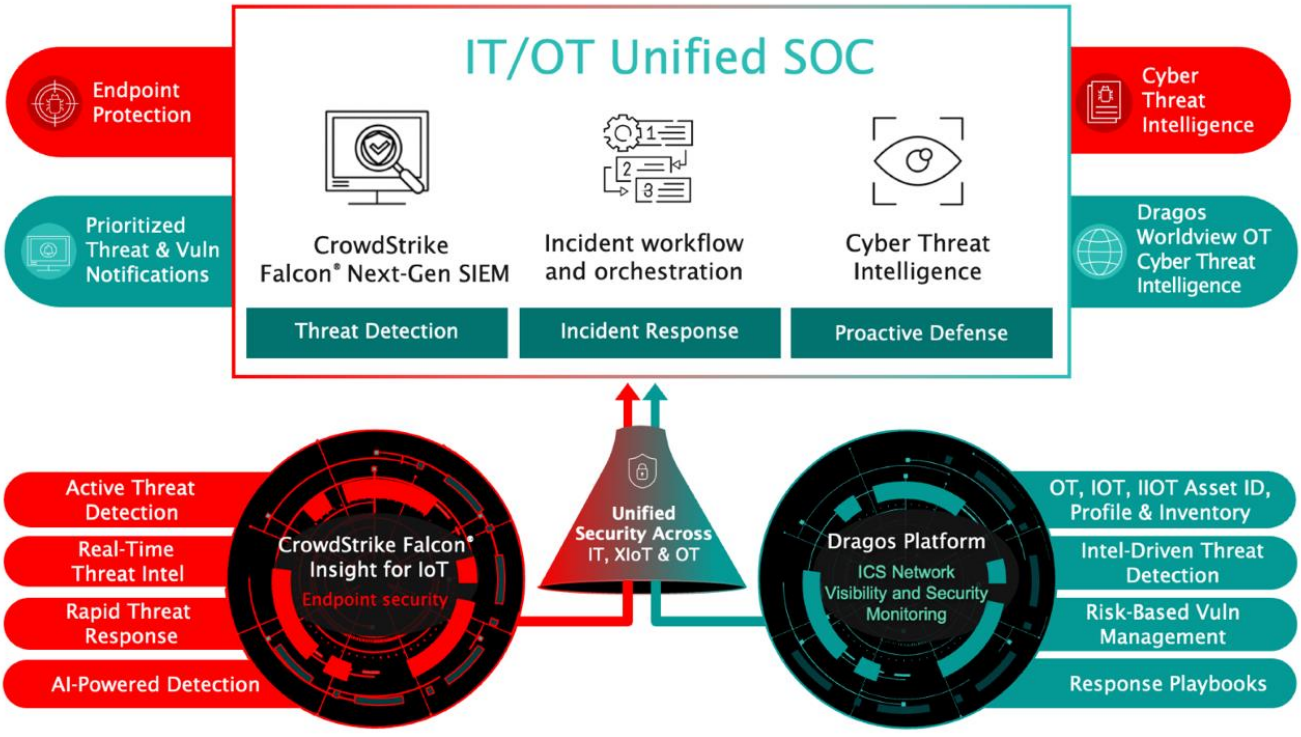
sales@dragos.com @DragosInc @Dragos, Inc.

These adversaries continually evolve their tactics, techniques, and procedures (TTPs), using subtle behaviors that get lost in the noise. Traditional threat detection systems struggle in OT environments because they rely heavily on IT-based signatures, broad anomaly-based modeling and configuration detections, resulting in an overwhelming number of alerts without actionable insights. This approach can overwhelm security operations teams, making it difficult to identify and respond effectively to OT-specific threats.

These challenges underscore the importance of integrating IT and OT into a unified Security Operations Center (SOC). Cybersecurity ownership is often fragmented across the organization, with IT and operations teams having different needs, skill sets, tools, and response processes. Integrating IT and OT enhances visibility and threat detection capabilities while streamlining incident response processes across the teams.

THE SOLUTION

Dragos and CrowdStrike have partnered to deliver an intelligence-driven cybersecurity approach that encompasses both IT and OT environments for a unified SOC. By leveraging the Dragos Platform, CrowdStrike Falcon® Insight XDR, and CrowdStrike Falcon Next-Gen SIEM, organizations can improve OT asset visibility, threat detection, and vulnerability management. This collaboration enables more thorough root cause analysis across IT and OT, leading to faster SOC investigation and response times and reducing mean time to recovery (MTTR).



Integrating asset visibility, vulnerability management, threat detection, and response, this joint solution also enables organizations to align to SANS ICS 5 Critical Controls to deliver an all-encompassing approach to securing ICS/OT systems against the sophisticated threat landscape.

HOW IT WORKS

CrowdStrike Falcon® Insight XDR, CrowdStrike Falcon Next-Gen SIEM, and the Dragos Platform integration can be configured within the respective platforms.

The Dragos Platform enables OT network visibility from Level 1 to Level 3 of the Purdue Model and at the IT/OT network boundary with multiple methods of data capture to assure environment availability and comprehensive coverages.

SOC Analyst have a unified IT/OT view with OT-Native Network Visibility & Monitoring

SOC and operations teams can have a unified view of IT/OT networks with automated discovery, management, and continuous monitoring of assets in OT environments.

Protect the complex and diverse assets within your organization's OT environment using asset data from the Dragos Platform integrated into CrowdStrike Falcon® Discover for IoT. Achieve extended visibility and security across ICS networks through CrowdStrike's Unified Threat Console, encompassing devices such as programmable logic controllers (PLCs), remote terminal units (RTUs), human-machine interfaces (HMIs), historian databases, engineering workstations (EWs), and more. By unifying ICS asset information and context, analysts can minimize blind spots and streamline asset management, empowering security operations teams to make better-informed decisions to secure your OT environment.

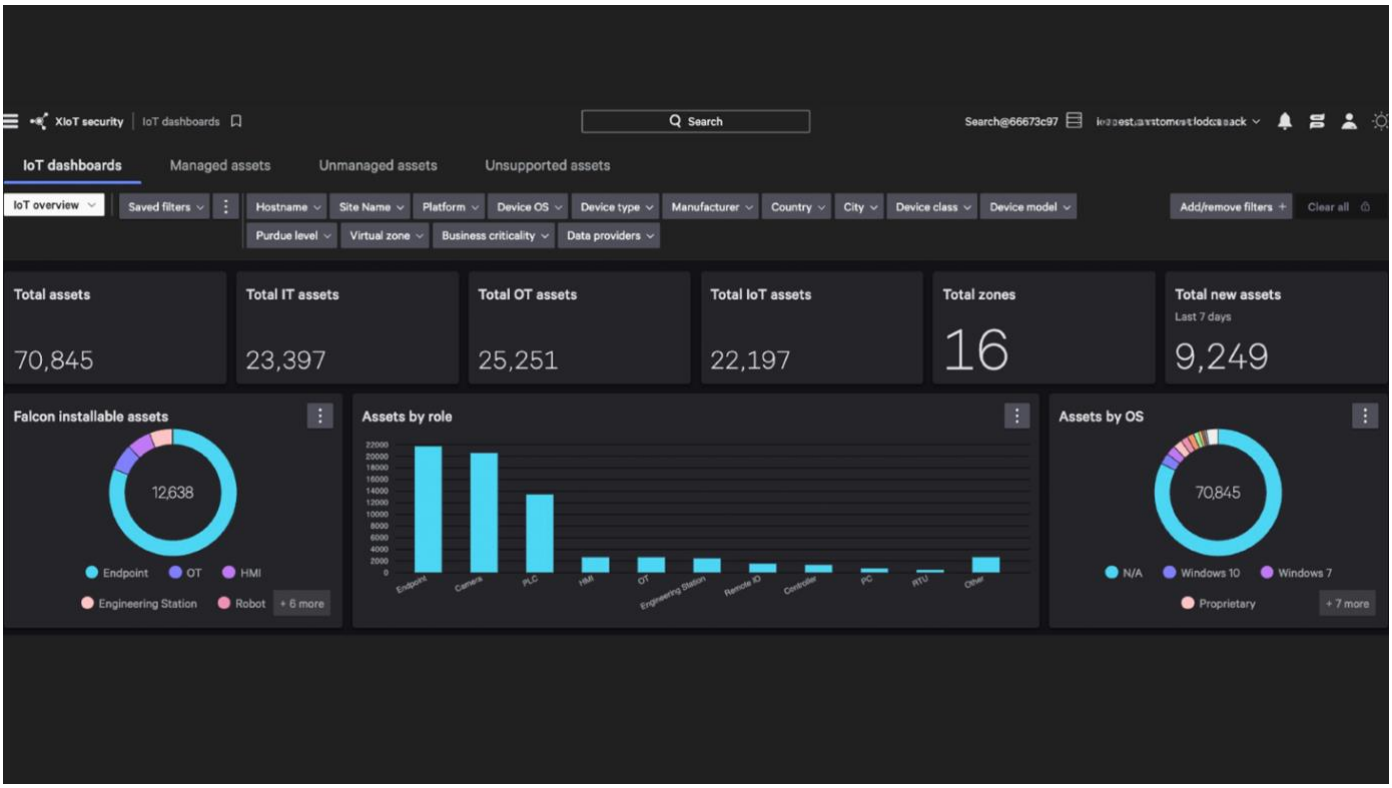


Diagram 1. CrowdStrike Falcon® Discover for IoT dashboard showing ICS assets from the Dragos Platform.

The Dragos Platform automates discovery, management, and monitoring across all assets within the OT environment (OT, IT, IoT, and IIoT). It utilizes insights from 600+ protocols, network data, and logs, laying a foundation for effective vulnerability management, threat detection, and incident response with superior security and operational efficiency.

With CrowdStrike Falcon® Discover for IoT, customers can leverage asset discovery, detections, and vulnerability management details within the Dragos Platform for a seamless bilateral flow of information. This can be integrated with CrowdStrike Falcon Next-Gen SIEM to centralize log management, enable real-time detection with unified data, facilitate rapid collaboration and search, enhance the SOC with Generative AI, and prevent breaches through workflow automation.

Get Started – Easily ingest OT assets from the Dragos Platform into Falcon® Discover for IoT.

Dragos Platform Data Connector: Input the Dragos API key information into CrowdStrike Falcon® to ensure the Dragos SiteStore data is routable into Flacon.

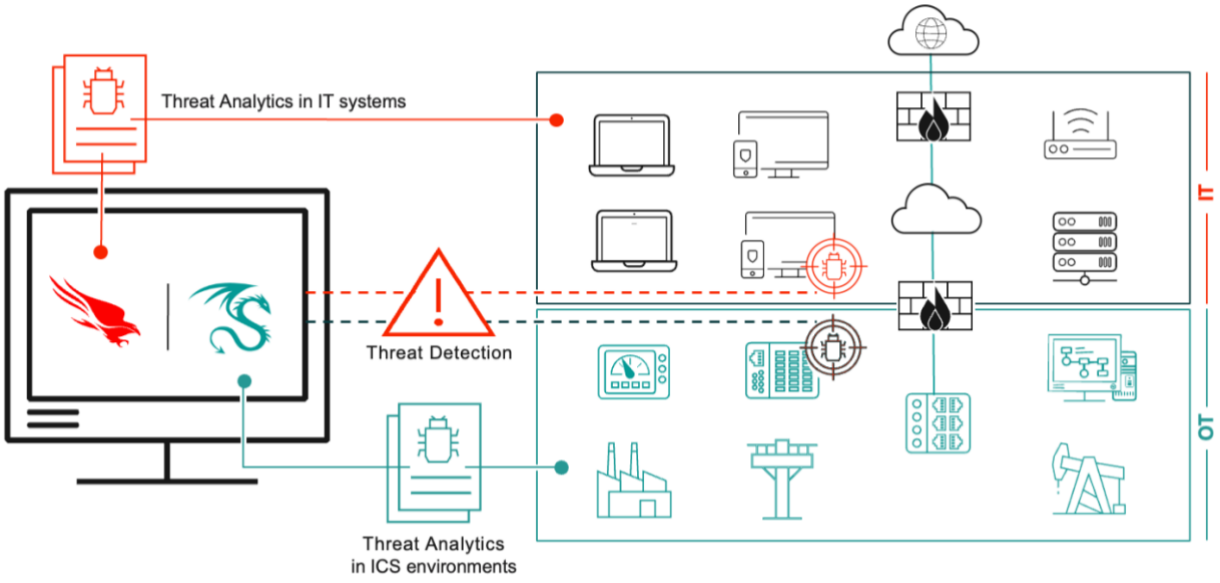
Request a demo today:
https://www.dragos.com/request-a-demo/

Products:
- CrowdStrike Falcon® Insight XDR/Discover for IoT
- CrowdStrike Falcon Next-Gen SIEM
- The Dragos Platform

Additional information:
https://marketplace.crowdstrike.com/listings/dragos-platform-data-connector

SOC teams can consolidate workflows for better detection and coordinated incident response

Dragos's OT-specific high fidelity, low noise threat detection enhances CrowdStrike Falcon's detection capabilities allowing SOC analysts to rapidly pinpoint malicious activity in ICS/OT networks with in-depth context of alert insights to reduce false positives and provide clear prioritization. Dragos's OT-specific intelligence also helps analysts detect ICS threats in IT environments before they pivot to OT networks.



Analyst can quickly correlate notifications with a timeline view of historical insights which allows for a comprehensive timeline of events, aiding in the identification and analysis of incidents. Leveraging the MITRE ATT&CK framework, analysts can then easily map detected threats to specific adversary TTPs.

Incident Responders can better coordinate response efforts by using CrowdStrike's extensive detections on edge ICS devices combined with Dragos's in-depth understanding of OT environments with tailored response strategies that prioritize operational uptime alongside security threat mitigation.

The Dragos Platform enhances an organization's response plan to speed up forensics and enable quick resolution with embedded case management and integrated response playbooks developed by OT security experts. Forensic artifacts are abstracted and well organized so incident responders can easily create cases to initiate investigations, accessing relevant activity logs and timeline views. This comprehensive approach ensures thorough and efficient incident investigations.

Enrich OT assets with Endpoint insight for thorough investigations

Enrich Dragos Platform's asset visibility and detection capabilities further by leveraging Windows-based devices managed by CrowdStrike Falcon® Insight XDR. By integrating endpoint asset information from CrowdStrike, the Dragos Platform provides enriched and enhanced device details of known assets, including operating system data, IP addresses, MAC addresses, endpoint hostnames, associated Active Directory (AD) domains, and additional custom attributes. This visibility enhances your understanding of the organization's attack surface. Furthermore, the integration offers additional context on edge devices in OT environments, allowing users to forward CrowdStrike Falcon detections of known assets to the Dragos Platform for accelerated remediation and coordinating response efforts.

Get Started – Improve threat detection and incident response with Endpoint asset enrichment for OT

Dragos Endpoint Asset Enrichment for OT: Input the Falcon API key information into the Dragos Platform to ensure Falcon® data is routable into the Dragos SiteStore.

Request a demo today:
https://www.dragos.com/request-a-demo/

Products:
- The Dragos Platform
- CrowdStrike Falcon® Insight XDR

Additional information:
https://marketplace.crowdstrike.com/listings/dragos-endpoint-asset-enrichment-for-operational-technology-ot

BENEFITS AND IMPACTS:

- **Maximize value, investment, and visibility:** Combined domain experience and integrated technologies to optimize both enterprise (IT) and industrial (OT) security environments.
- **Address OT-Specific Threats**: Dragos Platform leverages deep knowledge of OT-specific tactics, techniques, and procedures (TTPs). This approach not only enables precise threat identification but also provides a deep contextual understanding that guides rapid, informed response actions.
- **Combating Alert Fatigue**: Dragos Platform counters alert fatigue triggered by anomaly-based threat detection with high-confidence indicators, significantly reducing alert fatigue and ensuring teams focus on the most relevant and actionable threats.
- **Secure the Environment with Network Segmentation Context**: Get a complete view of devices and their related segments, including information on virtual zones, Purdue Levels and ICS Protocols to effectively secure your environment.
- **Compliance Aligned**: Support compliance with NIST SP 800-82, IEC 62443, ISA/IEC 62443, NERC CIP, ISO/IEC 27001, CIS Controls, and FIPS 199 and 200 as well as alignment with recommended best practices for ICS cybersecurity, the SANS ICS 5 Critical Controls.

For more information, please visit **dragos.com/partner/crowdstrike/**

About Dragos, Inc

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

Learn more about our technology, services, and threat intelligence offerings:

Request a Demo | Contact Us

sales@dragos.com @DragosInc @Dragos, Inc.