DRAGOS THREAT HUNTING

OVERVIEW

The Dragos Threat Hunting Service helps you find undiscovered threats in your industrial control systems (ICS) networks and identify weaknesses in architecture, security controls, and policies and procedures to avoid compromise. Leveraging the Dragos Platform, Dragos threat hunters work independently or in addition to your local ICS security team to find threats non-invasively without operational disruptions or downtime.

THE DRAGOS DIFFERENCE

Dragos is comprised of the industry's most experienced team of ICS security practitioners. Our team has been on the front lines of every significant industrial cybersecurity attack globally, including the 2015 and 2016 Ukraine attacks, CRASHOVERRIDE, and TRISIS.

Leveraging our team's combined knowledge and deep understanding of adversaries' ever-changing tactics, techniques, and procedures, the Dragos Threat Hunting Service offers customized ICS cybersecurity based on the most up-to-date intelligence of adversary behavior, so you can prevent significant compromises and neutralize threats in their tracks.

COMPREHENSIVE VISIBILITY

In-depth insight into industrial assets and the ICS threat landscape

NON-INVASIVE ANALYSIS & ZERO DOWNTIME

Passive analysis does not interfere with regular operations

BACKED BY THE DRAGOS PLATFORM

Hunts supported by the Dragos Platform's in-depth asset identification, threat detection, and response capabilities

REDUCED RISK

Identify and remediate gaps in defenses to build a stronger security posture

TRANSFERRED KNOWLEDGE

Learn from our team of experts to understand industrial risks and execute informed analyses

TAILORED, CONSEQUENCE-DRIVEN HUNTS

Customized hunts and assessments based on your organization's specific needs and budget

Find Undiscovered Threats

- Identify weaknesses in architecture, security controls, and policies and procedures
- Get in-depth visibility of your industrial assets and the ICS threat landscape
- Comprehensively understand your industrial environment

Reduce Adversary Dwell Time and Operational Downtime

- Detect latent threats
- Identify and prioritize the most critical threats that need attention
- Detect and eradicate undetected attackers in your ICS network to prevent cyber incidents

Prepare For and Combat Future Industrial Incidents

- Learn likeliest attack vectors on your ICS
- Find and eliminate gaps in defenses to avoid serious incidents
- Leverage intelligence-driven knowledge of adversary behaviors from Dragos experts

HOW IT WORKS

The Dragos Threat Hunting Service pairs our ICS experts with the advanced asset identification, threat detection, and response capabilities of the Dragos Platform to provide a comprehensive understanding of your ICS environment.

With these insights, our team identifies architecture weaknesses, searches for known adversary fingerprints, and leverages our team's understanding of your specific environment and threats to find previously unrecognized threat actors, malware, and breaches.

DRAGOS THREAT HUNTING SERVICE OPTIONS

The Dragos Threat Hunting Service can be customized to suit your organization's security maturity and specific environment needs.

	1 | Remote Collection Customer provides Dragos with data remotely	2 | Onsite Collection with Remote Analysis Dragos collects customer data and performs analysis at Dragos HQ	3 | Managed Threat Hunting On-site deployment of Dragos Platform for data collection
Asset Discovery	✓	✓	✓
Threat Modeling	N/A	✓	✓
Operational Impact Analysis	N/A	✓	✓
Threat Detection	✓	✓	✓
Continuous Collection and Operation	N/A	✓	✓

To learn more about Dragos Threat Hunting or other professional services please contact sales@dragos.com or visit dragos.com/services