BROCHURE

DRAGOS
SAFEGUARDING CIVILIZATION

Dragos Industrial Cybersecurity

Your Best Defense Against Industrial Cyber Threats

Specialized threat groups target operational technology (OT) and industrial control systems (ICS), posing significant risk to electric utilities, oil and gas, water systems, transportation networks, and manufacturing operations. These industrial environments are different – they house equipment that communicates via specialized protocols and with networks that are sensitive to extraneous traffic. ICS/OT systems control physical processes, rather than bytes of information, where a security incident could have a high impact.

Where information technology (IT) incidents lead to loss of information, OT cyber impacts can include loss of life, impact to the environment, and loss of revenue-producing operations. That's why Dragos's global mission is to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day.

Leading OT Cybersecurity Technology and Experts Trusted Around the Globe

Dragos was founded in 2016 by the people who created the ICS cyber mission for US Government agencies. The founders saw the problem of persistent OT cyber attacks by a growing number of adversaries was not being addressed. So, they hired the most experienced team of ICS/OT security practitioners – threat hunters, researchers, and incident responders - to help build the Dragos Platform and OT security programs. Now hundreds of global industrial organizations – including 6 of the 10 largest oil and gas companies and 9 of the 10 largest US electric utilities – trust Dragos industrial cybersecurity solutions.

> Dragos knows their market, knows what it takes for ICS and OT cyber security.
>
> — DRAGOS CUSTOMER —
> Shared on Gartner Peer Insights

Gartner peerinsights

4.8 Rating • 24 Reviews
(as of May 16, 2023)

Visibility into Industrial Assets, Threats, and Vulnerabilities with The Dragos Platform

Dragos is rooted in OT. Our technology provides continuous security monitoring of ICS/OT networks and assets, with vulnerability management that takes a risk-based approach practical for industrial environments. The platform integrates a continuous stream of threat and vulnerability intelligence from our WorldView OT Threat Intelligence unit and updates response best practices from our Professional Services team – all to deliver the most effective protection.

- **Asset discovery, inventory, and profiles** to understand and track the ICS/OT attack surface
- The most effective **behavior-based threat detection** to identify real threats as validated by MITRE ATT&CK for ICS
- **Risk-weighted vulnerability scoring** with prioritization and risk mitigation practical for ICS/OT systems
- Expert **response playbooks** tailored to threat scenarios for rapid event investigation
- Optional OT Watch managed **threat hunting** and Neighborhood Keeper **collective intelligence network**

DRAGOS OT SECURITY PLATFORM

ICS Network Security Monitoring & Risk-Based Vulnerability Management

VISIBILITY	Asset inventory, network monitoring & logging, with risk-rated vulnerabilities
DETECTION	Identify threat behaviors by analyzing OT systems comms to avoid the noise of anomaly engines
RESPONSE	Triage and investigate events, simplified with prescriptive incident response

Threat Detections & Vulnerabilities → **WORLDVIEW THREAT INTELLIGENCE**

Incident Response Playbooks → **OT PROFESSIONAL SERVICES**

Dragos OT Threat Intelligence and WorldView Intelligence Service

Dragos Threat Intelligence provides visibility of adversary threats, malware, and vulnerabilities impacting industrial sectors. Intelligence-driven behavioral detections, indicators of compromise (IOCs), and refactored ICS/OT vulnerabilities are codified in the Dragos Platform, with detailed research and reports available through a subscription to WorldView, including:

- OT adversary tactics, techniques, and procedures (TTPs) and IOCs to integrate into your SOC
- Refactored CVSS scores reflecting OT impact and exploitability of ICS vulnerabilities
- Enriched mitigations and alternatives to provide OT-practical risk reduction
- Technical analysis of OT-targeted malware
- Defensive recommendations from ICS/OT experts

Dragos Professional Services

With deep industry knowledge and OT expertise, our Professional Services team is your trusted advisor against the backdrop of a constantly evolving threat landscape. We're here to help you to assess current capabilities, gain insights into best practices for cyber resilience, and help create a stepwise plan to reduce risk. We provide a full range of OT cyber services, starting with a Rapid Response Retainer:

Rapid Response Retainer

Access to experienced OT responders for analysis, investigation, and consultation for incidents or intrusions. Use the retainer to activate key services.

Readiness Assessment

Review of documents, best practices, & IR maturity included in the retainer

OT Cybersecurity Assessment Suite

Assess cyber architecture & programs, understand critical systems, evaluate vulnerabilities, & consequences of an attack

Penetration Tests & Network Vulnerability Assessments

Evaluate potential attack pathways in your environment

Tabletop Exercises

To practice & refine incident response plans

Threat Hunts

Detect, expose, & stop threats in your OT environment

Dragos Community Engagement

With Dragos, community comes first. To strengthen the collective industrial cyber defense we provide resources to build knowledge and defend against attacks — including free resources through Dragos OT-CERT for small-to medium-sized organizations with limited budgets.

We also provide access to the largest community of industrial organizations sharing real-time threat information through Neighborhood Keeper. Together we can protect the industrial environments that are critical to meeting our world's most essential needs.

Industrial Automation OEMs and Technology Partners

Dragos works with the industrial automation vendors like Rockwell Automation, SEL, GE, Emerson Automation Solutions, Honeywell, Yokogawa Electric, and many others to make sure we understand the communications, network traffic, and systems environments that can benefit from Dragos protection.

We also partner with numerous OT and IT technology vendors. Our unique expertise in the OT can help drive convergence of systems and processes that streamlines operation and security.

Dragos Platform Integrations Provide OT Intelligence for IT Infrastructure Convergence

Threat Intelligence Platform (TIP)

WorldView reports data on industrial adversaries, campaigns, IOCs & TTPs available via portal, email, API, & STIX.

Firewall

Dragos OT device inventory for firewall policy, Dragos threat detection notifies firewall to isolate devices. Monitoring helps validate firewall policies.

IT Service Management

Integrates Dragos asset inventory & vulnerabilities to gain complete asset view across IT/OT estate.

SIEM/SOAR

Dragos integrates OT alerts, forensic data, & IOCs to simplify SOC triage & streamline investigations.

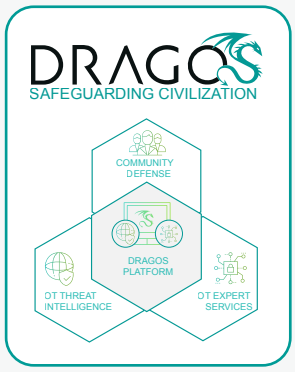
TAP/Packet Broker/Traffic Aggregator

Send data to Dragos to simplify deployment & hardware requirements.

Endpoint Security

EDR information enhances Dragos OT device profiles, Dragos OT detections integrate into EDR to block malicious activity

WORLDVIEW THREAT INTELLIGENCE → **DRAGOS PLATFORM** VISIBILITY • DETECTION • RESPONSE ← **OT PROFESSIONAL SERVICES**



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.

To learn more about our technology, services, and threat intelligence offerings, visit **dragos.com** or connect with us at **sales@dragos.com**.