Operations Technology Cybersecurity Solutions for Federal Agencies

ICS/OT Security Technology and Services

Thank you for downloading this Dragos solutions brief. Carahsoft is the public sector distributor for Dragos Cybersecurity solutions available via NASA SEWP V, ITES-SW2, and other contract vehicles.

To learn how to take the next step toward acquiring Dragos's solutions, please check out the following resources and information:

For additional resources:
carah.io/DragosResources

For upcoming events:
carah.io/DragosEvents

For additional Dragos solutions:
carah.io/DragosSolutions

For additional Cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
Dragos@carahsoft.com
844-445-5688

To purchase, check out the contract vehicles available for procurement:
carah.io/DragosContracts

For more information, contact Carahsoft or our reseller partners:
Dragos@carahsoft.com | 844-445-5688

SOLUTION BRIEF

Operations Technology Cybersecurity Solutions for Federal Agencies

ICS/OT Security Technology and Services

Dragos is on a mission to safeguard civilization from attackers trying to disrupt the operations of federal, civilian, defense, and intelligence agencies. Based in the Washington, DC area, Dragos is the only US-owned OT cybersecurity hardware vendor, intelligence, and services company. Nine of the 10 largest US electric utility companies, five of the 10 largest oil and gas companies, dozens of leading manufacturers, and several government agencies rely on Dragos to protect their enterprises amidst an ever-changing threat landscape. Dragos OT cybersecurity experts have been the first responders in the world's most significant industrial cyber-attacks, including the 2015 and 2016 power grid offenses in Ukraine and the 2017 Saudi petrochemical safety system attack.

Reasons to Choose Dragos

Industrial Control Systems (ICS)/Operations Technology (OT)

OT environments include different systems, network traffic, adversaries, and vulnerabilities than IT environments. When facilities modernize their operations, the IT network becomes part of the control system – and control systems have very different latency requirements to ensure employee and public safety. You need a team with process-level expertise to support your cybersecurity programs.

OT Expertise for Your Mission

It's difficult – borderline impossible – to recruit, hire, and retain a qualified OT cybersecurity workforce. Dragos has a full bench of ICS/OT operators and defenders ready to align with your mission. Our teams can help you reduce your threat surface, increase visibility into your cybersecurity posture, improve response capabilities, and streamline reporting.

Community Matters

Dragos provides the connective tissue between government, civilian agencies, and commercial customers, leveraging threat intelligence and lessons learned to optimize results for all stakeholders.

American-developed, American-owned

Dragos is the only American-owned ICS/OT cybersecurity company – and that matters when you're defending our interests around the world. The Dragos team comes highly recommended, with hundreds of cybersecurity experts serving within government and in critical industry sectors like energy, oil & gas, and manufacturing.

Current Federal Agency and Department of Defense Partners

How We Help Federal Agencies

Dragos technology protects everything from power grids to manufacturing plants to facility related control systems. Our unparalleled understanding of these environments strengthens the readiness and resiliency of your teams, enables secure modernization and innovation, and facilitates compliance while minimizing risk.

Dragos technology empowers you to answer these important questions:

- What is on my network?
- Who is on my network?
- What is happening on the network and how are my assets protected?

The Dragos Platform

The industry's most advanced ICS/OT cybersecurity software helps you visualize, protect, and respond to cyber threats.

Top Five Use Cases for the Dragos Platform

Asset Visibility

A comprehensive and real-time understanding of all assets in your environment is essential for network monitoring, threat correlation, and effective vulnerability management. Our customers use the Dragos Platform to identify crown jewel assets, create asset inventories, and identify unusual activity across thousands of devices.

Vulnerability Management

OT cybersecurity teams are overwhelmed by hundreds of vulnerabilities that potentially need to be remediated. Without simple, accurate, prioritized guidance, you'll waste time and money patching vulnerabilities that aren't important – and you can easily miss those that are truly critical. Dragos customers use the Platform to simplify compliance and reporting, prioritize vulnerabilities that matter most, and maximize remediation resources.

Threat Detection

Adversaries evolve their tactics, techniques, and procedures with subtle behaviors that are easily lost in the noise of your environment. Without actual intelligence, your team can easily suffer from alert fatigue and begin to ignore or undervalue relevant alerts while devoting unnecessary time and productivity to false alarms. Our Platform customers immediately see any unauthorized IT-OT traffic across complex networks, analyze file downloads quickly and easily, and detect potential adversaries in the environment in real time.

Incident Investigation

When faced with a potential incident, clear and carefully vetted guidance can be the difference between quickly restoring operations or making the situation worse. Dragos Platform users can analyze changes and forensic records, efficiently manage response and recovery, and leverage prescriptive playbooks with proven, tested response protocols.

Cross-Functional Operations Insights

Monitoring assets and properly dissecting and inspecting network traffic requires in-depth protocol coverage; otherwise, threats and asset details remain hidden. Dragos customers use the Platform to detect operational process errors quickly and efficiently, monitor ICS/OT network and device health, support ATO/RMF artifacts, and integrate active defense via SIEMENS Siber Protect.

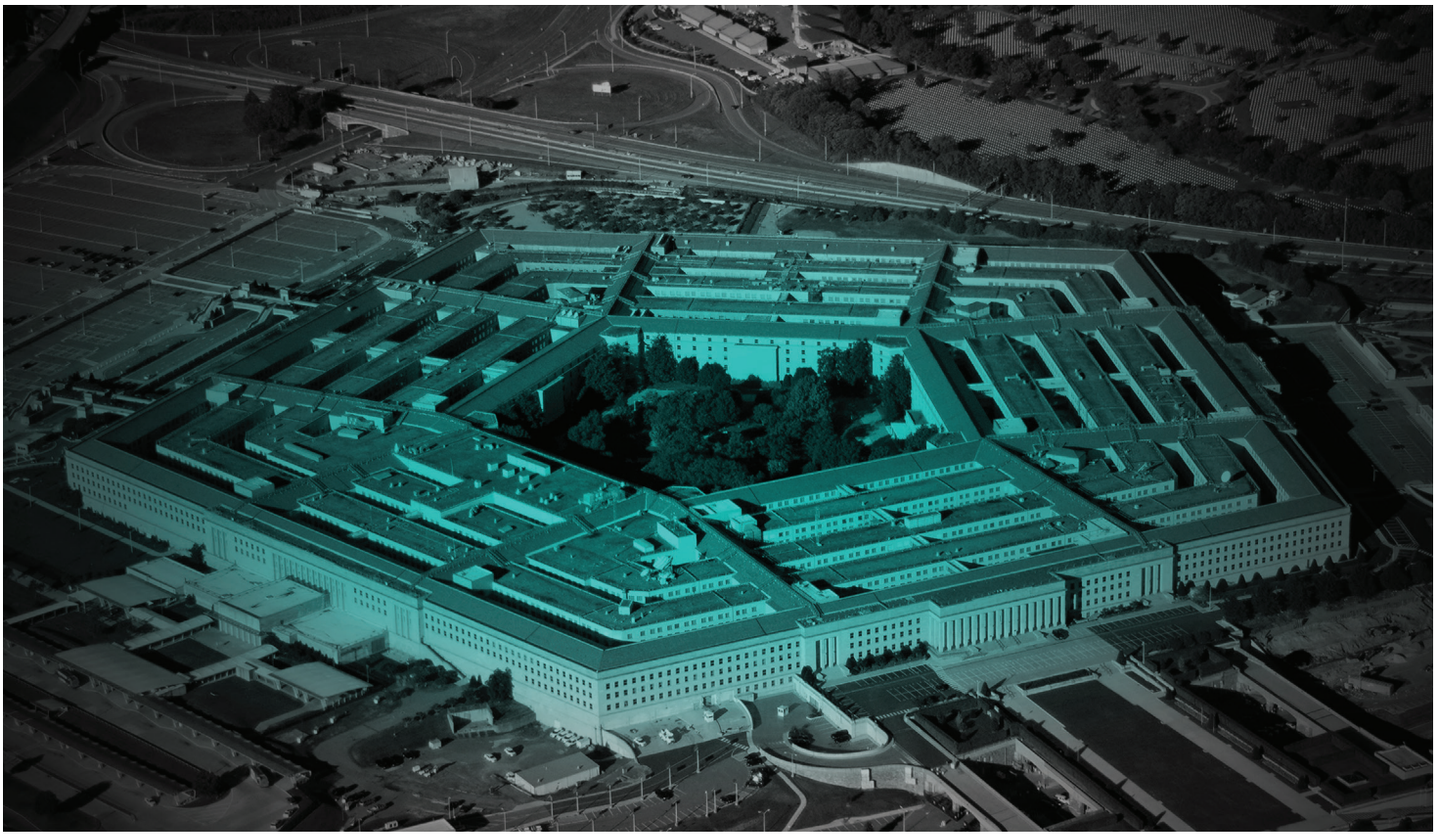
WorldView Threat Intelligence

Actionable Threat Intelligence and Defensive Recommendations

Backed by a team of industrial control systems cybersecurity experts with deep industry knowledge, Dragos WorldView threat intelligence offers in-depth visibility of threats targeting OT environments AND defensive recommendations to combat them. WorldView threat intelligence is an annual subscription service, providing access to regular reporting, critical alerts, executive insights, webinars, and more.

Use these WorldView tools to proactively defend your ICS networks and stay ahead of threats:

- Critical alerts, weekly reports, threat perspectives, quarterly insights, and dedicated threat feeds provide comprehensive insight of threats to your ICS
- Actionable defensive recommendations from a dedicated team of ICS intelligence analysts and practitioners to help you prepare for and combat cyber attacks
- Detailed information about global industrial adversary behaviors, including TTPs and victimology to understand ICS attackers and prevent them from going undetected on your networks
- The latest Indicators of Compromise (IOCs) to help you thwart potential attacks
- Partnerships with companies like Crowdstrike, ThreatQuotient, eclectic iq, ThreatConnect, Anomoli, Recorded Future, and others provide enhanced threat intelligence capabilities – and all of WorldView's threat intelligence reporting references MITRE ATT&CK for ICS TTPs



ICS/OT Incident Response

Proactive and Responsive Service to Prepare for, Combat, and Respond to ICS/OT Attacks

The Dragos Rapid Response Retainer is the cornerstone of your OT cybersecurity program, enabling you to respond quickly and recover confidently when attackers strike. Having a retainer in place is a proactive approach that bolsters your security posture and provides access to incident responders who have been on the front lines of cyber-attacks globally, are familiar with your environment, and are highly skilled at OT cybersecurity crisis management. A Rapid Response Retainer pairs perfectly with the Dragos Platform, because the Platform provides a powerful investigation workbench with detailed forensics records and prioritized guidance for vulnerabilities and risk mitigation.

1 24 X 7 ACCESS TO INDUSTRY-LEADING RESPONDERS

- ✓ When you're in crisis mode, you need experienced incident responders who understand your technology, have situational awareness and exercise good judgement.
- ✓ The Dragos team of experts are industry leading supporting customers with OT cybersecurity incidents on an international scale.
- ✓ Ensure you have the necessary support from a team that can analyze and investigate industrial cyber events, and consult with you on important executive, legal, regulatory, and insurance communications that may be necessary.

2 RAPID RESPONSE WITH THE DRAGOS PLATFORM

- ✓ While a subscription to the Dragos Platform is not required to purchase a retainer, it is highly recommended.
- ✓ Because the Dragos Platform provides continuous visibility to OT devices, profiles, traffic patterns, vulnerabilities and threats, sites with the Platform installed are eligible for expedited response times (SLA) based on the number of retainer hours purchased.
- ✓ With our technology in place, responders are better equipped to analyze, investigate, and perform root cause analysis on historical data within your environment when an event occurs.
- ✓ Non-retainer incident response or sites not equipped with the Dragos Platform receive our best-effort response time.

Neighborhood Keeper

A Global Threat Intelligence and Analytics Sharing Program

Currently, many government agencies have no continuous visibility into the critical infrastructure that is supporting mission assets across geographies. Dragos founded Neighborhood Keeper (a free, opt-in program for Dragos Platform customers) to collectively track ICS threat, asset, and vulnerability intelligence across geographic regions and industry sectors. Government organizations can participate in Neighborhood Keeper as trusted advisors, allowing agencies to visualize downstream risk to key locations and government assets. The program also enables information sharing between agencies and the private sector in a safe, secure, and productive way.

How It Works

Trusted Advisors:

Select governments, ISACs, or CERTs that are willing and able to contribute insights into the program for the benefit of the members

1

Dragos Platform customers deploy passive sensor in ICS/OT environment, and opt-in to Neighborhood Keeper. When detections fire in the environment, all data stays on premises with the customer and only anonymized insights are shared.

2

Neighborhood Keeper receives the anonymous alert and shares detections and insights across the community to inform them of what's occurring elsewhere, the prevalence of certain adversary methods, vulnerabilities, and risks to enhance their own security efforts.

3

Participants may also anonymously make an encrypted request for assistance from other members. Members who respond to that request must identify themselves to the requestor and include contact information. The requestor can then choose to reach out to the responder outside of Neighborhood Keeper to help them and coordinate response efforts.

You Can Rely on Dragos Technology and Services to Defend Your Critical Infrastructure

Cyber incidents result in an inability to execute missions internally and externally; threaten health and safety of the community; disrupt operations; and shake public trust in our government. Put our team of researchers, hunters, and defenders to work on your mission – you'll dramatically lower your risk AND you'll experience benefits like these:

Save Money

- Focused threat hunting and cybersecurity engagements, custom-built to suit your unique mission and cyber maturity level
- Accurate and uncontestable information prevents additional trips for data
- Contextualized and prioritized vulnerability recommendations enable accurate resource requests
- Efficient, real-time identification of malfunctioning components and devices lowers downtime and reduces maintenance costs across your enterprise

Save Time

- Run automated, continuous inventory cycles
- View live data without lengthy site interactions
- Identify process errors quickly and continuously
- Begin collecting data during the Dragos pre-site assessment and hit the ground running

Simplify Compliance and Reporting Requirements

- Meet Service Component Objectives, NDAA requirements, CDM goals, and other guidance including cyber terrain mapping, critical asset continuous threat monitoring, creating an OT zero trust framework, and ensuring OT asset visibility across multiple facilities
- Conduct tabletop exercises, establish baselines, and track progress
- Enable accurate briefings to leadership and simplify reporting

Minimize Risk and Improve Mission Resiliency

- Prioritized vulnerability management ensures exploitable risks are addressed first
- Intelligence-informed threat detection based on adversary tactics, techniques, and procedures allows earlier identification and remediation

Next Step: Learn more about Dragos and our technology, services, and threat intelligence – book a meeting today.

Dragos makes it easy to work with us by leveraging several different contract vehicles and certifications.

- UESC/UMCS (OEM Partnerships)
- GSA (Pending)
- SEWP (Multiple Partners)
- Army itES-3H/-3S
- DLA Tailored Logistics Support Program (TLSP)
- SBA 8(a)
- Native Alaskan, Native Hawaiian, and SDVOSB

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**.

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