



DRAGO



Industrial Threat Detection and Response Technology and Services



Safeguarding Civilization

The sustained, rapid advancement of many aspects of our civilization, particularly over the past century, is in many ways attributable to the strength and resilience of industrial infrastructure.

As industrial infrastructure has evolved, so, too, have the opportunities and challenges facing those responsible for it. The rise of networked industrial control systems (ICS) and the increasing interconnectivity of industrial infrastructure is the latest example, where numerous enhanced capabilities must be incorporated in ways that sustain its safety and reliability.

Today's industrial infrastructure is facing a new kind of challenge – industrial-specific cyber threats – that requires new approaches and additional measures to remain steadfast. Dragos' sole focus is to provide these measures, and to work as your trusted partner in safeguarding civilization.

PUTTING THE INDUSTRIAL INFRASTRUCTURE CYBER-THREAT LANDSCAPE IN CONTEXT

Persistent hype and speculation swirl around industrial infrastructure's vulnerabilities to cyberattack and the dire consequences that will follow. Dragos believes these so-called facts are largely overstated and discount the strength and resilience industrial infrastructure possesses. Even so, the threat is real, and while not a cause for fear among asset owners and their customers, it should drive a well-informed, targeted, and proactive response.

Arguably the most revealing thing about the current state of understanding of the industrial infrastructure threat landscape lies in the fact that the most frequently reported attack vector is "unknown" as neither asset-owners nor governmental security teams have adequate staff and ICS-focused technology to identify them. Even so, the specific tools and methods required to effectively map the threat landscape, increase situational awareness, and mount a strong, targeted defense are now available.

Their deployment is acting as a force-multiplier to frontline ICS defenders, bringing additional strength and resilience to the world's industrial infrastructure.

ICS CERT-REPORTED INCIDENTS (in a typical year)



The most frequently reported attack vector used against industrial infrastructure environments is actually "unknown" as neither asset-owners nor governmental security teams have adequate staff and ICS-focused technology to identify them.

THE CHALLENGES OF SECURING INDUSTRIAL INFRASTRUCTURE FROM CYBER THREATS

There is a critical shortage of staff with deep ICS cybersecurity knowledge across all industrial sectors today. This fact, coupled with the general lack of available ICS-focused cybersecurity technology solutions and increasing connectivity to enterprise networks and the Internet (IIoT/Industry 4.0), contributes to a broadening range of potential security vulnerabilities including:

- incomplete asset visibility
- insufficient industrial cyber-threat detection
- lack of situational awareness around what threats and vulnerabilities matter
- limited industrial specific incident response planning and resources

“ Where Dragos differentiates from many [competitors] is in the ICS-focused expertise of its team, reflected in its intelligence-centric approach, where its deep and detailed knowledge of the specifics of the ICS threat landscape are born out of experience.”

451 Research

WHY CHOOSE DRAGOS AS YOUR INDUSTRIAL CYBERSECURITY PARTNER?

The Dragos team knows ICS and industrial cybersecurity through direct industry and government experience and includes some of the world’s foremost experts in this highly-specialized area.

We are practitioners who have lived through and solved real security challenges. Our team members have responded to incidents including the Ukraine 2015 power grid attack, analyzed the CRASHOVERRIDE malware responsible for the Ukraine 2016 electric grid attack, analyzed the TRISIS malware responsible for the petrochemical facility attack in 2017, built and led the National Security Agency mission to identify nation-states breaking into ICS, and performed assessments on hundreds of assets around the world.

Our products and services leverage this knowledge and expertise to enhance our customers’ efficiency and effectiveness as ICS defenders. It is codified into our software, written into our ICS-focused threat intelligence reports, onsite with security teams hunting and responding to threats, and transferred through our industrial cybersecurity training classes.

We understand the differences between the enterprise IT and ICS domains, and the logical and cultural boundaries between them. Our products and services focus on filling the need for the knowledge and capabilities required to provide support in the ICS/ OT domain, including its mission, mean time to recovery (MTTR)-driven metrics, and safety and resilience-oriented priorities.

Enterprise/IT Domain	ICS Domain		
 Enterprise	 Supervisory	 Control	 Field
<ul style="list-style-type: none"> ➤ External and Partner Services ➤ Email Services ➤ Printers ➤ VoIP 	<ul style="list-style-type: none"> ➤ Engineer Workstations ➤ Auxiliary Systems ➤ Operator HMIs ➤ SCADA Front End 	<ul style="list-style-type: none"> ➤ RTs ➤ PLCs ➤ IEDs 	<ul style="list-style-type: none"> ➤ IEDs ➤ Actuators ➤ Sensors
IT Solutions Focus	Dragos ICS Focus		

The Dragos Team



“Dragos offers industrial customers industry-leading technology, services, and intelligence products, but our most important differentiator is our team and its ability to bring a practitioner’s perspective to all that we do. In addition to the depth of valuable, functional industry knowledge each team member brings to Dragos, they bring the insights that only come from experience and the deep commitment to safeguarding civilization that drives the Dragos mission.”

Robert M. Lee, Dragos CEO and Founder



LEADING INDUSTRIAL CYBERSECURITY

Headquartered in metropolitan Washington, DC, Dragos' team of industrial cybersecurity experts offers more than 100 years of combined experience – the largest concentration of such expertise in the industry. Coming from the U.S. intelligence community and private sector industrial companies, their experience includes:

- building and leading a first-of-its-kind mission in the U.S. National Security agency to identify and respond to state cyber threats targeting critical infrastructure and industrial networks
- advising all levels of ICS defenders and policy makers –from White House and U.S. Intelligence Community leadership, to asset owners' and operators' boards of directors, to the practitioners who fight the adversaries on a daily basis
- directing cyber-analysis for the Electricity Information Sharing and Analysis Center
- building and leading major energy companies' network security monitoring, forensics, and incident response teams
- developing the world's only ICS-specific incident response and cyber-threat intelligence training courses for SANS
- co-creating the Diamond Model of Intrusion Analysis, one of the most widely-used methodologies for organizing and analyzing targeted cyber threats
- directing incident response involvement in many of the world's most high-profile industrial cyber attacks
- principal role in uncovering and analyzing major malware threats to industrial infrastructure, including TRISIS and CRASHOVERRIDE



Dragos Ecosystem Overview

Our industry-first, ICS cybersecurity ecosystem provides industrial security defenders with unprecedented situational awareness over their environments, with comprehensive threat intelligence, detection, and response capabilities.



Each component is customizable to your ICS organization's individual needs--so you can implement only the products and services your organization requires.

“Dragos has sought to differentiate in the industrial threat detection and response market by taking an intelligence-driven approach through analytics. These paired with investigation playbooks made by their senior ICS services personnel help to codify the knowledge of the Dragos team into their software technology. The combination helps deliver effective threat detection and response”

Pat Daly, Associate Analyst, 451 Research

THE DRAGOS PLATFORM:

- The Dragos software technology is an automated network monitoring, threat detection, and response platform that passively identifies ICS assets and communications, alerts to malicious activity, and guides defenders step-by-step if a threat is found.

DRAGOS WORLDVIEW:

- WorldView is the industry's only product exclusively focused on ICS threat intelligence, providing updated threat intelligence weekly, monthly, and quarterly to empower our customers with the knowledge to stay ahead of malicious actors and build appropriate defenses to combat them.

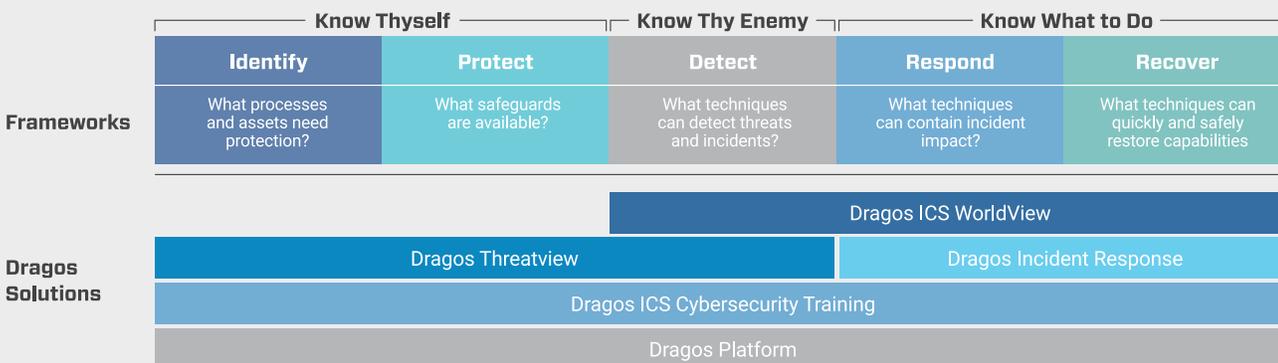
DRAGOS THREAT OPERATIONS CENTER:

- Dragos' Threat Operations Center provides services to ensure your organization is prepared throughout the entire threat lifecycle. Our threat hunters search for malicious activity on ICS networks and identify weaknesses in defenses, our incident response team responds to and neutralizes threats if assistance is needed, and our ICS training gives defenders hands-on experience and real-world applications.



DRAGOS SPANS THE ENTIRE INDUSTRIAL CYBERSECURITY BEST-PRACTICE FRAMEWORK

Dragos believes that for organizations to truly prepare for and defend against the ever-changing threat landscape, they must know their specific cybersecurity challenges and needs, know adversaries' capabilities and activities, and know how to appropriately respond. Our solution spans the entire ICS cybersecurity best-practices continuum, combining human intelligence analysts, ICS operations experts, and advanced technologies to enable asset owners to build and maintain the most effective cyber defenses possible.



THE DRAGOS DIFFERENCE



REAL-WORLD ICS PRACTITIONERS

Dragos is comprised of the most experienced industrial cybersecurity practitioners in the industry. Our team's extensive knowledge and hands-on experience facing ICS threats provide you with real-world application, trusted intelligence, and unparalleled confidence to defend your ICS organization.



CODIFIED KNOWLEDGE

Our team's knowledge and deep experience are codified throughout our technology, intelligence, services, and training and transferred to our customers, so they are empowered to establish resilient ICS security postures, while learning from the Dragos team every step of the way.



INTELLIGENCE-DRIVEN APPROACH

The Dragos team continually researches and learns about the ever-changing ICS threat landscape to keep our customers and community informed through in-depth intelligence, to stay ahead of adversaries, and to adapt and evolve our technology to defend against those who aim to disrupt civilization.

Dragos Platform

OVERVIEW

The Dragos Platform is the most technologically complete solution in the industrial cyber-threat detection and response market today. It is the first and only solution to codify the knowledge of the industry's most trusted ICS security experts and an intelligence-driven approach and integrate them with software technology.

WHO IT'S FOR

Industrial organizations seeking a highly effective cybersecurity solution expressly built for their networks, particularly those facing the challenge of building and retaining a high-performing industrial network/ICS.

WHAT IT DOES

Offers unprecedented insight into ICS assets and activity, as well as the threats and adversaries they face. It delivers the tools and knowledge to defend against threats and provides full visibility into networks across the entire industrial cybersecurity framework. It operates similar to an industrial-specific SIEM, network visibility, threat analytics, and response technology combination.

WHAT MAKES IT DIFFERENT

Intelligence-Driven Approach

The Dragos Platform uses threat behavior analytics (TBAs) to provide context-rich insight when detecting and alerting users to malicious adversary behavior on their ICS networks. TBAs are sequences of adversary tactics, techniques, and procedures characterized by the Dragos Threat Intelligence team through its global research tracking ICS threats, malware, vulnerabilities, and risks.

Instead of just detecting anomalies — contextless, potentially benign changes in an ICS environment — the Dragos Platform uses TBAs to identify specific adversary tradecraft, alert users with context to the detection and provide confident guidance to the incident response process.

Knowledge Transfer

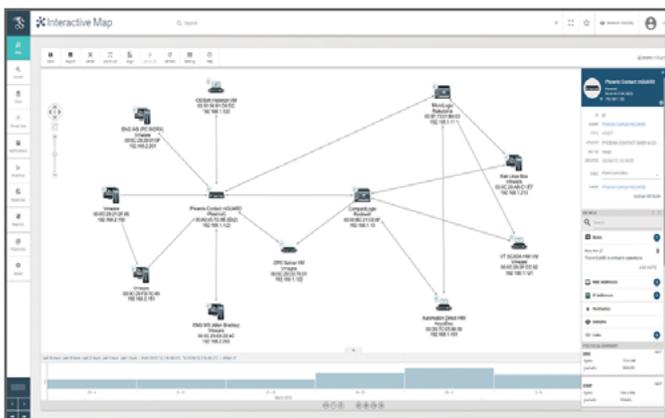
Dragos' technology and services are focused on empowering ICS security teams with the knowledge to establish a resilient ICS security posture and respond to incidents more effectively and efficiently. Each threat behavior analytic codified by the Dragos Threat Intelligence Team is tied to a specific investigation playbook, written by Dragos' Threat Operations Center team, to guide users step-by-step through the incident response process and ensure their investigation efforts are supported through expert intelligence and experience.

Breadth of Coverage

The Dragos Platform provides users with an unprecedented level of visibility into their ICS network activity and a broader range of asset discovery. The automated network monitoring systems passively ingest data from multiple sources—not just network captures—including data historians, host logs, controller logs, and specialized ICS gear (such as Schweitzer Engineering Labs' digital relay events and OSIsoft's PI System), providing a broader analysis of network and operational data for more efficient and effective threat detection and response.

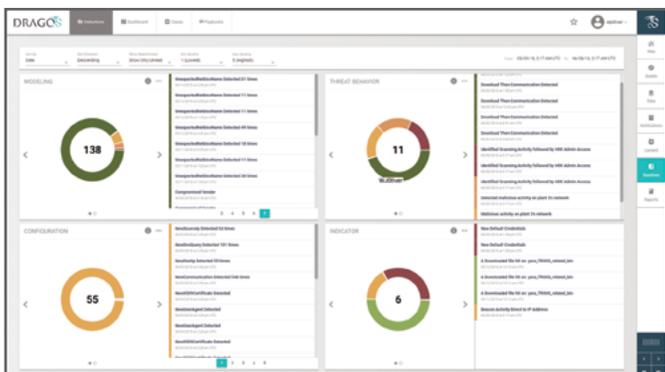
“The Dragos Platform provides us with a level of real-time, situational awareness and monitoring capabilities unparalleled in the industry today, which was never before possible within our windfarm networks. A high-value system for any organization whose operations are dependent upon ICS technology, processes, and protocols”

Marc DeNarie, Chief Information Officer, NaturEner USA



ASSET DISCOVERY

- Passively identify all network assets and communications
- Visualize and map network security zones and identify attack paths
- Set network baselines against which to monitor change
- Scalable to hundreds of thousands of assets across multiple sites



THREAT DETECTION

- Provides rich, real-time context in the form of highly-scalable threat analytics that require no "baking in"
- Indicators of Compromise, Machine Learning derived Anomalies, and Query-Focused Datasets support threat hunting
- Collects, stores, and analyzes logs and data from host systems, logic controllers, and data historians - not just data traffic

The screenshot shows the DRAGOS investigation playbooks and workbench. It features a list of tasks for analyzing network scanning activity:

1. Check the Zone Communication QFD to determine which hosts were scanned. This sort of high frequency QFD... (text continues)
2. Determine which communications are legitimate and which are not for the given asset or asset list. (text continues)
3. Using the asset list of unknown, unauthorized, or new communications, check the HTTP header QFD to d... (text continues)

 The interface includes a sidebar with navigation options and a top navigation bar.

INVESTIGATION PLAYBOOKS & WORKBENCH

- Use-case tools to manage incident response case notes, forensics, and collaboration
- Playbooks from Dragos experts drive standardized, best practice response
- Reduced workload in the form of step-by-step guides pared to the specific analytics that alert
- Reporting and dashboards monitor analyst and system activity

KEY BENEFITS

ICS FOCUSED

designed for ICS environments by ICS operations and cybersecurity experts

PASSIVE

no active scanning or querying of ICS

SCALABLE

designed to monitor as many as hundreds of thousands of assets across multiple sites

INTELLIGENT

intelligence-driven detection through threat analytics for faster, more effective threat detection and response

SUPERIOR TOTAL COST OF OWNERSHIP

threat behavior analytics and investigation playbooks drive down hard and soft security operations costs



NATURENER & DRAGOS, INC. CASE STUDY

Protecting Wind Farms Using the Dragos Platform

NaturEner implemented the Dragos platform in July of 2017, which consisted of nodes at each wind farm and a central monitoring node at its corporate headquarters in San Francisco. The Dragos Platform now monitors all wind farm networks and Energy Management System (EMS) networks.

“Over time, as we’ve monitored the infrastructure and learned how our devices are talking, we have a better sense of what is happening in our network. Girded with that knowledge and the Dragos platform tool suite, we hunt for issues, intrusions and improperly configured devices, thereby increasing our security footprint across the organization.”



CHALLENGES	SOLUTIONS
Subnets that Span Across Hundreds of Miles	The Dragos Platform aggregates subnet data to a centralized data store, allowing NaturEner analysts to review through a single platform
Sparse Subnet Monitoring	The Dragos Platform enables analysts to combine changes to baseline with threat behavior analytics, ensuring that even “low and slow” attacks are detected
Poor Management of Vendor Devices	The Dragos Platform passively monitors device communications across the network, so traffic can be organized into custom network zones, defined by NaturEner
Vendor Access & Inadequate Monitoring of Equipment	The Dragos Platform monitors three of NaturEner’s US network segments’ ingress and egress points of presence and core traffic, revealing vendor-to-device communications not previously monitored
Lack of Asset Inventory Visibility	The Dragos Platform parses traffic for unique source and destination information, allowing devices to be mapped and organized by custom zones, so analysts can view a devices’ history, last time seen, protocols used, and create alerts for any new device seen
Anomaly-Only Detections Insufficient in Complex Environment	The Dragos Platform applies custom threat behavior analytics that watch for a series of events, rather than a single event—providing context to alerts and specific playbooks on how to respond to threats if detected
Vast Network with Limited Resources	Through constant and passive monitoring, the Dragos Platform brings visibility of assets and network communications to a single platform for analysis and offers playbooks and case management, so analysts can leverage our team’s experience

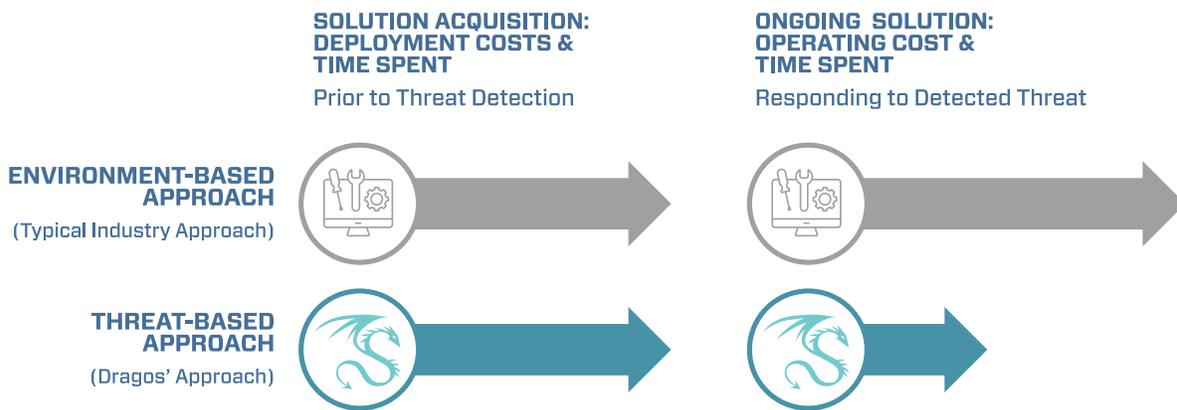
NaturEner operates 399MW of wind power for North America and is expanding into Alberta, Canada. As a leader in sustainable, compliant, renewable energy, NaturEner is also focused on protecting its assets and operations. Implementation of the Dragos Platform allows NaturEner to monitor for adversaries, optimize internal resources, and assume a proactive security program. NaturEner can continue to focus on energy generation and delivery, while being confident its infrastructure is protected.

Dragos Total Cost of Ownership

The Dragos Platform codifies the skills and knowledge of the industry's most trusted ICS practitioners and cybersecurity experts, providing all of the capabilities needed for a more scalable, efficient and effective defense. It leverages analytics and does not need to be 'baked in' to your environment.

ONGOING OPERATIONS COSTS DRIVE ICS CYBERSECURITY TCO

All ICS cybersecurity solutions have upfront costs to acquire and deploy, and across the major providers, including Dragos, in the marketplace today, these upfront costs generally fall within a similar range. The total cost of ownership equation is substantially driven by a solution's ongoing cost of ownership, including maintenance and downtime costs, which is where Dragos stands apart from all others.



“Dragos ICS Worldview provides National Grid with clearly articulated intelligence, backed by evidence and specific information to help us mitigate threats. The clear understanding Dragos has of the environment in which we operate allows us to cut through the hype around many potential industry vulnerabilities, so we can focus on the ones that matter most as we look after vital infrastructure and ensure supply to our customers.”

Phil Tonkin, Global Head of Cyber Operational Technology, National Grid

How a solution detects threats and the incident response capabilities it provides ICS defenders once they are detected significantly impacts its ongoing cost of ownership.

The vast majority of ICS cybersecurity solutions have similar ongoing costs of ownership, due to their reliance upon detecting threats as anomalies within an ICS environment and providing no further context to their detections. Dragos employs multiple threat detection techniques including the industry's sole threat behavior analytics-based approach and provides a range of capabilities beyond alerts that facilitate the most effective and efficient incident response and resolution. As a result of these key differences, the ongoing operating costs, reduced downtime and the TCO of the Dragos Platform can be significantly lower.

Dragos' unique threat behavior analytics detection and automated response capabilities enable a lower ongoing cost of ownership than environment-based only solutions.

DRAGOS' THREAT BEHAVIOR ANALYTICS DRIVE DOWN HARD AND SOFT SECURITY OPERATIONS COSTS

Dragos' threat behavior analytics mine the in-depth knowledge, intuition, and insight from expert ICS and cybersecurity sources around the world – most notably the Dragos Threat Operations Center – to weed out the forensic noise and alert fatigue to better prioritize and respond to threats before significant damage or disruption occurs. The Dragos Platform frees up security analysts to focus on the more strategic and sophisticated tasks of hunting for new threats, leading to further efficiencies and optimizations to industrial cybersecurity posture.



Dragos WorldView ICS-specific Threat Intelligence

OVERVIEW

Dragos ICS WorldView is the only industrial cybersecurity industry product focused exclusively on ICS threat intelligence. Prepared by our expert ICS/Operational Technology (OT) threat intelligence analysts, it is the essential supplement to any IT-focused intelligence product. It cuts through hype and speculation, offering an effective antidote to ICS cybersecurity concerns.

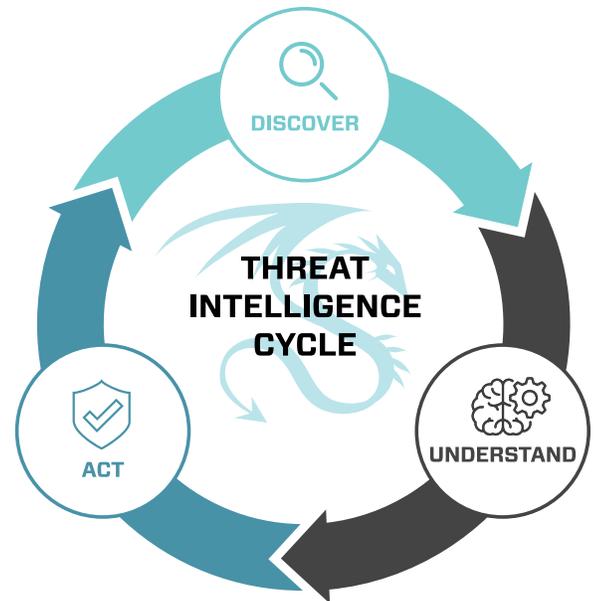
WHO IT'S FOR

IT and OT ICS defenders seeking ICS-focused intelligence to support both tactical decisions and strategic recommendations.

WHAT IT DOES

Provides a range of ICS-specific content to subscribers via e-mail, webinars, and the Dragos Intel Portal, including:

- ICS-themed malware identification and analysis
- ICS vulnerability disclosures and analysis
- ICS adversary behavior trends
- ICS threat/incident media report breakdown and commentary
- Cybersecurity conference presentations and researcher discoveries with Dragos' expert perspective



KEY BENEFITS

IMMEDIACY

critical threat alerts inform of rapidly escalating ICS threat situations

EFFICIENCY

expert threat identification and analysis combats alert fatigue

EFFECTIVENESS

reduce adversary dwell time and MTTR

INSIGHT

ICS vulnerability, threat, and incident assessments promote informed, timely, and confident decision-making

COMPREHENSIVENESS

broad span of ICS intelligence-gathering sources and techniques, including exclusive access to intelligence gained through the Dragos Threat Operations Center

Dragos Threat Operations Center ThreatView Service

OVERVIEW

Dragos ThreatView combines seasoned threat hunters, unparalleled ICS threat intelligence, and advanced technology to find hidden threats inside ICS networks and stop them in their tracks.

WHO IT'S FOR

ICS security stakeholders who recognize the challenges of truly understanding their ICS networks and the potential harm that comes from risks, unknown threats, or security coverage gaps.

WHAT IT DOES

Evaluates the visibility and defensibility of an ICS network and its related processes over the course of approximately six weeks. It identifies likely attack vectors, determines strengths of defenses, and identifies previously unrecognized malicious activity. Dragos provides a findings report, outlining the extent of the threat hunt, key observations, and recommendations for improvement.

Plan:

define engagement scope, review information, discuss goals, expectations, form ThreatView hypothesis

Collect:

aggregate ICS network activity and log data

Analyze:

analyze data to discover hidden threats and other issues

Report:

report any threats found, as well as other observations

Automate:

provide recommendations to resolve discovered issues and improve defenses on a sustained basis



KEY BENEFITS

RELIABILITY

minimize network downtime and reduce costs

BETTER INFORMED DECISIONS

understand the threat landscape for a specific ICS network with additional context related to the environment

SECURE

ICS network and related sensitive data never leaves company premises

NON-INVASIVE

engagement activity does not interfere with regular operations

Dragos Threat Operations Center Incident Response Service

OVERVIEW

Dragos Incident Response service helps asset owners prepare for, respond to, and recover from cyber incidents. Its elite team of experienced incident responders is available 24/7 to assist ICS operations, and help security personnel resolve crisis situations as quickly as possible. Like insurance, it manages the risks associated with the unknown and speeds recovery in the wake of an incident.

WHO IT'S FOR

Those looking to supplement existing OT and IT staff responsible for ICS operations reliability.

WHAT IT DOES

Reduces the time it takes to recover from and resume operations when incidents occur, reducing potential safety, financial, and/or reputational consequences.



Prepare

define key personnel, roles, processes, communication paths, and key constraints

Identify

classify incident and its cause(s), the extent of the breach, and operations impact

Eradicate

remove threat completely, including its root cause, and deploy improved defenses

Review & Adjust

interpret findings and lessons learned and adjust policies, procedures, and preparation to prevent reoccurrence

Contain

analyze, secure and stabilize the impacted ICS, and gather relevant forensics

Recover

bring ICS back online safely, monitor its behavior, and validate mitigations

Dragos Threat Operations Center TableTop Exercise Service

TABLETOP EXERCISE

Assess and improve your ICS organization's cyber incident response plan.

OVERVIEW

Dragos' Table Top Exercise (TTX) is a step-by-step method that demonstrates how a realistic attack may occur within your ICS environment. TTXs evaluate your organization's cyber incident processes and tools and discovers inefficiencies organizations can correct and learn from. Dragos experts design scenarios, based on their experience, in a collaborative workshop environment to assess your organization's response to the scenario and provide critical feedback.

METHOD

A TTX starts with a collaboration between Dragos experts and your organization to establish exercise objectives and develop an attack scenario. The exercise is performed at an on-site workshop, where the scenario is introduced step-by-step in a collaborative fashion.

WHO SHOULD PARTICIPATE

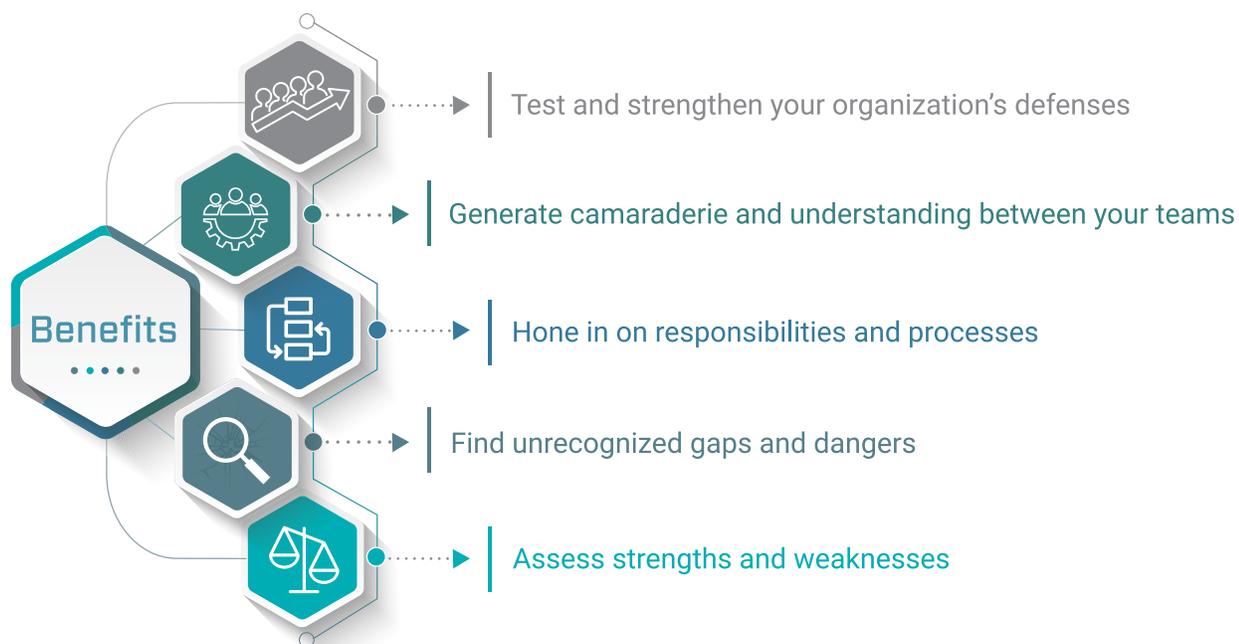
The most successful exercises include a range of staff across multiple disciplines and teams to include: IT, OT, information security, legal, public affairs, and business stakeholders. Each of these teams work together with different puzzle pieces to understand and respond to the scenario as it unfolds.

COLLABORATE EXECUTE COLLECT FEEDBACK

Dragos' TTX process consists of three phases:

- **Planning & Creation**
- **Exercise Execution**
- **After-Action**

Each phase's duration is tailored to your organization's specific objectives and requirements and can be modified if needed.



Threat Operations Center Dragos ICS Cybersecurity Training



OVERVIEW

Dragos ICS Cybersecurity Training increases the skills and capabilities of security teams operating in industrial environments. Our principal course, “Assessing, Hunting, and Monitoring Industrial Control System Networks” is an intensive five-day, hands-on course that covers ICS basics, ICS cybersecurity best practices, assessing industrial environments, ICS threat hunting, and industrial network monitoring. Courses are offered at Dragos’ state-of-the-art training center in Hanover, MD.

WHO IT’S FOR

ICS and OT security professionals seeking to increase their knowledge of ICS cybersecurity best practices and Dragos’ industrial security methodologies and technologies, as well as IT security professionals who want to expand their knowledge of industrial environments and how securing them differs from IT environments.

WHAT IT DOES

Provides hands-on and instructor-led training, incorporating real-world case studies and exercises designed to reinforce concepts learned. Students are placed in various roles designed to give context to the learning, as well as frame hands-on activities.



ASSESSING, HUNTING, AND MONITORING ICS NETWORKS

Course Overview

MODULE 1:

Introduction to Industrial Control Systems and Networks

MODULE 2:

Assessing Industrial Environments

MODULE 3:

Tools, Strategies, and Techniques for Successful Hunting in ICS

MODULE 4:

ICS Monitoring and Security Operations

KEY BENEFITS

INTENSIVE

students learn a wide range of critical skills in five days

HANDS-ON

classroom instruction is reinforced through labs, activities, and role-play

EXPERT INSTRUCTION

instructors are Dragos’ ICS cybersecurity experts



DRAGO 

Contact Information

1745 Dorsey Road Hanover, MD, 21076 USA |
dragos.com | info@dragos.com

