Dragos™ **Incident Response**

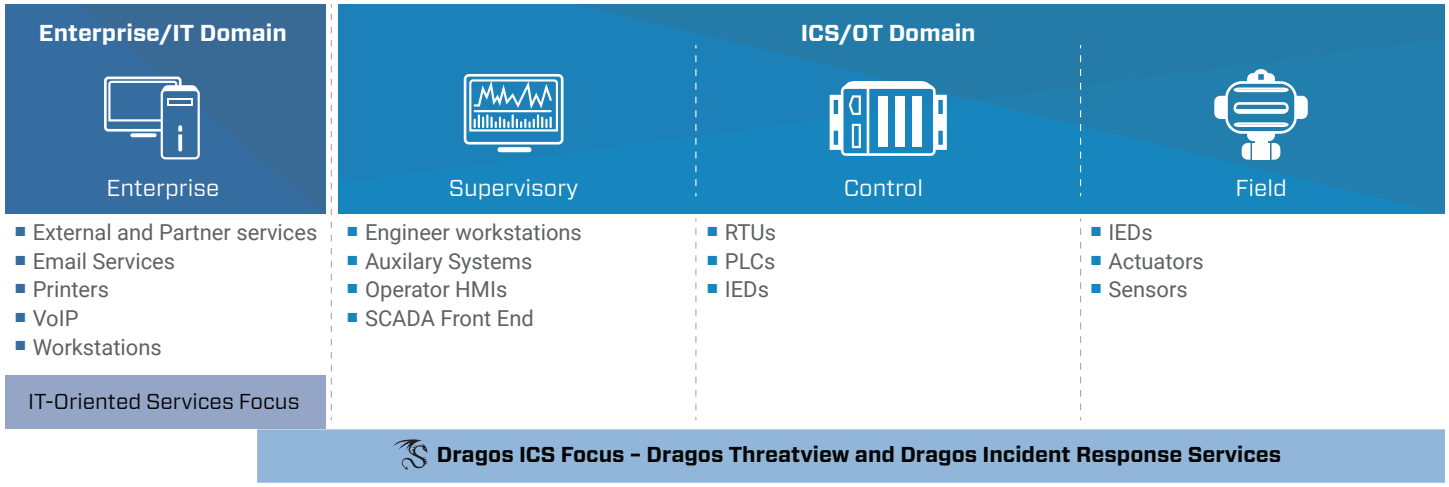
Experience is the key factor in effectively responding to an ICS security breach. Dragos Incident Response makes 40 years' combined experience in preparing for and responding to ICS threats available 24x7

Overview

The ICS threat landscape is still substantially uncharted, making timely and effective incident response all the more challenging. As the need for ICS incident response increases, Dragos has emerged as the industry's most-trusted team.

Upon discovery of a breach to an ICS environment the situation is often chaotic. The specifics of the breach are generally being seen for the first time by OT staff who may have little experience in handling a cybersecurity event, or IT staff that have limited exposure to ICS. These factors can lead to protracted resolution times that may carry serious safety, financial, and/or reputational consequences. Like insurance, Dragos Incident Response Service helps manage the risks associated with the unknown, and speeds recovery when incidents happen.

Dragos understands the major differences between the enterprise/IT and ICS/OT domains and the logical boundary between them. Its incident response expertise and capabilities are focused on filling the need for highly specialized resources to provide support in the ICS/OT domain, with a practitioners' understanding of its environment, including its mission, MTTR-driven metrics, and safety and resilience oriented priorities.



Dragos Incident Response Service Benefits

ICS Focused: Dragos incident responders have deep knowledge of the ICS/OT domain

Reduced Risk: increases preparedness before incidents and provides rapid mitigation when they happen

Trusted: Dragos provides the most experienced threat responders, best ICS threat intelligence, and advanced threat detection and response tools in the industry

Immediate: 24/7 telephone support and on-site support as quickly as within 24 hours

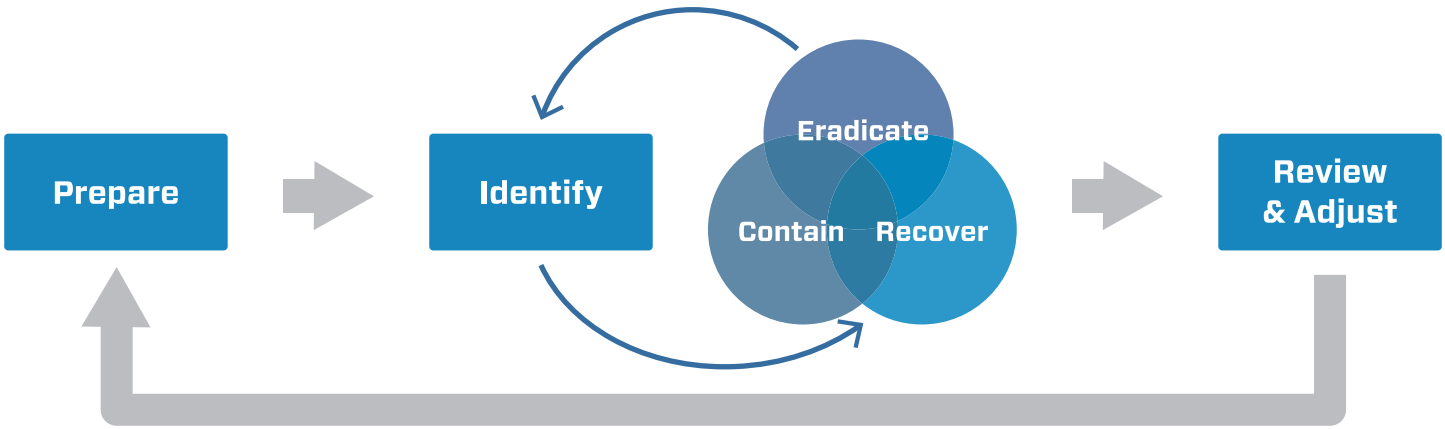
Flexible: options to support a wide range of needs and budgets, with hours applicable to towards incident response, training and threat-hunting services

Adaptable: capabilities applicable to non-existent/immature IR teams and more developed incident response programs

Dragos™ Incident Response

Dragos Incident Response: Before, During, and After an Incident

Working as an extension of the operator's own team, Dragos experts provide support before, during, and after incidents occur, leveraging its range of skills, tools, resources and experience to neutralize the threat and ensure all stakeholders have accurate and timely event, discovery and resolution information.



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

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

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

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

Review & Adjust: interpret findings and lessons learned and adjust policies, procedures and preparation to prevent reoccurrence

Dragos Incident Response Service Options

Dragos Incident Response Service standard plans are based on prepaid retainer hours with specific response time service level agreement (SLA) commitments, as well as a basic offering with a narrower scope of services and a best effort commitment only. Pre-paid retainer hours can be applied to training and threat hunting services by Dragos experts in addition to actual incident response situations.

	400 Tier	160 Tier	80 Tier	Basic Plan
Included annual hours	400+ prepaid hours	160-399 Prepaid Hours	80-159 Prepaid hours	Pay as you go
Hourly rate volume discount	28%	28%	19%	none
24/7 Incident Response Hotline	YES	YES	YES	YES
Responder remote contact established within (SLA)	8 hours	8 hours	8 hours	Best Effort/No SLA
Responder enroute to incident location within (SLA)	24 hours	24 hours	48 hours	Best Effort/No SLA
Customer-specific Dragos responders	YES			
Onsite readiness assessment	YES	YES	YES	
Proactive preparation and pre-planning	YES	YES	YES	
Post engagement findings report	YES	YES	YES	YES

Contact Information

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