DRAGOS

SOLUTION BRIEF

OT Incident Response Services

Rapid Response Retainer and 24/7 Access to OT Cybersecurity Experts.

OT Incident Response Services

The Dragos Rapid Response Retainer ensures 24/7 access to industry-leading OT cybersecurity experts. When an incident strikes in an xOT environment, elite responders are ready to contain and eradicate the threat, with the context to move immediately.

The Challenge

The First Hours Decide the Outcome

When an OT incident hits, the adversary doesn't wait for contracts to be signed. Organizations without preestablished response agreements lose critical days to procurement, environment discovery, and access negotiation while the attacker keeps moving. Responders without OT experience make it worse: containment steps that work in IT can halt production or create safety risks in operational environments.

THE SOLUTION

Dragos OT Incident Response Services Through The Rapid Response Retainer

01

Rapid Response Retainer

By pre-establishing agreements and documenting the environment in advance, Dragos can initiate forensic analysis, provide containment and recovery guidance, and support critical communications to executives, regulators, and stakeholders with minimal delay.

02

Incident Response

When activated, Dragos responders perform forensic analysis and provide instructions on containment, eradication, and recovery. For organizations running the Dragos Platform, SLA-backed response times begin with first contact within one hour and analysis underway within four, significantly reducing the window of exposure.

03

Preparedness & Proactive Services

The retainer also includes an incident response workshop to assess and improve your preparedness, and retainer credits can be applied to proactive security services such as architecture reviews, penetration testing, and tabletop exercises.

Why Dragos OT Incident Response Services

- ✓ Onboarding workshop to align to your OT journey
- ✓ Rapid response when an incident or breach occurs
- ✓ Responders experienced in OT crisis management
- ✓ Flexible retainer hours you can use for additional services
- ✓ Proactive preparedness before an incident occurs through scenario-based planning

What You Get With A Rapid Response Retainer

01

24x7 Access to Experienced OT Responders

Dragos responders support OT cybersecurity incidents worldwide, providing expert analysis, investigation, and guidance on executive, legal, regulatory, and insurance communications. They arrive backed by over a decade of Dragos data, context, expertise, cross-sector telemetry, and OTspecific adversary research.

02

Rapid Response With The Dragos Platform

A Dragos Platform subscription isn't required to purchase a retainer, but it is strongly recommended.

WITHOUT THE PLATFORM	WITH THE PLATFORM
✗ **Investigation Begins** Without historical OT network data, responders start an investigation blind. They must deploy technology on arrival and reconstruct the environment from whatever data survives.	✓ **Investigation Begins** Responders start with the environment already mapped and the evidence already collected, enabling immediate forensic analysis.
✗ **Root Cause Analysis** Root cause analysis stretches from days into weeks and depends on evidence that may no longer exist.	✓ **Root Cause Analysis** Continuous visibility into OT assets, traffic patterns, vulnerabilities, and threats provides the historical data needed to immediately analyze what changed, when it changed, and how the adversary moved.
✗ **Response Timeline** The first days of an incident are spent standing up collection, extending the window of exposure.	✓ **Response Timeline** Platform sites are eligible for SLA-backed response with first contact within one hour and analysis underway within four, significantly reducing the exposure window.

Response Times With Dragos Platform Deployed

*All retainer customers (with platform or without platform) receive first contact within an hour.

1 hour
First Contact*

4 hours
Start of Analysis

2 hours
Start of Analysis w/ OT Watch

48 hours
En Route

03

Proactive Preparation for Cyber Threats and Incidents

Every Rapid Response Retainer begins with onboarding. Optional Incident Response Plan (IRP) Workshops and Tabletop Exercises (TTX) can be initiated using retainer credits to improve your incident response plan.

✓ **Retainer Onboarding** INCLUDED
Assess your current incident response preparedness, document the environment, and understand the retainer activation process.

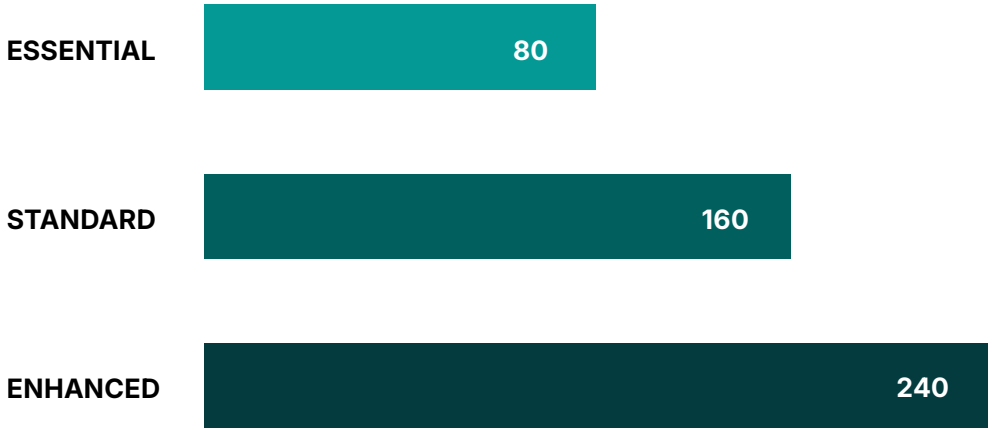
✓ **IRP Workshop** OPTIONAL
A structured session to review, develop, or refine an Incident Response Plan (IRP). Uses the PICERL framework and includes customized scenario playbooks and a roadmap for improving response capabilities.

✓ **TTX** OPTIONAL
Once you have a suitable IRP, a tabletop exercise can simulate OT cybersecurity drills. These exercises strengthen communication, coordination, and preparedness against xcyber threats.

04

Multiple Options With Flexible Retainer Hours

All tiers offer the flexibility to leverage unused hours on Dragos Professional Services.



About Dragos

Dragos delivers xOT cybersecurity for industrial and critical infrastructure, backed by a decade of frontline incident response experience. The Dragos Platform provides asset visibility, continuous monitoring, vulnerability management, and real-time threat detection, all powered by industry-leading intelligence. Dragos protects OT environments globally, including electric, oil and gas, manufacturing, water, and transportation.

Dragos is privately held and headquartered in Hanover, Maryland, operating globally across North America, EMEA, and APAC. Learn more about our technology, services, and threat intelligence offerings: request a demo or contact us.

Learn more: dragos.com