Rapid Response Retainer & Incident Response Services

The Dragos Rapid Response Retainer ensures 24/7 access to industry-leading OT cybersecurity experts for swift incident response. By pre-establishing agreements and documenting your environment in advance, a Dragos Rapid Response Retainer can significantly reduce the timeline to contain and eradicate the attacker.

If activated, Dragos's elite responders perform forensic analysis and provide instructions on containment, eradication, and recovery. We assist in critical reporting for executives, regulators, and stakeholders.

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

For Dragos Platform customers, the retainer offers priority response times, accelerated triage, and in-depth analysis—ensuring faster threat mitigation and enhanced security resilience. The Dragos Platform is a powerful investigation tool, offering detailed forensic records and prioritized guidance to identify vulnerabilities and mitigate risks effectively.

RETAINER BENEFITS

- 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

What You Get With a Rapid Response Retainer

1 24 X 7 Access To Industry-Leading Responders

When crisis strikes, you need experienced responders who understand your tech and act with insight. Dragos's industry-leading team supports OT cybersecurity incidents worldwide, providing expert analysis, investigation, and guidance on executive, legal, regulatory, and insurance communications

2 Rapid Response With The Dragos Platform

A Dragos Platform subscription isn't required to purchase a retainer, but it is strongly recommended. The Platform provides continuous visibility into OT devices, traffic patterns, vulnerabilities, and threats. Sites with the Platform are eligible for faster, SLA-backed response times. With our technology in place, responders can more effectively analyze, investigate, and conduct root cause analysis using historical data. Sites without the Platform or a retainer receive best-effort response.

3 Proactively Prepare for Cyber Threats and Incidents

Every Rapid Response Retainer begins with onboarding. Optional Incident Response Plan (IRP) Workshops and Tabletop Exercises can be initiated using retainer credits, used 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.
Tabletop Exercises (Optional)	Once you have a suitable IRP, a tabletop exercise can simulate OT cybersecurity drills. These exercises enhance communication, coordination, and preparedness against cyber threats.

4 Multiple Options With Flexible Retainer Hours

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

Retainer Tiers	Essential	Standard	Enhanced
Retainer Hours	80	160	240

Response Times With Dragos Platform Deployed (Otherwise, Best Effort)

First Contact*	Start Of Analysis	Start Of Analysis W/OT Watch	En Route
1 Hour	4 Hours	2 Hours	48 Hours

*All retainer customers receive first contact within an hour, whether the Dragos Platform is deployed at the site or not. Other response times are best effort for customer sites without the Dragos Platform.

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. Learn more about our technology, services, and threat intelligence offerings: **request a demo** or **contact us**.