OT Watch – Expert-Driven OT/ICS Network Monitoring & Visibility

Most industrial organizations struggle to defend their operational technology (OT) environments due to a lack of specialized cybersecurity talent, fragmented visibility, and the complexity of industrial control systems (ICS). Traditional IT-centric approaches don't translate to the OT world, and internal teams deserve help.

Industrial organizations need more than tools – they need ICS-specialized experts who understand industrial systems, network architectures, and adversary behaviors. Dragos OT Watch delivers exactly that. Our team of threat hunters, incident responders, security analysts, intelligence researchers, and platform specialists work alongside customers to help them confidently monitor OT networks, improve asset visibility, and continuously strengthen security defenses.

OT Watch and OT Watch Complete: Two Options to Fit Your OT Security Needs

OT Watch delivers proactive threat hunting, critical threat escalations, response playbooks, and detailed reporting to help improve OT security and decision-making. The OT Watch team uses the Dragos Platform and emerging threat intelligence to execute hunts across customer environments in real-time. OT Watch works with or without a dedicated SOC, integrating with existing teams, processes, or third-party providers to enhance and accelerate your cybersecurity maturity without adding internal burden.

> The Dragos OT Watch team, enabled by Dragos Platform technology, provides a level of visibility into our assets and threats that we did not have the expertise or bandwidth to do on our own.
>
> **Doug Short**
> **Chief Information Officer & CISO**
> **Trinity River**

OT Watch Complete includes everything in OT Watch and extends beyond threat hunting to take advantage of the full use-cases of the Dragos Platform essentially acting as your Dragos Platform operators. This includes tuning and optimization, 24/7 managed monitoring and alert triage, asset visibility and rogue device identification, vulnerability management, ongoing security hardening recommendations, and the ability for customers to interact directly with the OT Watch experts to gain operational guidance. Additionally, the Dragos incident response team is embedded in the OT Watch Complete team ensuring the same trusted experts who help you navigate high-pressure incidents are proactively engaged in your environments.

Continuous Risk Reduction

By partnering with Dragos, customers can implement meaningful and achievable security improvements over time. This includes reducing unnecessary alerts, refining asset groups, and addressing vulnerabilities and misconfigurations that adversaries exploit. Customers strengthen their defenses in ways that fit their unique operations, reduce long-term risk, and build more resilient security postures without overwhelming internal teams.

Compare What's Included

		Platform with OT Watch	Platform with OT Watch Complete
Cyber Threat Hunting	Investigations to uncover stealthy, long-dwell, and emerging OT threats that evade detection.	✓	✓
Critical Escalations	High-confidence escalations, validated by OT experts and enriched with operational context.	✓	✓
Response Guidance	Investigation playbooks or containment recommendations to support active incidents.	✓	✓
Weekly Customer Reports	Recent findings, custom threat hunts, and threat hunter actions within the customer environment.	✓	✓
Quarterly Insights	Reports highlighting fleet-level trends, emerging attack behaviors, and shared learning.	✓	✓
Onboarding Support	Guided onboarding, including initial Dragos Platform configuration, asset setup, and monitoring deployment.	✓	✓
Dragos Platform Health & Status	Monitoring platform connectivity, data ingestion, sensor coverage, and alert processing.	✓	✓
24/7 Security Monitoring	Monitoring to ensure alerts are acknowledged to catch and surface potential threats.		✓
Alert Triage & Investigation	OT analyst-led validation to filter noise and investigate alerts to deliver credible escalations.		✓
Baselining	Development of environment-specific asset baselines to improve detection accuracy and visibility.		✓
Vulnerability Reporting	Reporting of vulnerabilities, prioritized by operational impact and aligned with the OT asset inventory.		✓
Hardening Recommendations	Actionable guidance to improve segmentation, reduce exposure, and strengthen architecture.		✓
Asset Enrichment Support	Complete asset metadata by adding missing details to improve inventory accuracy and visibility.		✓
Zone Tuning & Configuration	Adjustment of asset zones, network segmentation, and platform configurations to optimize precision.		✓
Notification Tuning	Tuning of alerting thresholds and notification rules to reduce false positives and enhance relevance.		✓
Expert Interactions	Credit-based analyst time for custom use cases, threat hunts, and OT-specific security consultations.		✓
OT Watch Complete SLAs	Defined service levels for timely alert acknowledgment specific to OT Watch Complete.		✓
Priority Support SLAs	Priority access to Dragos support with fast response times for platform and monitoring issues.		✓
Platform & Content Upgrades	Ongoing delivery of Dragos Platform updates and KP content deployments to maintain high detection fidelity.		✓

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