With Dragos OT Watch, our ICS cybersecurity experts become part of your team, performing high severity notification triage and proactive threat hunting with the Dragos Platform to ensure threats don’t get overlooked. Our elite team of analysts proactively hunt for and report on threat activity in your ICS environment using the latest threat intelligence exclusive to Dragos customers. We work alongside your team to triage and investigate high severity notifications to reduce the burden on internal resources.

THE DRAGOS DIFFERENCE

Dragos is comprised of the industry’s most experienced team of ICS security practitioners, who have been on the front lines of every significant industrial cybersecurity attack globally, including the Ukrainian power grid attacks.

OT Watch offers the expertise of an elite group of ICS intrusion detection analysts and investigators, all dedicated to proactively hunting for adversary activity in your environment and on your behalf.

“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 nor the bandwidth to do on our own.”

Doug Short, CIO & CISO
Trinity River Authority of Texas

KEY BENEFITS

IMPROVE TIME TO RESPOND AND RECOVER
- Prioritized notifications of incidents with added context and recommendations
- Reduced alert fatigue
- Immediate support for critical situations

ACCELERATE TIME TO OPERATIONALIZE
- Immediately align people and processes to fully realize the value of your investment in the Dragos Platform
- ICS Cybersecurity experts continuously add context and tune the Platform based on what they see and learn from your environment
- OT Watch team will ensure your Platform instance always has the latest content to detect threats and enhance visibility

REDUCE MEAN TIME TO THREAT DISCOVERY
- Regular reports on threat hunt findings and response recommendations from Dragos Industrial Hunters
- Routine threat hunts based on newest adversary tactics, techniques, and procedures (TTPs)
- Built on the comprehensive capabilities of the Dragos Platform
OT Watch is managed threat hunting and notification triage remotely staffed by the Dragos team of Industrial Hunters.

**DRAGOS OT WATCH CAPABILITIES**

**MANAGED THREAT HUNTING + DETECTION + RESPONSE SUPPORT**

- **Managed Threat Hunting** – by a remote dedicated Dragos team using the latest intelligence-based IOCs and adversary TTPs
- **Notification Triage & Response Support** – high severity alerts escalated to designated customer personnel and support during an incident.
- **Alert and Asset Configuration Tuning** – enrichment of asset characteristics and alert severities
- **Map and Zone Configuration** – ongoing improvement of asset, zone, and network communication visualizations
- **System Health & Status Monitoring** – recurring environmental checkups and Dragos Platform optimization
- **Applying Knowledge Pack Updates** – regular updates to detections, characterizations, and playbooks in the Dragos Platform
- **Executive Reporting** – weekly reports on overall status of ICS environment, hunt findings and short/long term

To learn more about Dragos OT Watch, please contact sales@dragos.com or visit www.dragos.com/ot-watch.