



# DRAGOS OT WATCH

## MANAGED ICS/OT NETWORK VISIBILITY & THREAT DETECTION

With Dragos OT Watch, our team of ICS cybersecurity experts is part of your team, performing comprehensive asset identification, threat detection, and incident triage with the cloud-deployed Dragos Platform to ensure threats don't get overlooked. Similar to IT-focused MTH services, our elite team of analysts proactively hunt threat activity in your ICS environment based on the latest threat intelligence and operational data from Dragos and work alongside your team to triage and investigate to an incident before it becomes a significant breach.

### 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 2015 and 2016 Ukraine attacks, CRASHOVERRIDE, and TRISIS.

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



#### UNDERSTAND ICS ASSETS AND THEIR BEHAVIORS

- Establish visibility of assets on your OT network with a comprehensive architecture assessment
- Immediately improve your security posture by understanding what contractors and vendors are doing in your environment
- Regular reports of ICS assets and communications and any changes that occur



#### 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

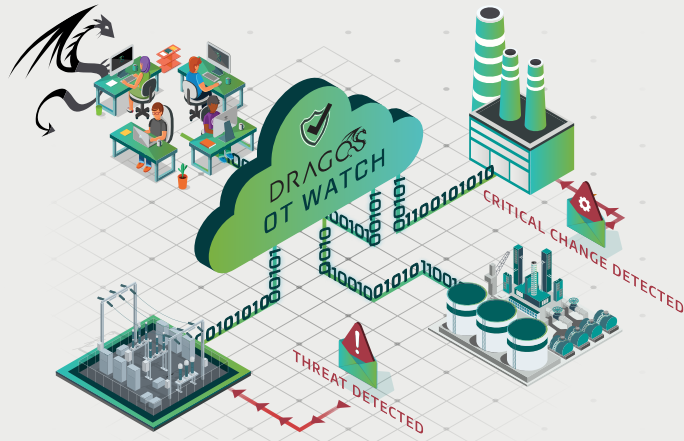


#### DECREASE RESPONSE AND RECOVERY TIME

- 24x7 notification of incidents with added context and recommendations
- Reduced alert fatigue
- Immediate support for critical situations

## OT WATCH

OT Watch is a cloud-deployed managed asset visibility and threat hunting solution remotely staffed by Dragos' team of Industrial Hunters



## DRAGOS OT WATCH CAPABILITIES

### MANAGED VISIBILITY + DETECTION + RESPONSE

- Ease of deployment & maintenance using the cloud-based Dragos Platform
- Dedicated Team of Dragos Industrial Hunters to remotely monitor your OT environment
- Visualization of asset characteristics and behaviors
- Visibility of changes over time with baselines and timeline analysis
- Routine, proactive intelligence-led threat hunts based on latest IOCs and adversary TTPs
- 24 x 7 monitoring and threat validation with multi-channel notifications to ensure awareness
- ICS threat landscape visibility via threat intelligence and analytics
- Cloud-scale telemetry enables integration of Dragos operational data and community use cases
- Recurring environmental checkups and Dragos Platform tuning

### Dragos OT Watch



Dragos Industrial Hunters



**DRAGOS PLATFORM**  
Visibility + Detection + Response

Note: Data gathering processes and procedures are GDPR compliant. Contact us to learn more.

To learn more about Dragos OT Watch, please contact [sales@dragos.com](mailto:sales@dragos.com) or visit [www.dragos.com/ot-watch](http://www.dragos.com/ot-watch).