Dragos™ **ThreatView**

Dragos ThreatView combines seasoned threat hunters, unparalleled ICS threat intelligence, and advanced technology to find hidden threats inside ICS networks - so they can be neutralized

Overview

Dragos ThreatView is a service that finds hidden threats in ICS networks that often go undiscovered. Backed by Dragos WorldView ICS intelligence and own their deep experience, Dragos' threat hunters methodically search for malicious activity while identifying weaknesses in defenses. Employing technology and automation tools including the advanced detection and response capabilities of the Dragos Platform, they find hidden threats quickly, efficiently and non-invasively, working as an extension of the local ICS security team. While doing so, they identify gaps in defenses and visibilities to improve the overall security posture. If assistance is required to neutralize a threat, it can be quickly provided by the Dragos Incident Response team.

The unique architectures and protocols of ICS networks and the developing state of ICS cybersecurity pose new challenges for many asset owners, confronting them with an unclear threat landscape and a shortage of ICS/OT cybersecurity expertise to help bring it into sharper focus. Dragos ThreatView helps overcome these challenges by synthesizing Dragos' deep ICS network knowledge, global threat intelligence, and threat detection and response experience, providing visibility, confidence and knowledge transfer. **Periodic threat hunting is a key strategy for reducing adversary dwell time within an ICS network and the corresponding safety, financial, regulatory or reputational risks that could accompany a serious incident.**

Dragos ThreatView Process and Engagement Details

A Dragos ThreatView engagement evaluates the visibility and defensibility of an ICS network and its related processes over an approximately six-week period. It integrates the entire Dragos ecosystem: platform, threat intelligence and threat operations into a threat hunting methodology that identifies likely attack vectors, determines strengths of defenses, and identifies previously unrecognized security gaps and malicious activity. Upon completion of the engagement Dragos provides a findings report outlining the extent of the threat hunt, key observations made and recommendations for improvement.

Plan: define engagement scope, review information, discuss goals, expectations, form ThreatView hypothesis

Collect: aggregate ICS network activity and log data

Analyze: analyze data to discover hidden threats and other issues

Report: report any threats found as well as other observations

Automate: provide recommendations to resolve discovered issues and improve defenses on a sustained basis

Dragos™ **ThreatView**

Specific elements of a Dragos ThreatView engagement include:

- IT, supervisory, control, and field device asset identification and relationship analysis
- Critical function (Crown Jewel) analysis
- Zone to Zone trust paths (network perimeter security)
- Pivot path likely vector analysis
- DNS activity and log review
- Indicator sweeps to find known malicious activity
- Behavioral analytics to find previously unknown malicious activity

Questions asset owners should be asking:

- What are we doing to understand the threats facing our ICS?
- How confident are we that our ICS has not been compromised?
- What are the likeliest vectors of an attack on our ICS?
- How will we respond to a cyber incident impacting our ICS?

Dragos ThreatView Service Benefits

Better Informed Decisions: identify gaps and opportunities to enhance security posture

Reduced risk: find hidden threats in an ICS network so they can be neutralized

Visibility: see the threat landscape for a specific ICS network and understand its context

Trusted: Dragos provides the most experienced threat hunters, best ICS threat intelligence, and advanced threat detection and response tools in the industry

Secure: ICS network and related data never leaves company premises

Non-invasive: engagement activity does not interfere with regular operations

Scalable: grow internal team capabilities through close interaction with Dragos experts

Dragos ThreatView Options

Included Features	ThreatView Gold	ThreatView Silver	ThreatView Bronze
Network capture analysis	YES	YES	YES
Onsite assessment	YES	YES	
Dragos Platform deployed for threat hunt*	YES	YES	
Dragos ThreatView results report and briefing	YES	YES	YES
Customized threat hunts	YES		
Attack and vulnerability Analysis	YES		

*for duration of ThreatView engagement

Contact Information

1745 Dorsey Road
Hanover, MD, 21076 USA
dragos.com | info@dragos.com

v.1.0 10/17 | Copyright © 2017 Dragos, Inc. All Rights Reserved.