DRAGOS and ANOMALI

Consolidated View of IT / OT Threat Intelligence Data

HIGHLIGHTS

- Analysts benefit from having a consolidated view of both IT and OT threat intelligence through a single pane of glass for improved visibility, reduced monitor fatigue, and faster incident response.
- Improved ICS vulnerability and threat awareness along with response recommendations enables a more proactive security stance across entire IT / OT environment at industrial organizations.
- Integration of Dragos WorldView OT threat intelligence reports and IOCs in existing Anomali Threat Platform installations means no additional infrastructure, reduced learning curve, and faster time-to-value.
- Anomali Threat Platform clients can easily evaluate Dragos WorldView ICS-focused threat intelligence via the Anomali Preferred Partner Store (APP Store)*.

* Users must be logged into ThreatStream to access the APP Store.

THE CHALLENGE

Threats against industrial organizations – including critical infrastructure sectors like electric utilities, oil & gas, manufacturing, water utilities and more – are increasing.

Adversaries are targeting both Information Technology (IT) and Operational Technology (OT) networks and despite the continued convergence of these networks, defending them requires a different skill set and mindset.

It is imperative that security analysts at industrial organizations have good coverage of both IT and OT threats, including reports providing insight into adversary targeting, the adversaries' tactics, techniques and procedures (TTPs), and Indicators of Compromise (IOCs).

Having an integrated data feed of reports and IOCs which covers both IT and OT threats will improve detection, response, and mitigation time when an adverse event does occur, when speed and efficacy are key.

Bottom line, analysts at industrial organizations need an aggregated approach for ingesting, leveraging, and acting on both enterprise IT and OT network threat intelligence. This data affords them faster identification of known threats and escalates responses to cyber events.

A VIEW FROM THE TRENCHES

"Dragos Worldview provides clearly articulated intelligence, backed by evidence and specific information to help mitigate threats. Dragos has a clear understanding of the ICS environment, and cuts through the noise surrounding *potential* industry vulnerabilities. This means we can focus on the issues that matter most as we look after vital infrastructure and ensure supply to our customers." – **Utility Company**

OT & IT THREAT VISIBILITY	OT & IT THREAT HUNTING
Challenge: Security teams lack holistic, unified understanding of the vulnerabilities and constantly evolving threat landscape across their entire IT / OT environment.	**Challenge**: While enterprise IT threat intelligence is well established and fairly commonplace, there is limited coverage of OT-focused threats. So, security teams have a fragmented view of threats in their IT / OT environments.
Solution: Integrate the ICS-focused Dragos WorldView threat intelligence into Anomali Threat Platform along with traditional IT threat intelligence to better inform analysts, and provide convenient access to both.	**Solution**: Leverage the ICS-focused Dragos threat intelligence feed of reports and IOCs in the Anomali Threat Platform to identify and prioritize threat hunting across IT and OT environments.
Benefit: Convenient, single pane of glass to view and understand threats and vulnerabilities across the entire IT / OT environment improves visibility, reduces monitor fatigue and speeds incident response.	**Benefit**: Analysts are able to conduct threat hunts based on realistic scenarios created from comprehensive IT and OT threat intelligence, thereby saving time and resources while reducing the potential impact of cyber events.

THE SOLUTION

Dragos has teamed with Anomali to provide customers with a universal view of threat intelligence that covers both IT and OT networks. Security teams at industrial organizations can view ICS-focused threat intelligence alongside the enterprise IT threat intelligence data from Anomali and other sources, providing analysts with improved overarching situational awareness and decision-making support.

Detecting, responding to, and mitigating threats in converged ICS environments requires industry expertise and an in-depth understanding of the tactics, techniques and procedures (TTPs) by which adversaries exploit gaps that may exist in IT and OT environments – delivered via contextually-relevant reports and IOCs.

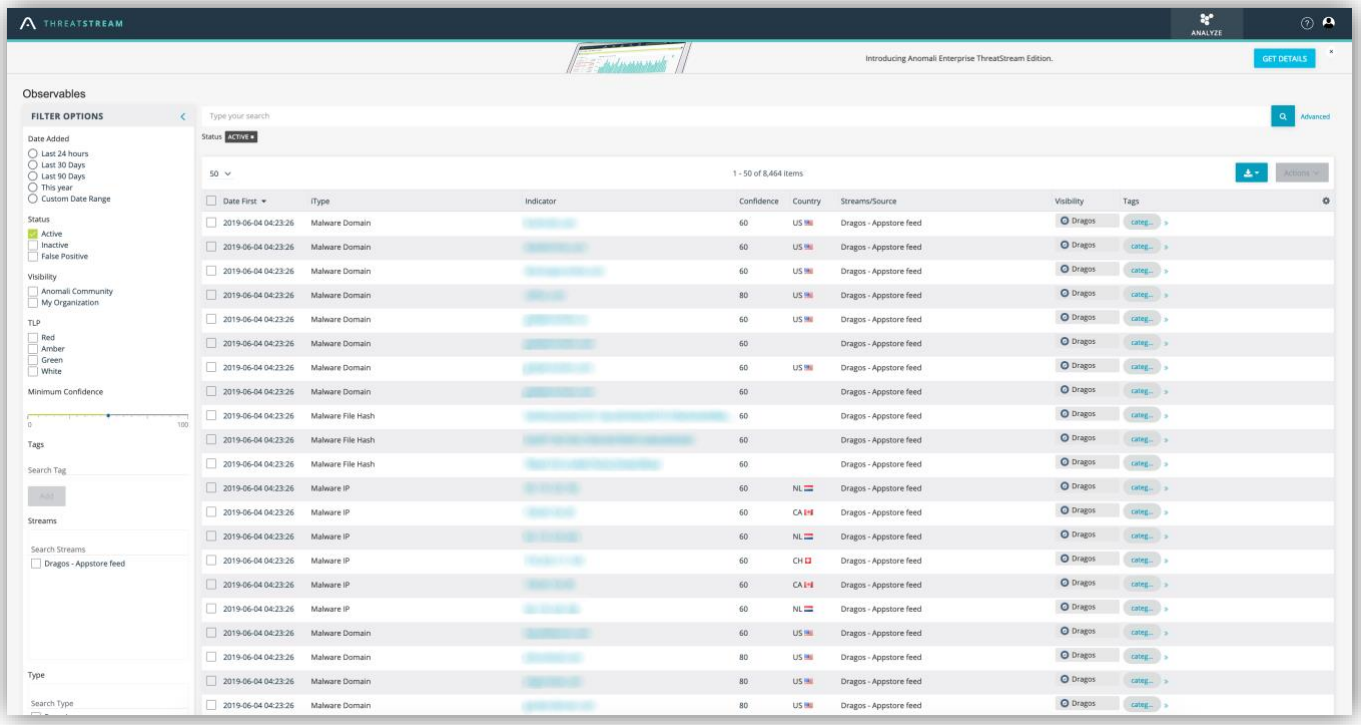
Ingesting the Dragos ICS-focused threat intelligence data via the Anomali Threat Platform improves visibility, reduces monitor fatigue and context switching, and speeds incident response. It also allows analysts to discern which IT-originating threats can impact ICS networks, and how.

This deep insight across the entire IT / OT environment enables cyber defenders at industrial organization to quickly identify and respond to threats, and provides them with defense recommendations to better prepare for and combat future cyber incidents.

ICS-FOCUSED THREAT INTELLIGENCE

Threat intelligence allows defenders to react to cyber events by better understanding the adversaries and their behaviors. Threat Intelligence reduces harm by improving decision making before, during, and after cybersecurity incidents – reducing operational mean time to recovery (MTTR), reducing adversary dwell time, and enabling root cause analysis. It is a necessary component of every cybersecurity program and significantly improves the efficacy of all existing elements.

However, there is no "universal" threat intelligence product, so organizations must match threat intelligence products to their internal threat profiles. Enterprise-focused threat intelligence developed around traditional IT environments will not satisfy the unique requirements for industrial control.



Therefore, industrial organizations and IT groups that have ICS in their environment should use an ICS-focused threat intelligence product, regardless of whether they are already receiving enterprise threat intelligence.

Anomali Threat Platform clients can easily trial and purchase the Dragos WorldView ICS-focused threat intelligence via the Anomali Preferred Partner Store (APP Store), enabling security analysts to engage with both enterprise IT threat data and ICS-focused data simultaneously to get a complete picture of a threat.

BENEFITS and IMPACTS

BENEFIT	IMPACT
Improved Visibility and Detection	Single pane of glass to view and investigate threats and vulnerabilities across the entire converged IT / OT environment, improving vulnerability & threat detection, reducing monitor fatigue and context switching, and speeding incident response (IR).
Extended Security	Comprehensive OT threat intelligence data allows security analysts at industrial organizations to seamlessly extend existing capabilities, thereby saving time and resources while reducing the impact of threats.
Simplified Account Management	Enable the Dragos ICS threat intelligence reports and ICOs in the Anomali Threat Platform via simple app purchase and activation, bringing industrial security into focus with ease.
Immediate Time-to-Value	Immediate and effective protection against all types of threats against both enterprise IT and industrial OT network assets.

To learn more about Anomali ThreatStream, please visit www.anomali.com/threatstream or contact info@anomali.com.

To learn more about Dragos WorldView, please visit www.dragos.com/worldview or contact info@dragos.com.