DRAGOS | TRUSTAR

PARTNER BRIEF

DRAGOS and TRUSTAR
Consolidated View of IT/OT Threat Intelligence Data

HIGHLIGHTS

- Security teams benefit from having a consolidated view of IT and OT threat intelligence for improved visibility, reduced monitor fatigue, and faster incident response.
- Integration of Dragos WorldView OT threat intelligence reports and Indicators Of Compromise (IOC).
- The Dragos app is available from the TruSTAR Marketplace.

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 different skills and approaches.

Security analysts at industrial organizations have a need to understand both IT and OT threats, via reports that outline Tactics, Techniques and Procedures (TTPs), and 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.

The 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.

This deep insight across the entire IT/OT environment enables cyber defenders at industrial organizations 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 can help reduce the impact of a cyber incident by providing foresight of adversarial behaviors observed across the globe. This helps improve decision making before, during and after an incident thus reducing Mean Time to Recovery (MTTR).

However, there are no “universal” threat intelligence products for 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 security teams that have ICS in their environment benefit from using an ICS focused threat intelligence product, in addition to receiving enterprise threat intelligence.

©Dragos, Inc. Dragos and TruSTAR

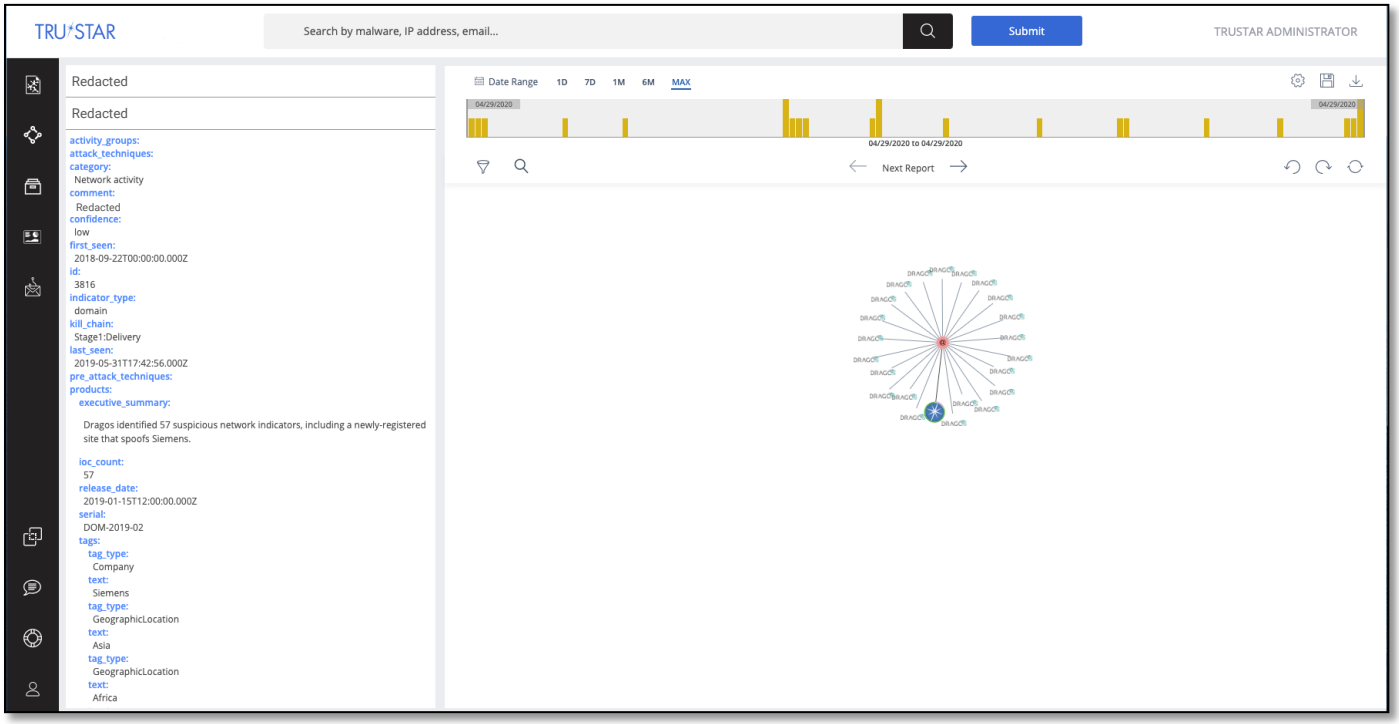
Joint clients of Dragos and TruSTAR can easily integrate the Dragos WorldView ICS-focused threat intelligence via the TruSTAR Marketplace, enabling security analysts to engage with both enterprise IT threat data and ICS focused data simultaneously to get a complete picture of a threat.

THE SOLUTION

Dragos and TruSTAR have combined 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 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 TTPs by which adversaries exploit gaps that may exist in IT and OT environments delivered via contextually relevant reports and IOCs.

Incorporating the Dragos ICS-focused threat intelligence data into the TruSTAR Intelligence Management Platform improves visibility, reduces monitor fatigue and context switching, and speeds incident response. Threat intelligence is automatically transformed to enrich workflows, allowing analysts to discern which IT-originating threats can impact ICS networks, and how.



BENEFITS AND IMPACTS

Benefits	Impacts
Improved Threat Visibility and Detection	View and investigate threats and vulnerabilities across the entire converged IT/OT environment, improving vulnerability & threat detection, reducing monitor fatigue and context switching, and improving 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 MTTR from threats.
Simplified Account Management	Enables the Dragos ICS threat intelligence reports and IOCs via the TruSTAR Marketplace, enhancing industrial security threat awareness.

For more information, please visit www.dragos.com or contact us at info@dragos.com

©Dragos, Inc. Dragos and TruSTAR