PARTNER BRIEF

DRAGOS and CYWARE

Consolidated View of IT & OT Threat Intelligence Data

HIGHLIGHTS

- Security teams benefit from having a consolidated view of IT and OT threat intelligence through a single pane of glass for improved visibility, reduced monitor fatigue, and faster incident response.
- Integration of Dragos WorldView OT threat intelligence Indicators Of Compromise (IOC).
- The Dragos App is available within the Cyware Threat Intelligence eXchange (CTIX) platform.

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. Having an integrated data feed of 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.

OT-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 MTTR.

However, there are no “universal” threat intelligence products to their internal threat profiles. Enterprise focused threat intelligence developed around traditional IT environments will not satisfy the unique requirements of operational technology and industrial control systems (ICS).

Therefore, industrial organizations and security teams that have ICS in their OT environment benefit from using a focused threat intelligence product, in addition to receiving enterprise threat intelligence.

DRAGOS | CYWARE

PARTNER BRIEF

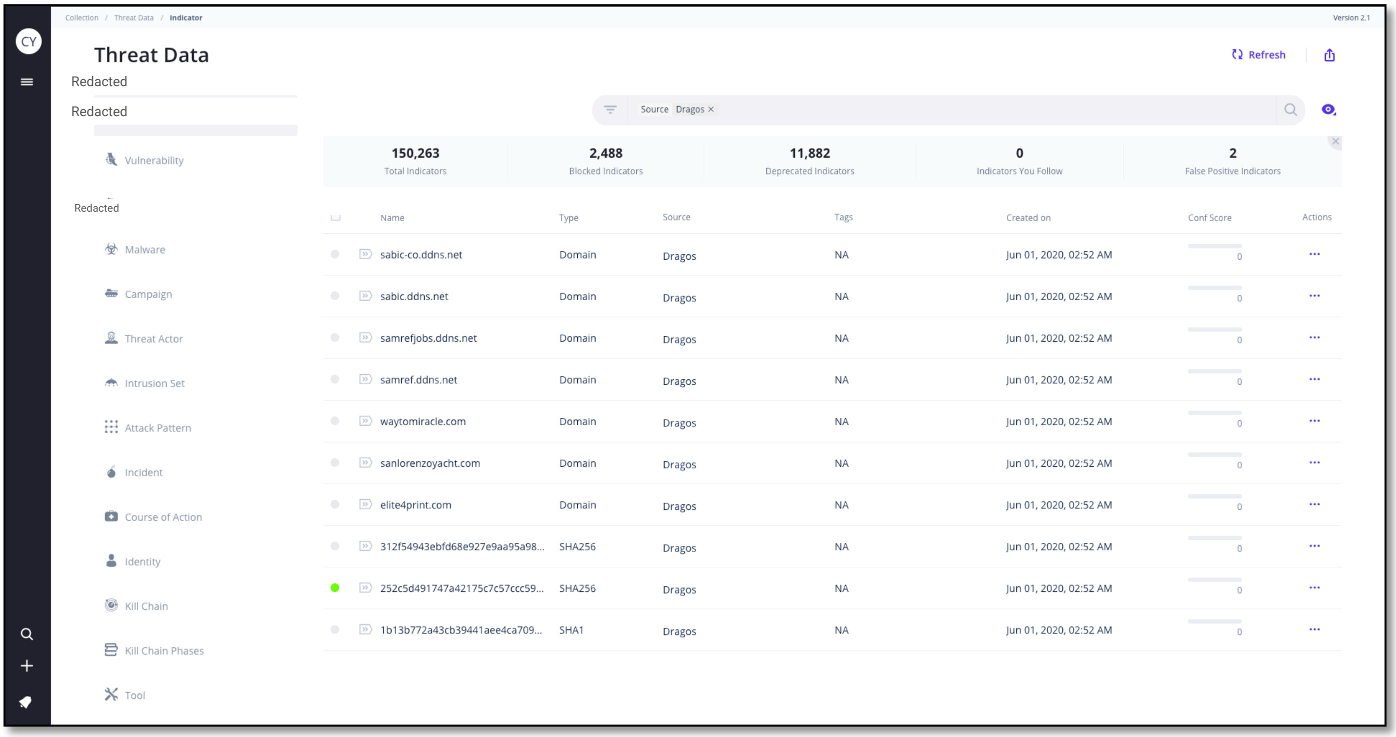
Joint clients of Dragos and Cyware can easily integrate the Dragos WorldView OT-focused threat intelligence via the **Cyware Threat Intelligence eXchange (CTIX) platform**, enabling security analysts to engage with both enterprise IT threat data and OTfocused data simultaneously to get a complete picture of a threat.

THE SOLUTION

Dragos and Cyware 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 OT-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/OT 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 OT-focused threat intelligence data into the Cyware Threat Intelligence eXchange (CTIX) platform improves visibility, reduces monitor fatigue and context switching, and speeds incident response.



150,263	2,488	11,882	0	2
Total Indicators	Blocked Indicators	Deprecated Indicators	Indicators You Follow	False Positive Indicators

Name	Type	Source	Tags	Created on	Conf Score	Actions
sabic-co.ddns.net	Domain	Dragos	NA	Jun 01, 2020, 02:52 AM	0	•••
sabic.ddns.net	Domain	Dragos	NA	Jun 01, 2020, 02:52 AM	0	•••
samrefjobs.ddns.net	Domain	Dragos	NA	Jun 01, 2020, 02:52 AM	0	•••
samref.ddns.net	Domain	Dragos	NA	Jun 01, 2020, 02:52 AM	0	•••
waytomiracle.com	Domain	Dragos	NA	Jun 01, 2020, 02:52 AM	0	•••
sanlorenzoyacht.com	Domain	Dragos	NA	Jun 01, 2020, 02:52 AM	0	•••
elite4print.com	Domain	Dragos	NA	Jun 01, 2020, 02:52 AM	0	•••
312f54943ebfd68e927e9aa95a98...	SHA256	Dragos	NA	Jun 01, 2020, 02:52 AM	0	•••
252c5d491747a42175c7c57ccc59...	SHA256	Dragos	NA	Jun 01, 2020, 02:52 AM	0	•••
1b13b772a43cb39441aee4ca709...	SHA1	Dragos	NA	Jun 01, 2020, 02:52 AM	0	•••

BENEFITS AND IMPACTS

Benefits	Impacts
Improved Threat 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 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/OT threat intelligence IOCs via the Cyware Threat Intelligence eXchange (CTIX) platform, enhancing industrial security threat awareness.

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

For more information on Cyware, please visit www.cyware.com or contact sales@cyware.com