DRAGOS AND SPLUNK

Maximizing IT and OT Datasets to Discover Industrial Threats

HIGHLIGHTS

- Improve visibility across IT and OT, while ensuring process effiencies.
- Utilize the Dragos OT Add-On datasets across Splunk Enterprise Security dashboards, correlation rules, and more.
- Events and notifications from the Dragos Platform are easily integrated into Splunk ensuring security analysts can effectively search, correlate and act upon suspicious threat activity.
- Security teams can easily consume Dragos WorldView Threat Intelligence directly within Splunk providing a consolidated view of IT and OT threat intelligence.

THE CHALLENGE

Threats against industrial organizations, including critical infrastructure sectors like the electric utility industry, oil & gas industry, manufacturing industry, and others are increasing. As these organizations continue the path of digital transformation, expanding network connectivity and process efficiencies, adversaries now target both Information Technology (IT) and Operational Technology (OT) networks. Despite the continued convergence of these networks, defending them requires different skills and approaches.

Cybersecurity analysts at industrial organizations need to understand and protect against both IT and OT threats. These analysts now look to an aggregated approach for ingesting, leveraging, and acting on both enterprise IT and OT network data for effective detection across both domains. This data affords them faster identification of known threats and expedites investigation of cyber events.

This deep insight is needed across the entire IT/OT environment to enable cyber defenders at industrial organizations to quickly identify and respond to threats and provides them with defense recommendations to better prepare for future cyber incidents.

THE SOLUTION

The Dragos Platform is industrial control systems (ICS) cybersecurity technology that provides comprehensive visibility of your ICS/OT assets and the threats you face, with best-practice guidance to respond before a significant compromise.

Backed by the industry's largest and most experienced team of ICS cybersecurity practitioners, Dragos WorldView threat intelligence arms your organization with in-depth visibility of threats targeting industrial environments globally and the tried-and-true defensive recommendations to combat them.

Splunk Enterprise Security collects and aggregates data from multiple sources at scale, allowing users to easily index, search & correlate events making it an effective tool for empowering security teams.

Splunk, an analytics-driven SIEM designed to quickly detect and respond to threats, is found in Security Operations Centers (SOC) as a core component for monitoring enterprise networks.

By leveraging technology from Splunk and Dragos, defenders can ensure they have maximum visibility across both IT and OT networks, improving overall threat detection, response, and post-incident mitigation when time is of the essence.

Together, this partnership expands the ICS cybersecurity ecosystem to ensure critical infrastructure and industrial organizations are better prepared with enhanced visibility that improves threat detection in OT environments, regardless of where an adversary may attack. Enabling more effective SOCs, threat hunts, and providing the ability to resolve incidents quickly to strengthen operational resilience.

Dragos and Splunk customers can easily leverage the power of both solutions to provide a universal view of both IT and OT networks for security operations.

TECHNOLOGY INTEGRATIONS AND ADD-ON APP

Now available through the Splunkbase App Store, Dragos has developed the Dragos OT Add-On to support integration between Splunk, the Dragos Platform, and Dragos WorldView Threat Intelligence. For more information on the available Splunk apps and integrations, please visit the Dragos Splunk App Page.

BENEFITS AND IMPACTS

BENEFITS	IMPACTS
Secure Digital Transformation	Seamlessly bridge the IT/OT divide between networks by bringing the two cybersecurity data sources together into one view.
Actionable Industrial Threat Intelligence	Indicators of Compromise (IOCs) from Dragos WorldView Threat Intelligence can easily be imported into Splunk via an app allowing analysts to view OT threat intel alongside existing feeds, further simplifying the process of detecting threat activity in your environment.
Improved Threat Visibility and Detection	Joint customers can integrate OT threat dectection from the Dragos Platform into their security operations, offering complete visibility across IT and OT.
Pre-defined Visualizations	Dragos apps provide default dashboards and visualizations to easily represent the data available from Dragos solutions with minimal configuration.

For more information, please visit www.dragos.com/partners/splunk
www.dragos.com/partner/splunk/app
or contact us at info@dragos.com