DRAGOS AND SPLUNK

Maximizing IT and OT Datasets to Discover Industrial Threats

HIGHLIGHTS

- Technology integrations ensure customers are able to improve visibility across IT and OT while improving process efficiencies.
- Security teams can easily consume Dragos WorldView Threat Intelligence directly into Splunk providing a consolidated view of IT and OT threat intelligence through a single pane of glass.
- Events and notifications from Dragos Platform are easily integrated into Splunk ensuring security analysts can easily search, correlate and act upon suspicious threat activity.
- The Dragos Add-On for Splunk allows users to utilize datasets from all Dragos solutions.

THE CHALLENGE

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

Adversaries target 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 need to understand both IT and OT threats. By leveraging technology from Splunk and Dragos combined with Dragos WorldView Threat Intelligence, defenders can ensure they have maximum visibility across both IT and OT networks. This improves overall threat 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 data for effective detection across both domains. 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.

THE SOLUTION

The Splunk technology platform 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 is a popular SIEM platform found in the Security Operations Center's (SOC's) as a core component for monitoring enterprise networks.

The Dragos Platform is an 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.

Dragos Threat Intelligence arms organizations with in-depth visibility of threats targeting industrial environments globally and the tried-and-true defensive recommendations to combat them.

This partnership expands the ICS cybersecurity ecosystem to ensure critical infrastructure and industrial organizations are better prepared with enhanced visibility that improves threat detection inclusive of OT environments, regardless of where an adversary may attack. It enables more effective SOC functions, more effective threat hunts, and the ability to resolve incidents.

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 APP'S

Dragos has developed multiple apps to support integration between Splunk and Dragos solutions (Platform and WorldView) which are now available through the Splunkbase app store.

Dragos Threat Intelligence App for Splunk

Existing Dragos WorldView threat intelligence subscribers can easily incorporate Dragos' industrial IOC's into their Splunk deployments to enable security analysts to utilize both enterprise IT threat data, and OT focused data simultaneously. This improves the overall efficiency of an analyst is not just understanding global threats from various sources but enabling easier detection of threat activity in their environment.

Dragos ICS Threat Detection App for Splunk

Users of the Dragos Platform can export notifications and events such as detected OT threat behavior directly into Splunk, where it can be analyzed and viewed by existing SOC teams. It provides cyber defenders at industrial organizations with a unified view of threats and events across the converged enterprise IT and industrial OT (operational technology) environment. Threats detected on OT networks via the Dragos Platform can now be easily integrated into Splunk deployments and visualized via the four types of detection dashboard, further enabling a more comprehensive response.

Dragos Add-On for Splunk

More advanced Splunk users can access data directly within Dragos Platform and Dragos WorldView Threat Intelligence such that custom queries and visualizations can easily be crafted to meet the needs of the organization.

For more information on the available Splunk apps and integrations, please visit the Dragos Splunk App Page.

BENEFITS AND IMPACTS

BENEFITS	IMPACTS
Actionable Industrial Threat Intelligence	IOC's from Dragos WorldView Threat Intelligence can easily be imported into Splunk via an app allowing analysts to view OT intel alongside existing intel feeds, further simplifying the process of detecting threat activity in your environment.
Improved Threat Visibility and Detection	Joint customers can integrate OT threat detections from 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.
User Flexibility	The Dragos Add-On for Splunk provides an easy mechanism for advanced Splunk users to utilize the data available from Dragos solutions, including Dragos Platform and Dragos WorldView Threat Intelligence. This customization allows analysts to use and view the data in a manner that is most useful for their needs.

To learn more about Splunk, please visit https://www.splunk.com
To learn more about Dragos, please visit https://dragos.com or email info@dragos.com

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