INTEGRATED TECHNOLOGY FROM DRAGOS AND SPLUNK

Utilizing IT and OT Data for Complete Threat Detection

HIGHLIGHTS

- Manage your IT & OT cybersecurity posture in a single view and create workflows to ensure you are resolving threats and vulnerabilities on both IT/OT networks.
- Provide context rich ICS/OT asset visibility that analyzes multiple data sources including protocols, network traffic, asset characterizations and anomilies.
- Reduce alert fatigue by utilizing Dragos's curated and exclusive Indicators of Compromise (IOCs) to look for malicious behavior that may be on your network.
- Combined technology improves OT awareness and response to OT threats by leveraging increased visibility.

OVERVIEW

As Operational Technology (OT) networks converge with Informational Technology (IT) networks within industrial organizations, it's becoming essential that security operations teams have complete visibility and correlation across both domains for effective threat detection and incident response. Technology integrations between Splunk and Dragos bridge this divide and improve visibility and process effficiencies to enable a more robust Security Operations Center (SOC).

THE CHALLENGE

Threats against industrial organizations, including critical infrastructure sectors like the electric utility industry, oil & gas industry, manufacturing industry, and more, 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 not only need to understand what IT and OT threats exist but also implement a program to detect and respond to them within their organization. It's imperative that security teams get the maximum value out of existing cybersecurity technology investments and integrating complementary platforms will also help provide more holistic visibility and improve security operations efficiencies.

Adversaries targeting OT often leverage internet connectivity from the enterprise networks to pivot into Industrial networks. Therefore, security teams responsible for the availability of both IT and OT networks need to quickly correlate any suspicious activity across both domains to ensure adversaries are detected early with very few places to hide.

THE SOLUTION

Effective cybersecurity starts with visibility across all systems and networks. The Dragos Platform is designed for industrial networks and enhances visibility of OT environments by providing complete asset discovery and threat detection, vulnerability management as well as enabling effective incident response. This in-depth context rich ICS/OT asset visibility analyzes multiple data sources including protocols, network traffic, asset characterizations, and anomalies to enable unmatched visibility of your ICS/OT environment.

Additionally, Dragos WorldView Threat Intelligence provides visibility of emerging, global, industrial threat activity that is shared via contextual reports and IOC's. Reducing alert fatigue, the Dragos Platform rapidly pinpoints malicious behavior on your ICS/OT network, providing in-depth context of alerts, and reduces false positives for unparalleled threat detection, giving customers the information needed to focus on the highest priority issues to mitigate risk, minimize downtime, and allocate cybersecurity resources where they are most needed.

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 Center's (SOC's) as a core component for monitoring enterprise networks.

Integrating Dragos and Splunk solutions provide security professionals with unparalleled coverage across IT and OT networks, resulting in greater situational awareness and decision making.

HOW IT WORKS

The Dragos OT Add-On can be installed and configured to connect to the Dragos Platform and ingest data into Splunk. You can then use the raw data to build queries and dashboards that provide value for your organization.

In order to take full advantage of Splunk's OT capabilities, install both Splunk Enterprise Security and the OT Security Add-on for Splunk. You can then follow the SOT Security Add-on for Splunk and Dragos OT Add-On configuration instructions to get access Dragos data inside these additional applications. This provides integration with Splunk's Asset Framework, advanced pre-built dashboards, and security alerting. This improved visibility, detection, and response capability gives security teams a blended IT/OT view allowing teams to appropriately prioritize analysis and response activities.

Dragos OT Add-On for Splunk

The Dragos OT Add-On bridges the IT/OT divide by bringing OT cybersecurity data from the Dragos Platform into Splunk Enterprise Security. This integration brings a set of Dragos Platform capabilities into Splunk, enhancing visibility of OT environments by providing complete asset discovery, threat detection, and vulnerability management as well as enabling effective incident response. This provides users with in-depth and context rich ICS/OT asset visibility that analyzes multiple data sources including protocols, network traffic, asset characterizations, and anomalies to provide unmatched visibility of your ICS/OT environment.

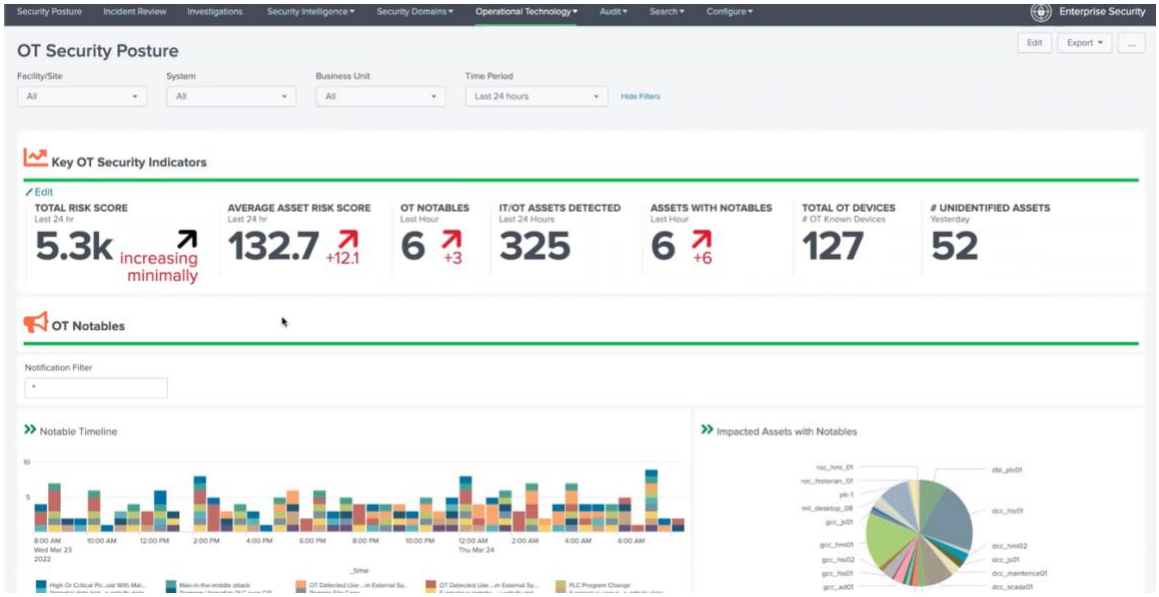

Figure. OT Security Indicators Dashboard in Splunk Enterprise Security using the Dragos OT Add-On

Improving OT Asset Visibility with Splunk

Once The Dragos Platform is installed into your OT network your SOC will have visibility into the industrial assets on the network (PLC's, HMI's, DCS, SCADA systems, etc.). The Dragos Platform's asset inventory and visibility capabilities provide the industry's most comprehensive and in-depth understanding of ICS environments, that includes comprehensive inventory of assets, devices, and details leading to faster triage of incidents through timeline analysis allowing Splunk users to group assets by zone to identify unexpected traffic.

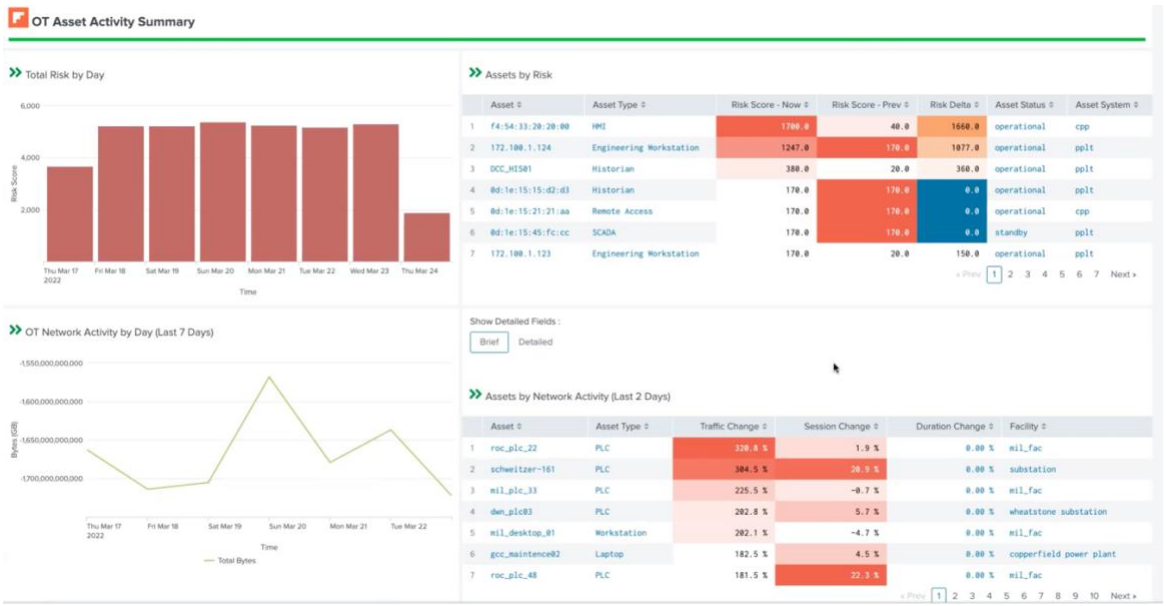

Figure. OT Asset Dashboard in Splunk Enterprise Security using the Dragos OT Add-On

Enhancing ICS Threat Detection with Splunk

Once Splunk users have accessed OT asset inventory and visibility, the Dragos Platform provides proactive anomaly & threat detection, and threat response & recovery capabilities. Notifications from the Dragos Platform are shared with Splunk where they can be categorized by their associated detection type and severity allowing focused prioritization on what's most important.

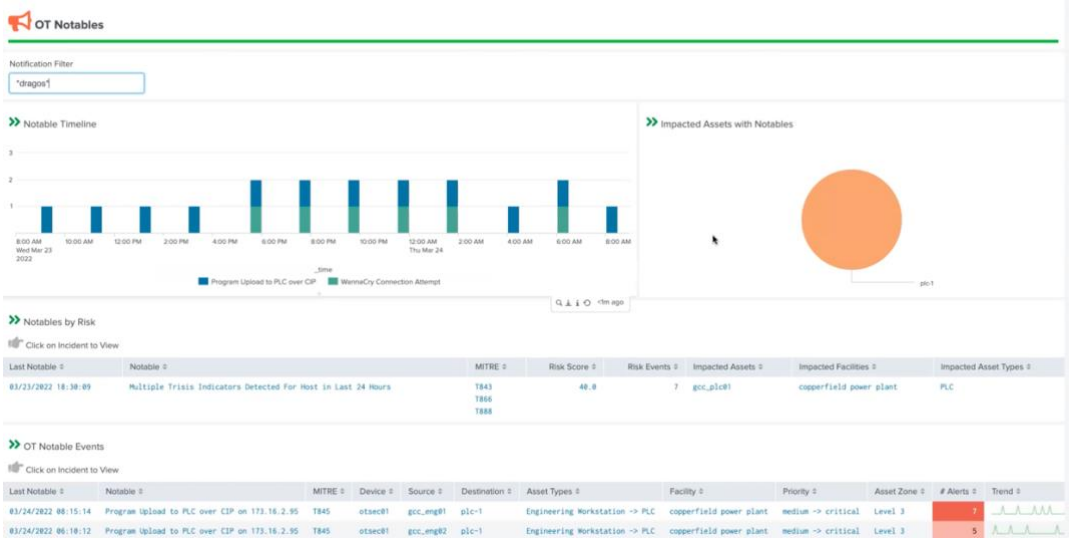

Figure. Searching OT Notable Events using the Dragos OT Add-On

Enable Threat Intelligence with Splunk

Provide an easy and automated way of visualizing OT-focused threat intelligence Indicators of Compromise (IOCs) from The Dragos Platform directly in Splunk to automate and give the ability to detect across existing data collection. This enables defenders to easily detect known malicious activities in network traffic, domains, and applications.

Note: All of the above capabilities require an active deployment of the Dragos Platform. Threat Intelligence capabilities require an active Dragos Worldview Threat Intelligence subscription.

ADVANTAGES OF THE INTEGRATED SPLUNK AND DRAGOS SOLUTIONS INCLUDE:

- Greater flexibility for Splunk users to incorporate OT data from the Dragos technology into workflows.
- Leverage the power of the industrial threat detection provided by the Dragos Platform within your existing security operations.
- Perform more thorough investigations and root cause analysis across IT and OT to reduce mean time to detection & recovery.
- Easily utilize Dragos Worldview Threat Intelligence Feed to search across Splunk environments.
- Spans the needs of security professionals for both IT and OT networks for improved situational awareness and decision-making.

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