UTILIZING IT AND OT DATA FOR COMPLETE THREAT DETECTION

Technologies Combine for Improved Visibility and Response

HIGHLIGHTS

- Technology integrations eliminates potential cybersecurity blind spots in the combined IT and OT environments.
- Combined technology improves OT awareness and response to OT threats by leveraging increased visibility
- Dragos Threat Intelligence App for Splunk simplifies access to threat Indicator's Of Compromise (IOC's) from Dragos Worldview subsciptions
- Dragos Threat Detection App for Splunk provides better correlation of detected OT threats from Dragos Platform alongside IT threats
- Dragos Add-On for Splunk provides flexibility in searching and visualizing data from Dragos solutions for improved situational awareness and decision making.

OVERVIEW

As Operational Technology (OT) networks converge with Information Technology (IT) networks, its becoming essential that security operations teams have complete visibitliy and correlation across both domains for effective threat detection and incident response. Technology integrations between Splunk and Dragos serve the purpose of improving visibility and process efficiencies to enable a more robust Security Operations Center (SOC).

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 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. Its 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 security starts with visibility across all systems and networks. The Dragos Platfom is designed for industrial networks and enhances visibility of OT environments by providing complete asset discovery and threat detection as well as enabling effective incident response. Additionally Dragos WorldView Threat Intelligence provides visibiity of emerging, global, industrial threat activity that is shared via contextual reports and IOC's.

Splunk technology 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.

Combining Dragos and Splunk solutions via integrations and apps provides security professionals with unparalleled coverage across IT and OT networks resulting in greater situational awareness.

HOW IT WORKS

Dragos has developed two Apps and an Add-on for Splunk to simplify Integration between the different technologies that enable great coverage and more produtivity within security operations. The Splunk Apps and Add-on, working in conjunction with the Dragos Platform & Dragos WorldView, provides defenders with the necessary tools to quickly prioritize, investigate, and respond to threats which can also help compliance requirements across both IT and OT environments.

Dragos Threat Intelligence App for Splunk provides an easy and automated way of utilizing OT-focused threat intelligence IOC's from Dragos directly into Splunk to automate detection across existing data collection. This app also provides easy visualization of IOC's via pre defined Splunk. Note - This app does requires an active Dragos Worldview subscription.

Figure 1: Dragos Threat Intelligence App Dashboard

Dragos ICS Threat Detection App for Splunk integrates the Dragos Platform technology for Industrial Control Systems (ICS) security with Splunk. The Dragos Platform provides passive ICS network monitoring, which produces improved asset identification & mapping, proactive anomaly & threat behavior detection, and threat response & recovery capabilities. It offers 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. Note - This app does requires an active Dragos Platform deployment.

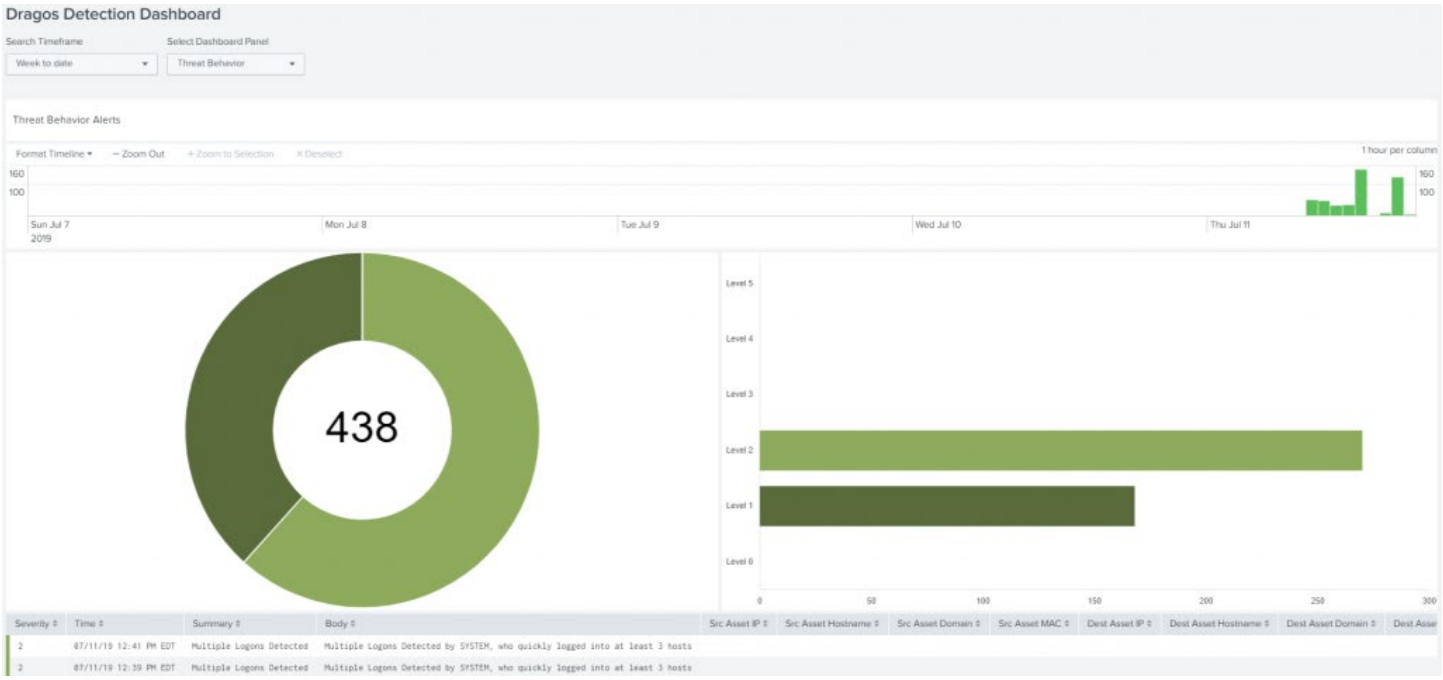

Figure 2: Dragos ICS Threat Detection App Dashboard

Dragos Add-on for Splunk provides the necessary logic for users to easily utilize data from Dragos Platform or Dragos WorldView so they are available in Splunk as a key value store or index. Splunk users can craft custom queries themselves or leverage the Dragos App's. This expands the ICS cybersecurity ecosystem to ensure critical infrastructure and industrial organizations are equipped with enhanced threat visibility and better analytics, resulting in more thorough protection of their OT environments - regardless of where an adversary may attack. It enables more effective SOC functions - more effective threat hunts, the ability to resolve incidents more quickly - for organizations concerned about ICS cybersecurity.

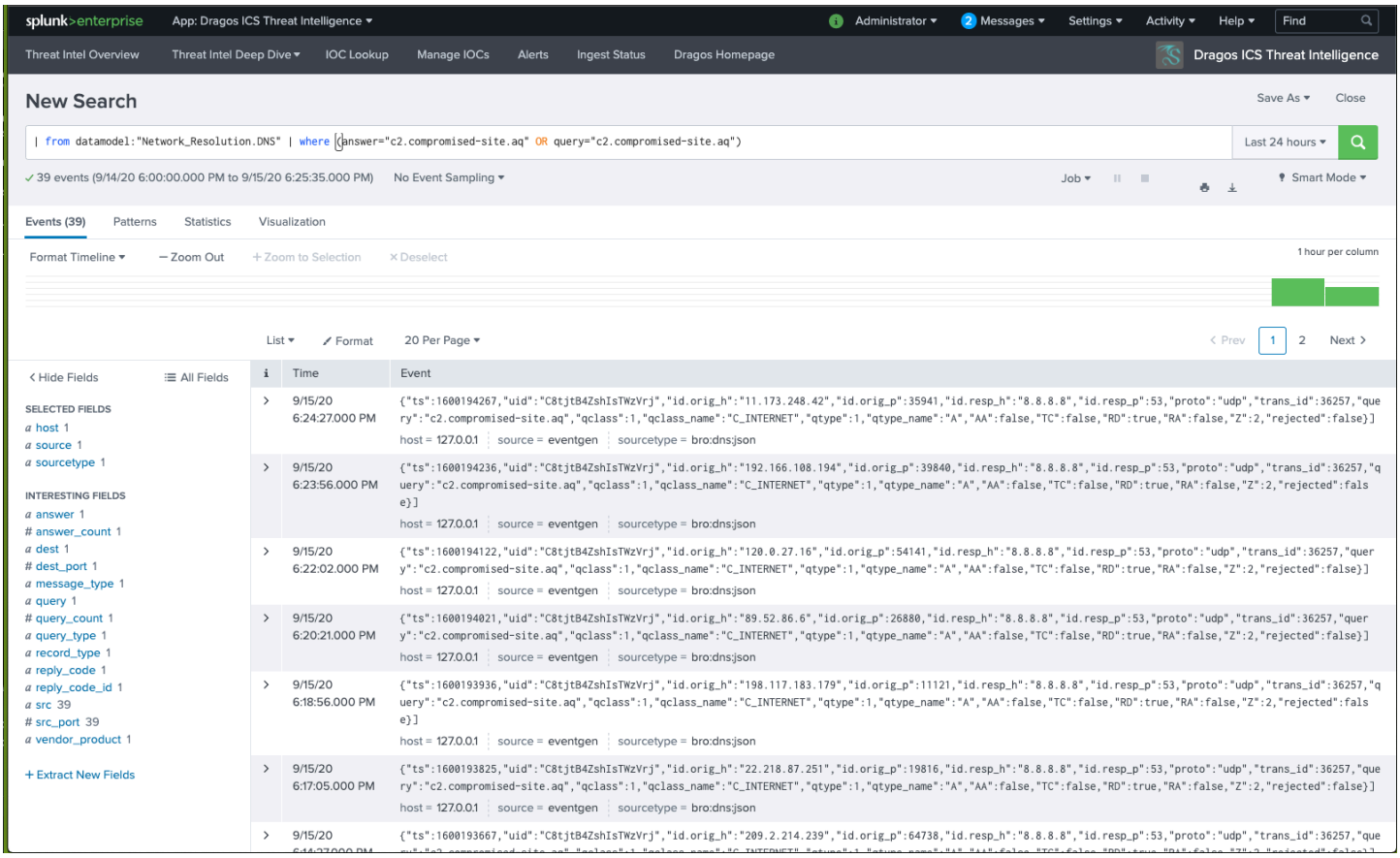

Figure 3. Searching Splunk Using the Dragos Add-On

ADVANTAGES OF THE JOINT SPLUNK AND DRAGOS SOLUTION INCLUDE:

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

Access to the Dragos Splunk Apps are available in the SplunkBase at:

- **Dragos Threat Intelligence App for Splunk - https://splunkbase.splunk.com/app/5232/**
- **Dragos ICS Threat Detection App for Splunk - https://splunkbase.splunk.com/app/4601/**
- **Dragos Add-on for Splunk - https://splunkbase.splunk.com/app/5231/**

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