INCREASED VISIBILITY OF OT THREATS

LogRhythm SIEM and Dragos Platform Combine for IT and OT Cybersecurity

HIGHLIGHTS

- Increases the value and performance of existing LogRhythm SIEM deployments by adding OT threat detection.
- Eliminates potential cybersecurity blind spots in converging IT and OT environments.
- Faster awareness and response to threats from adversaries by leveraging the increased visibility.
- The integration provides data connectors and graphical dashboards for ease of deployment.

OVERVIEW

Identification, Detection, and Response are a few of the critical components to a successful cybersecurity strategy. Dragos and LogRhythm are working together to improve these components for defenders to help protect against sophisticated attacks that impact both the information technology (IT) and operational technology (OT) environments.

THE CHALLENGE

Security teams at industrial organizations often have limited visibility into OT networks. Not just from an asset identification aspect but also the ability to detect Industrial Control System (ICS) focused threats. IT security tools are not optimized for OT environments and are based upon different technologies, protocols, policies, and skills, with unique consequences that require different approaches. There is an increasing demand for security teams to have a broader converged view that provides more holistic coverage of the entire network, including IT and OT. This demands that security teams face the challenge of supporting unfamiliar technology, systems, and threats while maintaining efficient workflows. The potential risk to businesses is magnified as ICS threats are increasing in frequency and sophistication with potentially significant consequences. The need to provide analysts with improved, complete situational awareness and decision-making support as efficiently as possible is critical.

THE SOLUTION

Effective security starts with visibility across all systems and networks. SIEM solutions are a core foundational component of effective security operations. LogRhythm's NextGen SIEM, working in conjunction with the Dragos Platform, provides defenders with the necessary details to quickly prioritize, investigate, and respond to threats and help compliance requirements across both IT and OT environments. The Dragos Platform is designed to provide asset visibility, Threat Detection, and Incident Response functions specifically for industrial environments. Through the technology integration, all notifications from the Dragos Platform can be sent to LogRhythm SIEM to enable security operations staff the necessary information to centralize potential detected threat activity.

HOW IT WORKS

The Dragos Platform is an ICS cybersecurity solution that provides defenders with unprecedented knowledge and understanding of their industrial assets and activity concerning threats, and especially threat behaviors, as well as providing the information and tools to respond. Unlike anomaly-based threat detection methods, the Dragos Platform also leverages threat behavior analytics as to the primary method of threat detection. They provide more context-rich insight into the threats, which reduces the meantime to recovery (MTTR). Threat behavior Analytics are characterizations of known adversary tactics, techniques, and procedures (TTPs) that rapidly pinpoint malicious behavior with a higher degree of confidence. Providing defenders with context-rich alerts and notifications is accompanied by investigation playbooks to help guide ICS cybersecurity practitioners with the steps to respond to threats efficiently. Dragos threat detections and playbooks are produced by the experienced Dragos team and are continuously updated to further enrich the Dragos Platform via Knowledge Packs. Combining technology and shared experience provides customers with a more scalable, efficient, and effective security operations team.

Via a technology integration with Dragos Platform, LogRhythm SIEM receives events and notifications observed from the OT network and displays it such that SOC analysts can then make informed decisions when investigating potential OT threats. This further decreases the gap between IT and OT visibility by collecting and visualizing data more consistently for enterprise SOC analysts. Event notifications are transferred from the Dragos Platform via SYSLOG using the Common Event Format (CEF). For more detail, refer to the Dragos User Guide for LogRhythm.

Since analysts and other security professionals often need to further aggregate all their detection technology into one view for efficiency and speed of response, the overall goal is to help get the right information to the right person at the right time to make the best decisions possible for the business.

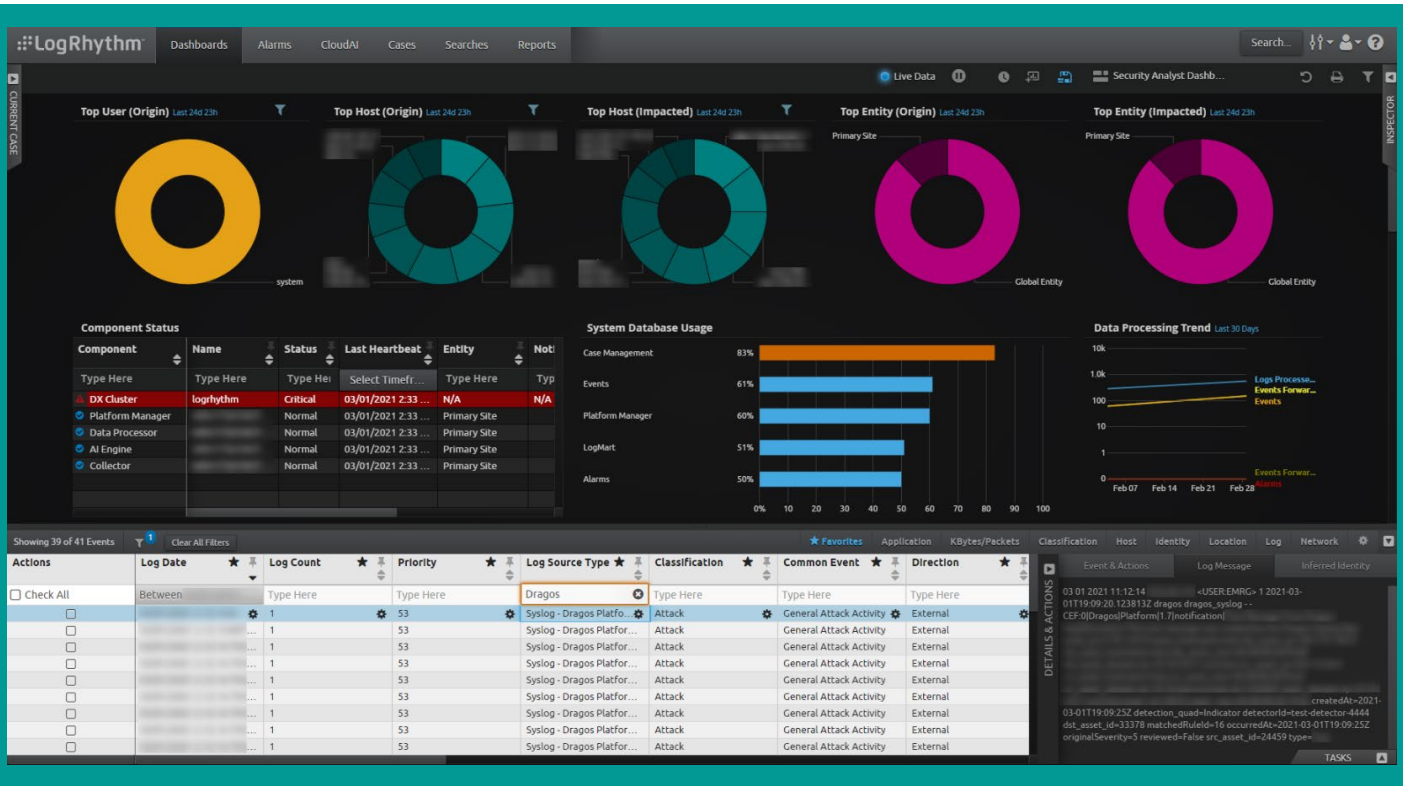

Figure 1 Dragos Platform Data represented in a LogRhythm SIEM dashboard

ADVANTAGES OF THE JOINT LOGRHYTHM AND DRAGOS SOLUTION INCLUDE:

- Seamless integration between the two technologies improves SOC efficiency for IT and OT.
- The Dragos Platform is continuously updated with new detection and response content through intelligence-driven Knowledge Packs.
- Spans the needs of analysts for both IT and OT networks for improved situational awareness and decision making.
- Reduces Mean Time To Detection (MTTD) of threats.
- Improves understanding and the ability to react to IT adversaries that often pivot from enterprise networks to OT.

Joint customers can access the new integration within LogRhythm today via the LogRhythm web console.

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