DRAGOS AND LOGRHYTHM

OT and IT Cybersecurity Combined for More Complete Threat Detection

HIGHLIGHTS

- Dragos and LogRhythm bring years of IT and OT security experience for those pursuing greater convergence of IT and OT networks.
- Technology integration between LogRhythm SIEM and Dragos Platform provides enhanced visibility of OT threat activity.
- Security teams can maximize the value of their technology investments through integration that enables comprehensive coverage of both IT and OT

THE CHALLENGE

Security executives at industrial organizations, including Chief Information Security Officers (CISO's), are often challenged to provide resources (both technology and personnel) across the entire Information Technology (IT) and Operation Technology (OT) environment. Enterprise security tools that provide analysts with visibility into the IT networks are fairly commonplace but offer limited capabilities for asset and threat identification for Industrial Control Systems (ICS). Since security teams are now required to have a broader converged view of the entire IT, (Industrial Internet of Things) IIoT, and OT networks, there is a need for technology that works together to help bridge the gap. The risk to the business is evident as the industrial threat landscape is prevalent and significant, and the need to provide security professionals with complete situational awareness and decision-making support is critical.

Often owners and operators of ICS across various industries lack visibility into the OT environment for effective threat detection. Additionally, It Is beneficial for security teams to have a thorough understanding of the sophisticated adversaries that are actively targeting both the IT and OT networks, which could lead to the disruption of systems leading to physical damage and loss of life. This puts increased pressure on the various stakeholders such as leadership, engineering, security specialists, vendors, etc., to ensure readiness with sufficient hardening, detection, and response mechanisms to neutralize the threat and reduce overall business risk.

Furthermore, a diverse ecosystem of different and complex technologies can add to inefficient business processes. Selecting the right partners and tools can have significant benefits down the road because technology deployments in OT environments have long lifecycles.

THE SOLUTION

LogRhythm NextGen SIEM is a popular technology deployed amongst many SOC teams that is used to aggregate and analyze threat activity across enterprise IT networks.

By leveraging the combined LogRhythm NextGen SIEM and Dragos Platform technology, customers benefit from integrated monitoring capability for both IT and OT environments.

While the LogRhythm SIEM infrastructure provides analysts with better visibility of enterprise IT, the combined visibility with Dragos OT threat detection capabilities delivers strong awareness

capabilities. LogRhythm and Dragos offer the right tools for the right environment for the most efficient response.

Protecting critical infrastructure requires a comprehensive approach – not a single vendor or product. To provide a complete solution, multiple technologies must operate together without introducing complexity, adversely impacting safety or availability, while helping security teams achieve their goals. Obtaining visibility of events across the enterprise (IT) and ICS (OT) network is essential to operational security and compliance. Understanding and enabling defenders with the ability to react to adversaries that often pivot from enterprise networks to OT is important.

There are a wide variety of technologies and protocols across the enterprise (IT) and ICS (OT) networks. Native support for these systems and their associated communications is a critical way to enable effective situational awareness and multi-zone protection. The Dragos Platform passively monitors ICS protocols across the network as well as logs and events collected from ICS devices. The Platform integration with LogRhythm NextGen SIEM gives defenders the ability to harness the power of real-time visibility and centralized management through a single platform. The Dragos and LogRhythm combination will focus on supporting some of the primary needs of critical infrastructure environments; cybersecurity protection without impacting operational safety or availability, situational awareness for improved decision-making abilities, and multi-zone protection support for assistance in continuous cybersecurity compliance.

BENEFITS AND IMPACTS

BENEFITS	IMPACTS
Enhanced Visibility of IT and OT Networks	Combining LogRhythm NextGen SIEM and the Dragos Platform ensures more effective asset visibility, threat detection, and response in both the IT and OT domains.
Intelligence-Driven Threat Detections	Utilizing comprehensive IT and OT threat intelligence as the primary method of detecting threats, which improves detection confidence and reduces alert fatigue.
More Efficient Security Operations	Integrating the technologies enables defenders with a more comprehensive workflow from initial threat detection through response, improving Mean Time To Recovery (MTTR).

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