DRAGOS AND IBM SECURITY

OT and IT Cybersecurity Combined for More Complete Threat Detection

HIGHLIGHTS

- Dragos QRadar® Device Support Module (DSM) provides enhanced visibility of OT assets into the IBM QRadar Security Information and Event Management (SIEM).
- Threat intelligence sharing between Dragos OT cybersecurity experts and IBM® Security's X-Force Team provides increased threat awareness to the greater community.
- The combined technical integration and threat intelligence sharing means better information to make informed decision.
- Maximize the value, investment, and visibility by integrating technologies optimized for both IT and OT security environments.
- Through the integration of the two offerings, analysts have improved workflow and efficiency of the security operations.

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 capability 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. Likewise, there is a gap in the Threat Intelligence information available to most Enterprise Security Operations Centers (SOC). 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

IBM Security has established itself as a decades-long leader in cyber detection and combining them with Dragos reduces the number of steps required for IT and OT threat detection and response.

Leveraging the combined IBM Security QRadar and Dragos Platform technology, customers benefit from integrated monitoring capability for IT and OT environments.

While the IBM Security infrastructure provides analysts with better visibility of enterprise IT, the combined visibility with Dragos OT threat detection capabilities delivers strong awareness capabilities. IBM Security and Dragos provide the right tools for the right environment for the most efficient response.

IBM Security's X-Force threat intelligence team, combined with Dragos Threat Intelligence research, provides the basis for a fully integrated solution that delivers a unique combination of Enterprise IT and OT awareness.

Protecting critical infrastructure requires a comprehensive approach — not a single vendor or product. In order 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 IBM Security's QRadar gives defenders the ability to harness the power of real-time visibility and centralized management through a single platform. The Dragos and IBM Security 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
Combined Domain Experience Partner	Leverages the industrial and enterprise cybersecurity expertise from Dragos and IBM Security to help uncover threats and improve overall security posture.
Enhanced Visibility of IT and OT Networks	Combining IBM QRadar 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