SOLUTION BRIEF

INCREASED VISIBILITY OF OT THREATS VIA TECHNOLOGY INTEGRATION

QRadar and Dragos Platform Combine for IT and OT Cybersecurity

HIGHLIGHTS

- Increases the value and performance of existing QRadar 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 IBM Security 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 threats to ICS 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. IBM Security's QRadar® solution, working in conjunction with the Dragos Platform, provides defenders with the necessary 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 QRadar to enable security operations staff the necessary information to centralize potential detected threat activity.

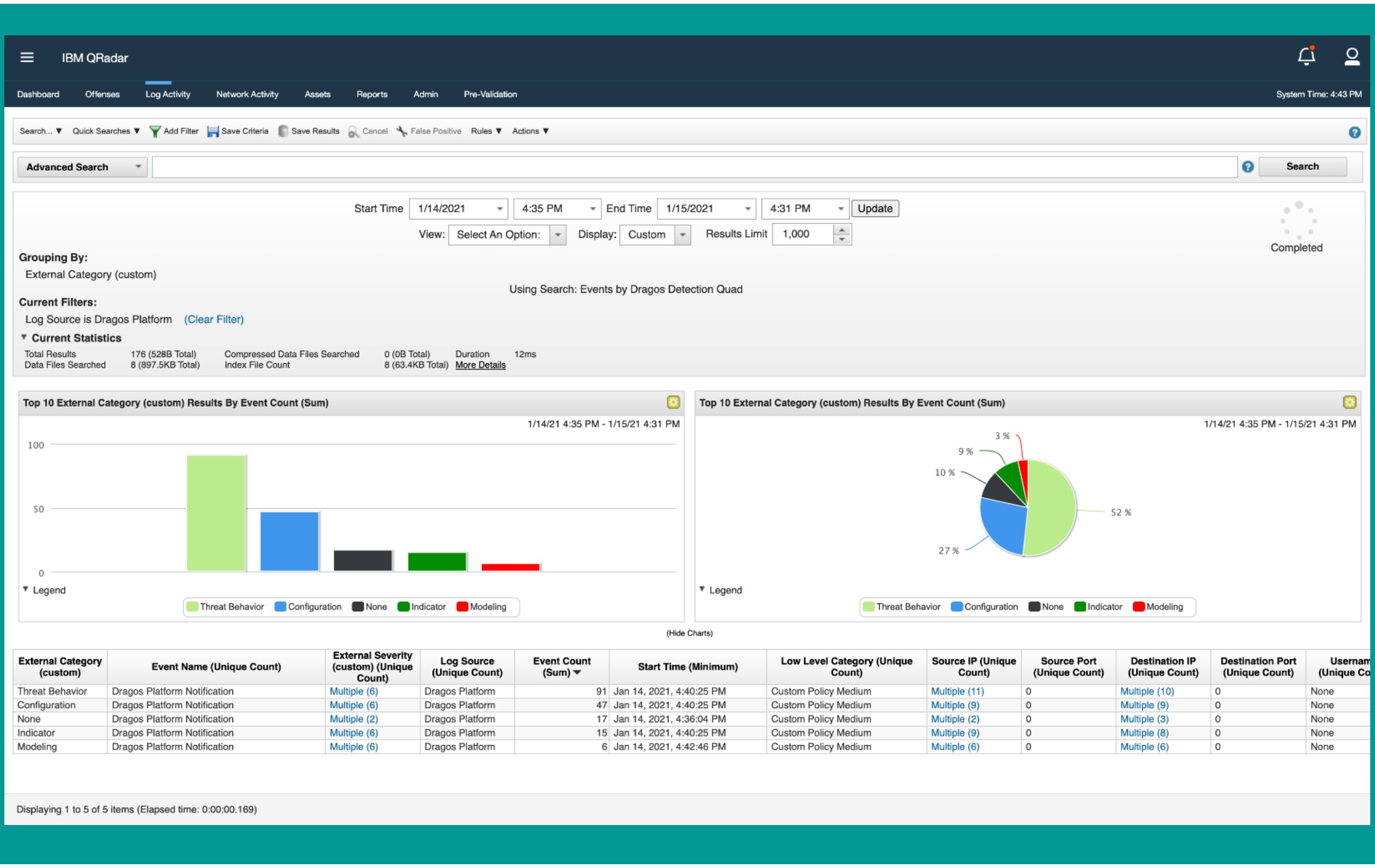
HOW IT WORKS

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 the primary method of threat detection as they provide more context-rich insight of 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, which are 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. The combination of technology and shared experience provide customers with a more scalable, efficient, and effective security operations team.

The QRadar integration with Dragos Platform receives data coming from the OT network and displays it such that enterprise SOC analysts can use it to make informed decisions when investigating potential OT threats. This further decreases the gap between IT and OT visibility by collecting and visualizing data in a more consitent manner for enterprise SOC analysts. Event notifications are transferred from the Dragos Platform via SYSLOG using the Log Event Extended Format (LEEF). For more detail refer to the Dragos User Guide for QRadar.

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 as the right time to make the best decisions possible for the business.

The image in Figure 1 below depicts how notifications from the Dragos Platform can be displayed within QRadar and subsequently leveraged by a security analyst to investigate and understand threats targeting OT environments.



System Time: 4:43 PM

Start Time 1/14/2021 4:35 PM End Time 1/15/2021 4:31 PM

View: Select An Option: Display: Custom Results Limit 1,000

Grouping By:
External Category (custom)

Using Search: Events by Dragos Detection Quad

Current Filters:
Log Source is Dragos Platform (Clear Filter)

▼ **Current Statistics**

Total Results	176 (528B Total)	Compressed Data Files Searched	0 (0B Total)	Duration	12ms
Data Files Searched	8 (897.5KB Total)	Index File Count	8 (63.4KB Total)	More Details	

Top 10 External Category (custom) Results By Event Count (Sum)

1/14/21 4:35 PM - 1/15/21 4:31 PM

Top 10 External Category (custom) Results By Event Count (Sum)

1/14/21 4:35 PM - 1/15/21 4:31 PM

External Category (custom)	Event Name (Unique Count)	External Severity (custom) (Unique Count)	Log Source (Unique Count)	Event Count (Sum) ▼	Start Time (Minimum)	Low Level Category (Unique Count)	Source IP (Unique Count)	Source Port (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Usernam (Unique Co
Threat Behavior	Dragos Platform Notification	Multiple (6)	Dragos Platform	91	Jan 14, 2021, 4:40:25 PM	Custom Policy Medium	Multiple (11)	0	Multiple (10)	0	None
Configuration	Dragos Platform Notification	Multiple (6)	Dragos Platform	47	Jan 14, 2021, 4:40:25 PM	Custom Policy Medium	Multiple (9)	0	Multiple (9)	0	None
None	Dragos Platform Notification	Multiple (2)	Dragos Platform	17	Jan 14, 2021, 4:36:04 PM	Custom Policy Medium	Multiple (2)	0	Multiple (3)	0	None
Indicator	Dragos Platform Notification	Multiple (6)	Dragos Platform	15	Jan 14, 2021, 4:40:25 PM	Custom Policy Medium	Multiple (9)	0	Multiple (8)	0	None
Modeling	Dragos Platform Notification	Multiple (6)	Dragos Platform	6	Jan 14, 2021, 4:42:46 PM	Custom Policy Medium	Multiple (6)	0	Multiple (6)	0	None

Displaying 1 to 5 of 5 items (Elapsed time: 0:00:00.169)

Figure 1 Dragos Platform Data represneted in a QRadar dashboard

ADVANTAGES OF THE JOINT QRADAR AND DRAGOS SOLUTION INCLUDE:

- Seamless integration between the two technologies improves SOC efficiency.
- 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.

IBM QRadar customers can download the Dragos Platform Extension for QRadar from the IBM App Exchange at: https://exchange.xforce.ibmcloud.com/hub/extension/e049f59aa88dd568d3b96c41ce85d1b9

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