SOLUTION BRIEF

IMPROVING THREAT DETECTION IN INDUSTRIAL NETWORKS

Technologies Combine for IT and OT Cybersecurity

HIGHLIGHTS

- Better monitoring and threat detection capabilities of the OT environments.
- Combining the technologies broadens the security operations coverage and understanding of OT focused threats.
- Increased efficiency for the security analysts through better coverage of the entire IT and OT environment.
- Faster awareness and response to threats from adversaries.

OVERVIEW

Identification, Detection, and Response are a few of the critical components to a successful cybersecurity strategy. Dragos and McAfee 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 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. Security Information and Event Management (SIEM) solutions are a core foundational component of effective security operations. McAfee® Enterprise Security Manager, the core of the McAfee SIEM solution, working in conjunction with the Dragos Platform, provides defenders with the necessary visibility and detection/response capabilities 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 the McAfee SIEM to enable security operations staff the necessary information to centralize potential detected threat activity.

The Dragos Platform detects and displays ICS threats in four different ways, which are then displayed locally on the four types of detection dashboard, but also shared with McAfee SIEM where initial response teams can perform validation and then triage the notification.

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, and also 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 image in Figure 1 depicts a sample architecture on how the Dragos Platform and the McAfee Enterprise Security Manager can integrate to help protect IT and OT systems.

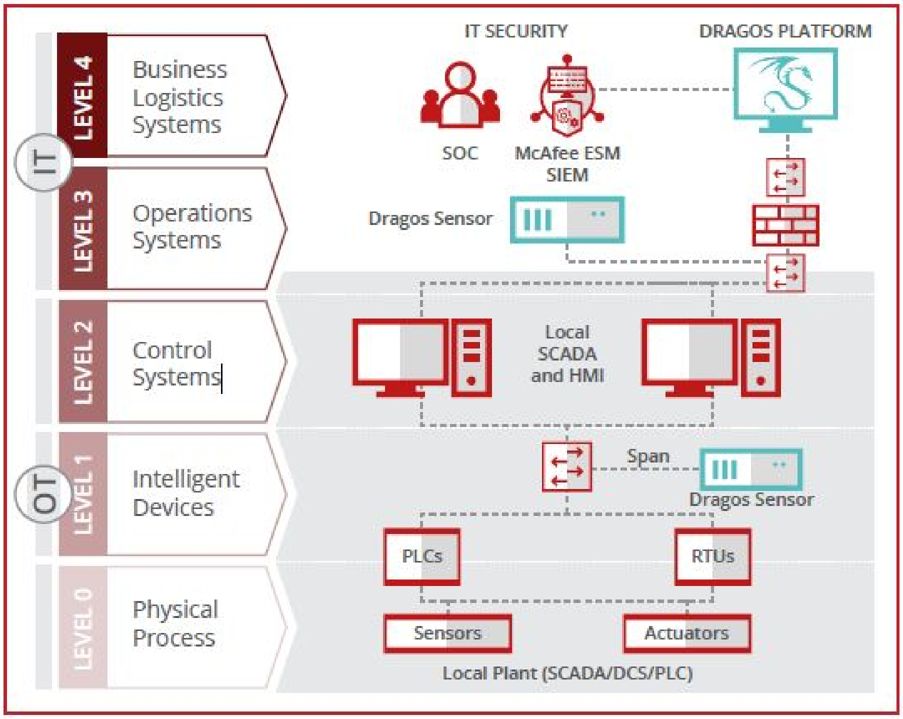
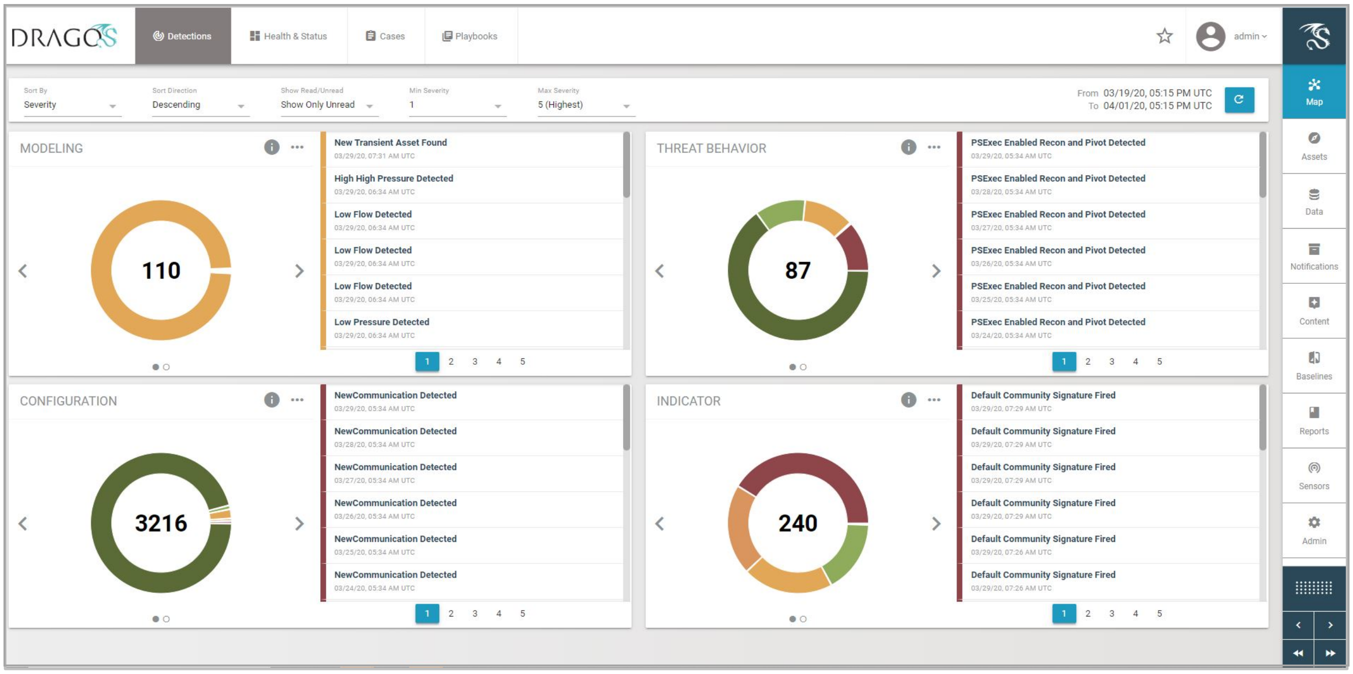


Figure 1. Example of an architecture combining Dragos Platform and the McAfee Enterprise Security Manager in an industrial control environment.

Since analysts and other security professionals often need to further aggregate all of 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 McAfee IT-based detection indicators and Dragos OT level detections form a technology combination and complete solution. The joint solutions provide the needed intelligence required for the security operations team to uniformly support the requirements across both the IT and OT environments.

The image below depicts how the threat behavior analytic notifications from the Dragos Platform can be displayed within the dashboard view of the McAfee Enterprise Security Manager and subsequently leveraged by a security analyst to understand threats targeting the OT environment.



Sort By: Severity
Sort Direction: Descending
Show Read/Unread: Show Only Unread
Min Severity: 1
Max Severity: 5 (Highest)
From 03/19/20, 05:15 PM UTC
To 04/01/20, 05:15 PM UTC

MODELING

New Transient Asset Found
03/29/20, 07:31 AM UTC
High High Pressure Detected
03/29/20, 06:34 AM UTC
Low Flow Detected
03/29/20, 06:34 AM UTC
Low Flow Detected
03/29/20, 06:34 AM UTC
Low Flow Detected
03/29/20, 06:34 AM UTC
Low Pressure Detected
03/29/20, 06:34 AM UTC

THREAT BEHAVIOR

PSExec Enabled Recon and Pivot Detected
03/29/20, 05:34 AM UTC
PSExec Enabled Recon and Pivot Detected
03/28/20, 05:34 AM UTC
PSExec Enabled Recon and Pivot Detected
03/27/20, 05:34 AM UTC
PSExec Enabled Recon and Pivot Detected
03/26/20, 05:34 AM UTC
PSExec Enabled Recon and Pivot Detected
03/25/20, 05:34 AM UTC
PSExec Enabled Recon and Pivot Detected
03/24/20, 05:34 AM UTC

CONFIGURATION

NewCommunication Detected
03/29/20, 05:34 AM UTC
NewCommunication Detected
03/28/20, 05:34 AM UTC
NewCommunication Detected
03/27/20, 05:34 AM UTC
NewCommunication Detected
03/26/20, 05:34 AM UTC
NewCommunication Detected
03/25/20, 05:34 AM UTC
NewCommunication Detected
03/24/20, 05:34 AM UTC

INDICATOR

Default Community Signature Fired
03/29/20, 07:29 AM UTC
Default Community Signature Fired
03/29/20, 07:29 AM UTC
Default Community Signature Fired
03/29/20, 07:29 AM UTC
Default Community Signature Fired
03/29/20, 07:29 AM UTC
Default Community Signature Fired
03/29/20, 07:26 AM UTC
Default Community Signature Fired
03/29/20, 07:26 AM UTC

Figure 2. How threat notifications and alerts are displayed.

Advantages of the joint McAfee and Dragos solution include:

- 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 complete situational awareness and decision-making.
- Reduces mean time to detection of threats and the ability to react.
- Improves understanding and the ability to react to IT adversaries that often pivot from enterprise networks to OT.

Access to the McAfee SIEM Rules, that includes the Dragos Data Source Type, is available via electric download, with your Grant Number, at: https://www.mcafee.com/enterprise/en-us/downloads/my-products.html

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