INTEGRATED TECHNOLOGY FROM DRAGOS AND FORTINET

Technologies Combine for IT and OT Cybersecurity

HIGHLIGHTS

- Increases the value and performance of the user's existing SIEM and firewall deployments by adding OT threat detections.
- Improved asset visibility from the Dragos Platform to optimize Fortinet deployments .
- Combining the Fortinet and Dragos technologies brings increased visibility of OT focused threats to the enterprise.
- Reduces potential cybersecurity blind spots across IT and OT environments.
- Faster awareness and response to threats from adversaries by leveraging the increased visibility.

OVERVIEW

Identification, Detection, and Response are a few of the critical components to a successful cybersecurity strategy. Dragos and Fortinet 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, and the capability to manage network traffic between those systems. SIEM tools like Fortinet's FortiSIEM and firewall solutions like the FortiGate NGFW are core foundational components of effective security operations. As a complement to these, the Dragos Platform is designed to provide asset visibility, threat detection, vulnerability management, and incident response functions specifically for industrial environments.

Visibility of assets and potential threats in OT environments are often not available to Enterprise or IT tools because of network isolation, unique protocols, and distinct operating conditions of the different environments.

The FortiSIEM solution, working in conjunction with the Dragos Platform, provides defenders with the necessary capability to quickly prioritize, investigate, and respond to threats and help compliance requirements across both IT and OT environments. Through the technology integration, notifications from the Dragos Platform can be sent to FortiSIEM to enable security operations staff the necessary information to centralize potential detected threat activity.

When it comes to asset visibility, the Dragos Platform is able to generate and populate asset sync profiles that are sent to FortiGate for inclusion in address groups where firewall administrators are able to apply appropriate policies for traffic management. Likewise for threat detections, notifications in the Dragos Platform can generate response actions based on configurable rules that populate address groups in FortiGate.

HOW IT WORKS

The Dragos Platform is an ICS/OT 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 into the threats, which reduces the mean time 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.

USE CASE: More Informed Firewall Policies (NGFW)

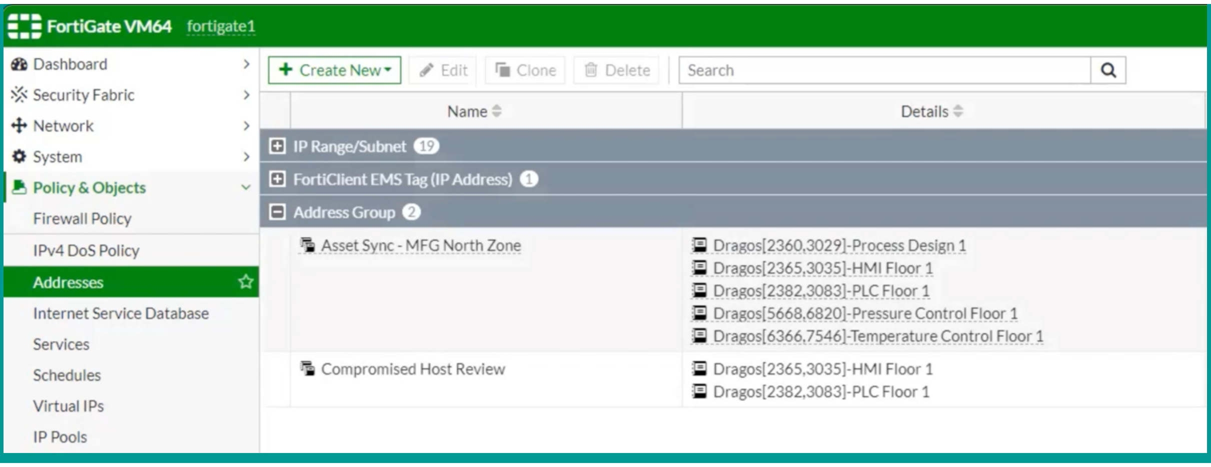
One of the fundamental challenges industrial asset owners face is having a complete and accurate inventory of their connected devices. For companies looking to maximize the visibility of assets and threat detection in their OT environment, the Dragos Platform integration with FortiGate enables significantly improved decision making for firewall administrators.

The Dragos Platform helps address this by building a continuously updated asset list by analyzing network traffic and capturing detailed asset information and communications. These assets can be grouped and managed by a variety of properties based on asset attributes like “hardware vendor” or “firmware version”, or configurable parameters like which zone the asset is associated with.

After the attributes have been configured, a list of assets matching the defined criteria is shown to the user before saving the asset sync profile. This list of assets can be exported and synchronized to address groups in FortiGate for easier management by a firewall administrator who can then apply appropriate policies. Although manual review is recommended in most situations, customers have the option of automating policy enforcement to the extent that their operations workflow allows.

When it comes to threat detection in OT networks, the Dragos Platform presents users with a list of notifications that signal potential threats requiring further investigation. These notifications trigger based on certain configurable conditions created in the Dragos rules engine. Once triggered, response actions are sent to FortiGate where the threat is either quarantined or blocked based on decisions made by the FortiGate firewall administrator, and the policy applied to any asset groups as updated by the Dragos Platform. Examples of both the "asset sync" and "threat response" address group types are shown in Figure 1.

Figure 1. FortiGate address groups populated by the Dragos Platform.



Name	Details
IP Range/Subnet 19	
FortiClient EMS Tag (IP Address) 1	
Address Group 2	
Asset Sync - MFG North Zone	Dragos[2360,3029]-Process Design 1 Dragos[2365,3035]-HMI Floor 1 Dragos[2382,3083]-PLC Floor 1 Dragos[5668,6820]-Pressure Control Floor 1 Dragos[6366,7546]-Temperature Control Floor 1
Compromised Host Review	Dragos[2365,3035]-HMI Floor 1 Dragos[2382,3083]-PLC Floor 1

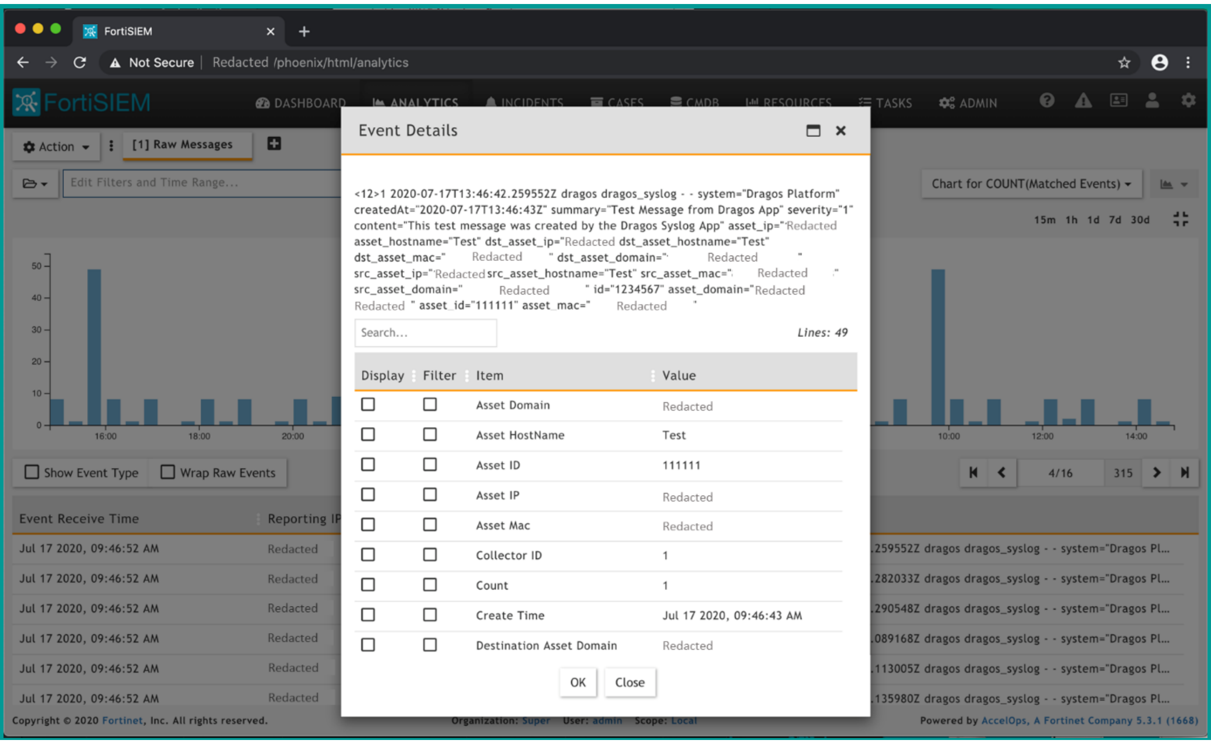
USE CASE: Improving Detection and Response (SIEM)

The FortiSIEM integration with the Dragos Platform receives data coming from the OT network and presents it in a way that the enterprise SOC analysts can use to make informed decisions when evaluating potential threats. It decreases the gap between IT and OT by collecting and visualizing data in a manner familiar with your enterprise SOC analysts.

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 at the right time to make the best decisions possible for the business. FortiSIEM fed with Dragos OT-level detections form a uniquely integrated technology combination. The joint solution provides the needed visibility required for the security operations team to uniformly support the requirements across both the IT and OT environments.

The image below (Figure 2) depicts how the threat behavior analytic notifications from the Dragos Platform can be displayed within FortiSIEM and subsequently leveraged by a security analyst to understand threats targeting the OT environment.

Figure 2. FortiSIEM with Dragos Platform data displayed.



Event Details

```
<12>1 2020-07-17T13:46:42.259552Z dragos dragos_syslog - - system="Dragos Platform"
createdAt="2020-07-17T13:46:43Z" summary="Test Message from Dragos App" severity="1"
content="This test message was created by the Dragos Syslog App" asset_ip="Redacted
asset_hostname="Test" dst_asset_ip="Redacted dst_asset_hostname="Test"
dst_asset_mac="      Redacted      " dst_asset_domain="      Redacted      "
src_asset_ip="Redacted src_asset_hostname="Test" src_asset_mac="      Redacted      "
src_asset_domain="      Redacted      " id="1234567" asset_domain="Redacted
Redacted " asset_id="111111" asset_mac="      Redacted      "
```

Search...

Lines: 49

Display	Filter	Item	Value
□	□	Asset Domain	Redacted
□	□	Asset HostName	Test
□	□	Asset ID	111111
□	□	Asset IP	Redacted
□	□	Asset Mac	Redacted
□	□	Collector ID	1
□	□	Count	1
□	□	Create Time	Jul 17 2020, 09:46:43 AM
□	□	Destination Asset Domain	Redacted

OK Close

Event Receive Time	Reporting IP	
Jul 17 2020, 09:46:52 AM	Redacted	.259552Z dragos dragos_syslog - - system="Dragos Pl...
Jul 17 2020, 09:46:52 AM	Redacted	.282033Z dragos dragos_syslog - - system="Dragos Pl...
Jul 17 2020, 09:46:52 AM	Redacted	.290548Z dragos dragos_syslog - - system="Dragos Pl...
Jul 17 2020, 09:46:52 AM	Redacted	.089168Z dragos dragos_syslog - - system="Dragos Pl...
Jul 17 2020, 09:46:52 AM	Redacted	.113005Z dragos dragos_syslog - - system="Dragos Pl...
Jul 17 2020, 09:46:52 AM	Redacted	.135980Z dragos dragos_syslog - - system="Dragos Pl...

Copyright © 2020 Fortinet, Inc. All rights reserved. Organization: Super User: admin Scope: Local Powered by AccelOps, A Fortinet Company 5.3.1 (1668)

ADVANTAGES OF THE INTEGRATED FORTINET AND DRAGOS SOLUTIONS INCLUDE:

- Simple integration between the technologies providing seamless interoperability.
- 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 improves the ability to react quicker.
- Improves understanding and the ability to react to IT adversaries that often pivot from enterprise networks to OT.

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