SOLUTION BRIEF

FortiSIEM and the Dragos Platform Deliver Security Visibility

Increased Cybersecurity Visibility Leveraging IT/OT Convergence

Executive Summary

Identification, detection, and response are a few of the critical components to a successful cybersecurity strategy. Dragos and Fortinet are partnering to improve these components for defenders to help protect against sophisticated attacks that impact both the information technology (IT) and operational technology (OT) environments.

Challenge

Security teams at industrial organizations often have limited visibility into OT networks—not just from an asset identification perspective, 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. Security teams face increased challenges requiring support of unfamiliar technologies, systems, and threats while maintaining efficient workflows. The potential risk to businesses in the form of cyber threats to OT environments is increasing in frequency and sophistication with potentially significant consequences. The need to provide analysts with improved, complete situational awareness and decision-making support is critical.

Joint 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. The FortiSIEM solution, working in conjunction with the Dragos Platform, provides defenders with the necessary tools 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 FortiSIEM to enable security operations staff the necessary information to centralize potential detected threat activity.

The Dragos Platform is an 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 of the threats, which reduces the mean time to recovery (MTTR).

Joint Solution Components

- Fortinet FortiSIEM
- Dragos Platform

Joint Solution Benefits

- Increases the value and performance of the user's existing SIEM by adding OT threat detections
- Better identification of assets from the OT environments in the user's enterprise SIEM
- Combining the Fortinet and Dragos technologies brings increased visibility of OT focused threats to the enterprise
- Eliminates potential cybersecurity blind spots in the combined IT and OT environments
- Faster awareness and response to threats from adversaries by leveraging the increased visibility

FORTINET FABRIC-READY

Threat behavior analytics are characterizations of known adversary tactics, techniques, and procedures (TTPs) that rapidly pinpoint malicious behavior with a higher degree of confidence. They provide defenders with context-rich alerts and notifications, which are accompanied by investigation playbooks to help guide OT 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 provides customers with a more scalable, efficient, and effective security operations team.

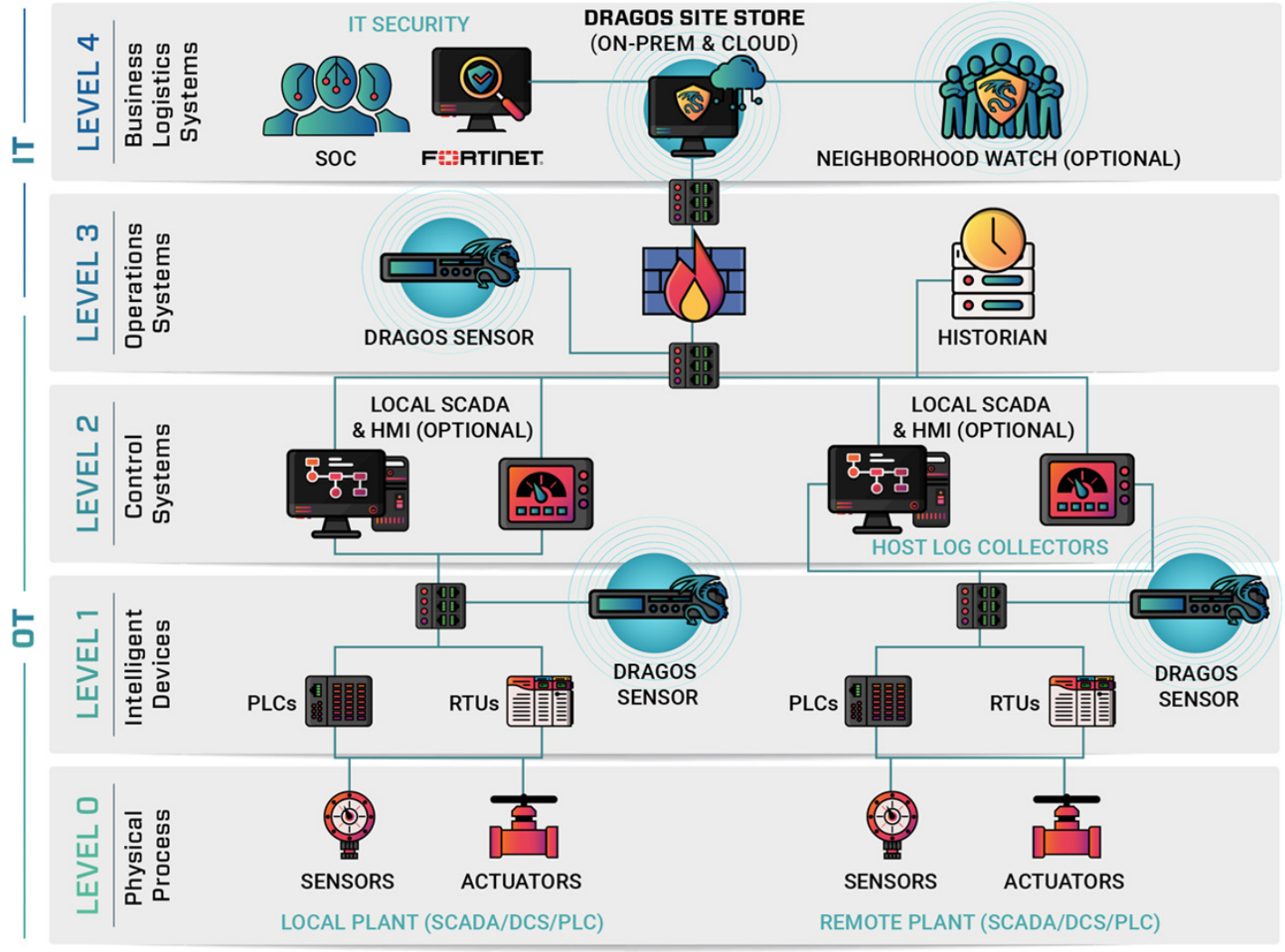

Figure 1: The Dragos platform deployment program.

The combined implementation of FortiSIEM with the Dragos Platform optimizes data coming from the OT network and presents it to security operations center (SOC) analysts, enabling them to make informed decisions and properly act on potential threats. FortiSIEM uses machine learning (ML) to detect anomolous behavior combined with advanced risk scoring to deliver refined analysis of data. Dynamic user identity mapping coupled with real-time event correlation can be used for incident migitation for an array of vendors. Dragos' addition to the Fortinet Open Fabric Ecosystem Partner Program, resulting in the application programming interface (API) integration with FortiSIEM, allows for powerful data enrichment and analysis to arm OT practitioners with precise details to make correct decisions. The combination of the FortiSIEM and the Dragos Platform decreases the gap between IT and OT by collecting and visualizing data familiar to an enterprise SOC analyst.

Advantages of the Joint FortiSIEM and Dragos Solution Include:

- Simple integration between the two technologies (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 the ability to react
- Improves understanding and the ability to react to IT adversaries that often pivot from enterprise networks to OT

About Dragos

Dragos, Inc. is an industrial cybersecurity company focused on some of the community's hardest problems. The ecosystem our team has built is specifically tailored for industrial environments such as those found in industrial control system (ICS), Supervisory Control and Data Acquisition (SCADA), and Distributed Control System (DCS) environments. Our software platform and services help operators protect infrastructure sites such as power grids, water distribution sites, oil refineries, gas pipelines, manufacturing, and more. The Dragos team exists to safeguard civilization. Learn more at https://www.dragos.com/.

May 11, 2021 5:40 AM

D:\Fortinet\2021 Rebranded templates\Solution Briefs\May\Refresh\Dragos\sb-fortisiem-and-dragos-platform-5112021\sb-fortisiem-and-dragos-platform-5112021

814452-A-0-EN