SOLUTION BRIEF

INTEGRATED TECHNOLOGY FROM DRAGOS AND CISCO

Secure and Manage Cyber Risk in Industrial Control Systems (ICS)

HIGHLIGHTS

- Improve OT asset visibility and inventory with the Dragos Platform for better Cisco Adaptive Security Appliance (ASA) firewall deployments.
- Enhance IT/OT network north-south boundaries and micro-segment OT networks to prevent unauthorized east-west communication.
- Rapidly pinpoint malicious behavior on ICS/OT networks, providing in-depth context of alerts and reducing false positives for unparalleled threat detection.
- Deliver comprehensive ICS/OT vulnerability management with corrected, enriched, and prioritized guidance.
- Enable faster threat awareness and response, to ensure uptime, resilience, and the safety of industrial assets and personnel.

OVERVIEW

Asset visibility, threat detection, prevention and response are critical components to a successful cybersecurity strategy. Dragos and Cisco are working together to improve these solutions for defenders to help protect against cybersecurity threats that impact both the information technology (IT) and operational technology (OT) environments.

THE CHALLENGE

Cybersecurity is a key component of modernization and regulatory requirements for digital transformation efforts, as cyber threats have become a major concern. Security teams at industrial organizations across the utilities and manufacturing sectors are tasked with assessing risks to their environments and adhering to audit and compliance programs. Implementing these practices comes with increasing Industrial Control System (ICS) connectivity and an expanding attack surface as companies embrace digital transformation.

Because of these challenges, there is an increasing demand for security teams to have a broader view of the entire network, including IT and OT, where they often have limited visibility into their OT networks—not just from an asset identification aspect but also from the ability to detect ICS-focused threats. The risk to these organizations is magnified as threats to ICS increase in frequency and sophistication, with potentially significant consequences. Now the need to provide analysts with improved, complete situational awareness and decision-making support as efficiently as possible is critical.

THE SOLUTION

To address these challenges and successfully secure OT environments, stakeholders from both IT and OT teams must work together to architect a “defense-in-depth” cybersecurity strategy that includes asset visibility, threat detection, and prevention technologies, ultimately enabling IT and OT professionals to improve facility operations while maintaining the availability of the network and protecting plant processes.

As a foundational complement to firewalls, the Dragos Platform, an Industrial Control System (ICS) cybersecurity technology, delivers unmatched visibility of ICS/OT assets and communications. It allows teams to rapidly pinpoint threats through intelligence-driven analytics to identify and prioritize vulnerabilities and provide best-practice playbooks to guide teams as they investigate and respond to threats before they cause significant impacts on an organization's operations, processes, or people.

Cisco's Adaptive Security Appliance (ASA) Firewalls work in conjunction with the Dragos Platform, to provide defenders with the necessary capability to quickly prioritize, investigate, and respond to threats and provide network segmentation to reduce threats from moving unchallenged through the network.

Together, this solution protects OT assets from potential threats, segments industrial networks, and builds compliance towards a variety of industrial standards, regulations, and guidelines such as NERC-CIP, ISA/IEC 62443, CFATS, and ANSI/AWWA G430, allowing you to capture the benefits of your industrial digitization efforts across both IT and OT environments.

HOW IT WORKS

Figure 1 shows a high-level integration of Cisco firewalls and the Dragos Platform, based on the Purdue model architecture. In this scenario, the Dragos Platform provides defenders with unprecedented knowledge and understanding of their industrial assets and activity, potential threats, and provides 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 false positives and lowers "mean time to detection." 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.

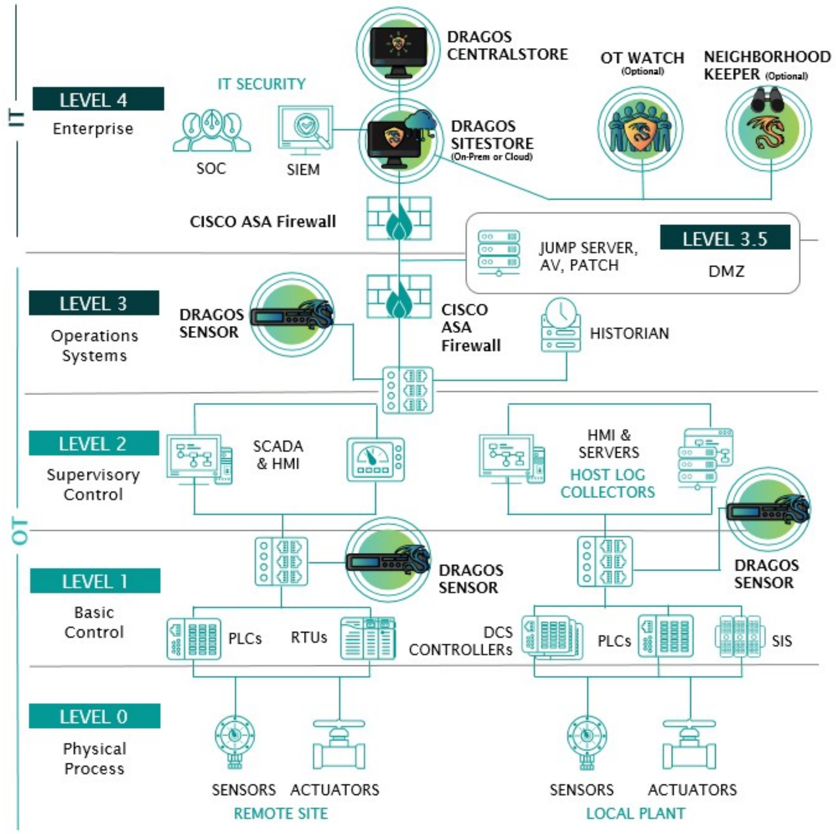

Figure 1. Deployment architecture representation based on the Purdue Model

Cisco firewalls are placed in strategic prevention points, giving the ability to block attacks before they reach critical OT systems. The threats from the Dragos Platform are sent to Cisco ASA where firewall administrators can easily make policy adjustments to enable control and containment of the environment to better prevent disruption and minimize risk exposure of critical operations.

USE CASE: More Informed Firewall Policies

One of the fundamental challenges industrial asset owners face, is having a complete and accurate inventory of their connected devices. Industrial companies inherently understand that the equipment operating in their environments is critical to the success of their business. Unfortunately, over time the complexity of these environments increases, inventories change, technology ages, systems drift out of compliance with configuration standards, new vulnerabilities are discovered, and the simple challenge of having full visibility into your environment so it can be properly secured becomes a never-ending struggle.

Cybersecurity analysts face an internal challenge—alert fatigue. Many anomaly-based threat detection methods are known to create high numbers of notifications with false positives on configuration changes or firmware updates, with little transparency and context into why the alerts occur. This additional time researching alerts burns cybersecurity resources, taking attention away from mitigating risk and minimizing downtime, which are priorities. The Dragos Platform addresses 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 various 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 Cisco ASA for easier management by a firewall administrator who can then apply appropriate policies.

The Dragos Platform rapidly pinpoints malicious behavior on your ICS/OT network, providing in-depth alert context, and reducing false positives for unparalleled threat detection. In addition to threat detection, users are presented with prioritized vulnerability guidance with “Now, Next, Never,” giving defenders the information needed to focus on the highest priority issues requiring further investigation. These notifications trigger based on certain configurable conditions created in the Dragos rules engine. Once triggered, response actions can be executed by the Cisco firewall administrator and the policy applied to any address groups as updated by the Dragos Platform.

ADVANTAGES OF THE CISCO AND DRAGOS SOLUTION INCLUDE:

- Simple integration between the technologies provides enhanced interoperability.
- Continuously updated detection and response content through The Dragos Platform’s intelligence-driven ‘Knowledge Packs.'
- Spans the needs of analysts for both IT and OT networks for improved complete situational awareness and decision-making.
- Contribute to meeting a variety of industrial standards, regulations, and guidelines such as NERC-CIP, ISA/IEC 62443, CFATS, ANSI/AWWA G430, and others.
- Improved ability to react to IT adversaries that often pivot from enterprise networks to OT.

For more information, please visit dragos.com/partner/cisco
or contact us at info@dragos.com