INTEGRATED TECHNOLOGY FROM DRAGOS AND PALO ALTO NETWORKS

Securing Industrial Control Systems (ICS) Against Cyberthreats

HIGHLIGHTS

- Improve OT asset visibility and threat detection with the Dragos Platform for better Palo Alto Networks NGFW optimization.
- Enhance IT/OT network north-south boundaries and micro-segment OT networks to prevent unauthorized east-west communication.
- Rapidly pinpoint malicious behavior on your ICS/OT network, 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 Palo Alto Networks 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

As industrial organizations face modernization and regulatory requirements for digital transformation efforts, cyberthreats have become a serious challenge. Cybersecurity teams across the utilities and manufacturing sectors are tasked with assessing these risks to their environments and adhering to audit and compliance programs. Implementing these practices comes with various challenges through increased Industrial Control Systems (ICS) connectivity, including unique protocols, legacy systems, unfamiliar technology, 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.

The Palo Alto Networks Next-Generation Firewall (NGFW) offers a prevention-focused architecture that is easy to deploy and operate. Automation reduces manual effort so your security teams can replace disconnected tools with tightly integrated innovations, focus on what matters, and enforce consistent protection everywhere. ML-Powered NGFWs inspect all traffic, including all applications, threats, and content, and tie that traffic to the user, regardless of location or device type.

Together, this solution protects OT assets from potential threats, helping segment industrial networks and build compliance with various industrial standards, regulations, and guidelines, such as NERC-CIP, ISA99/IEC62443, CFATS, and ANSI/AWWA G430. This allows teams to capture the benefits of industrial digitization efforts across both IT and OT environments while being able to see risks, reduce attack paths, and secure a wider range of environments.

HOW IT WORKS

Figure 1 shows a high-level integration of Palo Alto Networks NGFWs 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, 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 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.

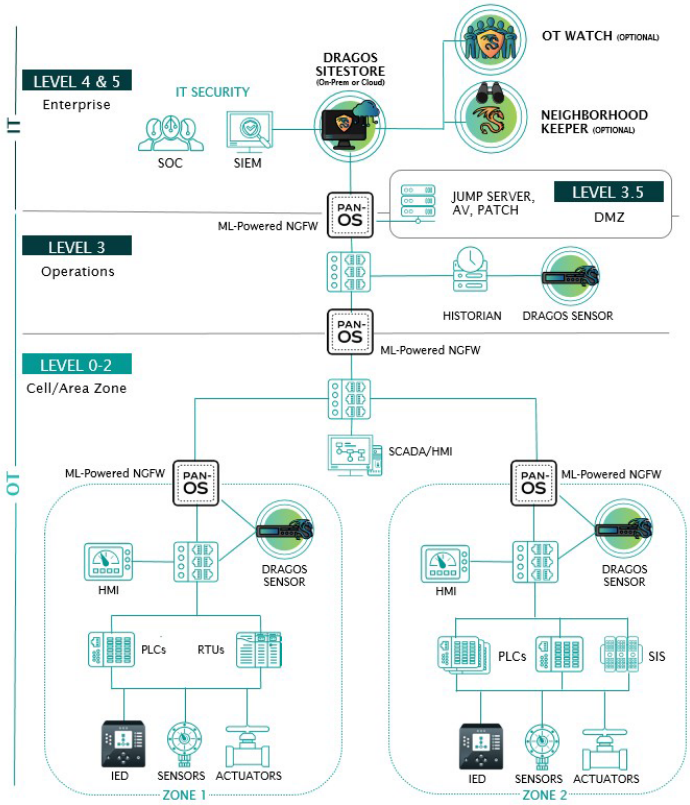

Figure 1. Deployment architecture representation based on the Purdue Model

The Palo Alto Networks NGFW is 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 Palo Alto Networks NGFWs 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 Palo Alto Networks NGFWs 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. Users are presented with prioritized 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 Palo Alto Networks firewall administrator and the policy applied to any address groups as updated by the Dragos Platform.

ADVANTAGES OF THE PALO ALTO NETWORKS AND DRAGOS SOLUTION INCLUDE:

- Simple integration between the technologies provides enhanced interoperability.
- Continuously updated new 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, ISA99/IEC62443, 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/palo-alto-networks
or contact us at info@dragos.com