DRAGOS AND PALO ALTO NETWORKS

Unify IT & OT Cybersecurity for Industrial Control Systems (ICS)

HIGHLIGHTS

- Ensure the integrity of your OT environment with combined asset visibility, threat detection, response, and prevention capabilities.
- Enhanced situational awareness providing customers with improved visibility of various IT and OT threat detection technologies across the entire organization.
- Maximize the value, investment, and visibility with integrated technologies to optimize both enterprise (IT) and industrial (OT) security environments.
- Provide asset operators a more comprehensive workflow from initial threat detection through response, improving Mean Time To Recovery, with technology integration and IRR Services.

THE CHALLENGE

Chief Information Security Officers (CISO's) and cybersecurity executives in critical infrastructure sectors, including utilities and transportation, oil and gas, and manufacturing are often challenged to manage both technology and personnel resources across their entire Information Technology (IT) and Operation Technology (OT) environment.

As security teams are required to have a broader converged view of their IT and OT networks to properly assess risk and vulnerabilities, the challenge of bridging that gap with the right cybersecurity technology and architecture is more prevalent than ever.

Enterprise security tools can provide analysts with visibility into the IT networks but offer limited capability for asset and threat identification for Industrial Control Systems (ICS) and OT networks. Because of this, the risks to the business are evident as the industrial threat landscape is significant leading to the need to provide cybersecurity professionals with complete situational awareness and decision-making support.

When owners and operators of ICS lack visibility in their OT environments, this can lead to ineffective threat detection and IT/OT network segmentation.

Not having this thorough understanding of the sophisticated adversaries that are actively targeting both the IT and OT networks can lead to the disruption of systems, physical damage, and even loss of life. This puts increased pressure on the various stakeholders such as leadership, engineering, security specialists, vendors, etc. to ensure readiness with sufficient hardening, detection, and response mechanisms to neutralize potential threats and reduce overall business risk.

Cybersecurity executives and architects often face challenges with tool sprawl, disparate systems, and complex technologies that can add to inefficient business processes. Selecting the right partners, tools and integrated solutions can have significant long-term benefits, as technology deployments in OT environments tend to have long lifecycles.

THE SOLUTION

The Palo Alto Networks Next-Generation Firewalls (NGFW) and the Dragos Platform integration provides defenders with a scalable cybersecurity solution that bridges IT and OT environments to better manage risk, empower audit and compliance, and accelerate digital transformation initiatives.

This solution offers the necessary capabilities to quickly prioritize, investigate, and respond to threats, while incorporating network segmentation to reduce threats from moving unchallenged laterally through the network. Providing complete asset visibility, the Dragos Platform can generate and populate asset sync profiles sent to Palo Alto Network NGFWs for inclusion in address groups where administrators can 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 Palo Alto Networks—all designed to ensure the uptime, resilience, and safety of industrial assets and personnel.

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.

Codified with the expertise of the industry's largest, most experienced team of ICS/OT practitioners, Dragos advanced threat detection and analytics effectively help identify ICS/OT threats, including adversary behavior and tradecraft, while providing accurate and prioritized recommendations to better manage the full spectrum of vulnerabilities.

Palo Alto Networks NGFW offer 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. You can align security with your business policies and write rules that are easy to understand and maintain. The NGFWs have been globally deployed in multiple critical infrastructure sectors, including utilities and transportation, oil and gas, and manufacturing, to prevent successful cyberattacks on ICS and SCADA.

In addition to the technology integration, Dragos has also partnered with Palo Alto Networks Unit 42 for deeper integration of threat intelligence and incident response services for joint customers. Unit 42 provides a threat-informed approach to incident response that enables security teams to understand adversary intent and attribution while enhancing protections offered by the Dragos Platform and services to stop advanced attacks. Unit 42 partners with the Dragos team of ICS experts who have been on the front lines of significant industrial cybersecurity attacks globally.

BENEFITS AND IMPACTS

BENEFITS	IMPACTS
Combined Domain Experience	Leverages the industrial and enterprise cybersecurity expertise from Dragos and Palo Alto Networks to help uncover threats and improve overall security posture.
Enhanced Visibility of IT and OT Networks	Integrating the Dragos Platform with Palo Alto Networks NGFW ensures more effective asset visibility, threat detection, and response in both IT and OT domains.
Intelligence-Driven Threat Detection	Utilizing comprehensive IT and OT threat intelligence as the primary method of detecting threats, which improves detection confidence and reduces alert fatigue.
Empowered Adherence of Regulations	Integrating the technologies improves security practices, safeguards data, and empowers adherence of regulations – leading to process efficiency improvements, while minimizing fines, penalties, and reputational impacts.
Informed Incident Response Services	Providing a threat-informed approach to incident response that enables security teams to understand adversary intent and attribution while enhancing protections and services to stop advanced attacks.

For more information, please visit dragos.com/partner/palo-alto-networks
or contact us at info@dragos.com