DRAGOS AND TRELLIX

Improving Threat Detection and Response Across Industrial Networks

HIGHLIGHTS

- Integration improves visibility and interoperability of various IT and OT threat detection technologies across the entire organization.
- Customers benefit from the mutual intelligence-driven approach to cybersecurity and experience across both enterprise (IT) and industrial (OT) environments.
- Maximize value and detection efficacy from existing cybersecurity investments by integrating technologies optimized for both IT and OT security environments.
- Integrated security solutions provide more efficient workflows that allow defenders to dramatically reduce Mean Time To Revocer (MTTR) from threats with fewer resources.

THE CHALLENGE

Owners and operators of Industrial Control Systems (ICS) across various industries have a responsibility to ensure safe and reliable operations. Security executives at industrial organizations, including Chief Information Security Officers (CISO's), are often challenged to provide resources (both technology and personnel) across the entire Information Technology (IT) and Operation Technology (OT) environment. Enterprise security tools that provide analysts with visibility into the IT networks are fairly commonplace but offer limited capability for asset and threat identification for ICS in industrial operations. Since security teams are now required to have a broader converged view of the entire IT, IIoT, and OT networks, they need technology that works together to help bridge the gap. The risk to the business is evident as the industrial threat landscape is prevalent and significant, and the need to provide security professionals with complete situational awareness and decision-making support is critical.

Additionally, security teams need to have a thorough understanding of the sophisticated adversaries that are actively targeting both the IT and OT networks, which could lead to the disruption of systems leading to physical damage and 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 the threat and reduce overall business risk.

THE SOLUTION

Dragos and Trellix™ (formerly McAfee) are working together to provide a more comprehensive approach to protecting critical infrastructure. In order to provide a complete solution, multiple technologies must operate together without introducing complexity, adversely impacting safety or availability, while helping security teams achieve their goals. Visibility and understand across the enterprise (IT) and ICS (OT) network is essential for security and compliance. This enables defenders to react to adversaries that often pivot from the enterprise to the OT network.

Trellix is a leading cybersecurity-focused company that has been prevalent in protecting critical infrastructure and industrial organizations around the world for more than a decade. Trellix has been widely validated and adopted by industrial OEM's as their cybersecurity technology of choice that utilizes technologies including Security Information and Event Management (SIEM) and Endpoint Detection &

Response (EDR). The Dragos Platform and supporting ICS security service offerings provide capabilities needed to protect critical infrastructure with speed and confidence. This means less downtime and fewer disruptions, so organizations can focus on maintaining safe and secure operations. This partnership allows the combination of Dragos technology and experiential knowledge of the industrial control security domain with Trellix's technology to span the visibility needs of security analysts. This combined intelligence driven threat detection across IT and OT networks improves the overall situational awareness, including asset visibility, threat detection, and guided response to reduce the Mean Time To Recovery (MTTR). The joint solutions and domain experience provide the tools and knowledge to help build internal expertise to protect the entire network.

There is a wide variety of technologies and protocols across the enterprise (IT) and ICS (OT) networks. Native support for these systems and their associated communications is a critical way to enable effective situational awareness and multi-zone protection. The Dragos Platform passively monitors ICS protocols across the network as well as log's and events collected from ICS devices. The Platform integration with Trellix technology gives defenders the ability to harness the power of real-time visibility and centralized management through a single platform. The Dragos and Trellix combination will focus on supporting some of the primary needs of critical infrastructure environments; cybersecurity protection without impacting operational safety or availability, situational awareness for improved decision-making abilities, and multi-zone protection support for assistance in continuous cybersecurity compliance.

BENEFITS AND IMPACTS

BENEFITS	IMPACTS
Combined IT-OT Domain Experience	Leverage the industrial and enterprise cybersecurity expertise from Dragos and Trellix to help uncover threats and improve overall security posture.
Build Internal Team Expertise	Train industrial cybersecurity teams to ensure knowledge transfer and expertise and develop robust internal defensive capabilities.
Intelligence-Driven Threat Detections	Utilizes comprehensive IT and OT threat intelligence as the primary method of detecting threats, which improves detection confidence and reduces alert fatigue.
Enhanced Visibility of IT and OT Networks	Combining the Trellix Enterprise Security Manager and the Dragos Platform ensures more effective asset visibility, threat detection, and response in both the IT and OT domains.
More Efficient Security Operations	Integrating the technologies enables defenders with a more comprehensive workflow from initial threat detection through response, improving Mean Time To Recovery (MTTR)

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