CONVERGED INDUSTRIAL EDGE NETWORK ARCHITECTURE SOLUTION

Simplfying the IT and OT Information Exchange

HIGHLIGHTS

- Build a zero-trust, deny-by-default network from control centers to substations
- Improved asset visibility from the Dragos Platform by utilizing SEL OT SDN deployments
- Streamline threat detection & response via Dragos Platform and Juniper technology integrations
- Standardized digital infrastructure layer for frictionless information exchange between vendors, systems, devices, and domains
- Automation of repetitive data entry which reduces configuration errors and strain on human resources

OVERVIEW

The Converged Industrial Edge is designed to secure and simplify information exchanges across disparate parts of a network in a manner that strengthens the system's cybersecurity posture, reduces maintenance costs, adds greater situational awareness, improves reliability, and preserves the integrity of the IT and OT domain performance requirements.

THE CHALLENGE

Critical infrastructure markets, like utilities, face multiple challenges and must evolve their business practices to survive and thrive in a fast-changing, dynamic market. Power utilities have become significant targets for criminal syndicates and malicious nation-states as their reliance on a more digital and connected infrastructure increases. In 2021, the US Federal government called for urgent action to protect electric grid distribution systems, which the government identified as vulnerable to cyberattack. With the flow of energy to homes and businesses at risk, utilities must strengthen their cybersecurity. The goals of improving cybersecurity, lowering the cost of operations, and increasing business agility without impact to critical services can be achieved with novel, automation-forward communications for IT and OT, but is the literal equivalent of upgrading a plane's engines while it is in flight. The Converged Industrial Edge was developed in response to the ever-growing connectivity and cybersecurity demands placed on critical infrastructure. These demands, in some cases, have resulted in overly complex network architectures that are prone to misconfigurations due to repetitive manual tasks, limit system visibility, increase maintenance and operational costs, and increase the cyber-attack surface. Additionally, it can take months to engineer, test, and deploy any desired network changes based on shifting business needs.

THE SOLUTION

Effective security starts with visibility across all systems and networks, and the capability to manage the network traffic between those systems. Dragos, Schweitzer Engineering Laboratories (SEL), and Juniper Networks collaborated on a solution that simplifies the orchestration, lifecycle, and security of network communications within IT to OT and OT to OT environments. At its core, the Converged Industrial Edge (CIE) is an open, multivendor solution architecture built to support the safety, reliability, security, and long-life cycle requirements of critical infrastructure environments. The CIE also brings comprehensive asset visibility, vulnerability management, threat detection, and response capabilities to the environment. The result is a best practices approach for securely sharing information between IT and OT networks. By securing and simplifying information exchange across

disparate parts of a network, the CIE strengthens the environment's overall cybersecurity posture, reduces maintenance costs, adds greater situational awareness, improves grid reliability, and preserves the integrity of each domain's performance requirements.

HOW IT WORKS

As a core component of the CIE solution, the Dragos Platform provides complete visibility of all assets within the network, including the communication details, detects threat activity on the network, and gives defenders the ability to investigate and then mitigate a potential threat from within a single application. As a result of the CIE solution, integrations now exist between the Dragos Platform and SEL OT Software Defined Networking (SDN) and Juniper Networks systems. The SEL OT SDN integration allows defenders to have an even greater level of asset visibility by ingesting system details and logical connection information even before those systems communicate across the wire. Through this technology integration, defenders can know precisely what devices are allowed on the network and what communication paths should exist, and notifications can be triggered if there is any deviation from this baseline. The integration with Juniper Networks provides defenders with the necessary capability to quickly prioritize, investigate, and respond to threats across their OT environments. Through the technology integration, the Dragos Platform sends context-rich notifications, including recommended response actions, to a Juniper firewall via a work order management system. If approved by the appropriate staff, the work order system will send the recommended response action instructions to the Juniper SRX firewall to help mitigate the threat activity before it can cause operational disruption (see Figure 1). This unique combination of technology and integrations will provide defenders with a more secure, reliable, efficient, and effective security operations team.

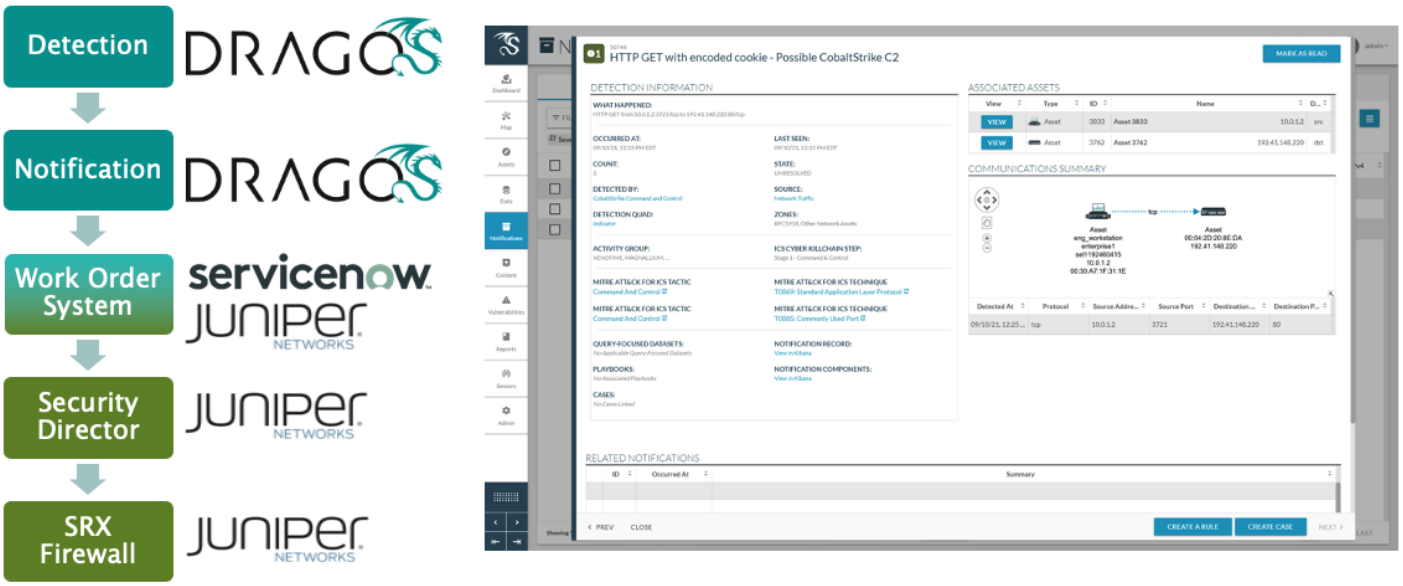

Figure 1. Workflow integration between Dragos Platform and Juniper Networks Security Director.

Industry transitions are creating an opportunity to drive more business value while building a better, more secure, and reliable infrastructure. The transition relies on a modern industrial edge that is able to meet the unique requirements of OT and IT systems. Dragos, SEL, and Juniper have collaborated to create an integrated, proven solution for the Converged Industrial Edge that enables utilities and industrial enterprises to meet evolving requirements at higher levels of reliability and with greater operational efficiency.

For more information, please visit www.dragos.com or contact us at info@dragos.com