DRAGOS AND OWL CYBER DEFENSE

A More Complete ICS Security Architecture

HIGHLIGHTS

- Interoperability of the Dragos Industrial Cybersecurity Platform and Owl Data Diode Technology has been successfully tested and validated.
- Customers can deploy Dragos and Owl technologies together to create more secure cybersecurity architectures in ICS networks.
- The joint architecture guarantees safe, continuous monitoring of industrial networks for uninterrupted asset identification and threat detection while maintaining a robust perimeter.
- Dragos and Owl have combined ICS experience to assist customers in helping customers secure their OT networks.

THE CHALLENGE

With the proliferation of Industrial IoT (IIoT), Industry 4.0, and cloud-based technologies for enhanced automation and analysis of large volumes of data, operational technology (OT) managers are faced with the challenge of making industrial networks more accessible for legitimate business drivers without significantly increasing cybersecurity risks. This balance requires an architecture that provides secure OT network perimeters with controlled data flow and complete network visibility for effective threat detection and response. Some regulated industries are even required to have clearly defined perimeters that use only approved technologies for the transfer of information in/out of the protected network.

As a result, cybersecurity stakeholders are tasked with reducing upstream connections (attack surfaces), which might compromise OT networks, while maintaining full visibility into those networks for a comprehensive approach to prevent, detect, and respond to threats.

THE SOLUTION

Owl's Data Diode technology provides physical protection of OT networks at OT network perimeters. The Data Diodes enable seamless IT/OT integration, providing safe, enterprise-wide visibility into OT networks with physical segmentation.

The Dragos Industrial Cybersecurity Platform is a passive network monitoring tool that enables complete visibility into industrial control systems (ICS) networks. It allows users to visualize industrial assets and their communications, detect threats as they occur, and utilize prescriptive workbench tools for more efficient investigations and response while avoiding operational impacts to the existing security team's operations.

The combination of Owl Data Diodes and the Dragos Industrial Cybersecurity Platform enables safe monitoring of ICS/OT networks, providing a more secure and effective approach to improved threat prevention, detection, and response.

TECHNOLOGY

The Dragos Industrial Cybersecurity Platform consists of network appliances referred to as Sensors and a centralized server known as the SiteStore, which can be deployed on-premise or in the cloud. The Dragos platform provides passive network monitoring, enabling threat detection and response capabilities:

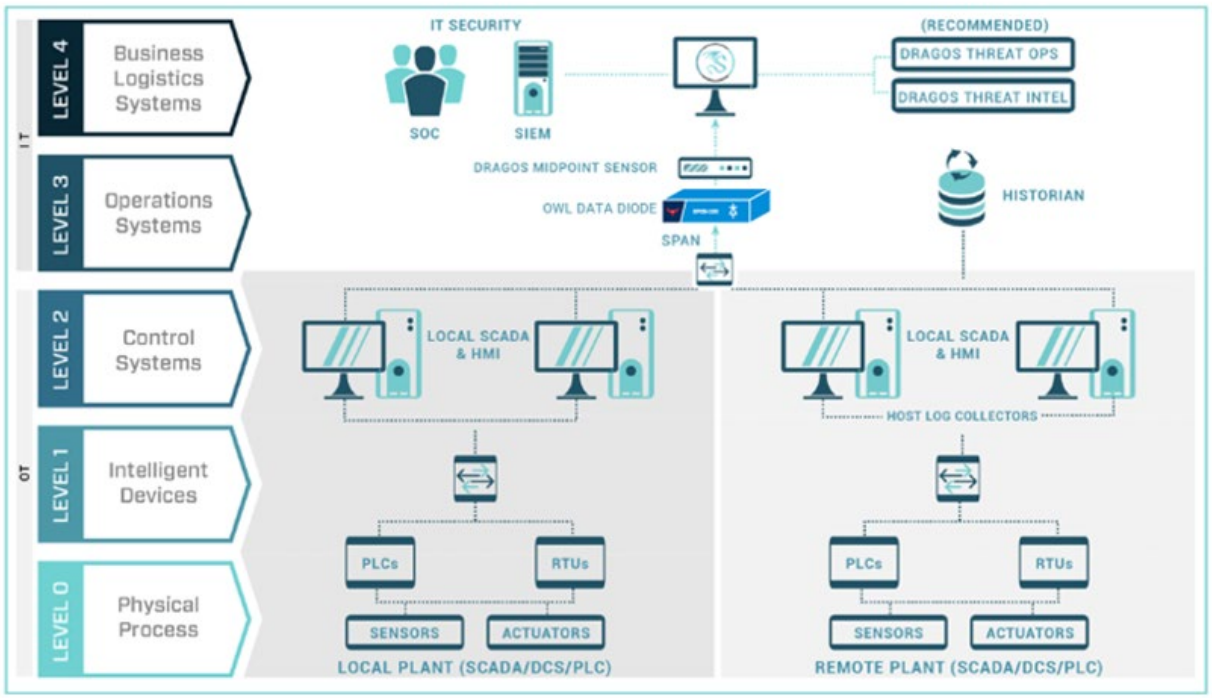
- Asset Identification – industrial assets communicating on the network are identified and characterized so that analysts can visualize the complete operations environment.

- Threat Detection – by leveraging threat intelligence of known malicious activity, Dragos utilizes Threat Behavior Analytics to automatically provide notifications when known malicious behavior has been detected in the ICS network with appropriate context regarding what the behavior means and what should be done.
- Incident Response - Investigation Playbooks and query-able datasets guide analysts on the appropriate response path, leveraging all the network, host, and system data available, to help scale industrial-specific security knowledge across teams of diverse backgrounds.

Owl Data Diodes are hardware-enforced devices that provide secure, deterministic transfers of communications in one direction only. Data Diodes are routinely deployed to gather network packet captures, system logs, SNMP traps, historian data, OPC data, and other security monitoring and operations intelligence from a trusted industrial network to an untrusted network. Since the data diode is physically able to send information in only one direction, there is no possibility of threat activity pivoting from untrusted networks into trusted network segments that would put OT networks at risk.

Owl Data Diodes provide enforceable, air-gapped network segmentation, while providing complete visibility of the OT network traffic necessary for the Dragos Platform, for monitoring and threat detection. The Dragos Platform and Owl Data Diode technology have been tested and validated for compatibility to enable safe and continuous monitoring of industrial assets.

ARCHITECTURE



In the example architecture above, the core switch at the boundary of level 2 and 3 networks is configured to produce SPAN / Mirror traffic from the trusted OT network for security monitoring. The Data Diode is configured to gather packet captures from that port and transmit that data one-way to the untrusted network, where the data diode emulates the OT SPAN port to the Dragos sensor beyond the perimeter. Network Packet Transfer System (NPTS) mode within the data diode allows the Dragos sensor to monitor traffic from a protected OT network without the sensor being installed within the protected network, which is more secure and requires minimal changes to the OT network architecture.

Please refer to the Interoperability Guide for more information.

BENEFITS AND IMPACTS

BENEFITS	IMPACTS
Validated Interoperability	Industrial enterprises are assured that the Dragos Industrial Cybersecurity Platform will function properly in environments using Owl Data Diode technology.
Secure Architecture	Industrial enterprises enjoy both in-depth security monitoring and strong OT perimeter protection to enable safe visibility into OT networks.
Complementary Technologies	Industrial enterprises can continuously monitor OT networks and production operations while maintaining a layer of physical protection to prevent cyberattacks against OT networks.
Extensive Experience	The combined experience of Dragos and Owl in many different industrial environments across multiple industry verticals provides greater confidence to industrial security professionals focused on securing OT infrastructure.
Convenient Management	Dragos Sensors can be managed, updated, and adjusted safely and easily beyond the perimeter on IT networks, without needing to be installed on OT networks.

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