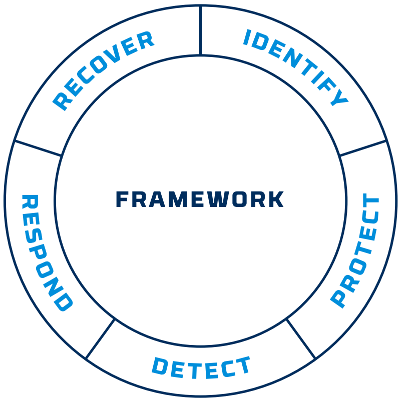
SOLUTION BRIEF

OWL AND DRAGOS

Visualize, Detect, & Respond to OT Cybersecurity Threats

COMBINED SOLUTION KEY BENEFITS

- Securely transfer ICS/OT data to the Dragos Platform for monitoring and investigation
- Maintain the air-gap of OT networks
- In-depth ICS/OT asset and device visibility
- Rapidly identify and pinpoint threats
- Reduce ICS/OT cybersecurity risk
- Reduce threat discovery time
- Decrease incident response time
- Prevent catastrophic downtime
- Amplify ICS/OT resources



The combination of Owl data diodes and the Dragos Platform helps organizations meet NIST cybersecurity recommendations.

Visibility of ICS/OT Assets

Protection of critical Operational Technology (OT) networks requires sound edge security, combined with comprehensive monitoring. A perimeter must be established, and cybersecurity products should be deployed to identify if that perimeter has been bypassed. To protect critical infrastructure networks, a common practice has traditionally been to establish an air gap to disconnect OT networks from “untrusted” or less secure networks, the internet, and the outside world. Critical infrastructure organizations cannot afford any level of compromise or loss of operational assurance. When an air gap is established, the risk of a cyberattack drops dramatically, however, humans are fallible – mistakes can be made, and threats can still be introduced through a variety of threat vectors. Therefore, critical infrastructure organizations have recognized the need for a solution that provides centralized visibility into their networks, even with an air-gapped architecture, for stronger security. Owl Cyber Defense and Dragos have joined forces to provide centralized visibility to ICS/OT assets through a secure, one-way data transfer.

Dragos Platform

Built specifically for industrial organizations, the Dragos Platform delivers unmatched visibility of industrial control systems (ICS) and OT network assets and communications, rapidly pinpoints threats through intelligence-driven analytics, and provides best-practice playbooks to investigate and respond to threats before they cause significant impacts to operations, processes, or people. Analyzing multiple data sources, including protocols, network traffic, data historians, host logs, asset characterizations, and anomalies, the Dragos Platform provides unmatched visibility of ICS/OT environments from any location. Rapidly pinpointing malicious ICS/OT network behavior, this platform provides an in-depth context of alerts and reduces false positives for unparalleled threat detection. The Dragos Platform provides expert-authored playbooks to guide security teams step-by-step throughout investigations, decreasing response time and improving the efficiency of teams’ workflows. Due to the air-gapped architecture of most OT networks, critical infrastructure organizations recognize the need for a hardware-based solution to securely transfer ICS/OT data one-way out to the Dragos Platform and this can be achieved through Owl data diodes.

Owl Data Diodes

Owl data diodes provide a secure, deterministic, one-way transfer of ICS/OT data to the Dragos Platform for monitoring and investigation. While maintaining the air-gapped architecture of OT networks, Owl prevent threats from entering back into the OT network and restricts adversarial movement within. Owl data diodes transfer raw network packets, from within a protected network, to a Dragos sensor to support analysis of network communications in the Dragos Platform.

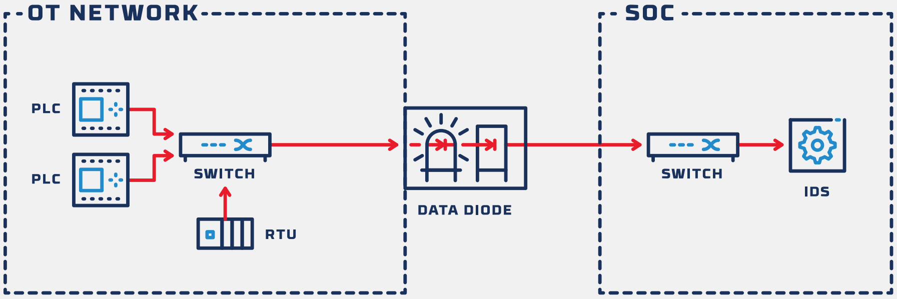
Owl & Dragos Combined Solution

SECURE, ONE-WAY TRANSFER OF OT RAW NETWORK PACKETS TO THE DRAGOS PLATFORM

Critical infrastructure operators require absolute network isolation for their processes and the control systems that manage them. The monitoring and business networks are separated from the control networks by an air gap. Network traffic from the control network is sent to the Owl data diode from a network tap or span port, providing copies of all network packets, without impacting the production network. The Owl solution communicates the network packets through an optical data diode to the monitoring network, where Dragos sensors can watch traffic in real-time and provide valuable alarms and notifications to security staff. The customer achieves the combined security of air-gapped isolation, plus asset identification, threat detection, and response from Dragos.

RAW NETWORK PACKET TRANSFER

Raw Ethernet packets are transferred out of the OT network to the Dragos Platform for analysis



OWL Cyber Defense

Owl Cyber Defense cross domain, data diode, and portable media solutions provide hardened security checkpoints for absolute threat prevention and secure data availability. Certified by the U.S. government, independent testing authorities, and international standards bodies, Owl technologies and services help to secure the network edge and enable controlled unidirectional and bidirectional data transfers. For over 20 years, clients worldwide in defense, intelligence, and infrastructure have trusted Owl's unmatched expertise to protect networks, systems, and devices.

DRAGOS

Dragos has a global mission: to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The expert practitioners who founded Dragos were drawn to this mission through their decades of experience in the US Military and Intelligence Community going head-to-head with cyber attackers who threaten the world's industrial infrastructure. Our solutions combine advanced technologies for asset identification, threat detection, and response with the battle-honed insights of our elite team of industrial control systems (ICS) cybersecurity experts. We arm enterprises with the tools to identify threats and respond to them before they become significant breaches.