



TENABLE AND OWL

Balancing Air Gapping with Secure Accessibility

The Challenge

Industrial Control Systems (ICS) are the bedrock of manufacturing process and critical infrastructure. Convergence of the IT and OT environment is one of the larger factors contributing to the increase in attack surface and vectors. What was once physically airgapped now requires technology to view and manage IT and OT activity and threats without creating new ones. As such, one of the major challenges facing organizations is to safely and seamlessly gain visibility and move data from the operational (OT) environment to the IT infrastructure without introducing any new threats.

The Joint Solution

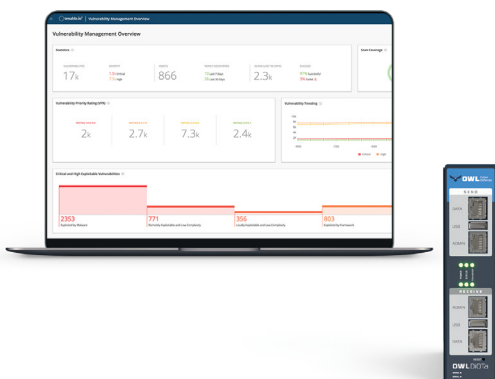
The Tenable Industrial Cybersecurity Suite protects industrial networks from cyber threats, malicious insiders, and human error. From threat detection and mitigation to asset tracking, vulnerability management, configuration control and device integrity checks, Tenable's ICS security capabilities maximize the safety and reliability of operational and critical infrastructure environment. The Tenable Suite delivers comprehensive situational awareness across all sites and their respective OT assets.

Owl Cyber Defense is a leader in data diode and cross domain network cybersecurity. Owl develops market-first, one-way data transfer products to meet a variety of operational needs, from entry level to enterprise

With today's emerging threats, while it is essential to have full visibility, security and control between IT and OT environments, it is also essential to ensure that where appropriate, the OT network is separated from the IT network. In such cases, Owl data diodes can provide the security necessary.

With this tested and proven joint solution, customers can trust that the internal and critical network is physically inaccessible from the external network while their sensitive network is being monitored by the Tenable solution.

Tenable and Owl work together to pass data needed while ensuring the data diode-based airgap between networks. Tenable's sensor is located on the critical/OT network and forwards captured traffic to the Tenable Core Platform which resides outside of the OT network. Owl separates the two networks but the Sensor to ICP traffic can securely pass through it.

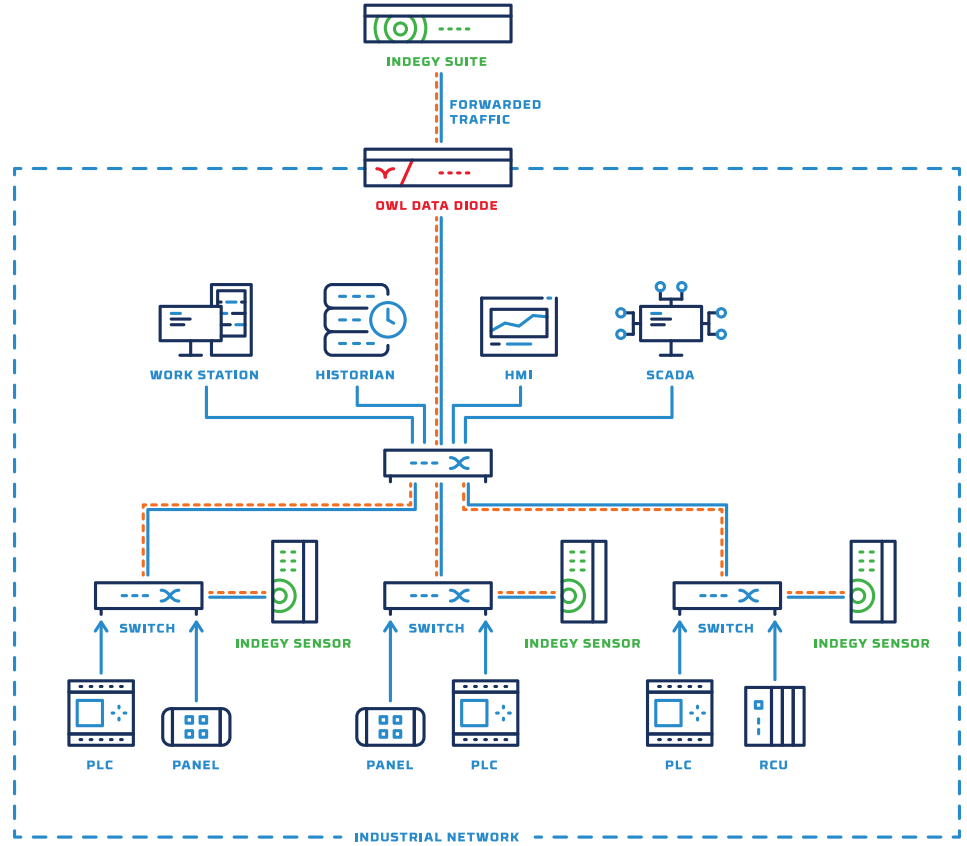


CHALLENGES

- Critical OT assets are air-gapped to ensure security from monitoring and threat detection
- Software-based firewalls are vulnerable to zero-day exploits & easy to misconfigure
- Legacy and highly regulated systems are vulnerable and not updateable
- Physical access required to obtain monitoring data

SOLUTION ELEMENTS

- Owl DiOTa, or DIN-Rail data diode with Talon proprietary software
- Tenable Industrial Cyber Security Suite



Results

- The joint solution enables visibility of critical OT assets that were previously air-gapped from IT without introducing risk of lateral threats
- Tenable OT data flows seamlessly through the Owl diode
- The integrated solution makes it easy to configure and deploy network sensors in segments protected by the Owl data diode
- Detect threats that are blocked or stopped by the data diode
- Advanced 360 degree visibility solution available for delivering both IT and OT updates to security systems in isolated networks

OWL Cyber Defense