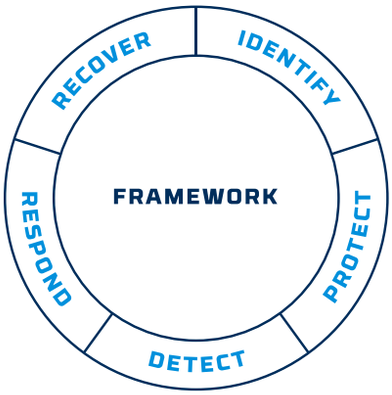
DATA SHEET

OWL Cyber Defense

Securely Transfer OT Data to a SIEM or IDS Solution



The combination of a data diode and a SIEM/ IDS solution helps organizations meet NIST cybersecurity recommendations.

Securely Transfer and Monitor OT Network Data

How does your organization remotely monitor data from operational technology (OT) systems and devices? The most common monitoring solutions include security information event management (SIEM) systems and intrusion detection systems (IDS) on an IT or cloud network. The challenge is getting data from those OT systems to a remote location for monitoring. By combining Owl data diodes with a SIEM or IDS solution, an air gap is created, with no way for outsiders to gain access back into the OT network.

Edge Security – Air Gap

To protect OT networks, a common practice has traditionally been to establish an air gap – physically disconnecting the network from "untrusted" or less secure networks, such as the internet. Industrial and 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, organizations have recognized the need to maintain a SIEM or an IDS to provide centralized visibility into their networks, even with an air-gapped architecture.

Implementing SIEM & IDS Solutions

Besides securing their OT networks with air gaps, transferring data remotely provides a variety of additional benefits:

- **SIEM/IDS Effectiveness**: By securely transferring data out of the OT network, organizations can centralize monitoring and optimize their SIEM/IDS investment
- **Staffing Costs**: If organizations don't make SIEM/IDS data available remotely, they need additional Security Operations Center (SOC) staff inside the secure network, 24x7x365
- **Archiving Requirements**: Like other operational data inside the secure network, organizations cannot rely on a single site to preserve data; a remote location also serves as a backup

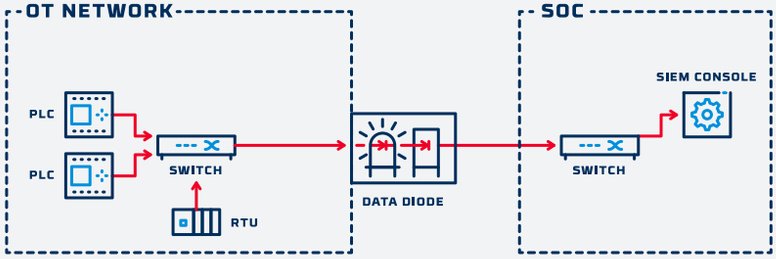
Safely Transfer Data to a SIEM/IDS

With Owl data diodes, data can be securely transferred to a SIEM and/or IDS of choice. With an unhackable, deterministic one-way transfer of data, critical infrastructure organizations can improve security, reduce costs, optimize their SIEM investment, and backup data successfully. Owl data diodes are versatile and can transfer multiple protocols simultaneously. For example, a data diode that is used for historian replication can also be used to communicate log data to a SIEM, increasing efficiency and reducing costs.

USE CASES: DATA TRANSFER TO SIEM/IDS WITH OWL DATA DIODE

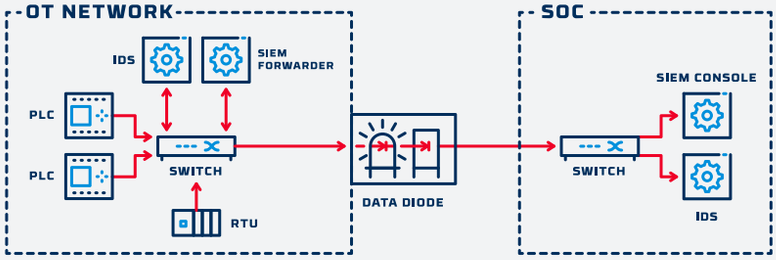
RAW LOG DATA OUT

Application log messages and other event/alert information are transmitted to a SIEM solution outside the OT network



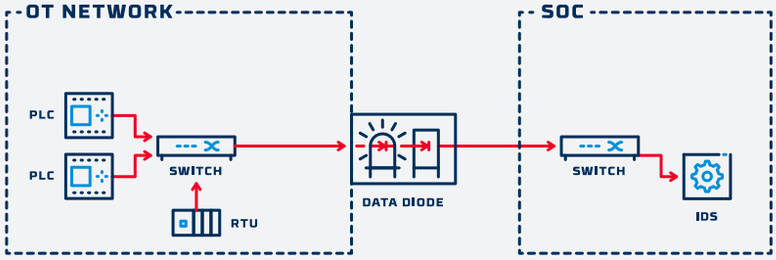
PROCESSED SIEM AND IDS DATA CONNECTED OUT TO SOC

SIEM and IDS components aggregate and filter data inside the OT network and communicate upstream to centralized management applications



RAW NETWORK TAP OUT TO IDS

Raw Ethernet packets are sent out of the OT network for analysis in an external IT or SOC network



THIRD-PARTY VENDOR INTEGRATIONS

LogRhythm · splunk> · Thomason Technologies, LLC (uncommon customer commitment) · FORTINET · NOZOMI NETWORKS · Indegy

PROTOCOLS SUPPORTED

- Syslog
- UDP
- TCP/IP
- Modbus
- OPC DA/A&E
- SMTP
- SNMP
- Files (FTP/SFTP)
- Raw Ethernet Packets
- Proprietary Formats

OWL Cyber Defense

Owl Cyber Defense Solutions, LLC leads the world in data diode and cross domain network cybersecurity. With a constant focus on customers in the military, government, critical infrastructure, and commercial communities, Owl develops market-first, one-way data transfer products to meet a variety of operational needs, from entry level to enterprise.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com

@OwlCyberDefense

203-894-9342 | Info@owlcyberdefense.com

D077 | V1 | 2-20-2020