OWL Cyber Defense

USE CASE

OPSWAT Kiosk Centralization of Alarms and Events

Case Summary

INDUSTRY

Critical Infrastructure, Power Generation

CHALLENGES

Need to transfer alarm, event, and scanning results data from OPSWAT Kiosks to a centralized Security Information Event Management (SIEM), without using a two-way connection

SOLUTION

DiOTa, Owl's one-way transfer data diode, transfers Syslog messages to send alarm and event files to a centralized SIEM

BENEFITS

Kiosk customers do not need to perform weekly manual retrievals of alarm, event, and scanning result files from each OPSWAT Kiosk

Company Overview

OPSWAT.

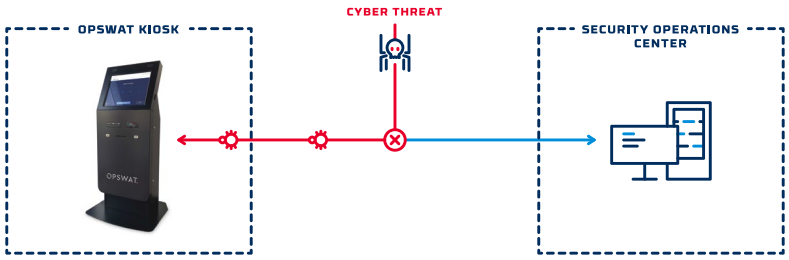
OPSWAT protects critical infrastructure with products that focus on threat prevention and process creation for secure data transfers and safe device access. 98% of U.S. nuclear power facilities trust OPSWAT for cybersecurity and compliance.

Cybersecurity Challenge

OPSWAT's MetaDefender Kiosk acts as a digital security guard, inspecting all portable media for malware, vulnerabilities, and sensitive data. These kiosks are air-gapped from the utilities network infrastructure to prevent attacks; however this prevents visibility to alarm and event files that need to be collected and monitored. OPSWAT faces the challenge of protecting their kiosks, while still delivering alarm and events data to be monitored, without using a two-way connection.

REQUIREMENTS

- Transfer Syslog data from the OPSWAT Kiosks to a SIEM
- Create an Electronic Perimeter between the OPSWAT Kiosk and the SIEM platform
- Cannot use a two-way connection
- Maintain air-gapped architecture



Solution

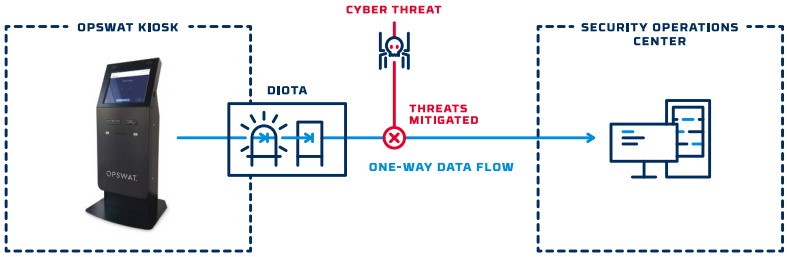
DiOTa, Owl's most affordable and compact data diode, was selected for a deterministic, one-way data transfer of Syslog messages as a UDP data stream. DiOTa maintains the Kiosk's air gap, while transferring alarm, event, and scanning results data to a SIEM through a hardware-enforced, one-way connection, preventing threats from entering the utilities Operational Technology (OT) network through data transfers.

DiOTa

Single-purpose data diode, built for deterministic, one-way data transfers of low volume data streams, with a maximum throughput of 5 Mbps

Results

- Secure, one-way data transfer of Kiosk alarm, event, and scanning result data to a SIEM
- Owl DiOTa will be installed into the Kiosk enclosure
- Customers can now monitor all OPSWAT Kiosks from a centralized SIEM
- Air gap is maintained
- No more manual data retrieval necessary from the OPSWAT Kiosks
- Two-way connection is not necessary



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

U037 | V1 | 9-21-2020