OWL Cyber Defense

WHITE PAPER

Owl Supports DHS Seven Strategies

DHS Provides Strategies for Thwarting Cyberattacks

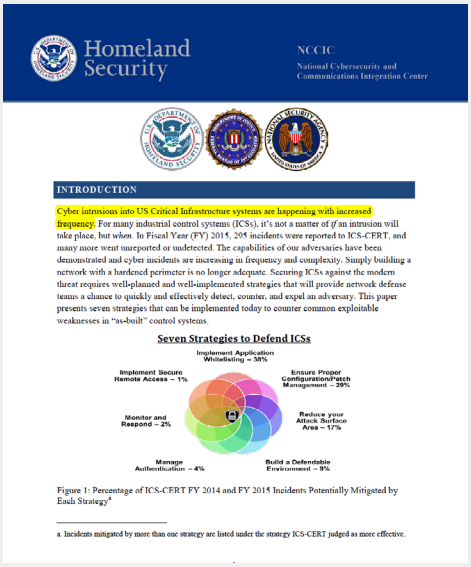
In order to reduce the risk of cyberattacks against critical infrastructure (transportation, energy, water, etc.), the Department of Homeland Security (DHS), operates the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). The ICS-CERT partners with various agencies, law enforcement, owners, operators and vendors to share information about industrial incidents and provides guidance for defense of control system environments against emerging cyber threats.

Many Industrial control systems are digital assets (SCADA, PLCs, historians) that operate and record activities in Operational Technologies (OT) networks encompassing a wide variety of plants, pump stations, refineries, substations, dams, etc. During 2015, the DHS noted that 295 security incidents were reported to the ICS-CERT with likely many more going unreported or undetected. That's at least one incident for every working day in 2015. For that same period, DHS reported that "… cyber incidents are increasing in frequency and complexity" and that "Securing ICSs against the modern threat requires well-planned and well-implemented strategies …".

Defending Industrial Control Systems

To address this growing cybersecurity threat to industrial control systems, the DHS, with contributions from experts in the FBI and the NSA, produced a paper called **"Seven Steps to Effectively Defend Industrial Control Systems."** [1] The paper provides seven strategies to counter cybersecurity vulnerabilities that were exploited in industrial control systems.

The strategies feature the use of data diodes and include white-listing, reduction of attack surfaces, managing authentication and providing secure remote access. The DHS concluded that these strategies are so important and effective, that if system owners had implemented them, 98 percent of the incidents the ICS-CERT responded to in both 2014 and 2015 would have been prevented.


Homeland Security

NCCIC
National Cybersecurity and Communications Integration Center

INTRODUCTION

Cyber intrusions into US Critical Infrastructure systems are happening with increased frequency. For many industrial control systems (ICSs), it's not a matter of *if* an intrusion will take place, but *when*. In Fiscal Year (FY) 2015, 295 incidents were reported to ICS-CERT, and many more went unreported or undetected. The capabilities of our adversaries have been demonstrated and cyber incidents are increasing in frequency and complexity. Simply building a network with a hardened perimeter is no longer adequate. Securing ICSs against the modern threat requires well-planned and well-implemented strategies that will provide network defense teams a chance to quickly and effectively detect, counter, and expel an adversary. This paper presents seven strategies that can be implemented today to counter common exploitable weaknesses in "as-built" control systems.

Seven Strategies to Defend ICSs

Figure 1: Percentage of ICS-CERT FY 2014 and FY 2015 Incidents Potentially Mitigated by Each Strategy[a]

a. Incidents mitigated by more than one strategy are listed under the strategy ICS-CERT judged as more effective.

Seven Strategies Form Defense-In-Depth

It takes layers of security to defend against today's cyberattacks; this layered approach is referred to as defense-in-depth. Owl's data diode products are used by many critical infrastructure operators today to build defense-in-depth security architectures.

How Owl Data Diodes Uphold All Seven Strategies

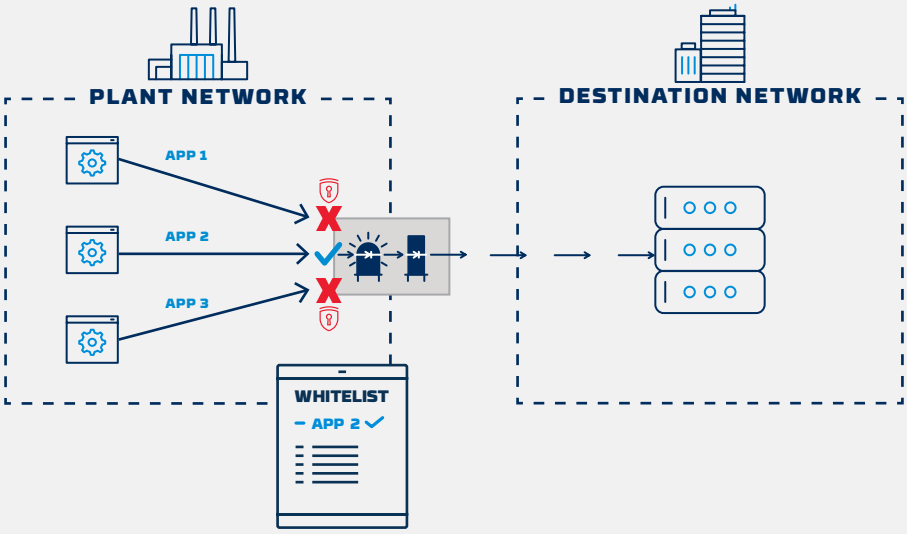
In three of the strategies the DHS explicitly recommends the use of data diodes. To help understand how Owl's data diode solutions support all seven strategies, we have created a matrix that matches Owl's data diode capabilities with the various recommendations made in the strategies.

However, Owl's defense-in-depth story doesn't end there. Not only do Owl's data diode products play a role in helping operators implement each of the strategies, those strategies are also designed into the data diodes to defend themselves with their own defense-in-depth strategies.

These capabilities are illustrated in the "Owl Data Diode Self-Defense" list on the back cover.

DHS Strategies:

APPLICATION WHITELISTING - Only allows predesignated applications to run, no need to be aware of new threats as only authorized software will run.



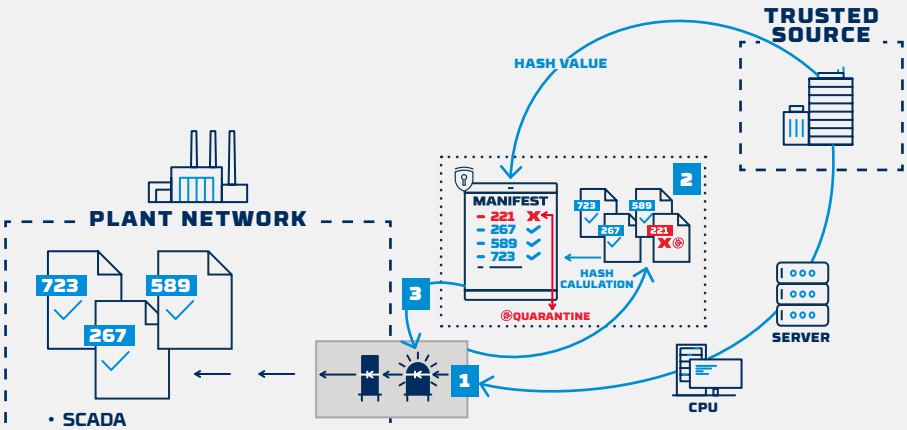
THE OWL SOLUTION

In keeping with whitelisting as a best practice, the Owl data diodes only accept data from known "whitelisted" data sources. Data sources are restricted to a unique combination of IP address, network port, and protocol. However, even in the event that a rogue application was able to hijack a valid outbound IP address, network port and protocol combination, it could only communicate with the blind, paired end destination, it couldn't "phone home" or attack targets of its own choice.

In the data diode, there are two mapping tables physically separated by the data diodes. The source side table maps a whitelisted data source to a channel for transfer to the destination side. On the destination side the channel is mapped to the true destination address. In this architecture, the source side doesn't know where or what the destination is. A rogue application could only communicate blindly with an unknown end point, using only the specified protocol, without receiving any kind of response in return.

1. APPLICATION WHITELISTING

CONFIGURATION & PATCH MANAGEMENT - Adversaries will always target a weak point or vulnerability. A system that is not hardened or is out of date becomes a target. Ensure systems are up to date, that external connections to the control network are limited and a secure method for introducing authenticated software patches is used.



1 Checksum on File

2 Checksum Verified Against Manifest

3 Verified Files Released, Others Quarantined

THE OWL SOLUTION

Designed to specifically address software update issues facing critical infrastructure operators, Owl developed the Secure Software Update Solution (SSUS) to help operators keep their systems current. SSUS securely transfers software patches and updates into the control center without the risk of using potentially contaminated laptops or portable media. The core data diode provides network-segmentation security while the application uses the vendor's secure hash code to verify the authenticity of each file. The files are also subject to antivirus scanning. Any issues found with the file cause it to be quarantined and prevent it from reaching the control network.

2. CONFIGURATION & PATCH MANAGEMENT

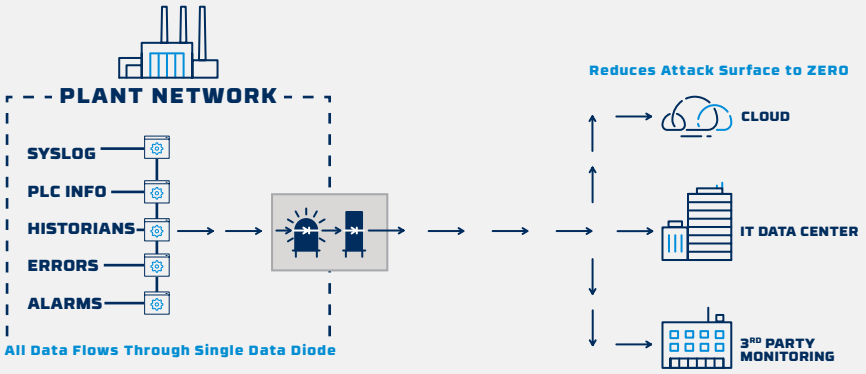
DHS Strategies:

3. REDUCE ATTACK SURFACE AREA

THE OWL SOLUTION

All Owl data diodes are based on our proprietary implementation of data diodes, and support the DHS recommendations for isolating ICS networks, locking down services, and protecting network segments. By definition, Owl data diodes only allow one-way communications over restricted paths. Not just reducing the attack surface but bringing it all the way to zero for one-way communcations. Owl also offers a bidirectional communication solution called ReCon. Two pairs of data diodes, contained within a single 1U box provide a restricted, single TCP/IP connection to provide bidirectional communication. Because data diodes are used in both directions, the layers of protection afforded to one-way communication are applied to the bidirectional solution.

REDUCE ATTACK SURFACE AREA - Isolate industrial control system (ICS) networks from untrusted networks, lock down unused services and ports, use a data diode to provide network segmentation, and if bidirectional communication is needed, use a single port over a restricted path.

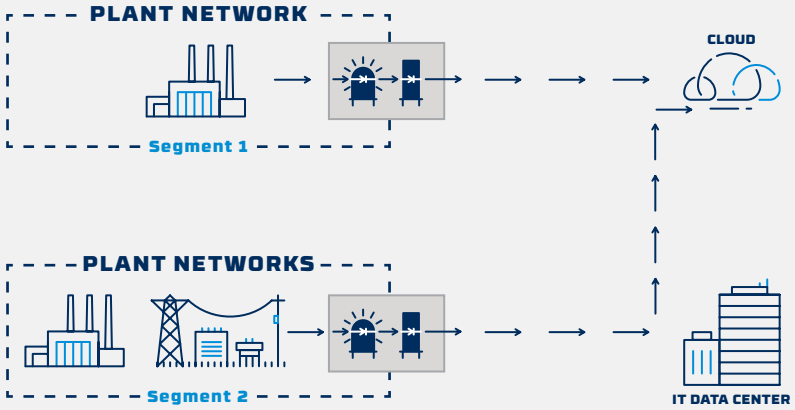


4. BUILD A DEFENSEABLE ENVIRONMENT

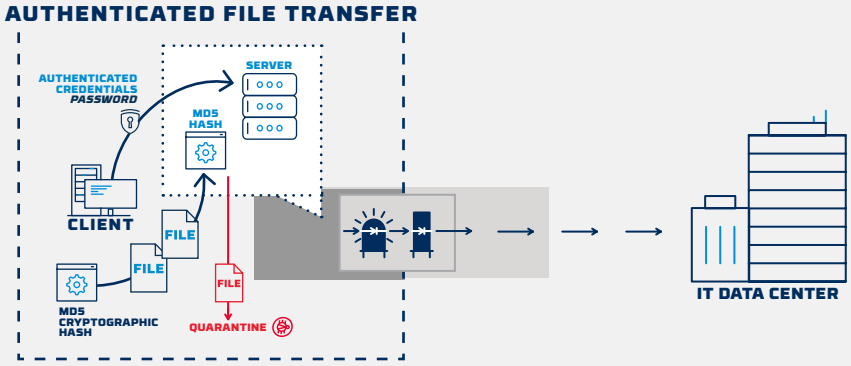
THE OWL SOLUTION

Providing network segmentation is the primary use case for Owl data diodes, which are designed specifically to allow only one-way communication. In keeping with a defense-in-depth strategy, Owl uses the ATM protocol to transfer data across the data diode, creating a protocol break between the protected network and outside threats. This restricts host-to-host paths and prevents infections from propagating from one segment to another. Data diodes do not perform or allow any IP routing and prevent all routable information (IP addresses, etc.) from ever crossing the data diode.

BUILD A DEFENDABLE ENVIRONMENT - Limit damage from network perimeter breaches. Segment networks and restrict host-to-host paths to prevent and contain the spread of infection.



MANAGE AUTHENTICATION - Prevent adversaries from masquerading as legitimate users. Stress length of passwords over complexity, reduce privileges to only those needed for each user class, change passwords at least every 90 days, require separate credentials for corporate (IT) and contol network (OT) zones.



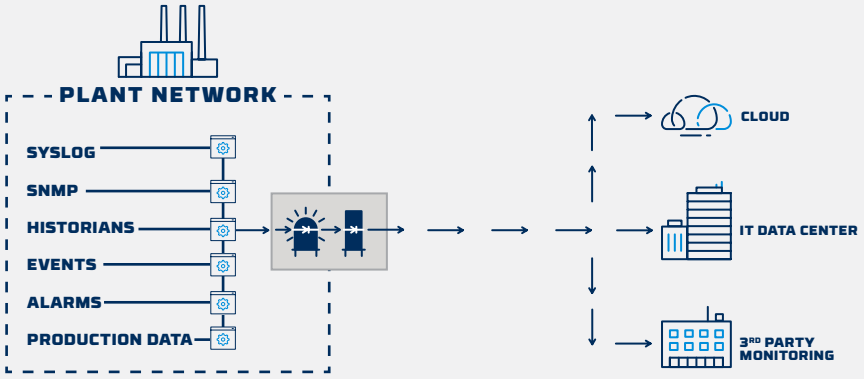
THE OWL SOLUTION

Not only do Owl data diodes follow the recommended provisions for long passwords, separating IT and OT users, changing passwords, and least privilege, it also provides authentication on the files it transfers. Using Owl's RFTS (Remote File Transfer Service), a more secure and robust version of protocols like FTP and NFS, the client/server architecture ensures unauthenticated files do not cross the data diode. The client runs outside of the data diode and is registered with the server application running on the data diode.

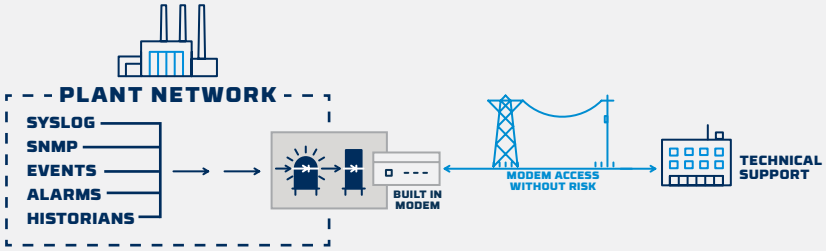
Each client user has to authenticate with the server using login ID and password over their assigned port otherwise files never even reach the data diode. The files are also assessed pre and post exchange between client/server using MD5 to make sure the correct files are queued for transfer.

5. MANAGE AUTHENTICATION

IMPLEMENT SECURE REMOTE ACCESS - Remove back doors and modem access, implement monitoring-only access, enforced by data diodes, do not rely on "read only" software configurations, and do not allow persistent remote connections.



- HARDWARE ENFORCED
- REMOTE MONITORING WITHOUT REMOTE ACCESS



THE OWL SOLUTION

Per DHS's recommendation to use data diodes, Owl data diode are specifically designed to facilitate secure, remote monitoring without incurring the risks of remote access. As a hardware-based solution, it does not rely on "read-only" software configurations, it eliminates backdoors, and monitoring information can flow across the Owl data diode to remote end-users. Remote engineers and technicians can observe systems in near real-time while equipment vendors can monitor their equipment and fulfill SLAs from centralized monitoring centers. Monitoring data can include tag information, alarms, alerts, SNMP traps, syslog messages, etc.

While modems can create risks to the control network, Owl has solved this problem by providing a data diode product that has a built-in modem. The control network is still protected behind the data diode; however, monitoring data is now available via secure remote access. The data is transferred across the data diode in the same way as on our standard data diodes and then stored on the IT side of the data diode. The built-in modem then allows remote users to "dial-in" to retrieve the data without ever opening up access to the control network.

6. IMPLEMENT SECURE REMOTE ACCESS

7. MONITOR & RESPOND

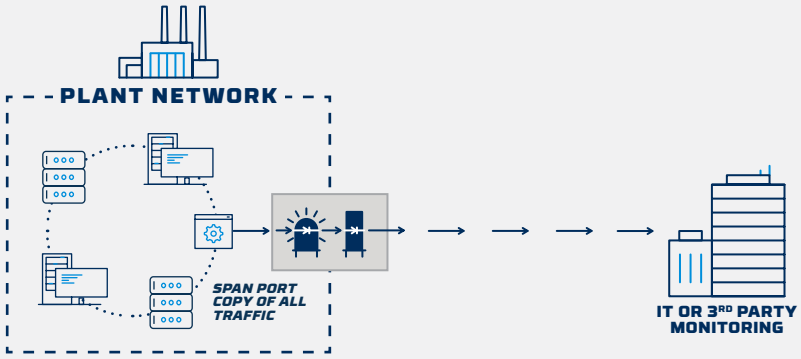
THE OWL SOLUTION

One of the options Owl data diodes provide is the ability to securely transfer network traffic to external networks for analysis. 100% of line-rate traffic can be captured and transferred to another enclave, allowing third parties to perform network analysis without ever accessing the control network.

Owl also has a product called Owl Performance Monitoring System (OPMS), which provides real-time monitoring, display and analysis of all connections between the control network and the data diode(s). OPMS will alert and notify if any data flows stop or get interrupted, which could be an indication of an attack. OPMS can also serve as a central collection point for syslog files and events, using keywords to alert staff of any activated alarms within the control network.

Since OPMS operates on the Owl data diode platform, in instances where a response plan to an attack includes disconnecting all Internet connections, OPMS can remain active. Information can continue to be transferred to external parties without creating any inbound threat vectors.

MONITOR & RESPOND - Watch traffic on ICS boundaries, monitor traffic within ICS network, use products to detect malicious software and attacks, perform login analysis, watch for access control manipulation.

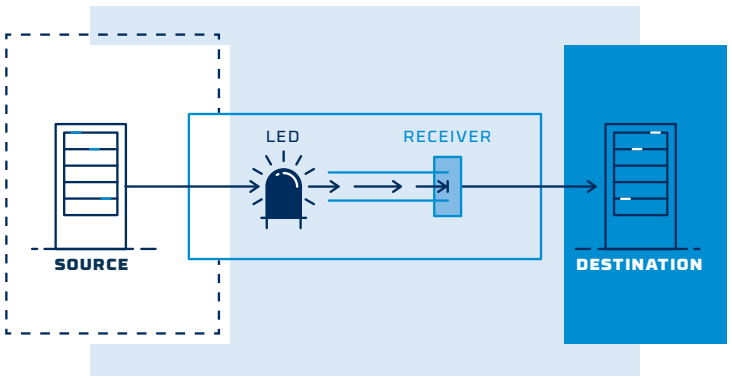


WHAT IS A DATA DIODE?

A data diode is a one-way communication device that enables the safe transfer of data between networks, and by its one-way nature provides unhackable network segmentation and security. Beyond the physical hardware that maintains a physical and electrical separation of source and destination networks, Owl intelligent data diodes include sophisticated software designed to increase security, provide unmatched connectivity and compatibility, and facilitate seamless one-way communication in a two-way world.

Intelligent data diodes effectively eliminate external points of entry to the sending system, preventing intruders and contagious elements from infiltrating the network. Securing a network's entire data outflow with data diodes makes it impossible for an untrusted network or threat actor to pass along malware, access your system, or make harmful changes.

Owl data diodes allow organizations to send data in real time to information management systems in financial, industrial, and government applications without compromising the security of their networks. Every day, data diodes protect some of the world's most valuable information and network infrastructure from theft, destruction, tampering, and human error, mitigating the potential loss of millions of dollars and countless hours of work.



OWL ADVANTAGE

THE GOLD STANDARD IN DATA DIODE TECHNOLOGY

- ONE-WAY BY DESIGN
- SECURE COMMUNICATION
- COMPLETE SEPARATION OF SOURCE & DESTINATION NETWORKS
- UNMATCHED PERFORMANCE
- UNPARALLELED SCALABILITY
- MULTIPLE FORM FACTORS
- LOWEST TOTAL COST OF OWNERSHIP
- TESTED & ACCREDITED SOLUTION
- SIMULTANEOUS MULTI-FUNCTION SOLUTION
- DEFENSE IN DEPTH
- INDUSTRY-LEADING MTBF (MEAN TIME BETWEEN FAILURE)
- FAST & EASY DEPLOYMENT

Owl Data Diode Self-Defense

You've seen how Owl's data diode solutions help operators implement the seven DHS strategies for defending industrial control systems in their networks. Owl has applied these same principles to the data diodes themselves. The architecture and design of the data diodes incorporates a true defense-in-depth model that offers layer upon layer of defensive measures that protect the data diode itself and helps ensure security policies aren't subverted through the actual devices that are supposed to be protecting the network.

The list below describes how each DHS Strategy is incorporated into the design of the Owl products for self-defense.

DHS Seven Strategies & The Owl Solution

1 **APPLICATION WHITELISTING** - The Owl data diodes protect themselves against unauthorized applications using two measures. The first is a whitelist of valid executables that are allowed to run on the data diode. The second is that under normal operating conditions, there is no mechanism for even loading files onto the data diode. This is achieved by not providing a command line interface or supporting any kind of file transfer capability through the menu system.These commands allow an application to submit a file for transfer to the HTTP proxy, running on the Source server

2 **CONFIGURATION & PATCH MANAGEMENT** - Since the data diode is hardware-based, patching is not required to keep the one-way policy in place and operational. Software changes or revisions never impact the operation of the data diode. Software patches are only needed to modify interfaces to network devices (OS changes, historians, OPC or Modbus interfaces, etc.), never to transfer data or prevent access to the network. Once the file is transferred, the HTTP application running on the Destination side of the Owl data diode receives the file

3 **REDUCE ATTACK SURFACE AREA** - The Owl system reduces its attack surface by shutting down all extraneous interfaces and services. Services like Ping can be turned off so that it cannot be identified. The only input/output are those required for data transfer. Owl provides a hardened Linux OS which is locked down according to secure operating-system guidance provided by the Center for Internet Security. Role-based menus offer additional protection during normal operation, eliminating command-line configuration and potential vulnerablilities due to command-line editing. Since the data diode is physically separated (source & destination), a privileged user on one side cannot access the other side.

4 **BUILD A DEFENDABLE ENVIRONMENT** - Owl systems have self-protection mechanisms that perform ongoing self-checks to detect changes in the applications or the configuration of the system. The solution can alarm and shutdown if the self-check fails. Changes can only be made by privileged users and need specific authorization before the system will become operational. Command-line access can create a threat vector, so during normal operation it is replaced with a role-based menu system.

5 **MANAGE AUTHENTICATION** - The Owl data diode solutions contain security measures that can support the security policies and procedures implemented in industrial control networks. Credentialed users can use passwords up to 14 characters long and password change intervals are configurable between 7 and 90 days. User roles are controlled by the Linux operating system and further constrained by the role-based menu systems with narrowly defined user roles. Not only are separate credentials for IT and OT networks required, but there is physical separation of the admin functions between OT and IT. There is no way to provision the OT side from the IT network and vice versa. In addition, the admin ports are further separated with each side having a dedicated ethernet connection distinct from data traffic.

6 **IMPLEMENT SECURE REMOTE ACCESS** - Owl provides the Owl Performance Management Service (OPMS) to remotely monitor and manage data diode solutions. Performance information, system health and application status data (log files, alarms, etc.) is supplied by both sides of the data diode and may be examined via a web-based interface. Both current and historical performance information is provided in a consolidated view. OPMS may be configured to generate email and/or SMS text alerts to notify administrators of anomalous transfer events, speeding analysis and system maintenance and/or intervention.

7 **MONITOR & RESPOND** - The Owl data diode performs self-inspection, notifying administrators of configuration or software changes that might indicate attempts to compromise the system. Extensive logging is incorporated into the data diode which can alert on abnormal activity. An auditor role is also included so that log files can be examined.

[1] *Seven Steps to Effectively Defend Industrial Control Systems*
https://ics-cert.us-cert.gov/Seven-Steps-Effectively-Defend-Industrial-Control-Systems

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.

@OwlCyberDefense 203-894-9342 | Info@owlcyberdefense.com