OWL Cyber Defense

USE CASE

Aggregated One-Way Data Transfer for CSfC Continuous Monitoring Systems

Use Case Summary

INDUSTRY

DoD/Intel

CHALLENGE

Simplify compliance by transferring log data from multiple CSfC enclaves to a single SIEM.

SOLUTION

XD Matrix

BENEFITS

Hardware-enforced one-way transfer of as many as 32 separate data flows through a single network appliance.

Cybersecurity Challenge

The National Security Agency's Commercial Solutions for Classified (CSfC) program requires continuous monitoring of network security functions.

Under the Continuous Monitoring requirements, numerous monitoring locations in CSfC's Black-Gray-Red architecture must deliver log data to Management Services systems and Security Information and Event Management (SIEM) solutions. When monitoring data is aggregated from multiple enclaves (for example, Black to Gray, or Gray to Red), an approved one-way transfer (OWT) mechanism is required to protect the independent sources from potentially malicious content. For large-scale deployments, this can result in a large concentration of OWT devices.

Compliance with these requirements using conventional OWT devices will consume an impractical amount of rack space and power. This approach will also create an administrative nightmare for network operators who need to configure, manage, and monitor an individual OWT appliance for every logging port connection.

USE CASE REQUIREMENTS

- Provide secure, hardware-enforced one-way transfer of log data to CSfC Continuous Monitoring systems.
- Reduce the number of necessary one-way transfer appliances by aggregating multiple data streams.
- Minimize latency by supporting 1Gb bandwidth for each input channel.
- Minimize SWaP-C demands.
- Deliver Syslog messages for each input channel to provide visibility into system status.

Solution

XD MATRIX

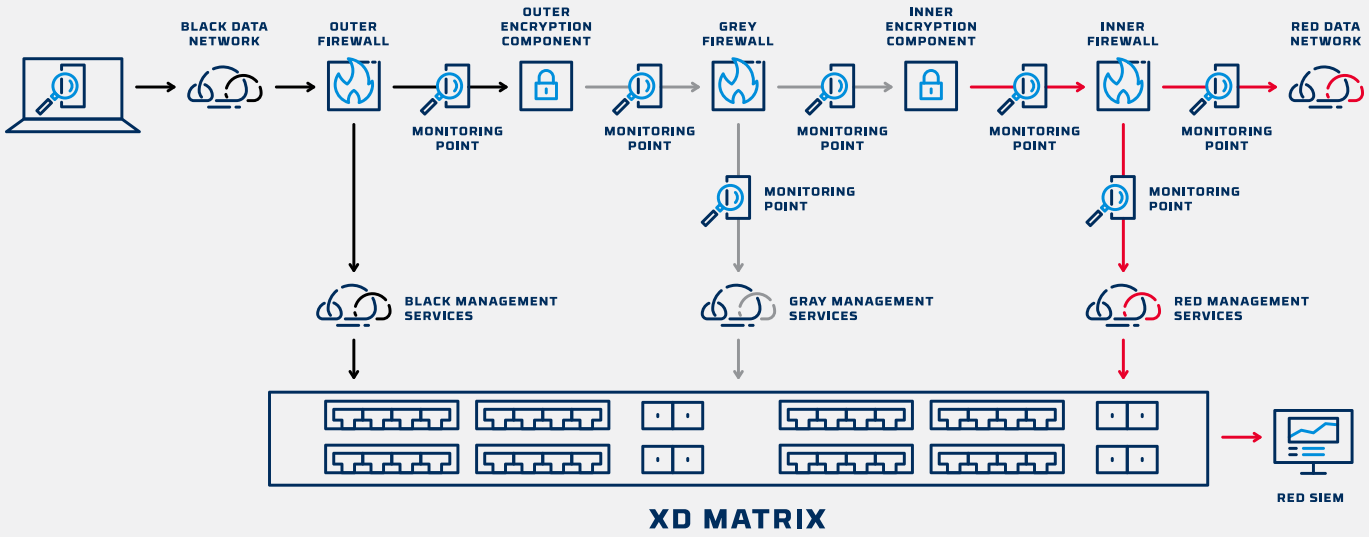
XD Matrix from Owl Cyber Defense is a one-way data transfer appliance that securely aggregates data flows and delivers them to monitoring enclaves for real-time network monitoring.

XD Matrix is a scalable solution that can aggregate between 8 – 32 1Gbe input data flows and deliver between 2- 8 10Gbe output data flows to the intended destination(s). XD Matrix enforces one-way data flow through FPGA logic and other hardware-based flow enforcement mechanisms. XD Matrix also performs FPGA-based packet level data filtering. XD Matrix's combination of hardware-based flow enforcement and packet filtering uniquely satisfies MITRE's D3FEND Network Isolation tactic through Broadcast Domain Isolation and Outbound Filtering techniques.

ARCHITECTURE

The CSfC Continuous Monitoring Annex allows for the consolidation of monitoring data from Black and Gray Networks to Gray and/or Red Management Networks to co-locate monitoring event data into a single SIEM. Consolidated monitoring can be accomplished through the implementation of "low-to-high" one-way data transfers from the Black and Gray Networks into the Gray or Red Network.

When used for consolidated monitoring, XD Matrix aggregates monitoring data from Black, Gray, and Red networks and transfers the data across hardware-enforced one-way data paths to a single Red Network SIEM.



This approach eliminates the need to purchase and support multiple SIEM solutions, and eliminates the need for security administrators to work across multiple network boundaries.