USE CASE

Continuous Monitoring for CSfC & High-Threat Networks

Unified Threat Detection with Hardware-Enforced Cross Domain Solutions

Summary

Challenges

Agencies using CSfC or collaborating with high-threat networks must maintain continuous monitoring across isolated security domains.

Solution

Owl's XD Bridge ST Cross Domain Solution together with an Owl Talon Protocol Filtering Diode provides a hardware-enforced Cross Domain Solution, securely aggregates monitoring data via NSA-approved one-way transfers.

Outcome

Secure multi-domain monitoring via centralized SIEM, compliance with rigorous U.S. Government requirements and domain separation preservation.

Challenge: Secure Continuous Monitoring

Agencies deploying Commercial Solutions for Classified (CSfC) and/or collaborating with potentially high-threat networks face a significant challenge in meeting the NSA's rigorous requirements for consolidating monitoring data across networks of different classification levels. Layered monitoring must be implemented to continuously establish baseline network behavior and promptly detect and mitigate threats.

Achieving comprehensive, real-time visibility across layered, multi-domain environments while maintaining strict separation and compliance often results in operational silos, increased complexity, and potential blind spots. Agencies need solutions that simplify compliance, streamline monitoring across domains, and ensure centralized, actionable security intelligence without compromising classified data or regulatory mandates.

Cross Domain Solutions for Secure Data Consolidation & Streamlined Monitoring

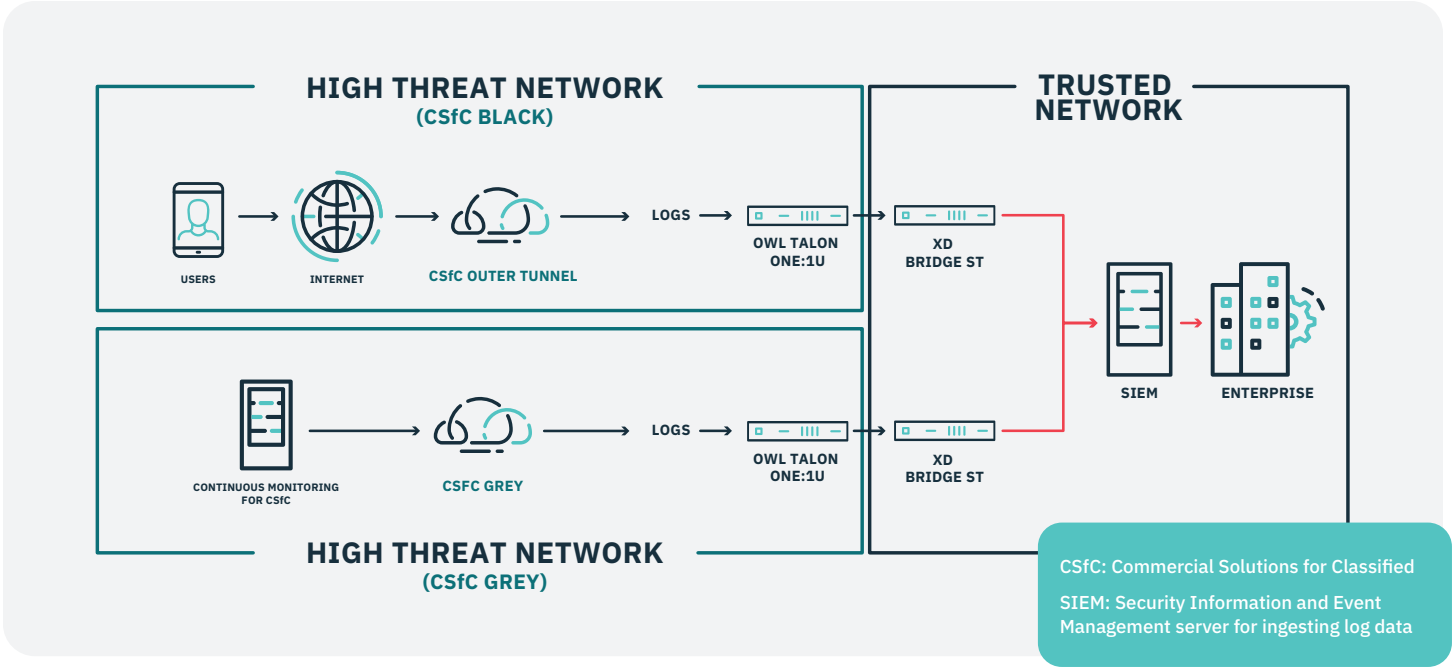
Cross Domain Solutions (CDS) enhance monitoring capabilities for both CSfC and high-threat networks (HTNs) by enabling secure data aggregation, advanced threat detection, and centralized analysis across segregated environments. Physically enforced unidirectional data flow via hardware-enforced cross domain solutions like Owl's XD Bridge ST and an Owl Talon Protocol Filtering Diode from CSfC or High Threat networks to a single SIEM prevents adversaries or threats leaking into critical networks and connects isolated security domains while maintaining data integrity.

Key Features

Improved TCO: Single SIEM instance decreases costs and improves SWaP.

Centralized Management: Move from fragmented visibility across multiple SIEMs to a single SIEM in Red that correlates events across layers for a unified view of the environment.

Meet Regulatory Requirements: Owl CDS adhere to rigorous U.S. Government standards and empowers agencies to meet the requirements of NSA's Continuous Monitoring Annex for CSfC.



How It Works

NSA guidance allows for centralizing security event data from lower-classification domains into higher ones using approved one-way cross domain solutions (CDS), but this must strictly adhere to “low-to-high” transfer policies and organizational data handling rules.

In the architecture above, a Owl Talon Protocol Filtering Diode and XD Bridge ST Cross Domain Solution deployed alongside each CSfC or high-threat network securely aggregates security monitoring log data from its associated network to a single Red Network SIEM. Hardware-enforced CDS & protocol filtering diodes guarantee network separation and one-way-only transfer for secure data aggregation from Black, and Grey high-threat networks to Red SIEMs, ensuring NSA compliance while eliminating covert channels via protocol normalization and high-throughput transfers for real-time threat detection.

Rigorously Tested Secure Data Transfer

RTB-ready XD Bridge ST is a flexible, high performance cross domain solution (CDS) providing assured transfer for streaming or posting fixed format and structured data. XD Bridge ST provides data inspection and sanitization through a comprehensive linear pipeline filtering process using validated data schemas to ensure data is “clean” prior to transfer. Owl’s linear assured pipelines enable a wide range of high-to-low and low-to-high use cases, with support for XML, USMTF, VMF, and other data formats. Owl’s XD Bridge ST is available in a variety of form factors to meet a variety of operational needs, with bandwidth capabilities up to 10 Gbps.

Owl Talon One:1U is an all-in-one protocol filtering diode designed for secure, high-speed, one-way data transfers up to 1 Gbps. Built on Owl’s next-generation Talon platform, it features a modern web-based interface, supports multiple simultaneous protocols, and offers robust, hardware-enforced security with advanced OS hardening, disk encryption, and intrusion detection. Ideal for government and critical infrastructure, it delivers reliable, easy-to-configure protection for sensitive networks.