SOLUTION BRIEF

Fortinet and Owl Security Solution

Secure, One-way Data Transfers of NOC and SOC Analytics to Fortinet Security Information and Event Management (SIEM) Solution

Executive Summary

Fortinet and Owl Cyber Defense have partnered to deliver an ultra-secure solution to transfer critical, unidirectional analytics data from a customer's operational technology (OT) environment to a security information and event management (SIEM) platform. Our joint application programming interface (API) integrated solution combines Owl Cyber Defense's industry-leading, low-latency Data Diode technology with the Fortinet award-winning FortiSIEM, to deliver maximum visibility, correlation, and automated response while reducing complexity for network and security operations teams.

Joint Solution Benefits

- Unified, real-time network analytics from various sources
- Remote access to SIEM data
- Enables quicker response time to mitigate threats
- Cross-correlation of SOC and NOC analytics
- Hardware-enforced, one-way data transfer
- Air-gapped—network physical separation
- Self-learning asset inventory
- Multitenancy for MSPs/ MSSPs
- Supports various protocols

Centralize NOC and SOC Analytics

Centralizing network operations center (NOC) and security operations center (SOC) analytics to protect your OT network can be challenging. Many organizations are adopting SIEM solutions to gain centralized visibility of critical data. However, vendors providing SIEM services can be costly and difficult to deploy, use, and set up. In addition to these challenges, managing the security and availability of the data may be difficult to maintain. Customer demands have driven vendors to address these challenges in a way that provides a unified data collection and analytical way to detect security issues from diverse information sources, including logs, performance metrics, Simple Network Management Protocol (SNMP) Traps, security alerts, and configuration changes in a secure, one-way data transfer manner.

Together, Fortinet and Owl Cyber Defense have partnered to combine solutions that provide an air-gapped, hardware-enforced, one-way data transfer of SIEM data in a NOC/SOC environment for machine and network data analytics. Owl Cyber Defense has become a member of the Fortinet Fabric-Ready Program and integrated with our open APIs to seamlessly pass data to our FortiSIEM platform. This holistic and scalable solution will provide organizations a patented view of Internet of Things (IoT) to cloud analytics that are actionable from network security and performance, and meet NIST compliance standards.

Joint Solution Description

The FortiSIEM and Owl Cyber Defense integrated solution provides a deterministic one-way transfer of secure data for SIEM delivery and the Fortinet FortiSIEM patented collection of actionable analytics to tightly manage security, performance, and compliance standards. All these capabilities are delivered through a single pane of glass. The combination of a one-way data diode and the FortiSIEM solution enables a quicker response time to prevent and mitigate threats, through the collection of logs and analysis of security events from multiple sources. The combined solution also provides a more efficient way of triaging and investigating alerts.

With the data diode providing a secure one-way path of data to the SIEM, the SIEM can quickly and automatically detect breaches and various other security concerns. With the onslaught of constant and new threats, this integration allows for security teams to keep up with a barrage of security data that is collected, wherever they are located.

By implementing data diodes and FortiSIEM, critical data can be delivered to any location for remote monitoring. Without a data diode to securely transfer SIEM data to the right destination for monitoring, organizations will need to invest in additional SOC staff inside the

secure network on a 24/7/365 rotating schedule to monitor the data. The secure remote location also provides a way to archive data successfully, serving as a backup location for organizations to rely on to preserve data.

Use Case

A power generation organization has selected Fortinet and Owl to successfully introduce one-way data diodes with FortiSIEM services to securely transfer all network data to a remote, centralized environment for business analytics to identify any malicious behavior or alerts outside of the scope of policies. This will provide the IT team with the visibility to quickly respond accordingly to address the issues before they become more serious.

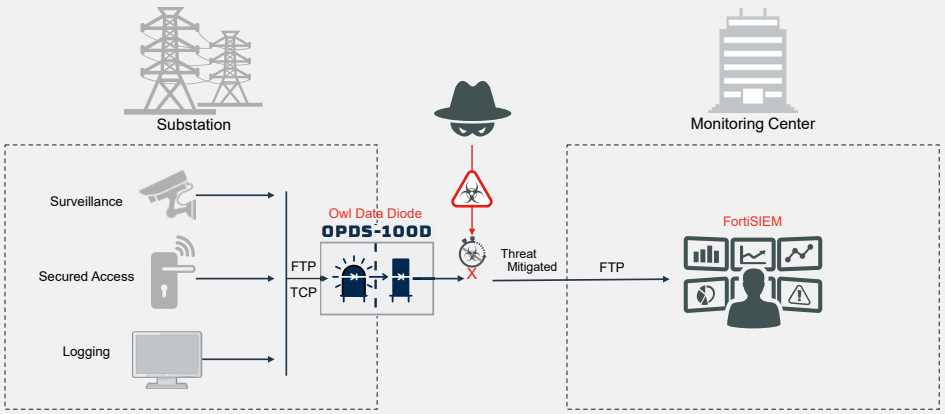
Owl's hardware-based one-way data diode will provide a secure flow of data in one direction only from the network to the FortiSIEM server. The FortiSIEM server will collect data from servers, networking equipment, security devices, and applications in real time, making it easier to detect and resolve specious activity and preserve business continuity.

Joint Solution Components

- Owl OPDS-100D one-way data diode to provide transfer of the SIEM collective data from the virtual network
- FortiSIEM supervisor virtual server to receive the parsed data in a way that is searchable for incident mitigation
- Window server to allow access to the SIEM server service by way of the URL to view the data that has been parsed from the endpoints on the network

Diagram of Joint Solution

DIAGRAM OF JOINT SOLUTION



Fortinet Security Fabric

The Fortinet Security Fabric is an architectural approach that unifies the security technologies deployed across the digital network, including multi-cloud, endpoints, email and web applications, and network access points, into a single security system integrated through a combination of open standards and a common operating system. These solutions are then enhanced through the integration of advanced threat protection technologies and a unified correlation, management, orchestration, and analysis system including FortiSIEM. Fortinet secures the largest enterprise, service provider, and government organizations around the world.

Owl Cyber Defense One-Way Data Diodes

Owl data diodes provide a deterministic, hardware-enforced, one-way data transfer of SIEM data to enable organizations to remotely monitor operational technology (OT) data, no matter their location. Data diodes sit at the edge of an OT network, physically preventing threats to the OT network, while simultaneously allowing data to transfer out of the network in a highly controlled, deterministic manner. Owl Cyber Defense Solutions, LLC leads the world in data diode and cross domain network cybersecurity, focusing on customers in the military, government, critical infrastructure, and commercial communities.

FORTINET

www.fortinet.com

June 23, 2020 12:56 AM

703061-0-0-EN

D:\Fortinet\Solution Briefs\Grey Solution Brief\Owl Cyber Defense\sb-FA-fortinet-and-owl-security-solution-6232020