SOLUTION BRIEF

OWL Cyber Defense

LogRhythm

OWL AND LOGRHYTHM

A COMPREHENSIVE SECURITY INTELLIGENCE SOLUTION FOR INCIDENT DETECTION & PREVENTION

JOINT SECURITY SOLUTION FEATURES:

- Complete network segmentation and isolation
- Hardware-enforced network security, bound by the laws of physics
- Quick mitigation and recovery from security incidents
- Identification of true behavior anomalies
- Secure bi-directional communication by using two independent, one-way paths

SECURITY PRODUCTS:

- **Owl:** ReCon, OPDS-100, OPDS-1000, OCDS-1000
- **LogRhythm:** NextGen SIEM Platform

Securely Monitor and Analyze Log Data from Sensitive Networks

Operators of sensitive networks not only have to contend with monitoring system activity, but how to access that data from their SOCs and monitoring centers. Owl world-class data diode solutions combined with LogRhythm's best-of-breed unified NextGen Security Information and Event Management (SIEM) Platform provide a seamless, highly secure solution for monitoring system data while keeping sensitive networks isolated.

Owl data diode cybersecurity devices provide hardware-enforced network isolation and secure data transfer with an in-line protocol break. This allows safe transfer of system logs from sensitive networks to the LogRhythm NextGen SIEM Platform for analysis while maintaining absolute network security assurance. Owl data diodes also don't require regular patching or maintenance to stay secure, and the enforcement mechanism never becomes less effective over time.

The LogRhythm NextGen SIEM Platform uniquely delivers enterprise-class SIEM, for centralized visibility, security analytics for threat detection, and incident response workflow automation to help you detect and respond to threats. LogRhythm accurately detects an extensive range of early indicators of compromise and provides an integrated response workflow, enabling end-to-end Threat Lifecycle Management. The deep visibility and understanding delivered by the LogRhythm NextGen SIEM Platform enables enterprises to secure their networks, comply with regulatory requirements, and increase productivity.

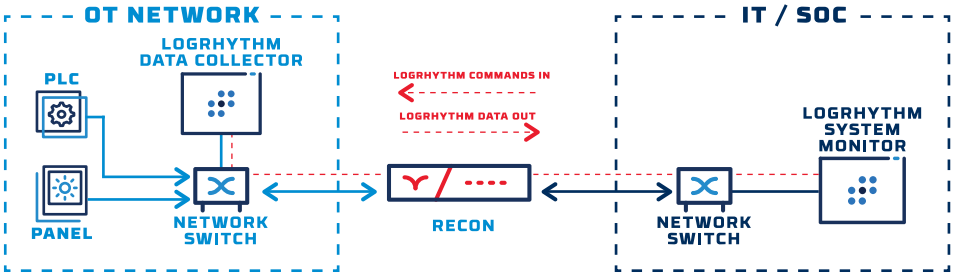
CONCLUSION

The joint Owl and LogRhythm solution empowers businesses to identify true behavioral anomalies, internal and external threats, and prevent data breaches based on accurate enterprise security intelligence — all while keeping the secure network isolated from external threats.

Use Cases

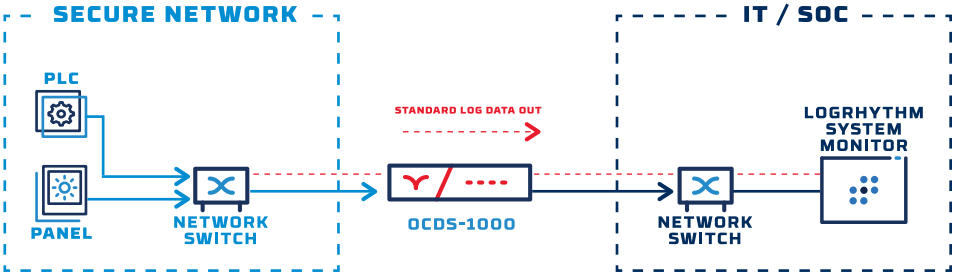
POWER GENERATION

To take full advantage of LogRhythm's detection and response capabilities, the customer utilized Owl's ReCon device for bi-directional communication. ReCon provides hardware-level network isolation, while permitting essential security actions sent from LogRhythm servers in the SOC to endpoints inside the secure network. This approach is much safer than a firewall because the solution provides a protocol break in both directions and requires matching configurations on both sides of the data diode for data to flow.



GOVERNMENT/DOD

In a situation where system logs need to be transfered to another network for evaluation, an Owl data diode or cross domain solution (CDS) can work in tandem with LogRhythm's system monitor to transfer the log data out without exposing the secure network. System log data is communicated from the secure network through the data diode/CDS to a security operations network while keeping the secure network isolated. Once transferred, the data is collected in the LogRhythm system and inspected for identification of potential threats.



ABOUT LOGRHYTHM

LogRhythm is a world leader in NextGen SIEM, empowering thousands of enterprises on six continents to successfully reduce cyber and operational risk by rapidly detecting, responding to and neutralizing damaging cyberthreats. The LogRhythm NextGen SIEM Platform combines advanced security analytics; user and entity behavior analytics (UEBA); network detection and response (NDR); and security orchestration, automation, and response (SOAR) in a single end-to-end solution. LogRhythm's technology serves as the foundation for the world's most modern enterprise security operations centers (SOCs), helping customers measurably secure their cloud, physical, and virtual infrastructures for both IT and OT environments. Built for security professionals by security professionals, the LogRhythm NextGen SIEM Platform has won countless customer and industry accolades. For more information, visit logrhythm.com.

ABOUT OWL CYBER DEFENSE

Owl Cyber Defense 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, visit owlcyberdefense.com.

@OwlCyberDefense

203-894-9342 | sales@owlcyberdefense.com