Red River's Security Operations Center as-a-Service (SOCaaS)

A well-developed and well-run Security Operations Center (SOC) can help strengthen the security posture of any business. However, building and maintaining an effective SOC in-house can be costly and complex. We can help.

GET FLEXIBLE & SCALABLE SUPPORT WITH SOCAAS

Red River's Security Operations Center as-a-Service (SOCaaS) provides 24/7/365 support, monitoring cybersecurity threats across your network(s), cloud environment(s), applications and endpoints. Our senior analysts conduct threat monitoring through industry leading cloud native SIEM (Security Information and Event Management) and AI (Artificial Intelligence) platforms to provide organizations with real-time log monitoring and analysis to detect anomalies. When a threat is detected, an analyst examines available indicators and takes appropriate actions to communicate and/or remediate the issue within strict SLAs (Service Level Agreements).

Red River's SOCaaS provides:

| Advanced Network Intrusion Detection System (NIDS) | User Behavioral Analytics | Dark Web Scans | Asset Discovery | Extended Detection and Response (XDR) |

TECHNOLOGY DECISIONS AREN'T BLACK AND WHITE. THINK RED.
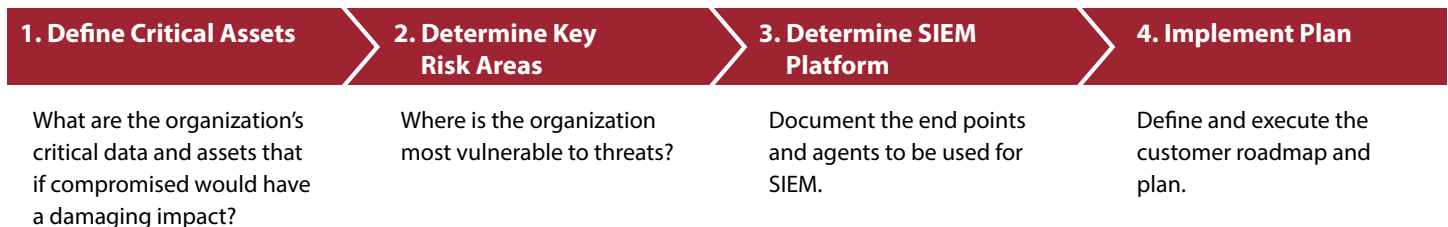
ENSURE COMPLIANCE

If your organization has an existing SOC that is not fulfilling its mission, SOCaaS defends against advanced threats and ensures compliance with regular reporting across multiple standards. Red River's approach provides customized reports, alarms, and tailored processes to meet everyday compliance challenges. The integrated SOCaaS Compliance Daily Reporting, specific compliance requirements met through SIEM content, log retention, and configuration development, sets the stage for your efforts in meeting a variety of compliance standards such as:

- CMMC
- FEDRAMP
- SOC 2, Type I/II
- PCI DSS
- HIPAA
- HITRUST
- NIST 800-53
- ISO 27001

STEPS TO TRANSITION TO SOCaaS

We help organizations evaluate their needs and leverage current processes and systems to migrate to a SOCaaS solution **with industry-leading monitoring technology**. Here are our key steps to implementing SOCaaS:

1. Define Critical Assets	2. Determine Key Risk Areas	3. Determine SIEM Platform	4. Implement Plan
What are the organization's critical data and assets that if compromised would have a damaging impact?	Where is the organization most vulnerable to threats?	Document the end points and agents to be used for SIEM.	Define and execute the customer roadmap and plan.

With our SOCaaS, you receive all of the benefits of a SOC without the cost, complexity, and time investment of an internal operation. **Contact us** today to get started.

Red River