Frontline Cyber a global IT / Cyber Security company is searching for a Security Operations Center (SOC) lead to join their team in Idaho Falls, Idaho.

Candidates must have strong SOC strategy experience.

Role:

The Security Operations Centre (SOC) lead will plan, direct, and control the SOC functions and operations. Ensure the monitoring and analysis of incidents to protect People, Technology and Process addressing all security incidents and ensuring timely escalation. Direct the Cyber Intelligence capability to identify potential threats delivering strategic reports and strategies to minimize the impact of the threat.

- Responsible for SOC strategy.
- Leading and managing the Security Operations and team of security operational staff members
- Primarily responsible for directing security event monitoring, management and response and cyber intelligence
- Ensuring incident identification, assessment, quantification, reporting, communication, mitigation, and monitoring
- Ensuring compliance to policy, process, and procedure adherence and process improvisation to achieve operational objectives
- Revising and develop processes to strengthen the current Security Operations Framework, review policies and highlight the challenges in managing SLAs
- Responsible for overall use of resources and initiation of corrective action where required for Security Operations Center
- Ensuring daily management, administration & maintenance of security devices to achieve operational effectiveness
- Ensuring threat management, threat modeling, identify threat vectors and develop use cases for security monitoring
- Creation of reports, dashboards, metrics for SOC operations and presentation to Sr. Mgmt.

QUALIFICATIONS

Required Skills/Experience

• Bachelor's degree or 4 years equivalent experience with focus in Information Security
• Ability to lead and manage a team of security engineers and analysts
• 3+ years of experience as a Senior Security Engineer
• Experience building, maintaining, and operating SIEM technologies
• Working knowledge of web application firewalls, load balancers and proxies

• Demonstrated experience in computer security combined with risk analysis, audit, and compliance objectives
• Experience with Web Vulnerability
• Experience with Application penetration testing
• Experienced with customer technology assessment and security risk analysis

Recommended Skills/Experience

• Experience supervising technical resources
• Direct interaction with customers
• CISSP certification
• Solid understanding of Project Management principles
• Familiarity with Information Security requirements of Compliance audits
• Experience with SIEM tools
• Python scripting experience
• Experience working with information security practices, networks, software, and hardware
• Expert knowledge of TCP/IP, common protocols, and standards
• Experience with DLP and IPS/IDS systems
• Experience with security scanning tools

To apply, please send your resume to contact@frontlinecyber.us