Job Title: **SOC Lead** | Reports to: **Security Practice Manager**

SUMMARY

At TBC, our core values are Passion, Partnership and Innovation. Every day our team of highly qualified engineers and administrators work hard to empower our clients to transform and grow their companies. The role of the SOC Lead is to lead the security operation team as they deliver managed security services to customers through a broad suite of information security infrastructure, work with other TBC operations teams to ensure TBC policies are followed, constantly work on improving the security of TBC and its customers, and to coordinate investigation and reporting of security incidents. Additionally, the SOC Lead will also have leadership, management and accountability responsibilities for less experienced engineers and analysts.

ESSENTIAL DUTIES AND RESPONSIBILITIES

Includes the following.

- Leadership, management and accountability for members of the security operations team
- Oversee the transition of customer services from the security delivery engineers to the security operations engineers
- Manage security responsibilities, including firewalls, proxy systems, logging, and other security devices
- Deliver excellent customer service though incident management and regular customer update meetings
- Create and review reports on security events and monitoring
- Develop and maintain security policies
- Raise awareness of security policies and develop corresponding procedures
- Provide security expertise to the company and to our clients
- Assist in the enforcement and monitoring of Compliance regulations
- Investigate and respond to security violations
- Design and conduct training for corporate security education and awareness programs
- Define security requirements and review systems to determine if they have been designed to comply with established security standards. Develop new standards as necessary.
- Establish and manage relations with vendors and related equipment suppliers
- May perform other duties as assigned

QUALIFICATIONS

Required Skills/Experience

- Bachelor's degree or 6 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
- Strong process-oriented individual with experience in ITIL concepts
- 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
- ITIL v3 or v4 Foundation Certification
- Familiarity with Information Security requirements of Compliance audits
- Experience with Splunk, Elasticsearch, and Kubernetes
- 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

HOW YOU KNOW IF THIS JOB MIGHT BE FOR YOU

A successful candidate will be well versed and capable in the following areas:

- You are motivated and driven to deliver value. You take ownership of your responsibilities and follow through on all client and team member requests and questions.
- You have deep technical skills and enjoy developing the skills of others.
- You have career goals that are aligned with a technical leadership track (management).
- You can translate business requirements into detailed technical designs.
- You like meeting and working with new people. You are comfortable engaging with people at all levels in an organization.
- You are comfortable with change and multi-tasking. You enjoy learning new concepts and are quick on your feet. When things change, you know how to "roll with the punches".

WORKING CONDITIONS

To perform this job successfully, an individual must be able to perform each essential duty satisfactorily. The requirements listed in this job description are representative of knowledge, skill and/or ability required. Reasonable accommodations will be made to enable individuals with disabilities to perform the essential functions.

A typical day in the life of a SOC Lead might include

- Meeting with and/or communicating with clients
- Leadership, management, and accountability for less experienced engineers
- Developing technical documentation for solution procedures and/or designs
- Leading solution design discussions
- Completing project deliverables
- Contributing to product development
- Work estimation and resource capacity management
- Deployment Planning & Strategy
- Deploying and testing systems-related solutions
- Working with technical writers to draft case studies and white papers
- Leveraging monitoring applications to track and manage infrastructure performance and capacity
- Participate in on-call rotations (escalation) for production support
- Vendor Management

Limited travel may be required.