

Job Title: **Senior Security Engineer** | 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 a Senior Security Engineer is to support day-to-day data security operations. He or she supports and maintains a broad suite of information security infrastructure, is accountable for security and networking infrastructure component availability and integrity, monitors compliance with IT security policy, and coordinates investigation and reporting of security incidents.

ESSENTIAL DUTIES AND RESPONSIBILITIES

Includes the following.

- Manage security responsibilities, including firewalls, proxy systems, logging, and other security devices
- Serve as an escalation point to security engineers and analysts
- Work with security architects to design solutions which scale and integrate with other TBC services
- Align services and solutions to meet the strategic needs of customers and tie TBC services to the business value they provide
- SME in multiple areas/technologies
- Deliver excellent customer service
- Train and mentor security engineers and analysts to improve their understanding and skillset
- Create and review reports on event anomalies
- 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
- Define security requirements and review systems to determine if they have been designed to comply with established security standards
- Develop new standards as necessary
- Analyze business needs, researches and recommends solutions
- Establish and manage relations with vendors and related equipment suppliers

QUALIFICATIONS

Required Skills/Experience

- B.S. Degree in Computer Science or equivalent experience
- 5+ years delivering information security infrastructure support and related services with a minimum of 8 years IT experience
- Consulting or managed services provider experience
- Working knowledge of web application firewalls, load balancers and proxies
- Experience with the design and configuration of a network DMZ
- Demonstrated experience in computer security combined with risk analysis, audit, and compliance objectives
- 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
- Strong process-oriented individual with experience in ITIL concepts
- Security + certification
- CISSP certification

Recommended Skills/Experience

- CASP, CEH, GIAC Certs or other security certifications
- Solid understanding of Project Management principles
- ITIL v3 or v4 Foundation Certification
- Familiarity with Information Security requirements of Compliance audits
- Hands on experience with Splunk, Elastic Search and ServiceNow
- Python and/or Go programming experience

HOW YOU KNOW IF THIS JOB MIGHT BE FOR YOU

- 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 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 an Senior Security Engineer might include

- Implementing and configuring security components
- Working collaboratively with team members (administrators, engineers, PM’s, etc.)
- Meeting with and/or communicating with clients
- Developing technical documentation for solution procedures and/or designs
- Leading solution design discussions
- Completing project deliverables
- Assisting with work estimation and product development
- Developing skills of and providing oversight to less experienced engineers
- Deployment Planning & Strategy
- Working with technical writers to draft case studies and white papers
- Conducting security assessments through vulnerability testing and risk analysis
- Analyzing security breaches to identify the root cause
- Performing both internal and external security audits
- Supporting Compliance audits (relating to security policy)
- Escalation for Incident Response
- Sales support, as needed

Limited travel may be required.