Sr. Security Engineer

SpearTip - Mission Statement
Blend cutting-edge technologies, unique skill sets and proven military cyber counterintelligence strategies, SpearTip partners with our Partners to protect shareholder value, shield corporate reputations and enhance long-term profits.

Core Values

TENACIOUS

- Tireless in pursuit of answers; never give up until we find a solution
- Resolute in our desire to exceed client expectations
- Insistent on holding ourselves to a higher standard

CONTINUOUS LEARNING

- Grow our people to grow the business
- Enrich our minds to improve our company culture and personal life
- Help others to excel; serve as a knowledge base for each other, our clients, and our community

CONSISTENT

- Develop, follow, and improve internal processes to achieve our corporate vision
- Listen, ask questions, get the facts, make better decisions
- Committed to be the best
- Focus, focus, focus!

ACCOUNTABLE

- Uncompromising integrity, always transparent, honest, and direct
- Treat others with dignity, care, empathy, and consideration
- Rely on others and be reliable
- Demand excellence

DECISIVE

- Get it done, don't delay it
- Overcome roadblocks, push through issues
- Act with autonomy; make intentional decisions

COLLABORATIVE

- Partner with our clients to produce superior results
- Be a team player; seek input and advice from co-workers
- Make it a practice to listen first and then be heard

Position Description
This position will be responsible for leading a team within SpearTip's Security Operations Center. The team will be focused on protecting company assets including information systems, networks, devices, and data from threats, such as security breaches, advanced malware, and other attacks by cyber-criminals.

Characteristics Requirements
Not all of the following requirements are expected for every potential candidate. SpearTip considers both the character of person and their experience when making hiring decisions. For a strong candidate, SpearTip is willing to offer training (internal and external) to fill knowledge gaps.

Personal Attributes:

- Creative brainstormer willing to build solutions collaboratively to solve complex cyber security problems
- Self-motivated, decisive decision maker with the ability to take ownership and willingness to be accountable
- Willing to stick with difficult problems to consistently produce the best solution for our partners and willing to champion new technology and different approaches
- Desires to be immersed in a training culture to both develop others and improve self

Educational and Experience:

- Computer Science, Cybersecurity, or Information Systems Bachelor's Degree or equivalent professional experience in a cybersecurity, development, or IT operations role
- Master's Degree in Cybersecurity, Computer Science, Business Administration desired but not required
- Multiple Intermediate or Expert Level Cyber Security Certifications – desired but not required (e.g. GREM, CISSP, CISM, GCIH, GCFA, etc.)
- Leadership experience and/or training desired
- Fluent in incident handling procedures (NIST.SP.800-61r2)
- Experience or knowledge of with digital forensic tools (for example, FTK, EnCase, Magnet Axiom)
- Experience or knowledge of memory forensic tools (for example, Volatility)
- Experience or knowledge of enterprise detection and response tools (Carbon Black, CrowdStrike, Sentinel One, Cylance, etc.)
- Experience or knowledge of SIEM tools (Splunk or LogRhythm)
- Proficient in Windows and Linux operating systems
- Proficient in computer networking concepts

Responsibilities:

- Responsible for leading a team of cyber security professionals within SpearTip's Security Operations Center in providing services including Risk Assessment, Incident Response, Digital Forensic, and Managed Detection and Response engagements
- Responsible for the supervision of an operations team that includes 5-6 team members
- Participate directly in and delegate tasks related to technical engagements as required
- Responsible for ensuring a good partner experience throughout the engagement and responsible for solving partner issues
- Maintain and cultivate working knowledge of Axiom, ShadowSpear, SpearPortal, and additional Digital Forensics and Managed Detection and Response tools
- Data collection, analysis, and report writing - collect and document the timeline of events, collect, analyze, and validate findings, and provide "best practice" recommendations to the client; with the understanding that your recommendations have significant impact to client operation
- When required by the nature of the engagement, act as a consulting or expert court witness
- Problem solve; independently and in a team environment

- Exercising independent judgment and discretion, communicate/coordinate with clients regarding alerts, project updates, and project status throughout an engagement
- Responsible for the timely completion of engagements and appropriately communicate project status and workload to company leadership through the required channels
- Maintain current certifications (as applicable)
- Problem solve independently and in a team environment
- Be available for short-term periodic travel to support regional, national, and international clients
- Be willing to work towards new certifications with proper training at SpearTip's expense at the discretion of company leadership
- Attend and actively participate in the Operations L10 Meetings and EOS process
- Project Management - Exercising independent judgment and discretion, communicate/coordinate with clients regarding alerts, project updates, and project status throughout an engagement
- Responsibilities subject to change at the discretion of company leadership

Benefits:

- Health Insurance Coverage – 100% coverage plan, current employee contribution is $0
- Dental & Vision Coverage – current employee contribution is $0
- Participation in 401(K) Plan, employer match of 100% for the initial 3% of contribution and 50% for next 2% of contributed funds, immediate vesting
- SpearTip approved holidays (currently 8 approved holidays)
- Personal leave days