Security Analyst

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 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 necessary knowledge gaps.

Educational and Experience:

- Computer Science, Cybersecurity, or Information Systems Bachelor's Degree or equivalent professional experience in a development or IT operations role
- Knowledge of incident handling procedures (NIST.SP.800-61r2)
- Knowledge of Windows and Linux operating systems
- Experience with security technologies (SIEM, EDR, Antivirus) desired but not required

Responsibilities:

- Triage and validate alerts from Managed Detection and Response tools
- Conduct threat intelligence research based on metadata from events to associate an event with known campaigns or threat actors
- Project Management - Exercising independent judgment and discretion, communicate/coordinate with MD&R clients regarding alerts, project updates, and project status throughout an engagement
- 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 operations
- Maintain and cultivate working knowledge of SpearPortal, ShadowSpear, and additional Managed Detection and Response tools
- Problem solve; independently and in a team environment
- Attain new technical certifications with proper training at SpearTip's expense (at the discretion of company leadership).
- Be available for short-term periodic travel to support regional, national, and international clients – with appropriate lead time
- 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