Security Analyst, ShadowSpear Overnight

Mission Statement

Our mission is simple: day by day, engagement by engagement, shift by shift, alert by alert, we defend our partners from cyber threats. Daily we save jobs, businesses, communities, governments, and livelihoods, and ultimately allow them to fulfill their own missions.

We are driven by our core values: tenacious, consistent, decisive, continuous learning, accountable and collaborative. These values define our culture, and we strive to employ technical experts who have the right character, attitude, and motivation necessary to deliver exceptional service to our clients. We are looking for new talent in the St Louis area to be a part of our growing team!

Job Description

In this role, the successful applicant will be responsible for analyzing our current managed detection and response systems and assets, recommend and implement solutions, and provide an excellent customer service experience with clear, concise, and professional communication. The overnight security analyst should have knowledge relating to maintaining software, hardware, and the ability to work independently to keep SpearTip at the forefront of threat detection and remediation. We are seeking an overnight security analyst who is ready on day one to impact the quality of our managed detection and response operations, maintain a structure with scalability, and contribute to our overall organizational growth.

Responsibilities

- Maintain and strengthen business-critical security operations and managed detection and response team
- Data Collection, Analysis, and Report Writing - collect and document the timeline of events; collect, analyze, and validate findings
- Generate, triage, and validate security alerts from managed detection and response platform
- Troubleshoot hardware and software issues as they arise related to managed detection and response footprint
- Expand and maintain working knowledge of the managed detection and response platform and SOC-utilized toolsets
- Research, recommend, and implement appropriate information security solutions to clientele
- Problem-solve independently and in a team environment
- Exercise independent judgment and discretion
- Able to work 30-day rotation of day/nightshift, as well as after-hours and/or days outside of standard shift when needed due to client requirements
- Maintain current certifications (as applicable)
- Work towards new 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
- Attend and actively participate in the L10 Meetings and EOS process
- Responsibilities subject to change at the discretion of company leadership

Required Qualifications:
We consider a candidate's character, experience, potential, and desire to learn. For a strong candidate, we offer training and company-paid certifications to fill knowledge gaps.

- Minimum 2 years of information technology education and/or experience
- Ability to communicate with diverse professionals (clients, developers, engineers, and vendors)
- Work well within a structured environment yet be adaptable to quick changes
- Clear communication skills and be able to facilitate discussions to understand/resolve problems
- Knowledge of incident handling procedures, Windows, and Linux operating systems
- Working knowledge of current cyber risks and experience implementing security solutions
- Ability to effectively prioritize and execute tasks in a high-pressure environment
- Outstanding personal and teamwork skills
- Highly self-motivated and directed
- Independent problem-solving skills
- Strong written and oral communication skills
- Availability for short-term travel to support clients (less than 15% of time)
- Ability to work on-site in St Louis, MO
- Security clearance eligibility
- Eligible to work in the United States without sponsorship

Desired Qualifications:

- Computer Science, Cybersecurity, or Information Systems Bachelor's Degree, or equivalent professional experience in a development or IT Operations role
- Industry recognized intermediate certifications: Security+, Network +, PenTest+, and CYSA (or equivalent)
- Experience with security technologies (SIEM, EDR, Antivirus)
- 2 years' experience in a customer-service setting
- Law enforcement and/or military background
- IT MSP background
- Multilingual

Additional:
At SpearTip, we strive to protect our clients 24/7, 365 days a year from the ever-evolving changes in cybersecurity. We take pride in our results and what we achieve. We recognize that life isn't all about work; we promote a culture that supports your personal goals and enriches your professional goals.

We provide excellent benefits to our team members. You could be eligible for:

• 100% employer paid health, dental and vision coverage plans for you and your family members

- 401(K) Plan with 100% employer match up to the first 5%
- Paid Time Off program and paid holidays
- Opportunities to grow and promote through employee development and employer-paid training

We want people who want to grow with us! Are you ready to lead others and stop threat actors from victimizing companies? Apply and find out!