Security Engineer

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

The Security Engineer position offers a tremendous degree of variety in a challenging, multi-faceted team-oriented environment. In this role, you will be leading a team in the continuous monitoring of our partners' systems utilizing cutting-edge EDR and SIEM technologies. You will also be evaluating our practices, advising on best practices, and leading the implementation of changes making SpearTip the premier firm for cyber security defense.

Responsibilities

- Review current system security measures and recommend/implement enhancements
- Determine security requirements by evaluating business strategies and requirements
- Research information security standards
- Create and maintain SIEM rules across multiple ingestion types
- Gather relevant threat intelligence around IOC's
- Work with Linux machines for log ingestion and EDR deployment
- Develop project timelines for ongoing system upgrades
- Ensure team members have appropriate access to the IT system based on roles
- Configuration and knowledge of Azure best practices for response
- Implement security best practices across the environment to include verbal and written policy infractions where applicable
- Promptly respond to partners' security incidents and provide thorough post-event analyses
- Engage in group collaborative projects and effectively work in a team setting
- Participate in weekly leadership meetings
- Pursue continued technical education/certifications (at SpearTip's expense)

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 3 years of information technology education and/or experience
- Knowledge of incident handling procedures, Windows, and Linux operating systems
- Proficient in the use of Endpoint Detection and Response technologies
- Experience creating and maintaining SIEM rules for a variety of log sources
- Working knowledge of current IT risks and experience implementing security solutions
- Industry recognized intermediate certifications (Security+, Network +, CYSA)
- 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:

- Industry recognized advanced/expert certifications such as GSEC, CISSP
- 2 years experience in a customer-service setting
- Law enforcement and/or military background
- IT MSP background

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! If you love finding the needle in a haystack and stopping nation-state threats, this role is for you.