

Incident Response 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

In this role, you will be leading incident response engagements and provide exceptional customer support for our clients. You will also communicate and coordinate with clients regarding alerts, project updates, and project status throughout an engagement. In addition, you will provide “best practice” recommendations to our clients with the understanding that your recommendations have significant impact to client operations.

Responsibilities

- Project Management
- Data Collection, Analysis, and Report Writing - collect and document the timeline of events; collect, analyze, and validate findings
- Conduct forensic analysis relevant to network intrusion and other cyber threats
- Oversee timely completion of engagements and appropriately communicate project status and workload to company leadership through the required channels
- Assist in triage and validate of alerts from Incident Response tools
- Maintain and cultivate working knowledge of the ShadowSpear platform and SOC utilized toolsets
- Problem-solve independently and in a team environment
- Exercise independent judgment and discretion
- Able to work after hours and/or weekends 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

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.

- 3-5 years leadership experience
- Bachelor's Degree in Cybersecurity, Computer Science, Computer Engineering, Information Systems or related disciplines
- Knowledge of Windows operating systems, systems forensics, or troubleshooting techniques
- Proficient understanding of threat modeling, operational threat intelligence, and windows systems

- Experience with computer forensics tools and image/malware analysis
- Base knowledge of the agile methodologies and frameworks for team cohesion
- 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
- Ability to effectively prioritize and execute tasks in a high-pressure environment
- Outstanding personal and teamwork skills
- Highly self-motivated and directed
- Excellent organization skills
- Ability to work onsite in St Louis, MO
- Security clearance eligibility
- Eligible to work in the United States without sponsorship
- Experience working in a team setting

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!