

Security Analyst

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

You will be primarily responsible for continuous monitoring and vulnerability scanning using various security tools to identify and deter potential incidents, network intrusions, and malware events. In addition, you will be deploying and maintaining our ShadowSpear Platform to assist in protecting our partners from falling victim to cybersecurity incidents.

Responsibilities

- Ongoing monitoring and alerting of Security Information and Event Management (SIEM) technologies
- Review and analyze log files for unusual or suspect activity
- Generate event tickets, triage, and validate alerts from Managed Detection and Response tools
- Analyze incident event data to develop preliminary root cause and corresponding remediation strategies
- Research, recommend, and implement appropriate information security solutions to our clients
- Conduct threat intelligence research
- Communicate/coordinate with our clients regarding alerts, project updates, and project statuses
- Data collection, analysis, and report writing
- Engage in group collaborative projects and effectively work in a team setting
- Learn and utilize SpearTip's ShadowSpear Platform
- 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 2 years of information technology education and/or experience
- Knowledge of incident handling procedures, Windows, and Linux operating systems
- 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 onsite 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
- Experience with security technologies (SIEM, EDR, Antivirus)
- 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! Are you ready to stop threat actors from victimizing companies and putting your response skills to the test? Apply and find out!