Job Analysis

Anthony Waterman

Department of Cybersecurity

IDS 493

Dr. Sherron Gordon-Phan

May 12th, 2024

Abstract

VerSprite Staffing connects professionals with employers to fill full-time or contracted positions. VerSprite Staffing is seemingly a good recruiting outfit with multiple job offers in security. Focusing on the Junior SOC Analyst position, I find that this is a job offers a lot for applicants. This position offers a competitive salary with minimal experience required while also offering the applicant the chance to learn new systems while gaining experience in the security field and additional exposure to security consulting. This position requires some hard and soft skills from the applicant with a primary focus of soft skills. This is due to the position of this role in the hierarchy. This role seems to offer a few unstated challenges such as learning systems, tools, and procedures. Based on the role and the requirements, I feel that this is a role I would apply for.

Junior SOC Analyst

This role is considered a blue team position in which the primary function is to protect company assets such as networks, servers, workstations, along with other things. This job post highlights these responsibilities by stating, “This position plays a critical role in protecting our client organizations by monitoring, analyzing, and responding to security events.”. We can see that this position can be considered entry level. Although the job post lacks the words “entry level”, we can ascertain that information based on a few different areas of the post. This post states, “The ideal candidate will have a strong foundation in cybersecurity principles and be eager to learn and grow their skills in a fast-paced environment.”. We can infer this position is entry level based on the ideal candidate statement. The requirement of having a strong foundation of cybersecurity principles is a key indicator of this. We can infer the nature of this position from the responsibilities section. The responsibilities section utilizes general language to describe the junior analyst’s responsibilities. An example of this language would be, “Investigate and assess potential security incidents to determine their severity and impact.”. With higher level cybersecurity positions, we would see reference to a specific tool to investigate incidents. The vague language used symbolizes the entry level nature of this position. This post does state some preferred experience however, there seems to be more of an emphasis on academic experience than professional experience. We can infer this by looking at the qualifications section. One of the qualifications is a bachelor’s degree with preferred experience in security operations and exposure to security tools. The main qualifications they want would be taught in an academic setting. This post specifically states, “strong understanding of cybersecurity principles and best practices.”. Cybersecurity principles and best practices are taught at the academic level.

Responsibilities

There are several responsibilities that come with this position. All these responsibilities utilize general wordage rather than offering specifics. Some of the responsibilities include monitoring and analyzing security alerts, investigating, and assessing security incidents, performing root cause analysis, documenting incidents, escalating incidents, assist with procedure development, staying up to date on threats/vulnerabilities, and participating in drills. We can infer a few things that would be helpful for this role that the employer does not list. One of these things being self-discipline. Self-discipline would help tremendously in this role, especially when one of the responsibilities is to constantly review new security threats or vulnerabilities. Some helpful experience for this role would be network experience or some form of network training. The post does not state network experience is required however, it's important to understand network protocols and how networks operate so the applicant can better understand how to defend the organization. The understanding of networks also allows for the applicant to know possible attack vectors.

Skills, Experience, Qualifications

This position is not demanding when it pertains to the qualifications or experience required for the position. Most of the skills required would be considered soft skills rather than hard skills. Based on the job post, we can infer they want interpersonal skills, time management skills, problem solving skills, and adaptability. They reference these skills by stating in the qualifications section that the applicant must have, "Strong communication and documentation skills…Ability to work effectively in a fast-paced and dynamic environment…Ability to

prioritize and manage multiple tasks simultaneously…Team player with strong work ethic…Excellent analytical and problem-solving skills". These statements all reflect soft skills rather than hard skills. The qualifications also list hard skills in a general form; cyber threat intelligence understanding and understanding of cybersecurity principles. Based on the setup of the job posting, we can surmise that he most important skills would be soft skills. Although this post lists hard skills above most of the soft skills, this position requires more soft skills than hard skills.

Value of Position

This position offers great value to new cybersecurity graduates due to its nature. By understanding the language used, we inferred that this position is entry level. Many cybersecurity positions require years of experience or multiple certifications. With this position requiring neither of these things, it's a great motivator for applicants to apply. Along with current motivators, this job offers some future motivators as well. Because this position offers exposure to security consulting, the applicant can look forward to learning other aspects of cybersecurity and building experience that they can transfer to another career path. The exposure to consulting and the experience gained from this position is extremely important for future growth in this industry. As stated previously, many cybersecurity positions require experience and certifications to be considered as a candidate. This entry level position gives the applicant the opportunity to earn the experience and certifications to move freely throughout the industry.

Possible Challenges

Although this position offers good benefits to an entry level employee, there may be some unstated challenges that the applicant may have to deal with. The biggest challenge would

be adjusting to a more professional work environment. Although this is not a bad thing, many positions utilize a lax approach when it comes to a work setting. Security companies often offer a very professional, almost ridged, setting due to the severity of their work. Another challenge an applicant would encounter would be the need to learn a company's systems and tools. Regardless of the professional/academic experience an applicant may have, companies generally utilize their own intranet or communication platforms. In the case of a security position, they may utilize an analysis tool the applicant is unfamiliar with. If the applicant is entry level, there may be an even larger learning curve. The need to become familiar with multiple tools and systems to the point of normal operation can be a daunting task. This severity of this challenge can be reduced based on the team dynamic highlighted in the job post.

Am I a Good Fit?

After analyzing this post, I can conclude that I am a good fit for this position. This is based on different factors ranging from my academic career to my professional career. Through my professional career, I have had the ability to build upon my soft skills, many of which directly correlate with what the job poster wants in their candidate. My ability to problem-solve, communicate, document, and multi-task all come from my professional background. These skills are highlighted in the qualifications section of the post. The post states, "excellent analytical and problem-solving skills…Strong communication and documentation skills…Ability to work effectively in a fast-paced environment". Although I offer many other skills, these soft skills align directly with what the employer wants. I also meet the qualifications for hard skills. The post states, "Strong understanding of cybersecurity principles and best practices…Strong understanding of Cyber Threat Intelligence fundamentals". I've taken classes during my academic career that have covered these areas. These classes are Cybersecurity Fundamentals

and Cybersecurity Techniques and Operations. These classes taught me how to understand the fundamental nature of cybersecurity and how to operate within this field.

Works Cited

(n.d.). *VS Staffing Jobs and Career* [Review of *VS Staffing Jobs and Career*]. Indeed. https://www.indeed.com/cmp/Vs-Staffing/jobs?jk=a22b7ab223218b86&start=0&clearPrefilter=1