IDS 493 Job Ad Research

In today's rapidly evolving digital landscape, the field of cybersecurity plays a vital role in safeguarding sensitive information and protecting against information security incidents. As aspiring professionals in the cybersecurity domain, it is crucial for us to understand the specific skills and qualifications desired by potential employers. By closely analyzing job advertisements, we can gain valuable insights into the expectations and demands of employers, assess our own skillsets, and determine our suitability for relevant positions. This essay aims to explore the skills and responsibilities outlined in a job advertisement for a Security Operations Center (SOC) Analyst, Tier 1 position, as described in a listing on Indeed.com by a company named Cybereason, while also considering how our educational background and experiences align with the requirements of the role.

SOC Analyst Tier 1 Purpose and Responsibilities

The position of SOC Analyst Tier 1 at Cybereason holds a significant role within the organization's Global Security Operations team. As a member of this elite team, the SOC Analyst Tier 1 is entrusted with providing Managed Detection and Response (MDR) and Managed Extended Detection and Response (MXDR) services to large organizations across the globe. The primary responsibility of this role is to serve as the initial point of escalation and conduct security analysis of the most critical endpoint alerts.

In addition to analyzing endpoint alerts, the SOC Analyst Tier 1 is tasked with piecing together the attack chain across complex environments, including cloud, identity, email, network, and endpoint. This comprehensive analysis aims to identify the tactics, techniques, and procedures (TTPs) employed by adversaries to better understand their actions and effectively respond to active breaches. The SOC Analyst Tier 1 actively engages in incident investigations, taking decisive steps to mitigate breaches and protect customers from advanced adversaries.

Threat hunting is another crucial duty of the SOC Analyst Tier 1, involving the proactive search for attackers or remnants of their activity across customers' environments. By leveraging their expertise, these analysts contribute to the analysis and research of new, emerging, or trending attacks, actors, malware samples, and TTPs. Furthermore, the SOC Analyst Tier 1 is expected to possess the ability to collect, process, and exploit open-source intelligence (OSINT) to enhance hunting capabilities and contribute to the creation of threat alerts.

Engaging in customer-facing interactions is an integral part of the SOC Analyst Tier 1 role at Cybereason. Effective communication is necessary not only with fellow SOC analysts but also with individuals ranging from SOC analysts to C-suite executives. This interaction allows for clear understanding and dissemination of vital information related to security incidents, investigations, and ongoing protection measures.

The purpose of the SOC Analyst Tier 1 role is to provide a strong foundation of security analysis, incident response, and threat hunting expertise within Cybereason's Global Security Operations team. This position plays a pivotal role in ensuring the effective and timely response to security incidents, as well as contributing to ongoing research and analysis to stay ahead of the evolving threat landscape. By fulfilling their responsibilities, SOC Analyst Tier 1 professionals assist in protecting organizations from cyber threats and strengthening the security posture of Cybereason's customers.

Required Skills for an SOC Analyst

The job advertisement for the SOC Analyst Tier 1 position at Cybereason provides a clear outline of the essential skills and qualifications expected from candidates. By analyzing the specific key terms and phrases mentioned in the ad, a comprehensive understanding of the required skillset can be derived. First and foremost, the ideal candidate should possess 1-3+ years of relevant cybersecurity experience, with a strong emphasis on working in security operations. This experience indicates the need for individuals who are familiar with the intricacies of security analysis, incident response, and threat mitigation.

The SOC Analyst Tier 1 position requires expertise in at least two of the following areas: endpoint security, malware analysis, threat hunting, penetration testing, incident response, reverse engineering, or digital forensics. Proficiency in modern operating systems, particularly Windows, is essential, while familiarity with OS X and Linux is advantageous. Strong knowledge of networking protocols and architectures is expected. Proficiency in scripting languages like Python, Bash, or PowerShell is crucial for enhancing task efficiency and customizing security operations.

Besides technical skills, the job ad emphasizes the importance of self-motivation, results-oriented mindset, and the ability to work independently. Strong organizational skills are necessary to handle diverse tasks and adapt to changing priorities. Constant improvement of processes and methodologies is highly valued in Cybereason's SOC Analyst Tier 1 position. Effective communication skills, both verbal and written, are essential for interactions across different levels of the organization, facilitating clear communication of technical information to non-technical individuals.

Skills that have already Been Developed

Having reviewed the listed foundational requirements for this position, I think many of my skills line up quite well for this position. I have an aptitude in all of the operating systems listed, as well as experience with the Python, Bash, and Powershell scripting languages. Having completed coursework in my studies at ODU, I’ve also performed analysis of malicious traffic and breached networks, as well as written research papers on these breaches. I already have a number of years of customer service experience as well, and am familiar with many of the environments they list that are required to be familiar with when responding to security breaches.

Skills That Require Development

The job listing specifies experience in digital forensics by name as one of the skills that they look for. I will be taking a digital forensics class in the fall that would directly apply here, but in addition fulfilling more of the other requirements would be excellent for this job and others, such as getting experience with the reverse engineering of malware.

Conclusion

In conclusion, the job advertisement for the SOC Analyst Tier 1 position at Cybereason highlights the desired skills and qualifications for candidates. The role involves crucial responsibilities such as security analysis, threat hunting, and effective communication. The required skills include expertise in cybersecurity domains, knowledge of operating systems and scripting languages, and personal qualities like self-motivation and organizational skills. While my skills align with some requirements, further development of my skills would improve my chances. Continuous learning is vital in this field's dynamic landscape.

References

Security *Operations Center (SOC) Analyst, Tier 1 (Eastern US). Remote.* (2023) Retrieved July 7, 2023, from https://www.indeed.com/jobs?q=cybersecurity&l=Remote&sc=0kf%3Aattr%28DSQF7%29%3B&rbl=Remote&jlid=aaa2b906602aa8f5&vjk=6593498fd562c6f3