Cybersecurity Specialist at Cyber Defense Labs - Job Ad Analysis

Rebecca Hight

Old Dominion University

IDS 493

Dr. Sherron Gordon-Phan

October 29, 2024

Abstract

This analysis explores the role of a Cybersecurity Specialist at Cyber Defense Labs, a position that aligns well with my skills and my degree in Cybercrime. The job focuses on strengthening a client's security through Identity and Access Management (IAM) and Privileged Identity Management (PIM), areas that compliment my degree and career goals. Some key responsibilities are assessing security measures, detecting and addressing threats, ensuring compliance, and managing security tools like SIEM and EDR. In addition to technical expertise, the job also seeks problem-solving skills that are essential for working with clients and collaborating with teams. Reflecting on my own skills, I feel my academic and internship experiences have prepared me for this position. However, there are areas for growth, like advanced knowledge in PAM and understanding industry compliance. I chose this job posting for my analysis because it perfectly captures a mix of technical and strategic skills in the cybersecurity field.

Cybersecurity Specialist at Cyber Defense Labs - Job Ad Analysis

Phoenix, Arizona based cybersecurity consulting services company, Cyber Defense Labs is currently looking for a Cybersecurity Specialist. The job role of the applicant will be a senior advisor within the organization, and the focus will be on working with a selected client on-site. In this position, the applicant will be responsible for enhancing and strengthening the client's Identity and Access Management (IAM) and Privileged Identity Management (PIM) environments. This position will include protecting client systems and information. The Cybersecurity Specialist is responsible for protecting and assessing the organization's networks, detecting intrusions, and supervising compliance involving IT standards and regulations (Gooch, 2024). Another important duty of the Specialist is to deploy and manage tools that are an organization's primary defense, such as critical security systems like Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and Privileged Access Management (PAM).

Due to the growing threat landscape in cybersecurity, Cyber Defense Labs needs an experienced Specialist who would be ready to solve both short-term and long-term problems. It combines technical expertise with critical thinking, and it gives the Specialist the task of managing incidents and addressing potential threats, all while aligning with business and industy standards. Additionally, because there is a focus on the on-site interaction with the client, this position highlights adaptability, teamwork, client-focused service, and access to the client's most valuable data and systems.

Key Responsibilities and Essential Skills

A Cybersecurity Specialist is a versatile position that requires knowledge in all kinds of cybersecurity areas and a drive in threat prevention. One of its key tasks is IAM and PIM solutions, which includes the designing, implementation, and administration of effective user access rights. This aspect of the role is very important in protecting a client's assets, as client's are able to grant access to the privileged areas of the system to any employee of their choice. Other important tasks include the administration of password management procedures, where the Specialist would ensure the implementation of strict password policies, frequent password changes, and proper password storage measures, which are essential in combating unauthorized access in cybersecurity (Gooch, 2024).

The Specialist will also install and manage security solutions for 24/7 monitoring, threat identification, and management of incidents, with most of them regarding SIEM, EDR, or PAM software. These tools are very important in assessing and countering threats in real-time. Furthermore, the Specialist will analyze, isolate, and resolve any security breaches. This job role requires strong technical expertise, problem-solving skills in a high-pressure environment, and the ability to analyze information with little oversight.

Aside from the technical expertise of the Specialist, the applicant will be responsible for developing security strategies with the IT department. This means that any cybersecurity solutions should be in compliance with privacy laws and laws like the GDPR, and HIPAA, but they should also support a businesses objectives and mission. In addition, Cyber Defense Labs recognizes the need to monitor new trends in the field, making research and professional development a key aspect of this job position.

Implied Skills and Attributes

Although the job description of Cybersecurity Specialist at Cyber Defense Labs lists several technical and strategic requirements, there are a few more soft skills or personal traits that are essential. First, multitasking is essential because the Specialist will have to work with several citical and sensitive processes simultaneously, such as the administration of IAM solutions and addressing cyber related incidents. This can also be implied given the work setting of the position, which requires on-site presence, which requires efficient time management to ensure timely and efficient delivery of client security needs.

Moreover, flexibility is mentioned as one of the skills outlined in the job description. The field of cybersecurity is relatively new, and professionals in this field need to adapt their mindset and skills to risks and new laws and regulations that frequently change. This requirement comes from the fact that to be effective, and the Specialist needs to evaluate and implement new cybersecurity trends in the client's infosec environment regularly. Additionally, interpersonal skills are essential since the specialist will be communicating with cross-functional teams, translating technical information to individuals who may not fully understand it, and building trust with clients by safeguarding their systems.

Personal Reflection on Preparedness

After considering the job description of the Cybersecurity Specialist, I realize that my academic knowledge and current internship experience have provided me with a solid foundation in principles of cybersecurity, which would align well to this job. In previous coursework, I have read and discussed information on Identity and Access Management and Privileged Identity Management systems, which has given me an understanding of access control solutions. I have used practical cybersecurity labs that have taught me about SIEM and EDR, which allows me to monitor and respond to threats in real-time.

As for interpersonal skills, my time spent working in customer-oriented positions as previous a law enforcement officer has provided me with good interpersonal and analytical skills, which are useful when it comes to handling an incident and presenting security issues to other groups. In addition, I have the ability to make schedules, prioritize tasks, and manage pressuring tasks, which is a crucial factor that will help me perform well in the highly dynamic environment of Cyber Defense Labs.

Identified Areas for Further Development

Although I have a strong understanding of security concepts, there are a few areas that I am aware will require me to grasp more firmly in order to meet the requirements of the Cybersecurity Specialist position. For example, I have worked with several security tools, but I plan on furthering my knowledge of systems mentioned in the job ad such as PAM and other complex SIEM configurations. More exposure with these tools would give me a better understanding on the threat identification and incident management processes.

Other areas that need improvement are regulations and industry benchmarks. I plan to study and obtain the certification of CISSP to gain more understanding and knowledge of compliance, such as GDPR and HIPAA, in order to align security practices with business and legal requirements. Obtaining a certification such as CISSP will not only strengthen my credentials in the field, but will also show my employer my dedication to his/her organization and highlight the fact that I am aware of current industry knowledge, which will provide me with the leverage I need to succed in this career field.

Conclusion

Cyber Defense Labs offers an opportunity to join its team as a Cybersecurity Specialist and strengthen and develop in a client-oriented cybersecurity consulting firm. The fact that this role

includes Identity and Access Management, Privileged Identity Management, and threat response aligns with my goal of building up work experience as a strong Cybersecurity Analyst. Based on my current experience and leveraging the fields of knowledge in PAM, SIEM, and regulatory compliance, I'm committed to becoming a well-rounded Cybersecurity Specialist. I hope to not only tackle technical challenges, but also with the right certifications and knowledge, help protect data, systems, and assets from cyber threats, adding value to the cybersecurity industry within a job position such as a Cybersecurity Speciailist at Cyber Defense Labs.

References

Harris, R., & Clayton, B. (2019). Editorial: The importance of skills – but which skills? *International Journal of Training Research*, 17(3), 195–199. https://doi.org/10.1080/14480220.2018.1576330

Burry, M. (2022, February 1). *How to decode a job advertisement*. The Balance. https://www.thebalancemoney.com/how-to-decode-a-job-advertisement-2061002

Henry, H. (2019, August 20). *Top soft skills in the 21st Century workplace*. Junior Achievement of South Florida. https://jasouthflorida.org/top-soft-skills-in-the-21st-century-workplace/

Gooch, C. (2024, October 23). *Cyber Defense Labs hiring cybersecurity specialist in Phoenix, AZ*. LinkedIn. https://www.linkedin.com/jobs/view/cybersecurity-specialist-at-cyber-defense-labs-4057810987/