Cybersecurity Opportunities: An analysis of Job Posting

Danny Choi

Old Dominion University

IDS 493 – IDS Electronic Portfolio Project

Dr. Sherron Gordon-Phan

October 28, 2025

Abstract

Job postings are prevalent, and the requirements to get hired can be found through an analysis of the posting. Finding key terms and comparing qualifications are successful methods for figuring out how suitable a role is. A job posting by Leidos was discovered, as a SOC analyst, and the listing was deeply analyzed to figure out the requirements, company environment, outlook, and how to prepare for the role.

Basic and preferred qualifications were observed, along with duties and responsibilities, while sharing personal thoughts and opinions on personal challenges, suitability, and motivation. The analysis threaded the water and was able to establish not just the technical skills or "hard skills," but also explored the soft skills and the requirements that aren't mentioned.

Information Technology (IT) is a field that has a plethora of expertise and opportunities, and I have decided to pursue my career in it. Life after college is daunting, but having a field that aligns with my interest makes the transition a lot easier and exciting. I am set to graduate next spring with a BS in Cybersecurity, and the hunt for the next step in my career has begun. Upon scouring the internet for job postings, I've come to a role that I believe would best fit my skillset. The role is for a Security Operations Center (SOC) Analyst for a company called Leidos. Luckily, my route to college has been a bit non-traditional, and in this essay, I will analyze the job description and examine what the company does, what the purpose and my responsibilities would be, the future outlook, what the skillsets and requirements are, and how my career so far has prepared me, as well as the challenges I expect to face. I will break down the job posting and analyze why I believe I would be a good candidate for this opportunity.

Company Overview and Job Purpose

Leidos is a company that has been operating for over half a century that specializes in science and technology "to deliver critical solutions to [their] customers' most demanding challenges" (Leidos, n.d.). Essentially, Leidos is a contractor that receives said contracts from different entities and sectors, like the government, and provides services and solutions to support different kinds of operations, research, and technology. The job listing is for a SOC analyst role to support the Department of Defense's (DoD) Fourth Estate Defense Agencies and Field Activities, which falls under the Defense Enclave Services contract. The contract's goal is to consolidate and refine the DoD's IT infrastructure, resources, and personnel, with the main objective being to enhance network capabilities

and security. The role of the SOC analyst is very crucial and would ensure the cybersecurity of said systems is up-to-date and secure, addressing vulnerabilities and threats while maintaining a secure network through different techniques like incident response and continuous monitoring.

The job description highlights the need for a strong cybersecurity background, primarily focused on Microsoft's cybersecurity solution. I would need to be able to work well in a team environment, cooperating with different IT teams as well as clients, analyzing, integrating, and distributing different cybersecurity solutions. These highlights suggest the importance of not just technical skills but having a balance of soft and hard skills, like communication and people skills.

Key Responsibilities and Duties

The Security Operations Center (SOC) is a centralized unit found within an organization that is responsible for monitoring, detecting, and reacting to cybersecurity threats in real-time while upholding the organization's information systems. The SOC analyst would be involved in supporting operations in the SOC, with operations including tasks such as incident investigation and monitoring, managing security alerts, determining resolutions, etc. The SOC analyst would be a crucial member of that team to satisfy and fulfill clients' needs and expectations. There are many roles a SOC analyst could fulfill, but for this specific listing, the specific roles and major responsibilities mentioned are incident response and recovery, monitoring and analysis, collaboration, reporting and documentation, and root cause analysis. These are some of the tasks and responsibilities that are expected to be completed daily. This doesn't include any further training, such as

cyber awareness and any other certifications that would improve security posture not just for me but for the organization. Leidos places an emphasis on creating a culture of readiness and vigilance to continue preparing for the ever-changing security landscape.

Skills and Qualifications Requirements

The job posting highlights several qualifications that are required for the role, including technical skills as well as experience. The qualifications include a bachelor's degree in a relevant field, typically something like cybersecurity or computer science, with at least 5 years of experience in a related role. Certifications, specifically DoD IAT Level II, like Security+ or CISSP, are desired, along with experience and knowledge of different network hardware and software topography to troubleshoot and investigate incidents effectively, while being able to triage, mitigate, and document these threats. Having a great understanding of not just the latest cybersecurity threats, but also of the tools, assets, and antivirus that are effective and widely used in the industry, is important. These qualifications highlight the desire from Leidos to hire someone who is not only technically sound but also able to manage and solve complex situations with limited supervision.

Reading between the lines

The job listing mainly highlights the technical skills that they would like when hiring someone, but there are implications for soft skills and qualities throughout the posting. For example, one of the main characteristics of the role is team collaboration. I inferred that this essentially means they are looking for someone with great communication and people skills. The importance of team collaboration is greatly emphasized, as one of the main tasks and responsibilities is the preparation of documentation and briefings to present to team

members and upper management, while also coordinating and organizing with other teams. Having effective communication is important, as it allows for a shared understanding of what needs to be done, which in turn allows for greater coordination to maximize efficiency and effectiveness.

Another aspect that can be built off communication is customer service. The role will involve effectively dealing with not only team members but also clients and customers who have services through Leidos. This includes not just average civilians but can also include government, military, and businesses that Leidos has contracts with. The listing says they want someone "who fits mold … someone who melts it down" (Leidos, 2025). Being able to break down confusing and challenging networking and cybersecurity terminology to get the message across effectively is important and highly suggested.

Additionally, the job posting mentions one of Leidos' quotes: "the restless, the over-caffeinated, the ones who ask, 'what's next?'" (Leidos, n.d.). This saying suggests the company culture, and Leidos highly emphasizes adaptability as well as initiative. This showcases the fast-paced environment and the ever-changing security landscape, and the ones who succeed are those that remain vigilant and ready to accept the challenge.

Future Indicators

Cybersecurity is a field that is continuing to grow as the world becomes more reliant on technology. However, due to this reliance, cyberattacks continue to grow. According to the Global Cybersecurity Outlook 2025, a survey concluded that 49% of companies believe that they "do not have the workforce to meet their cybersecurity objectives" (World Economic Forum, 2025). The demand for cybersecurity-skilled applicants is growing as the

lack of skilled cybersecurity specialists continues to grow. Leidos is a major company that plays into the cybersecurity sector, and having the ability to be a part of this will allow me to continue learning as well as grow in my career. For this role specifically, being able to support a government-supported contract will allow me to develop specialty and expertise in cybersecurity for government sectors and continue pursuing my aspirations and personal motivations.

Personal Motivations

I've always been interested in technology as a kid and always wanted to pursue a career in this field. Being prior military, the federal contracting side is something that I am currently pursuing. Leidos is a leading innovator in technology and cybersecurity, so I would like to learn from the best. I believe my educational background as well as my experience would make me an ideal candidate for this role. I was in the military and served as an Information Technology Specialist. This role included network management, technical support and training, mission support, just to name a few. I was able to learn the basics of what makes a network and was often given troubleshooting tasks that made me critically think toward a resolution. I was able to learn the basics of network monitoring, proper documentation, and team collaboration, which are all vital components of this job listing. To further add onto this, I am currently a system administrator for Apex Systems, where I am continuing to grow my knowledge of networking while dealing with customers.

For education, I am currently getting my Bachelors in Cybersecurity, and I have one of the required certifications, which is Security+, and am working towards another

certification called CYSA+. I believe that my experience, as well as my educational background, make me a strong candidate to fulfill this role.

Challenges

The biggest challenge I personally would face would be changing from a networking position to cybersecurity. Cybersecurity and networking go hand in hand, but they do have major differences that would make it challenging. The listing mentions monitoring tools, or tools in general. For networking, we use tools like Putty, Wireshark, and virtual machines, which cybersecurity also uses, but the implications would be different. The ad tone is something that gives me positive reinforcement—or I should say motivates me—to challenge myself: "If you're already scheming step 20 while everyone else is still debating step 2… good. You'll fit right in" (Leidos, 2025). This is something that I should get plastered on my wall, so every day I wake up motivated and ready to take on the challenges of the world. The job posting overall does a great job of framing the role and challenges that come with it; it is a rewarding and great opportunity, highlighting Leidos as a whole.

Conclusion

In conclusion, the Leidos SOC analyst position is something that I would be greatly interested in and aligns perfectly with my goals. It is an entry-to-mid-level position that is not only technical but also requires soft skills to adapt to the changing security landscape. I've highlighted the roles and responsibilities, outlook, requirements for this job listing, as well as why I would be a good fit, along with challenges that I might face with this role. Overall, this is a great opportunity that will allow me to contribute greatly to addressing

growing cyberattacks, while learning and developing my expertise working for a great company like Leidos.

References

Leidos. (n.d.). *Our history*. Leidos. https://www.leidos.com/company/history

Leidos. (2025, October 21). *SOC Analyst*. ClearanceJobs. https://www.clearancejobs.com/jobs/8602843/soc-analyst

World Economic Forum. (2025, January 13). *Global Cybersecurity Outlook 2025*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf