Cybersecurity Analyst Job Analysis

Kunal Patel

Old Dominion University

IDS 493 (Electronic Portfolio Project)

Dr. Gordan Phan

10-28-2025

Abstract

This is a study of the cyber security analyst job posting posted by General Dynamics Information Technology (GDIT) and this position requires experience and proficiency with network monitoring devices and technical expertise as well as problem solving ability; In addition to reviewing the applicants education history, the paper reviews the job requirements and job duties; Furthermore, the paper will evaluate the culture and expectations of the company and highlight the necessity of both hard and soft skills to fulfill the responsibilities of the job; The paper also connects the skills required to perform the responsibilities of the job posting to course work and internship experiences.

Introduction

Cybersecurity is a rapidly growing area of employment that requires more experienced and qualified employees. With increasing demands for cyber-protective employees, federal and national security agencies are in particular need of highly skilled workers. As such, working as a Cybersecurity Analyst at General Dynamics Information Technology (GDIT) represents a chance to work in a constantly changing environment. My desire for innovative solutions and my interest in national defense make GDIT a great place to start or continue a career in cybersecurity; therefore, this paper analyzes the job posting for a Cybersecurity Analyst at GDIT and examines both the requirements of the job postings for the Cybersecurity Analyst position and how my educational and internship experience have prepared me to meet those requirements. Through an examination of the company's culture, the specific responsibilities of the Cybersecurity Analyst position, and the current trends in the cybersecurity profession, this paper clearly demonstrates why I would be a strong applicant for the Cybersecurity Analyst position at GDIT.

Summary of the Job and Responsibilities

Cybersecurity Analyst, GDIT is a Full-Time Position in Manassas, VA that supports the Department of State. The role of the Cybersecurity Analyst is critical to protecting the Nation's Digital Infrastructure by Monitoring Systems, supporting Cyber Mission Objectives, and providing an additional layer of protection to support the Department of State's cyber mission. To be eligible for this position, the candidate will need to have a valid Top-Secret SCI Clearance, as all work will be classified. In addition to the classification requirements, the candidate must have the ability to perform routine maintenance (patching, Firmware Updates, Configuration

Changes) and troubleshooting on a day-to-day basis. The Cybersecurity Analyst will escalate any unresolved technical issues to Senior Technicians or Engineering Staff when necessary. Additionally, the posting lists tools that the Cybersecurity Analyst will be required to utilize, including but not limited to: Splunk, ScienceLogic, Tenable Security Center, and Symantec Endpoint Protection. As well as the requirement of the candidate having extensive knowledge of Cisco Networking Equipment, VMWare Products, and an understanding of Core Concepts relating to Network, Compute, and Storage Systems.

In addition to the Technical Requirements of the Role, the Cybersecurity Analyst will also be expected to document Incidents, Procedures, and Lessons Learned. Documentation will ensure continuous improvements in Incident Response Processes and Support Operational Readiness. This Combination of Technical Knowledge, Attention to Detail, and Communication Skills is essential in performing the duties and responsibilities associated with this Role.

Additional Skills, Experience, and Training

Although the advertisement lists an array of technical skills required for the position, other skills could also be advantageous in completing the duties of this job. The requirement for handling time-sensitive work appears to be essential based on the use of language such as "respond to alerts and incidents timely," suggesting that working under pressure will likely be necessary due to the urgency indicated using "alerts" and "incidents." In addition to the routine maintenance activities that appear in the job posting, regarding organizing and tracking the numerous incidents and updates expected to be generated from the work, it is suggested that the individual will need strong organizational skills. While the requirement for security clearance and the type of work described imply that the employer expects the candidate to have high levels of trustworthiness and discretion, these expectations are not explicitly stated in the job posting.

Company Culture and Fit

The General Dynamics Information Technology (GDIT) has been providing deep and ongoing support for the United States Government in its missions, especially as it relates to Cyber Security. The language that was used in the advertisement ("impactful work", etc.) illustrates a very strong sense of a company with a "mission". The company also promotes an innovative work environment using "AI-powered career tools" and a very strong Internal Mobility Team to help employees grow in their careers. In addition, the advertisement states that GDIT has "an award-winning culture of innovation" and emphasizes Work-Life Balance through its Comprehensive Benefits Package and Paid Time Off. Given these company values, I believe a candidate for the Cyber Security Analyst job at GDIT should have the technical skills to do the job and have a commitment to National Security as part of their responsibility. It also appears that the work environment will be very collaborative, there will be opportunities for continual learning, and there will be many options for Career Advancement. Based on my Background in cybersecurity and my passion for protecting Critical Infrastructures, I believe I am a good match for this type of company culture.

Motivators and Future Growth

Cybersecurity is quickly becoming a high-demand job market as many government agencies and defense-related organizations increase hiring to meet their cyber mission objectives. Organizations such as GDIT will continue to invest in their Cyber Security Teams due to the continually evolving threat environment and increasing sophistication of cyber threats against organizations with critical information and/or systems. The advertisement for GDIT indicates that GDIT has "many pathways to build a fulfilling career while supporting cyber missions," which matches the growing need for well-trained professionals in this sector. Furthermore, the increasing adoption of emerging technologies, including Artificial Intelligence (AI) and Machine Learning (ML), and Cloud Computing, is creating an unprecedented opportunity for professionals to acquire knowledge of and adapt to the latest tools and methodologies used by professionals to combat cyber threats. GDIT's focus on developing AI-based career development tools and Digital Modernization demonstrates GDIT's commitment to being a leader in these areas of innovation, providing a significant opportunity for career growth in cutting-edge aspects of cybersecurity.

Why I'm a Good Fit

Based on both my academic and internship experiences within Cybersecurity, I believe that I would be an excellent fit for the position you are offering. I've had extensive training and hands-on experience working with Network Monitoring Tools such as Splunk and Tenable Security Center. I also have a solid understanding of many of the fundamental security practices and protocols, such as patch management, firewall configurations, and system troubleshooting. The education I received in Computer Networks and Cybersecurity provided me with the technical knowledge required for the position; however, the internship experiences I had allowed me to hone my problem-solving skills and build upon those communication skills, which the job description emphasizes.

Conclusion

This role as a Cybersecurity Analyst at General Dynamics Information Technology is a highly rewarding position where you can be a part of advancing technology for national security. The requirements of the role include both the technical skills set necessary for the position and your ability to solve problems and communicate effectively; each of these aspects is outlined within the job advertisement. Based upon my education in cybersecurity and my internship experiences, I believe I have developed the knowledge base and skills needed to meet the demands of this position. I also believe that General Dynamics' commitment to innovation, employee growth, and collaborative work environments will provide me with the best possible opportunity to grow professionally and contribute to the advancement of the cybersecurity field. I feel that my skills, experience, and enthusiasm for the field of cybersecurity will enable me to be competitive for this position.

References

General Dynamics Information Technology. (2023). *Cybersecurity Analyst job post*. Indeed. https://www.indeed.com/viewjob?jk=133b7e6a62d1d6ed

Harper, J., Atkinson, R., Henry, M., Harris, P., & Clayton, S. (2022). *Cybersecurity: Concepts and practices*. XYZ Publishing.