Writing Assignment One: Job Analysis

Ashley Barasebwa

Old Dominion University

IDS 493

Dr. Gordon-Phan

January 31, 2025

Abstract

This paper will discuss a job posting for a Cyber Security Engineer position at Lockheed Martin, examining the company's mission, the role's responsibilities, and the qualifications required for candidates. The analysis explores the explicit and implicit skills mentioned in the advertisement, such as proficiency in Linux and Windows operating systems, experience with vulnerability scanning, and knowledge of risk management frameworks. Also, the job advertisement’s structure and phrasing provide insight into the company’s expectations, including teamwork, technical curiosity, and adaptability. The paper further discusses how prior coursework and professional experiences align with the position’s technical and soft skill requirements, illustrating preparedness for the role. Lastly, the discussion considers the industry's growth trends, organizational culture, and the challenges the position may present, providing a comprehensive evaluation of the role's significance within Lockheed Martin and the cybersecurity field.

Writing Assignment One: Job Analysis

Cybersecurity is an essential field in today’s digital landscape, where protecting critical information systems from cyber threats is necessary for a country’s stability. As organizations, particularly those in government and defense sectors, expand their cybersecurity initiatives, the demand for skilled professionals continues to grow. This paper analyzes a job posting for a Cyber Security Engineer position at Lockheed Martin, evaluating the company’s expectations, the skills required, and how prior coursework and experience align with the role. By closely examining the job listing, this paper identifies both explicit and implied qualifications while discussing broader industry trends that impact the position’s significance.

Lockheed Martin is a global security and aerospace company that provides advanced technology solutions to government and commercial clients. As an industry leader in cybersecurity, Lockheed Martin designs secure systems that protect national security interests. The Cyber Security Engineer position is a key role within the company’s Space business unit, focusing on developing, integrating, and verifying security solutions for government clients. The job’s primary responsibilities include applying an interdisciplinary approach to cybersecurity, engaging with non-cyber teams to implement solutions, and assisting with the development of cyber plans and procedures. These responsibilities indicate that the role requires both technical expertise and cross-functional collaboration skills.

The job posting lists several technical qualifications necessary for the role. Among the fundamental requirements, candidates must have a solid understanding of Linux and Windows operating systems, experience with vulnerability scanning and patching, knowledge of Ansible, and familiarity with the Risk Management Framework (RMF) and NIST SP 800-53 guidelines.

These qualifications highlight the need for proficiency in system security and compliance protocols.

In addition to technical skills, the listing suggests several key soft skills. The mention of “team player” implies that the candidate must work well in collaborative environments, while “technical curiosity” signals the company’s interest in candidates who are willing to learn and adapt to new challenges. Furthermore, the requirement for an active security clearance showcases the importance of trustworthiness and adherence to security protocols. While not explicitly stated, the ad suggests that strong communication and problem-solving skills are essential, as cybersecurity professionals must often explain complex issues to non-technical stakeholders.

Beyond the explicitly stated qualifications, the structure of the job posting reveals additional expectations. The ad lists technical competencies first, suggesting that a strong foundation in cybersecurity principles is the primary criterion for selection. However, the inclusion of “serving as a cyber representative to non-cyber teams” indicates that candidates must also possess interpersonal skills to facilitate collaboration across departments. The ad’s emphasis on security certifications, such as Security+ and CSSLP, further suggests that the company prioritizes candidates with validated knowledge.

The listing’s language also hints at the complexity and demands of the role. The requirement for an active Top-Secret security clearance (with an investigation within five years) suggests that the candidate will handle highly sensitive information, requiring a deep understanding of national security policies. Also, the mention of cloud technologies, such as Kubernetes and Docker, implies that the company is focused on modern, scalable security solutions. This suggests that continuous learning and staying updated with technology trends are crucial for success in this role.

The cybersecurity field is experiencing rapid growth due to increasing cyber threats targeting both public and private sectors. According to reports from the Bureau of Labor Statistics, cybersecurity jobs are projected to grow significantly over the next decade, driven by advancements in cloud computing, artificial intelligence, and regulatory compliance requirements. Lockheed Martin's emphasis on the Risk Management Framework (RMF) and National Institute of Standards and Technology (NIST) guidelines aligns with the growing need for government contractors to meet high-security standards. The increasing reliance on cloud-based services further emphasizes the demand for professionals skilled in cloud security frameworks. These industry trends suggest that cybersecurity professionals who continuously update their skills and certifications will have strong career prospects in organizations such as Lockheed Martin.

My academic and professional experiences align well with the qualifications outlined in the job posting. Coursework in operating systems and cybersecurity principles has provided a strong foundation in Linux and Windows environments, while hands-on projects involving vulnerability assessments have enhanced my understanding of risk management frameworks. Also, classes in network security and ethical hacking has prepared me for responsibilities such as penetration testing and compliance assessments. Internships have also played a crucial role in developing practical cybersecurity skills. While working as an intern at a cyber facility, knowledge was gained with artificial intelligence, vulnerability scanning, and data information tools. This hands-on experience closely aligns with the job posting's requirement for vulnerability scanning expertise. Furthermore, participating in cybersecurity competitions and earning industry certifications, such as Security+, has strengthened my technical competency and demonstrated my commitment to professional development.

While my skills and experience align with many of the job's requirements, certain aspects may present challenges. For instance, the listing requires experience with cloud-native technologies such as Kubernetes and Helm. While I have the foundational knowledge of cloud security, I recognize the need to gain deeper expertise in these technologies to be fully prepared for the role. Additionally, obtaining the CSSLP certification, as required by the position, will be an important next step to enhance my qualifications. Another potential challenge is the security clearance requirement. Although I meet the eligibility criteria as a U.S. citizen, obtaining a Top-Secret clearance involves an extensive background check and approval process. Understanding the clearance process and ensuring compliance with all necessary requirements will be crucial steps in preparing for a career in this field.

The job posting provides insight into Lockheed Martin's company culture, which emphasizes innovation, integrity, and corporate responsibility. The company highlights its commitment to employee development, flexible work schedules, and competitive benefits, suggesting that it values work-life balance and professional growth. Additionally, Lockheed Martin's focus on collaboration and interdisciplinary approaches indicates that employees are encouraged to contribute beyond their specific technical expertise.

The listing also reflects a structured, high-security work environment, as evidenced by the requirement for an on-site presence and government security clearance. This suggests that the company prioritizes strict security measures, reinforcing the importance of discipline and adherence to protocols. The presence of alternative work schedules, such as four-day workweeks, also demonstrates the company's flexibility in supporting employee well-being.

The Cyber Security Engineer position at Lockheed Martin represents a compelling opportunity for professionals seeking to contribute to national security through advanced cybersecurity solutions. By analyzing the job posting, it is evident that Lockheed Martin seeks candidates with strong technical skills, collaborative abilities, and a commitment to continuous learning. While the listing explicitly states key qualifications, reading between the lines reveals additional expectations, such as adaptability and strong communication skills.

My academic background and internship experiences have prepared me well for many of the role’s responsibilities, particularly in system security, vulnerability assessment, and compliance frameworks. However, further development in cloud security technologies and obtaining the CSSLP certification will strengthen my qualifications. Overall, this position aligns with both my professional aspirations and the evolving demands of the cybersecurity industry, making it a compelling career path for the future.

References

Lockheed Martin. (2025, January 9). *Cybersecurity engineer*. Lockheed Martin Careers. https://www.lockheedmartinjobs.com/job/king-of-prussia/cybersecurity-engineer/694/70114723136

National Institute of Standards and Technology. (2025, January). *Home*. U.S. Department of Commerce. https://www.nist.gov/