Analyzing a Cybersecurity Analyst Job Posting at Bridge Core

Donte Staves

School of Interdisciplinary Studies, Old Dominion University

IDS 493: Electronic Portfolio Project

Dr. Sherron Gordon-Phan

October 28, 2025

Abstract

This paper gives an in-depth analysis of the Cybersecurity Analyst position at Bridge Core in McLean, Virginia. By examining the job advertisement, this essay identifies some key aspects such as the organization's mission, the responsibilities of the position, and the technical and interpersonal skills required for success. The analysis interprets both clear qualifications and implied expectations., considering how the structure and language of the ad reflect company culture and industry needs. Furthermore, the essay connects the listed qualifications to my academic preparation through coursework like cybersecurity fundamentals, system security, and the social aspects of cybersecurity. Drawing on research by Harris and Clayton (2018), this paper emphasizes the balance between technical proficiency and transferable skills in professional readiness. The findings show that Bridge Core seeks adaptable, technically skilled, and communicatively competent professionals that are capable of supporting security objectives through proactive cyber defense operations.

Introduction

The field of cybersecurity is continuing to grow rapidly as organizations and governments face escalating threats from progressively sophisticated adversaries. Bridge Core, a technology integration and consulting firm supporting federal agencies, has recently posted a job advertisement for a position as a Cybersecurity Analyst. This essay analyzes the posting to identify the company's expectations for the role, the clear and implicit skills sought, and how my own educational background aligns with the requirements of the position. The analysis will demonstrate that Bridge Core emphasizes technical proficiency, operational adaptability, and effective communication which are qualities that are consistent with both industry standards and the foundational principles of cybersecurity education. As Harris and Clayton (2018) note, modern employers are not only seeking technical mastery but also "transferable skills" like communication, adaptability, and problem-solving that allow processionals to thrive in dynamic environments (p.196).

Company Overview and Purpose of the Job

Bridge Core positions itself as a company that "enables our clients' mission by integrating innovative technologies and implementing adoption processes that modernize the digital workplace." This language proposes a focus on modernization, efficiency, and technical leadership in federal operations. The organization describes its teams as "high, energy, unified," and "diverse," highlighting collaboration and adaptability as part of its workplace culture. The Cybersecurity Analyst role supports this mission by detecting analyzing and responding to cyber threats within government networks. According to the ad, the analyst will "utilize SIEM systems,

network security tools, and log analysis tools to detect, analyze, and respond to security threats" and "apply knowledge of operating systems, network protocols, and security technologies to safeguard organizational assets." These responsibilities indicate that this is a hands-on, operationally focused position that plays a key part in protecting national security information. The requirement of a TS/SCI clearance with a polygraph gives furth confirmation that this is role involves working with classified or sensitive data.

Analysis of Required Skills and Qualifications

The posting has listings both technical "hard" and interpersonal "soft" skills. Among the most highlighted are experience in a "Cyber Incident Response Team, Security Operations Center, or similar cybersecurity role," as well as proficiency with "SIEM systems, network security tools, and log analysis tools." These requirements indicate the operational side of cybersecurity, emphasizing real-time analysis and response to threats. Additionally, the ad highlights the need for knowledge of "operating systems, network, and security technologies," along with familiarity with the MITRE ATT&CK framework. Together, these terms indicate that Bridge Core values candidates with both theoretical and applied knowledge of cybersecurity defense models. The DoD 8570 IAT-II certification requirement mentioned underlines the federal compliance aspect of the position, aligning it with Department of Defense workforce standards. Harris and Clayton (2018) argue that employers increasingly require professionals to demonstrate both domain-specific expertise and the "capability to apply such skills in real-world contexts" (p.197). Bridge Core's focus on both tool proficiency and analytical reasoning aligns with this view which is an indication that the company expects its analysts not only to know how to use cybersecurity technologies but also when and why to apply them strategically as well.

Unstated and Implied Skills

While the ad clearly lists many technical qualifications, various soft skills are implied as well. For example, the mention of "shift work, including some evenings, nights, and weekends" implies a need for time management, flexibility, and stress resilience which are qualities necessary for maintaining performance in a 24/7 operational environment. The ability to "solve complex problems with analytical and problem-solving skills" also proposes a need for critical thinking and independent decision-making, as analyst may have to act fast in response to unfolding cyber incidents. Harris and Clayton (2018) discuss how modern workplaces increasingly recognize these transferable competencies as "core employability skills" which are critical for sustaining performance amid chance (p. 198). In this context, Bridge Core's ad implies that a successful analyst must be able to adapt to shifting threat landscapes while maintaining composure and clarity under pressure. Additionally, Bridge Core's use of words like "innovative," "trusted," and "skilled" implies a culture that rewards creativity, reliability, and technical excellence. Therefore, the ad communicates indirectly that successful candidates must not only possess technical expertise but also demonstrate integrity, adaptability, and initiative.

Industry Context and Motivations

The demand for cybersecurity professionals continues to rise. According to CompTIA (2024), "From a jobs perspective, CompTIA's Cyberseek tool reports nearly 470,000 U.S.-based job openings with cybersecurity-related skills between May 2023 and April 2024, demonstrating the broad demand for cybersecurity skills across many different job roles." Bridge Core's emphasis on SIEM analysis, threat detection, and the MITRE ATT&CK framework aligns with

these trends, reflecting the growing need for constant monitoring and proactive defense. Moreover, the requirement for a TS/SCI clearance places this role within the national security sector which is an area where threats are persistent and evolving. Bridge Core's focus on supporting "government agencies in their mission" reveals that the company's main motivation is protecting critical federal infrastructure. This context suggests that future growth in this sector will depend on cybersecurity professionals capable of integrating new technologies like artificial intelligence and automation into defense operations.

Alignment with Educational Preparation

My coursework in cybersecurity has provided the foundation needed for this role. In CYSE 300: Introduction to Cybersecurity, I developed an understanding of core cybersecurity principles which include confidentiality, integrity, and availability. These are concepts directly related to safeguarding organizational assets as required in the job posting. CYSE 301: Cybersecurity Techniques and Operations expanded my ability to use practice tools working in Virtual Machines to simulate different scenarios and incident detection and response. This aligns closely with Bridge Core's focus on "analyzing and responding to security threats" using SIEM and network tools. Courses like CYSE 270: Linux Systems for Cybersecurity and CYSE 280: Windows Systems Management and Security provided me with good familiarity in both major operating systems. This dual-system knowledge mirrors the ad's requirement for proficiency across multiple environments. Finally, CYSE 201S: Cybersecurity and the Social Sciences helped me understand human factors, communication, and organizational behavior which are skills that would help me effectively "communicate technical information to non-technical stakeholders," as required by Bridge Core. This academic preparation reflects what Harris and Clayton (2018) call a "balanced approach to skills development," where educational institutions

equip learners with both discipline-specific knowledge and "generic capabilities" that enable them to effectively into professional environments (p.199).

Company's Culture and Professional Fit

Bridge Core's description of its workforce as "trusted, skilled, and diverse" reflects a culture that values teamwork, inclusion, and reliability. Its commitment to being an "equal opportunity workplace" and its mission to "build tailored, client focused solutions" indicate a collaborative and mission-oriented environment. The company's culture appears to be well-suited to professionals who are both technically competent and self-driven. The tone of the ad is confident but not excessively corporate and communicates a sense of purpose tied to public service. For someone passionate about contributing to national cybersecurity efforts, Bridge Core offers both challenge and meaning. The ad's presentation is professional and encouraging, which suggests that employees will be supported while being expected to perform at a high level.

Soft Skills and Anticipated Challenges

Reading between the lines, one can infer that adaptability, attention to detail, and team coordination are essential in a job such as this one. Working in a 24/7 environment as mentioned by the ad, requires not only technical readiness but also the ability to manage fatigue and maintain focus during irregular hours. Communication across teams and agencies can be challenging at times, so emotional intelligence and clear writing skills are crucial. Potential challenges include the high-stakes nature of national security work and the constant evolution of threats. Another challenge would be the 24/7 work environment and always being prepared to respond to an incident at almost any time of the day. However, with a job such as this one, it's

not only essential but crucial to have quick responses to any to potential cyber incidents that could occur.

Conclusion

The Bridge Core Cybersecurity Analyst position embodies the intersection of technical expertise, analytical reasoning, and collaborative communication within a mission-critical environment. The company's emphasis on operational excellence, innovation, and diversity reflects both its culture and its strategic importance in federal cybersecurity operations. The ad's structure reveals a list of priorities. First being mastery of tools, second being analytical awareness, and third being interpersonal communication. My academic preparation in cybersecurity fundamentals, systems management, and human-centered security aligns closely with the expectations for this position, which could possibly make me a strong candidate for this position. Ultimately, this analysis demonstrates how closely academic preparation in cybersecurity mirrors industry needs, underlining the importance of both technical and soft skills in defending critical infrastructure and supporting national security.

References

Bridge Core. (2025). *Cybersecurity Analyst* [Job Advertisement]. Indeed. https://www.indeed.com/viewjob?jk=8abd0a9c47eb5c40&from=shareddesktop_copy

Harris, R., & Clayton, B. (2018). The importance of skills–but which skills?. *International Journal of Training Research, 16*(3), 195-199.

State of cybersecurity 2024. CompTIA Report. (n.d.). https://www.comptia.org/en-us/resources/research/state-of-cybersecurity-2024/