

Cybersecurity Job Advertisement Analysis

Quan Burchette

IDS 493

April 6, 2026

Employers are increasingly looking for candidates with a combination of technical expertise and interpersonal qualities as cybersecurity continues to gain importance across industries. Both explicit and implicit expectations are revealed in job adverts, which offer important insight into what companies value when employing cybersecurity specialists. These advertisements can be analyzed using text analysis to find recurrent trends in communication tactics, organizational culture, and skill requirements. Three cybersecurity job postings are examined in this essay: an information security analyst position at Capital One, a cybersecurity analyst position at IBM, and a Security Operations Center (SOC) analyst position at Booz Allen Hamilton. This study uses a content analysis methodology based on Lipovac and Babac to analyze how these postings convey the necessary skills and qualifications and how they reflect broader trends in the sector. In line with Lipovac and Babac's findings that contemporary job advertisements increasingly emphasize organizational identity and interpersonal skills alongside technical expertise; cybersecurity job advertisements place a strong emphasis on soft skills and company branding in addition to technical competencies like threat analysis and network security.

The first job posting examined is for a Cybersecurity Analyst position at IBM. System monitoring, vulnerability detection, and cyber threat response are the main responsibilities of the position. "Analyzing security incidents," "implementing security controls," and "collaborating with cross-functional teams" are among the duties (IBM, 2025). Experience with tools like SIEM

systems and familiarity with threat detection frameworks are prerequisites for the role. The second job posting is for a SOC Analyst position at Booz Allen Hamilton (2025). To protect organizational systems, this position requires teamwork, incident response, and real-time threat monitoring. "Continuous monitoring," "incident triage," and "communication with stakeholders" are highlighted in the job description. It also emphasizes how important flexibility is in a fast-paced setting. The third job opening is for a Capital One information security analyst. The main responsibilities of this position include enterprise system security, compliance, and risk assessment. According to Capital One, duties include "conducting security assessments," "developing mitigation strategies," and "ensuring regulatory compliance." Both technical know-how and effective communication abilities are necessary for the role.

By finding patterns, themes, and frequencies of elements, content analysis is a research technique used to methodically assess textual data. According to Lipovac and Babac, terms and phrases in job adverts can be categorized into themes including firm branding, soft skills, and technical skills.

A qualitative content analysis method was applied in this investigation. Each job advertisement's key terms and phrases were analyzed and grouped into the following categories, technical competences, or hard skills, Interpersonal skills, or soft skills, and Action verbs (explaining duties) Language used in company branding. Both qualitative interpretation and quantitative observation of recurrent themes are possible with this method.

This analysis's main research question is: What abilities and characteristics are most valued in cybersecurity job postings, and how do these priorities correspond with more general

industry trends noted by Lipovac and Babac? This inquiry seeks to ascertain whether job advertisements prioritize corporate identity and soft skills in addition to technical requirements.

Soft vs. Hard Skills Hard talents are heavily emphasized in all three job ads. Typical technical specifications consist of familiarity with cybersecurity frameworks

familiarity with SIEM tools

knowledge of network security

Capabilities for responding to incidents for instance, Capital One stresses "risk assessment and mitigation strategies," but IBM mandates that candidates "analyze and respond to security incidents." Soft skills, however, are also well-represented. Every posting has specifications like:

Teamwork and communication abilities

Problem-solving skills in particular, Booz Allen Hamilton emphasizes the importance of "communicating findings clearly to stakeholders," suggesting that technical expertise is not enough. Utilizing Action Verbs, the commercials make extensive use of action-oriented verbs like: Examine, Track, and React

Work together

Develop This is consistent with the findings of Lipovac and Babac that verbs are often used in job advertisements to communicate responsibilities and expectations. These verbs emphasize the dynamic nature of cybersecurity roles by generating a sense of activity and urgency. firm

Branding The firm culture and branding are the main topics of any commercial. For instance, IBM prioritizes worldwide impact and innovation.

Booz Allen emphasizes national security and mission-driven projects.

Capital One encourages teamwork and a technologically advanced workplace. This is consistent with the finding by Lipovac and Babac that employer branding is becoming increasingly

important in job advertisements. Companies try to attract candidates by portraying themselves as desirable workplaces instead of just listing qualifications. Certain skills are not expressed clearly; instead, they are implied. For instance, statements like "handle multiple incidents simultaneously" imply time management even when it isn't stated explicitly (Booz Allen Hamilton). In a similar vein, allusions to "fast-paced environments" imply adaptation. In cybersecurity positions, where experts must react swiftly to changing threats, these implicit skills are essential.

Comparison to Lipovac and Babac The results of this analysis are in good agreement with the study conducted by Lipovac and Babac. They discovered that job postings: Prioritize both technical and soft skills.

Make use of powerful action verbs

Incorporate important company branding in a similar vein, the cybersecurity job postings examined here: Have a lot of references to soft skills

When describing duties, use action verbs.

Give organizational identity a significant amount of room. One distinction, though, is that cybersecurity job posts prioritize technical proficiency more than the generic job ads Lipovac and Babac examined. This is perhaps because the field is so specialized.

The advertising' phrasing alludes to a cooperative and demanding workplace. Words like "fast-paced," "dynamic," and "team-oriented" suggest that workers must perform well under duress. The advertisements typically have a positive tone, highlighting chances for advancement and fulfilling work. For instance, Booz Allen Hamilton emphasizes the chance to support national security, which can be appealing to those looking for jobs with a purpose. Several of the requirements listed in these job postings are in line with my present skill set. I have a basic

understanding of cybersecurity principles, such as threat analysis and network security.

Additionally, my academic and professional experiences have helped me improve soft skills like communication, critical thinking, and problem-solving. This study does, however, also point up areas that need work. For instance, earning certifications like CompTIA Security+ and getting practical expertise with SIEM technologies will bolster my credentials. Additionally, success in cybersecurity roles will depend on my ability to perform well under pressure.

This data shows that, in keeping with the complexity of the industry, cybersecurity job postings call for a blend of hard and soft abilities. Although hard skills are still important, businesses are placing a greater emphasis on teamwork, communication, and flexibility. The results closely match those of Lipovac and Babac's study, especially about the emphasis on company branding and the usage of action verbs. However, because cybersecurity job is specialized, technological skills are more important. Overall, this study emphasizes the significance of honing both technical and interpersonal abilities and offers insightful information on industry expectations. To prepare for a career in cybersecurity, I will use these insights to direct my future academic and professional development.