#1 Writing Assignment: Content Analysis of Job Advertisements.

Content Analysis of Cybersecurity Job Advertisements

Mohammed Aljuboor

IDS 493

Dr. Kat LaFever

ODU

09-28-2024

#1 Writing Assignment: Content Analysis of Job Advertisements.

Content Analysis of Cybersecurity Job Advertisements

This article provides a content analysis of job adverts for cybersecurity positions. Content analysis is a qualitative research method that systematically examines textual data to uncover patterns and themes (Krippendorff, 2013). The goal of this research is to gain a better understanding of the abilities, certifications, and experiences that are required in cybersecurity professions so that I can tailor my personal career preparation and application materials. The study focuses on job postings for cybersecurity analyst opportunities that match my educational background and professional goals. This analysis is critical for modifying my CV, cover letter, and ePortfolio to meet industry demands and expectations, ensuring that I show myself as a competitive candidate in the job market.

This study investigates the characteristics and abilities emphasized in four job adverts, analyzes similar tendencies, and examines how these findings will influence my career development. The analysis begins with outlining the types of cybersecurity employment I want to pursue, followed by an examination of common patterns in job advertisements. The main topics covered are essential technical abilities, desired certifications, and common soft skills such as communication and teamwork. In the parts that follow, I will explain the job roles I am looking for and the commonalities observed in the job advertising studied.

I am looking for a full-time career as a cybersecurity analyst, with a focus on threat detection, incident response, and network security monitoring. Ideally, I'd like to work for a mid-sized to large national corporation with an established cybersecurity department. The occupations I examined are all full-time and require cybersecurity knowledge to safeguard firms from potential cyber threats. The job names in the adverts included "Cybersecurity Analyst," "Threat Analyst," and "Information Security Analyst," but they all require comparable responsibilities centered on protecting digital infrastructure.

The employment I researched is full-time, which aligns with my professional objectives. Three of the four positions needed regular office attendance, while one provided a hybrid work environment with some remote flexibility. I am open to both in-office and hybrid employment if they provide professional development and learning. In terms of duties and responsibilities, all four positions place an emphasis on network security monitoring, vulnerability identification, incident response, and forensic investigation in the event of a security breach. I have prepared for these tasks through my coursework and hands-on lab activities, particularly in Windows Systems Management and Security (CYSE 280), as well as my research into the influence of ransomware on national cybersecurity policies. Each advertisement emphasized the need to have experience with intrusion detection systems (IDS) and security information and event management (SIEM) tools, which I have begun to learn in class.

Only one of the advertisements referenced travel, which would account for 10% of the time spent doing security assessments at offsite locations. I am open to tasks that require little or no travel, but my preference is for a position that allows me to focus on technical responsibilities in an office setting. In terms of credentials, all four job postings needed a bachelor's degree in cybersecurity or a similar discipline, which is consistent with my present studies at Old Dominion University. Three of the advertisements mentioned certifications like CompTIA Network+ and CompTIA Security+ as preferred qualifications. I do not have these qualifications yet, but I aim to acquire them after graduation as part of my career development plans.

The four adverts had several common terms, including "communication skills," "team collaboration," "problem-solving," and "attention to detail." For example, "communication" was repeatedly identified as a talent required for working with other teams and documenting security events.

I have gained great communication skills through group projects in my classes, and I will make sure that this is reflected in my eportfolio. The need of teamwork was also highlighted, since cybersecurity analysts routinely engage with IT personnel and management to design security measures and respond to breaches. By integrating artifacts from group projects and internships in my ePortfolio, I can demonstrate my ability to collaborate effectively as part of a team.

One ad mentioned remote work, offering a hybrid work environment with two days of work from home per week. This flexibility appeals to me, yet it is not required for my job hunt. Compensation for the posts ranged between $70,000 and $90,000 per year, depending on experience and credentials. Benefits often included health insurance, 401(k) matching, and opportunities for continuing education, all of which are essential considerations for me when accepting a job offer.

The companies advertising these roles varied in size from mid-sized to major corporations. I'm interested in working for a mid-sized or large corporation because they typically have well-established cybersecurity teams and provide greater options for professional development and specialization. Two of the organizations operate worldwide, which could lead to opportunities to work on global security challenges, an area of interest that I would like to pursue further in my career.

To do this content analysis, I coded the four adverts to discover reoccurring themes and keywords. I used color coding to distinguish between technical capabilities, soft skills, certificates, and responsibilities. Experience with SIEM tools was one of the most common technical criteria across all advertising, appearing in three out of four. This skill is vital for real-time monitoring of security events and incident response, a core responsibility of cybersecurity analysts. Other common technical talents included vulnerability assessments, penetration testing, and understanding of security system management. These tools and abilities are critical for detecting and mitigating security risks.

Another common theme was certification, with CISSP and CompTIA Security+ stated as preferred qualifications in three of the advertisements. While these certificates are not necessarily needed, they can increase a candidate's competitiveness. I intend to obtain these qualifications to fulfill industry standards and boost my employability.

All four-job advertising emphasized soft skills, specifically communication and teamwork. Effective communication is critical for cybersecurity analysts when explaining technical challenges to non-technical colleagues and collaborating on security solutions. The widespread use of the term "team collaboration" suggests that employers reward applicants who can work well in interdisciplinary teams. In addition, two advertisements promoted problem-solving abilities, with a focus on the capacity to promptly identify and manage security incidents. I will reflect these skills in my ePortfolio by highlighting group projects and case studies that demonstrate my ability to communicate and solve problems in a team environment.

One of the advertisements emphasized the significance of attention to detail, which is essential for cybersecurity analysts who must monitor systems for irregularities that may suggest security breaches. This attention to detail is something I've learned from my coursework, particularly when evaluating network data for potential vulnerabilities.

In conclusion, this content analysis identified major trends in the skills, credentials, and responsibilities necessary for cybersecurity analyst positions.

The consistent emphasis on SIEM tools, certifications, communication, and teamwork underlines the critical skills I must continue to hone. By structuring my resume, cover letter, and ePortfolio to meet these industry standards, I can position myself as a qualified and competitive applicant in the cybersecurity job market. The knowledge gathered from this research will direct my professional development, ensuring that I am ready to satisfy the needs of companies in this industry.

References:

- Krippendorff, K. (2013). Content analysis: An introduction to its methodology (3rd ed.). SAGE Publications
- Neuendorf, K. A. (2017). The content analysis guidebook (2nd ed.). SAGE Publications