Introduction

In this paper I will be providing a content analysis for the different jobs in cybersecurity. I will be doing this by looking at the job ads on indeed to see some of the most wanted skills and determine the skills in the field. I will be looking at entry level cybersecurity positions for this paper just to help myself when I graduate. When trying to apply content analysis to these specific job descriptions I will have to firstly describe what content analysis is. According to LaFever, content analysis is “A qualitative analysis method that focuses on analyzing communication taken from primary and secondary data or artifacts” (LaFever,2024). The qualitative analysis method will allow me to see the opinions and research analysis not limited to but including surveys, case studies, and text analysis. Looking at the entry level of cybersecurity positions, this content analysis will allow not only me put other entry level cybersecurity professionals in the know as far as what skills they need but also allow me to get well acclimated with the expectations of the cybersecurity field. Now in the next section I will describe the job findings I found that are entry level and can help show a more comprehensive look at the cybersecurity field.

General Job Description

The jobs that I am looking for are in the cybersecurity field, more specifically a cyber analyst position or a data forensic specialist position. With these positions I will have to use a diverse set of tools at my disposal to complete my job. This includes but is not limited to SIEM (Security Information and Event Management), IDS (Intrusion Detection Systems), and IPS (Intrusion Prevention Systems). The jobs that I have selected are as follows Cyber Security Defense Analyst- (Entry Level), IT Security Professional, Vulnerability Threat Management Analyst, Special Agent: Cybersecurity/Technology Background. Some common themes with these jobs include technical proficiency, analytical skills, threat identification and response, and collaboration and communication skills. The four jobs listed have their own distinct responsibilities but share these foundational elements that underscore the importance of cybersecurity in today's digital landscape. All these roles require a solid understanding of various cybersecurity tools and technologies. The adequacy of firewalls, IDS, and other threat detection tools is needed to be successful across the board. Each position emphasizes strong analytical abilities as they must analyze threats, identify vulnerabilities, and evaluate potential risks to the organizations systems. Recognizing patterns in traffic and knowing the indicators of compromise and how to mitigate them is an important feat for these positions. Threat management as a whole goes beyond just monitoring traffic it uses traffic monitoring as tool or procedure to identify a specific threat or vulnerability. These cybersecurity positions also need to go beyond the technical skills needed. There is an increase in a need for soft skills such as collaboration and communication, continuous learning and adaptation, and problem-solving orientation. Effective communication skills are vital in all roles. Cybersecurity itself is a collaborative effort, often involving cross departmental teams to ensure that security protocols are understood and implemented. In some cases, institutions like special agencies may involve liaising with law enforcement or other governmental agencies. Given the rapidly changing environment of technology professionals must commit themselves to the job whole heartily and be able to learn and have to stay in touch with the ever-evolving nature of cyber threats and vulnerabilities. Each role needs to use that knowledge that they learned to create proactive approaches to cybersecurity threats. The ability to think critically and creatively will be at the upmost importance to devise effective defense strategies for threat mitigation and response. With all these similarities these roles have their own distinct responsibilities that don't necessarily overlap from each position. Cyber security defense analyst focuses on monitoring systems for anomalies, analyzing security incidents, and implementing defensive measures. This role involves real time analysis and response to cybersecurity threats. IT security professionals are in a broader scope of cybersecurity but often time are a primary resource for specialized security standards and policies. They also implement preventative security measures to support end users and business units according to the position summary by University of North Carolina at Chapel Hill. Vulnerability Threat Managment Analyst specifically concentrates on identifying and managing vulnerabilities within systems. This position includes conducting risk assessments, prioritizing risks, and coordinating remediation efforts. Being a special agent involves investigative work often related to cybercrime. This role may require law enforcement training and skills in forensic analysis, as well as collaboration with other agencies to combat cyber threats. When looking at all these jobs they are all full-time and are great starting options for someone trying to get into cybersecurity and I would be willing to work at any of these respective agencies. The jobs provided a general requirement that was empirical between all of them which was a bachelors in related fields and to have 1-3 years of work experience in cybersecurity. I have prepared for this by getting an internship and a part time position involving cybersecurity and different database schemas. I also have gotten CompTIA Security Plus to show my skills that I have obtained this certification is one that is a standard for entry level cybersecurity positions. These positions have some level of remote work expect the special agent position because they deal with top secret information regarding the government. In the job descriptions linked below they have plenty of similar keywords such as analysis, monitoring, communication, vulnerability. These jobs ads speak of the communication aspect of just being able to not only being able to work in teams and collaborate in teams but also be able to communicate the tech related issue or concern to someone who is not well versed in the field. This was explicitly stated in the IT Security Professional job posting at the University of North Carolina at Chapel Hill. To show my skills off in my eportfolio I will be using projects, assignments, and certifications. The term monitoring was shown in these job ads when speaking of monitoring systems because in cybersecurity you are always trying to manage a set of data to keep its confidentiality, availability, and integrity. To ensure that the CIA Triad is met we must monitor the data to make sure no changes happen or make sure there is no breach in the data set (Confidentiality, Integrity, and Availability: The CIA Triad | Office of Information Security | Washington University in St. Louis, 2024). This also includes ensuring the data is readily available for use at the request times of the organization. The vulnerability term comes up often and is in the context of searching for the vulnerability or doing some level of threat hunting. Threat hunting “is the practice of proactively searching for cyber threats that are lurking undetected in a network (Taschler, 2022)”. Analysis was a final word that was either explained or mentioned directly when looking at these job ads. Analysis in the cybersecurity field is a main skill or duty for most positions. In the context of the job ads analysis will be used hand in hand with the monitoring duty stated earlier. Analysis of network traffic is imperative to these jobs because it allows you to notice any indicators of compromise on your system. Benefits were spoken of throughout all of these ads, they were all speaking about paid time off. The Special Agent, Vulnerability Threat Management Analyst, and IT Security professional positions made mention of health insurance plans. The FBI is offering the Special Agent position, and they are a national company, but you may have to move to other parts of the globe to complete your job. I would love to work for the FBI because I believe I have a strong sense of morals and can determine what is right from wrong use critical thinking to make logical decisions. The FBI is a leader in the cybercrime field as it has been established for 116 years and has 20,000 employees (Topic: The FBI, 2024). Lockheed Martin is an aerospace company and has over 122,000 employees and has been established since March 15,1995. They are a leader in aerospace engineering and show it through the various contracts and opportunities they get at a global level. I would like to work at Lockheed Martin to be able to support the common person and make sure that “networks that our citizens and the world depend upon each minute: Financial assets. Healthcare information. Critical infrastructure. Hazardous materials. The uninterrupted flow of energy that keeps modern life moving” are all up and running (Cyber Security Defense Analyst, n.d.). The University of North Carolina at Chapel Hill posted the IT Security Professional job ad, and I don't think I would like to work here after looking at the job. They do not have specific tasks for their employees, and it seems it goes above and beyond just cybersecurity. The University of North Carolina at Chapel Hill is a nationally renowned institution that has been established since Dec 11, 1789 (History and Traditions - the University of North Carolina at Chapel Hill, 2021). They have 9,704 staff members and 4,234 faculty members (Carolina by the Numbers | UNC-Chapel Hill, 2024). The Vulnerability Threat Management position was made available by Citi Bank, and they have 239,903 employees that work at a global level and have been in business since October 8, 1998 (Number of Employees at Citigroup by Region 2022 | Statista, 2022). I would like to work over at Citi Bank because of the accurate daily,weekly,and monthly expectations they describe in the job description. They are a leader in the banking scene, and they seem to take cybersecurity with high levels of importance based off the specific needs they want for this position and how descriptive they are in the job description.

Content Analysis

The similarities and skills that were stated in the previous section can be broken down into key concepts. Technical skills can be broken down into knowledge of cybersecurity tools, programming skills, and familiarity with networks and systems. Analytical skills can be broken down into threat detection and analysis, vulnerability assessment, and incident response capabilities. Collaboration breaks down into teamwork with IT departments, communication with stakeholders (or law enforcement for special agents). Continuous learning has staying updated with cyber threats, engaging in professional development, and attending training or certifications as key concepts. The problem-solving concept can be broken down into creative approaches to cyber security challenges, developing strategies for risk mitigation, and troubleshooting security incidents. The Cyber Security Defense Analyst uses technical skills to monitor systems using IPS or IDS. Analytical skills can be used in the life of a Cyber Security Defense Analyst by analyzing security events and identifying anomalies. Collaboration being used for the Cyber Defense Analyst is working with IT teams to implement effective security measures. The IT Security Professional position uses technical skills to develop security policies and has a substantial security posture in network defenses. An IT Security Professional also uses analytical skills to evaluate and prioritize vulnerabilities. An IT Security professional could also use continuous learning concept to participate in security training programs. A Vulnerability Threat Management Analyst uses technical skills to conduct vulnerability scans and use assessment tools. Vulnerability Threat Management Analyst use analytical skills to evaluate and prioritize vulnerabilities. A Vulnerability Threat Management Analyst uses the problem-solving concept to develop remediation strategies. A Special agent uses technical skills to perform forensic analysis and cybercrime investigation. A special agent will use collaboration skills to intercommunicate with law enforcement agencies nationwide. A special agent will also use continuous learning to keep up with cybercrime trends. When using coding we have to aggregate them into themes to complete the analysis. Doing this will allow us to see what specific skills are most sought after between these jobs and allow us to have repeatable and reliable research. Technical Proficiency can be coded into having skills in cyber security tools, programming, and systems knowledge are critical across all roles. Analytical Abilities can be coded into the ability to analyze threats and vulnerabilities being a common requirement. Collaboration and communication can be coded into working with various teams and stakeholders vital and particularly for roles that interact with law enforcement. Continuous learning can be coded into stating that ongoing education and adaptation to new threats are emphasized in all positions. Problem solving and Strategic Thinking can be described as a focus on innovative solutions to complex security challenges is present in all roles.

Conclusion

The qualitative coding shows how each job description can be analyzed conceptually to extract themes and insights about the skills and attributes essential in the field of cybersecurity. By categorizing the roles based on these themes we can better understand the collective requirements and expectations of entry level cybersecurity positions. Gathering the different requirements for each job allows us to gain a different perspective of the expectations for each position and how all these jobs show the different disciplines we may need to tap into to be successful in cybersecurity. The content analysis shows how similar but also how different each niche in cybersecurity is and how we can be successful. This will ultimately allow for students like me to find jobs and home in on these valuable skills that are sought after by these potential employers.

References

LaFever, K., Dr. IDS493 ContentAnalysis [Powerpoint]. Dr. Kat LaFever. https://canvas.odu.edu/courses/163600/files/37294767

Confidentiality, Integrity, and Availability: The CIA Triad | Office of Information Security | Washington University in St. Louis. (2024). Wustl.edu. https://informationsecurity.wustl.edu/items/confidentiality-integrity-and-availability-the-cia-triad/#:~:text=The%20CIA%20triad%20is%20a%20guiding%20model%20in%20information%20security

Taschler, S. (2022, March 15). Proactive Threat Hunting Guide | What is Cyber Threat Hunting? Crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/threat-hunting/

Cyber Security Defense Analyst. (n.d.). Indeed. https://www.indeed.com/jobs?q=cyber+security+entry+level&l=&from=searchOnDesktopSerp&vjk=8b20c91e246eb2ee

Topic: The FBI. (2024). Statista. https://www.statista.com/topics/10632/the-fbi/#:~:text=The%20FBI%20is%20comprised%20of%20a%20large%20number

istory and Traditions - The University of North Carolina at Chapel Hill. (2021, August 27). The University of North Carolina at Chapel Hill. https://www.unc.edu/about/history-and-traditions/#:~:text=UNC%20is%20the%20first%20public%20university%20in%20the%20nation

Carolina by the numbers | UNC-Chapel Hill. (2024, September 25). The University of North Carolina at Chapel Hill. https://www.unc.edu/about/by-the-numbers/#:~:text=Carolina%20is%20one%20of%20the%20nation%E2%80%99s%20few%20public%20flagship%20campuses

Number of employees at Citigroup by region 2022 | Statista. (2022). Statista. https://www.statista.com/statistics/1317344/number-of-employees-citigroup-by-

region/#:~:text=In%202022%2C%20Citigroup%20employed%20more%20than%20239%2C000%20people

Jobs listed below

1. **Cyber Security Defense Analyst- (Entry Level)**

https://www.indeed.com/jobs?q=cyber+security+entry+level&start=10&vjk=a735e5b31e4d8789&advn=9112618986767135

2. **IT Security Professional**

https://www.indeed.com/jobs?q=cyber+security+entry+level&l=&from=searchOnDesktopSerp&vjk=d6b5c0a3e5d9eb4a&advn=7983482308664392

3. **Vulnerability Threat Management Analyst**

https://www.indeed.com/jobs?q=cyber+security+entry+level&l=&from=searchOnDesktopSerp&vjk=231219bebf2a1eae

4. **Special Agent: Cybersecurity/Technology Background**

https://www.indeed.com/jobs?q=cyber+security+entry+level&l=&from=searchOnDesktopSerp&vjk=8b20c91e246eb2ee