In this essay, I will be providing a content analysis of four select cybersecurity adverts. These adverts range from internships to entry-level to high-end positions and contain four separate categories of cybersecurity jobs. Content analysis involves breaking down a selected piece of information or content into digestible, constituent parts to gather a deeper understanding of the whole piece of information provided. This can be done through many different methods, mainly qualitative research and through coding (LaFever, 2023). Using these methods of content analysis in cybersecurity adverts and job searches as a whole allows the viewer to pick up on specific tricks used by employers. Viewers are also able to gain a deeper understanding of the requirements the job advert lists, along with the scope of what the job entails. Using these methods for job adverts, internships, or general contracts allows whoever is reading to fully understand what they're signing up for. The major aspects this paper goes over are job environments, specific buzzwords used by employers, and job requirements. All of the job adverts researched contain similar information, as explained in the next section.

While I currently have an internship for a cybersecurity firm, I am currently looking for other internship opportunities at higher-end companies, with the eventual goal of landing a job as a cybersecurity analyst. Through doing my research for internships before the conception of this writing assignment and with the added research in preparation for this assignment, I've found most job advertisements related to cybersecurity contain extremely similar information to each other. Before delving further, I want to make it known that all of these job adverts were found through Indeed. The first job advert is for a Remote Associate Security Analyst at Parasons. This position is full-time and is entirely remote which requires little to no travel. The main responsibilities of this position are standard security practices such as monitoring and collaboration. The requirements for this position are one year in IT, cyber security experience,

and a bachelor's in computer security or related field. This position also has optional but preferred credentials which I have already or can gain fairly easily and quickly. A few common phrases in this position are their slogan “Imagine Next!”, “We”, and “You”. The introductory paragraph begins with the phrase “imagine” a multitude of times to suggest the viewer view themself as an employee of this company. This position has a lot of benefits such as a 401(k), paid time off, and different types of insurance. All around this position presents itself as a welcoming company looking for another cybersecurity analyst to benefit their team remotely. After viewing this ad and the three others I determined to be substantial, I noticed the similarities between them which allowed me to deepen my analysis and understanding of the content.

To fully flesh out my discoveries, I’ve decided to break down my results into three sections: job environments, advertiser buzzwords, and job requirements and expectations. Job environments/hierarchies/cultures can be gathered through the specific language used throughout an advert. Take for example companies that promote teamwork and collaborative work instead of individually. Companies like these commonly use phrases like “work closely with colleagues” (Moon, 2023). Due to the nature of cybersecurity, which promotes team monitoring and collaboration to better protect against threats from all aspects of job life, all of these advertisements promote teamwork and collaboration at the forefront, even if the job itself is remote. Where these companies differ, however, is how job culture is promoted. While all fields prefer teamwork and collaboration, as the job field leans towards the more experienced end, hierarchies have begun to become more professionally oriented and strict. On the inverse, entry-level and internship positions market their jobs as a relaxed place to thrive and comfortably pursue your career. Through my analysis, I came to the conclusion job environments largely depend on the experience required for the position listed. This made sense, as these entry-level

positions are there for the employee to gain experience and potentially stick with the company for higher-level positions, rather than getting right into the highly complex and strict higher-level fields. The higher level positions led themselves as more concise and a working unit, which made sense for the two jobs listed which were government and military based. While researching the cultures portrayed through job advertisements I began to notice the amount of similar buzzwords used by job advertisers across the board. This is what began to draw my attention.

To draw in as many potential candidates as possible, job advertisements need to be eye-catching and appealing to their target audience. This makes it easy to spot the countless "familiar phrases" job advertisements use to fulfill this goal (Burry, 2022). Entry-level positions will use phrases such as "where you can be yourself", "proactive", "endless growth opportunities", and "explore your passions" as introductory statements to catch a new hire's attention and to ease their potential fears of job searching. These job advertisements fit their target audience (newer, less experienced employees) by completely playing to their interests rather than trying to grab anyone from anywhere. Senior-level job advertisements tend to forgo this type of lingo and go straight into the details of the job description and requirements. These positions also tend to have little to no buzzwords besides eye-catcher. Through my analysis, I noticed these comforting phrases in the internship and entry-level advertisements, all tend to be rather similar in the way they attempt to portray their companies. I also noticed the frequency of buzzwords being used was related to the length of the job advertisement, most likely to maintain the viewer's attention. I then noticed the pattern of these buzzwords mainly being used right before the listing of job expectations and requirements, which allowed me to understand the effectiveness of this method.

Job requirements and expectations might seem minute at first, but I believe this is arguably the most important part of any advertisement. The job requirements and expectations must be portrayed accurately and be comprehensible enough for the average person to be able to understand without much effort. However, due to these positions searching for a multitude of candidates, is impossible for any single person to match perfectly (Burry, 2022). This requires advertisers to be a tiny bit vague in their requirements, to accurately portray their advertisement to enough people as possible with as little detail as possible. This is most noticeable in entry-level adverts, which attempt to prevent scaring off new hires by portraying their requirements in a vague but discernible way. Senior-level adverts and above will usually lay out their minimum requirements as their target audience is already well-versed in the job field and search. It's also important to note that some of these advertisements may be written to " reflect a desired future state, rather than a current reality", and as such may have some qualifications listed that might currently not be needed for the actual job itself (Harper, 2012, p.3). Through my analysis, I started to understand this method of listing job requirements and expectations as a way to find and reject targeted candidates as quickly as possible. As candidates are drawn in by the buzzwords and eye-catching introductions, the expectations are quickly laid out in a readable font to prevent those who might not have the right skill set or may not want the job from applying.

In conclusion, in my conceptual concept analysis, I found out how different job advertisers from internships to senior-level positions in the cybersecurity field portray themselves to find their best candidates. These advertisers convey their job environments, cultures, responsibilities, and requirements to their target audience through a mix of eye-catching buzzwords, readability, and layout to find the most suitable candidates for their laid-out

positions. Through my research and analysis, I found out how entry-level and internship positions portrayed themselves as relaxed, and easy to apply for positions, while senior-level and above adverts were a lot more concise while still using buzzwords to stick out from their counterparts.

References

Dr. Kat LaFever, KL. (2023) *Content Analysis* [15]. IDS 493, Old Dominion University. https://canvas.odu.edu/courses/142582/pages/module-4-%7C-assignments-and-additional-resources?module_item_id=4750986

Burry, M. (2022, February 1). How to Decipher a Job Advertisement. Retrieved from The Balance: https://www.thebalancemoney.com/how-to-decode-a-job-advertisement-2061002

Harper, R. (2012). The collection and analysis of job advertisements: a review of research methodology . In R. Harper, The collection and analysis of job advertisements: a review of research methodology.

Moon, T. (2023, January 30). *How to convey your company culture in job descriptions*. RecruitingDaily. https://recruitingdaily.com/how-to-convey-your-company-culture-in-job-descriptions/#:~:text=Use%20language%20that%20aligns%20with,%E2%80%9Cwork%20closely%20with%20colleagues.%E2%80%9D

Job Listings (From Internship to Senior Position)

1. Security Analyst: Internship Opportunities - Microsoft

Come build community, explore your passions and do your best work at Microsoft with thousands of University interns from every corner of the world. This opportunity will allow you to bring your aspirations, talent, potential—and excitement for the journey ahead.

As a Security Analyst Intern, you will execute security controls, defenses, and countermeasures to intercept and prevent internal or external attacks or attempts to infiltrate company email, data, e-commerce, and web-based systems.

At Microsoft, Interns work on real-world projects in collaboration with teams across the world, while having fun along the way. You'll be empowered to build community, explore your passions and achieve your goals. This is your chance to bring your solutions and ideas to life while working on cutting-edge technology.

Microsoft's mission is to empower every person and every organization on the planet to achieve more. As employees we come together with a growth mindset, innovate to empower others, and collaborate to realize our shared goals. Each day we build on our values of respect, integrity, and accountability to create a culture of inclusion where everyone can thrive at work and beyond.

Responsibilities

- Research attempted or successful efforts to compromise systems' security and determine next steps, including potential escalations.
- Develop and implement automation of security processes and procedures where possible and translate security policy into effective controls.
- Respond to security incidents, conduct threat intelligence and analysis, and use data analytics to drive security decisions.
- Conduct and support red/purple team operations or improve security posture.
- Maintain hardware, software, network firewalls, and encryption protocols, and they administer security policies to control access to systems.

Qualifications

Required Qualifications

o Currently pursuing a Bachelor's or Master's Degree in Statistics, Mathematics, Computer Science or related field

- Have at least one additional quarter/semester of school remaining following the completion of the internship.

The base pay range for this internship is USD $5,090 - $10,120 per month. There is a different range applicable to specific work locations, within the San Francisco Bay area and New York City metropolitan area, and the base pay range for this role in those locations is USD $6,690 - $11,030 per month.

Certain roles may be eligible for benefits and other compensation. Find additional benefits and pay information here: https://careers.microsoft.com/us/en/us-intern-pay

Microsoft is an equal opportunity employer. Consistent with applicable law, all qualified applicants will receive consideration for employment without regard to age, ancestry, citizenship, color, family or medical care leave, gender identity or expression, genetic information, immigration status, marital status, medical condition, national origin, physical or mental disability, political affiliation, protected veteran or military status, race, ethnicity, religion, sex (including pregnancy), sexual orientation, or any other characteristic protected by applicable local laws, regulations and ordinances. If you need assistance and/or a reasonable accommodation due to a disability during the application process, read more about requesting accommodations.

URL

(https://www.indeed.com/viewjob?jk=e59a95ac069d9fc1&tk=1hbeic8sri46k800&from=serp&vjs=3**)**

2. Associate Security Analyst (Remote) - Parasons

In a world of possibilities, pursue one with endless opportunities. Imagine Next!

When it comes to what you want in your career, if you can imagine it, you can do it at Parsons. Imagine a career working with intelligent, diverse people sharing a common quest. Imagine a workplace where you can be yourself. Where you can thrive. Where you can find your next, right now. We've got what you're looking for.

Job Description:

Parsons is looking for a talented **Associate Security Analyst** to join our team!

What you will be doing:

- Applies security best practices to ensure the protection of sensitive data and systems.
- Assists in monitoring and analyzing security events and alerts to identify potential threats or vulnerabilities.
- Contributes to the implementation and maintenance of security systems, tools, and technologies.
- Assists in performing vulnerability assessments.
- Supports the investigation and resolution of security incidents or breaches.
- Collaborates with all security teams to ensure the integration of security measures throughout the organization.
- Stays up to date with the latest cybersecurity trends, threats, and technologies.

What is required from you:

- Ability to work independently, and in an efficient and organized manner
- Strong analytical and problem-solving skills
- Ability to work collaboratively as part of a team
- Strong verbal communication and interpersonal skills
- A proactive and self-motivated approach to learning and professional development
- Excellent attention to detail and the ability to follow established procedures
- Basic knowledge of networking concepts, operating systems, and computer hardware
- Familiarity with common cybersecurity tools and technologies

- Knowledge of or experience in one of the following: operating systems like Windows or Linux, general networking and infrastructure fundamentals, or cybersecurity fundamentals
- A Bachelor's Degree in computer security, computer science, or another closely related IT discipline
- 1 Year experience in general information technology (IT)

Desired Qualifications

One of the following certifications

- CompTIA Security+
- CompTIA Network+

Minimum Clearance Required to Start:

Not Applicable/None

This position is part of our Corporate team.

We’re driving the future of the national security and critical infrastructure markets. Our employees work in a close-knit team environment to find new, innovative ways to deliver smart solutions that are used and valued by customers around the world. By combining unique technologies with deep domain expertise across cybersecurity, missile defense, space, connected infrastructure, transportation, smart cities, and more, we're providing tomorrow's solutions today.

Salary Range:

$68,400.00 - $119,700.00

We value our employees and want our employees to take care of their overall wellbeing, which is why we offer best-in-class benefits such as medical, dental, vision, paid time off, Employee

Stock Ownership Plan (ESOP), 401(k), life insurance, flexible work schedules, and holidays to fit your busy lifestyle!

The position may require a COVID vaccination or an approved accommodation/exemption for a disability/medical condition or religious belief as required by customer requirements and some cases federal, state, provincial or local mandates.

Parsons is an equal opportunity employer committed to diversity, equity, inclusion, and accessibility in the workplace. Diversity is ingrained in who we are, how we do business, and is one of our company's core values. Parsons equally employs representation at all job levels for minority, female, disabled, protected veteran and LGBTQ+.

We truly invest and care about our employee's wellbeing and provide endless growth opportunities as the sky is the limit, so aim for the stars! Imagine next and join the Parsons quest—APPLY TODAY!

URL

(https://www.indeed.com/viewjob?jk=beba18b22d523f35&tk=1hbef1154kkcj800&from=serp&vjs=3**)**

3. Cyber Security Analyst - ARKS Enterprises

Type:

Full-Time

Experience:

Mid-Senior level

Function:

Analyst

Compensation:

Negotiable

Location:

Virginia Beach, VA, United States

Cyber and Information Assurance specialist

Job Description:

Support a Navy client through rapidly assessing network traffic, detecting anomalies, and providing detailed reporting and alert handling mitigation strategies. Manage and administer network monitoring systems and provide assessments and implementations of solutions to meet network security requirements and modernization efforts. Ensure the successful performance of vulnerability and risk analysis on computer systems and applications during all phases of the system development life cycle. Liaison with external organizations to maximize coordination and effectiveness of network monitoring and modernization efforts. This position may require shift and weekend support.

Desired Skills & Experience:

Basic Qualifications

- 3+ years of experience with network administration
- 1+ years of experience with Cybersecurity
- Knowledge of networking protocols and multiple operating systems, including Windows, UNIX, and Linux
- Knowledge of network data anomalies, trend analysis, and corresponding mitigation strategies

- Must be able to qualify for TS/SCI clearance
- AA or AS degree in CS, IT, Information Systems, or Information Security desired
- DoD 8570.01-M Information Assurance Manager (IAM) level II Certification desired

Additional Qualifications

- Experience with advanced telecommunications, including LAN, WAN, routers, data communications, and connectivity
- Experience with data analysis, tools, and techniques
- Experience with reading and implementing results from vulnerability scanning tools, including Retina and Nessus
- Experience with IDS/IPS/HIPS and associated management tools, including SNORT, Sourcefire, McAfee Host Based Security System, and Sentinel
- Experience with developing alerts and setting policies within IDS/IPS/HIPS systems, including SNORT or Sourcefire or McAfee Host Based Security System
- Experience with packet analysis and the associated tools, including Wireshark and Ethereal
- Knowledge of standard network protocols and ports
- Knowledge of incident handling procedures from initial alert and reporting to mitigation and ticket closeout
- Ability to research and present findings on newly discovered network threats and articulate the degree of risk they may represent to network security

- Possession of excellent oral and written communication skills
- IAM Level II Certification, including GSLC, CAP, CISM, CISSP or Associate, or CASP desired

Clearance

Applicants selected will be subject to a security investigation and may need to meet eligibility requirements for access to classified information; TS/SCI clearance eligble.

URL

(https://www.indeed.com/viewjob?jk=12b1ea6055b443ca&tk=1hbef1154kkcj800&from=serp&vjs=3**)**

4. Information System Security Professional (Entry to Expert Level) - National Security Agency

Information System Security Professionals at NSA play a vital role in enabling security solutions by utilizing systems engineering and systems security engineering principles in: - defining information system security requirements and functionality - designing system architectures and designs - assessing the effectiveness of security solutions against present and projected threats - producing formal and informal reports, briefings, and direct input to the customer regarding security and functionality requirements, system architecture and security designs - conducting security engineering/hardening of the latest operating systems, tailoring them for use in the specific mission area - reviewing requests for security relevant changes on the mission infrastructures, ensuring risk is adequately mitigated - working with system owners to accredit/re-accredit critical mission systems. Depending on their experience and preferences, Information System Security Professionals are hired into positions directly supporting a technical

mission office or into Cybersecurity Engineering Development Program (CSEDP). The development program is 3 years in length and combines formal training and diverse work assignments.

Job Summary

Are you a cyber professional with the drive and expertise to be on the forefront of the cyber fight; tackling NSA's complex mission to defend against cyber threats of today and tomorrow? NSA, the nation's leading cyber agency, has exciting and challenging positions in Cyber Security Engineering and Cyber and TEMPEST vulnerability analysis/mitigation. Are you ready to help secure our Nation's critical Infrastructure? If so, NSA is the place for you!

Qualifications

THIS JOB OPENING ENCOMPASSES MULTIPLE POSITIONS. THE MINIMUM QUALIFICATIONS FOR EACH ARE BELOW: The qualifications listed are the minimum acceptable to be considered for the position. Degree must be in Computer Science or a related field (for example General Engineering, Computer Engineering, Electrical Engineering, Systems Engineering, Mathematics, Computer Forensics, Cybersecurity, Information Technology, Information Assurance, Information Security, and Information Systems).
INFORMATION SYSTEMS SECURITY DESIGNER Relevant experience must be in one or more of the following areas: computer or information systems design/development, programming, information/cyber/network security, vulnerability analysis, penetration testing, computer forensics, information assurance, or systems engineering. Network and system administration may account for some, but not all, of the experience. Completion of military

training in a relevant area such as JCAC (Joint Cyber Analysis course), Undergraduate Cyber Training (UCT), Network Warfare Bridge Course (NWBC)/Intermediate Network Warfare Training (INWT), Cyber Defense Operations will be considered towards the relevant experience requirement (i.e., 20-24 weeks course will count as 6 months of experience, 10-14 weeks will count as 3 months of experience). ENTRY/DEVELOPMENTAL Entry is with a Bachelor's degree and no experience. An Associate's degree plus 2 years of relevant experience may be considered for individuals with in-depth experience that is clearly related to the position. FULL PERFORMANCE Entry is with a Bachelor's degree plus 3 years of relevant experience, or a Master's degree plus 1 year of relevant experience, or a Doctoral degree and no experience. An Associate's degree plus 5 years of relevant experience may be considered for individuals with in-depth experience that is clearly related to the position. SENIOR Entry is with a Bachelor's degree plus 6 years of relevant experience, or a Master's degree plus 4 years of relevant experience, or a Doctoral degree plus 2 years of relevant experience. An Associate's degree plus 8 years of relevant experience may be considered for individuals with in-depth experience that is clearly related to the position. EXPERT Entry is with a Bachelor's degree plus 9 years of relevant experience, or a Master's degree plus 7 years of relevant experience, or a Doctoral degree plus 5 years of relevant experience. An Associate's degree plus 11 years of relevant experience may be considered for individuals with in-depth experience that is clearly related to the position. INFORMATION SYSTEMS SECURITY ENGINEER Relevant experience applying to all work levels: Completion of military training in a relevant area such as JCAC (Joint Cyber Analysis course), Undergraduate Cyber Training (UCT), Network Warfare Bridge Course (NWBC)/Intermediate Network Warfare Training (INWT), Cyber Defense Operations will be considered towards the relevant experience requirement (i.e., 20-24 weeks course will count as 6

months of experience, 10-14 weeks will count as 3 months of experience). ENTRY/DEVELOPMENTAL Entry is with a Bachelor's degree and no experience. An Associate's degree plus 2 years of relevant experience may be considered for individuals with in-depth experience that is clearly related to the position. Relevant experience must be in one or more of the following areas: computer or information systems design/development, programming, information/cyber/network security, vulnerability analysis, penetration testing, computer forensics, information assurance, systems engineering, or updating information assurance documentation (for example System Security Plans, Risk Assessment Reports, Certification and Accreditation packages, and System Requirements Traceability Matrices. Network and system administration may account for some, but not all, of the experience. FULL PERFORMANCE Entry is with a Bachelor's degree plus 3 years of relevant experience, or a Master's degree plus 1 year of relevant experience, or a Doctoral degree and no experience. An Associate's degree plus 5 years of relevant experience may be considered for individuals with in-depth experience that is clearly related to the position. Relevant experience must be in one or more of the following areas: computer or information systems design/development and with information assurance and accreditation processes (e.g., System Security Plans, Risk Assessment Reports, Certification and Accreditation Packages, and System Requirements Traceability Matrices). In addition, experience may include programming, information/cyber/network security, vulnerability analysis, penetration testing, computer forensics, information assurance, systems engineering, or network and system administration. SENIOR Entry is with a Bachelor's degree plus 6 years of relevant experience, or a Master's degree plus 4 years of relevant experience, or a Doctoral degree plus 2 years of relevant experience. An Associate's degree plus 8 years of relevant experience may be considered for individuals with in-depth experience that is

clearly related to the position. Relevant experience must be in one or more of the following areas: computer or information systems design/development and with information assurance and accreditation processes (e.g., System Security Plans, Risk Assessment Reports, Certification and Accreditation Packages, and System Requirements Traceability Matrices). In addition, experience may include programming, information/cyber/network security, vulnerability analysis, penetration testing, computer forensics, information assurance, systems engineering, or network and system administration. EXPERT Entry is with a Bachelor's degree plus 9 years of relevant experience, or a Master's degree plus 7 years of relevant experience, or a Doctoral degree plus 5 years of relevant experience. An Associate's degree plus 11 years of relevant experience may be considered for individuals with in-depth experience that is clearly related to the position. Relevant experience must be in one or more of the following areas: computer or information systems design/development and with information assurance and accreditation processes (e.g., System Security Plans, Risk Assessment Reports, Certification and Accreditation Packages, and System Requirements Traceability Matrices). In addition, experience may include programming, information/cyber/network security, vulnerability analysis, penetration testing, computer forensics, information assurance, systems engineering, or network and system administration.

Competencies

- Excellent problem-solving, communication and interpersonal skills - Is motivated - Works creatively and effectively in diverse environments

- Can juggle multiple priorities and assignments - Applies standards, policies, procedures and requirements for ensuring information security

- Possesses specialized skills that prevent, assess, and/or mitigate threats to information systems and infrastructures and the information contained in or transmitted by these systems. This may encompass: - threat and vulnerability analysis - risk mitigation - incident response - information assurance - risk management framework - configuration management - monitor system security plans - penetration testing - preparing accreditation documentation

Pay, Benefits, & Work Schedule

Salary offers are based on candidates' education level and years of experience relevant to the position and also taking into account information provided by the hiring manager/organization regarding the work level for the position. This position is hiring for Maryland and Texas. Salary Range: $81,233 - $183,500 (Entry/Developmental, Full Performance, Senior, Expert) Typical work schedule is Monday - Friday, with basic 8 hr/day work requirements between 0600 and 1800 (flexible). Exception: Very few positions may support 24x7 operations.

How to apply

U.S. Citizenship is required for all applicants. NSA is an equal opportunity employer and abides by applicable employment laws and regulations. All applicants and employees are subject to random drug testing in accordance with Executive Order 12564. Employment is contingent upon successful completion of a security background investigation and polygraph. Due to time sensitive communications regarding your application, please ensure your spam filters are configured to accept email from noreply@intelligencecareers.gov. Please review the job posting thoroughly to ensure you meet the described qualifications and are aware of all associated requirements. To apply for this position, please click the 'Apply' button located at the top right of

this posting. After completing the application for the first time, or reviewing previously entered information, and clicking the 'Submit' button, you will receive a confirmation email. We encourage you to apply as soon as possible, as job postings could close earlier than the closing date due to sufficient number of applicants, or the position is no longer available. You may be asked a series of questions depending on the position you apply for. Your responses will be used as part of the application screening process and will assist in determining your eligibility for the position. Be sure to showcase within your resume those experiences relevant to this position. Failure to provide the required information or providing inaccurate information will result in your application not being considered for this position. Only those applicants who meet all position qualifications, may be contacted to begin employment processing. Please remain diligent in monitoring email and your SPAM folder. Reasonable accommodations may be provided to applicants with disabilities during the application and hiring process where appropriate. Please visit our Diversity link for more information. This position is a Defense Civilian Intelligence Personnel System (DCIPS) position in the Excepted Service under 10 U.S.C. 1601. DoD Components with DCIPS positions apply Veterans' Preference to eligible candidates as defined by Section 2108 of Title 5 USC, in accordance with the procedures provided in DoD Instruction 1400.25, Volume 2005, DCIPS Employment and Placement. If you are a veteran claiming veterans' preference, as defined by Section 2108 of Title 5 U.S.C., you may be asked to submit documents verifying your eligibility.

DCIPS Disclaimer

The National Security Agency (NSA) is part of the DoD Intelligence Community Defense Civilian Intelligence Personnel System (DCIPS). All positions in the NSA are in the Excepted Services under 10 United States Codes (USC) 1601 appointment authority.

URL

(https://www.indeed.com/viewjob?jk=7d922db844e9d54a&tk=1hbef1154kkcj800&from=serp&vjs=3**)**