#1 Writing Assignment: Content Analysis of Job Advertisements

In this writing assignment, I am conducting a content analysis of four job advertisements in the field of Information Security. What I mean by content analysis is taking a deep look into something (in this case, job advertisements) and analyzing it in order to gain a greater understanding of what information being relayed means. In terms of this assignment, analyzing the contents of multiple job advertisements to better understand the common details that they may share, the unique details that some of them may and may not have, and merely being able to understand what it is that employers are wanting and/or asking for. This process alone is of great help as it enhances my ability to read and understand job advertisements. Performing such research on job advertisements for the type of job I plan to pursue is justified as knowing such information could help me be more prepared when applying for and completing interviews. During this content analysis, I analyze multiple job advertisements and can understand the information put out such as job requirements, salary, benefits, duties, etc. As well as grasp an understanding of the company for which the job advertisement is from.

Upon graduating I plan to seek employment in the field of Information Security. Specifically, the role of an Information/Cyber Security Analyst. The roles and responsibilities of an Information/Cyber Security Analyst can be broad depending on the needs of the company. Although, an Information Security Analyst is best described as someone within an organization who monitors the organization's network for security breaches and conducts investigations when there are any, maintains software such as firewalls, and protects sensitive information. In lesser

terms, an Information Security Analyst plans and carries out security measures to protect an organization's computer networks and systems (Bureau of Labor Statistics, 2023).

To begin, the first job ad, it is for a company named Predicate Logic Inc. The job title is Cyber Security Analyst, and it is a full-time position in Virginia Beach, VA. I would be willing to work in the role being offered as it is in relation to my major and aligned with my preferred career path. Duties and responsibilities of this job consist of but are not limited to providing Cybersecurity analysis support, conducting risk and vulnerability assessment and risk mitigation analysis, and maintaining compliance with Cybersecurity requirements. In a previous internship position, I performed such duties and found it quite interesting as well as challenging. The job advertisement mentions that travel is estimated to be less than 10%. I personally am not looking for a job that involves travel, but I am open to the idea if I absolutely must. In terms of credentials, requirements, and certifications, this job requires one to have experience with several things such as VMWare vSphere ESXi hypervisor, HBSS, ACAS, and possessing the Security + Certification. I do not have my Security + but is in the plans and is one of my goals to acquire. Within this job ad are a few words and phrases that I feel may occur often between the four job ads and they are "risk assessment", "contingency plan", and "maintain". The first two phrases are specific to a certain task, but the last word "maintain" will occur often as it is required for many Information/Cyber Security Analysts to maintain many things. I would likely include these terms and phrases in my portfolio as these are quite common among the selected job and it would likely catch an employer's eye. Not much communication is mentioned other than being able to assist remote users via chat, telephone, messaging, and email. According to Burry, "Companies tend to be coy when it comes to salaried positions. You may see phrases like "salary

commensurate with experience" or "competitive salary," which do not reveal too much. When it comes to benefits, however, companies will generally be direct" (Burry, 2022). In this case, Burry was correct for the pay but incorrect for the benefits as there are no mentions of remote work, and regarding pay and benefits, there are no mentions of salary, pay range, or benefits. This company seems to be on the smaller side of companies, but the culture of the job seems like it would be very strict and result based.

In addition, the next job ad is for the Jr. Information Security Analyst position at Ginia Inc. in Alexandria, Virginia. The role is full-time, and duties consist of writing standards, plans, policies, and procedures as well as performing vulnerability/risk assessments. The role is Hybrid Remote meaning that there will be a certain number of days in the office and a certain amount remote. I would be willing to work in this role as it would provide me with experience and is entry-level. There are no mentions of salary or pay range, but they do state that insurance such as dental, health, life, and life are available as well as other benefits like paid time off, parental leave, and retirement plans. There are very few requirements as it is entry-level, so a bachelor's degree is preferred as well as the ability to obtain public trust. In comparison to the first job ad, the phrase "risk assessment" reoccurs so I'd look to add that I have experience with this in my ePortfolio.

To follow, the third job ad is for the Junior Cybersecurity Analyst role at Leidos in Camp Springs, MD. This role is full-time and has a pay range of $53,300 - $96,350. The roles and responsibilities of this role are different from the first two as it does not mention risk assessments, but the term "monitor" was mentioned as the primary role of the job is to monitor

SEIM dashboards. Requirements consist of a bachelor's degree, less than two years of experience, and an active secret clearance. I have experience in this role and upon graduation, I will meet all the requirements for this position so I would be willing to apply for and work this job. There are no mentions of benefits, but the job is related to the Air Force so I'm sure that there is more to learn. The culture of this company seems welcoming after looking at the wording of the ad and seeing how enthusiastic the tone is.

Finally, the fourth job ad is for the Entry-Level Security Analyst position, and it is for a 12-month tenure with the option to extend. The job is with the company System One in Rockville, MD, and has a "negotiable" salary. Responsibilities include but are not limited to governance risk and compliance. This relates to the first two jobs with duties including risk assessments. The job is specifically for recent college graduates, so the requirements are slim other than obviously a bachelor's degree. It's hard to grasp what the culture of this company is from the ad as it is very straightforward, but I'd be willing to work it since it is for new college grads only.

As a result, of my conceptual content analysis, I was able to determine what phrases and terms could be used as codes. Key phrases and terms such as "risk assessment", "risk mitigation", "risk", and "monitor" are all codes for the job ads analyzed. They are codes because, in each job ad, one or more of these codes occur and make it obvious as to what skills need to be developed and brought to the table when applying for jobs such as the ones analyzed and ones similar in nature. Due to the frequency at which these codes occur, it is a must that these skills be

acquired and or experienced and added to my ePortfolio. According to Harper, “A key element of content analysis is to ‘code’ data in a way which will categorize it” (Harper, 2012, p. 38).

Conducting a content analysis on four job ads related to Information/Cyber Security has shown that there is so much information to look at and understand in job advertisements. The importance of being able to analyze such ads cannot be stressed enough as knowing how to properly analyze and interpret the information within an ad can help tremendously in preparing for an interview and or personal development. Analyzing these job ads, has opened my eyes to what skills, certificates, and requirements I must meet and possess in order to be prepared and furthermore successful in my desired field.

Enumeration

1. **First Job**

   Description: Predicate Logic is looking for a dynamic self-starting individual to join our Submarine Operating Authority Engineering team providing Cybersecurity, communications, and network technical support for the U.S. Navy Submarine Force. Predicate Logic is currently accepting resumes for a Cybersecurity Analyst opening in **Portsmouth, Virginia**.

   Duties and Responsibilities

- Maintain the applicable component suite fully operational and in compliance with Cybersecurity requirements.
- Provide Cybersecurity analysis support to include, controls analysis, risk assessments, risk mitigation analysis, and contingency plan development.
- Assist government personnel with maintaining strict configuration control of the applicable component suite.

- Conduct Risk and vulnerability assessment and risk mitigation analysis.
- Possess knowledge and comprehension of secure build techniques, tools, and practices of DISA Secure Technical Implementation Guidelines (STIG).
- Implement security-relevant mitigations.

Knowledge and Abilities

- Install, Configure, and Maintain a scalable and highly available virtual environment utilizing VMWare vSphere ESXi hypervisor
- Working knowledge of network analysis tools such as Wireshark.
- Ability to manage and audit the cybersecurity of applicable systems using tools such as HBSS and ACAS.
- Ability to perform log reviews of systems to analyze for evidence of exploitation.
- Ability to interface with remote users via chat, telephone, naval messaging, and email to assist in troubleshooting system functional issues.
- Security + Certification Required.

Experience

- First-hand experience required in the following areas:
- Cisco routers and switches
- VMWare ESXi 5.5 or later
- Server operating systems management
- Cyber security configuration compliance management/auditing
- Intrusion Detection and Mitigation
- Security Vulnerability Assessment
- DISA STIG Implementation
- First-hand experience is strongly desired in the following areas:
- HBSS
- ACAS
- Windows Server 2012 or later

- Windows 10 or later
- Linux Systems Administration
- Serial communications

Possess a current/active Top Secret security clearance. Must be eligible for SCI Access.

Ability to travel within the U.S. and foreign countries. Travel is estimated to be less than 10%. Send resume and cover letter to Predicate Logic, Inc at personnel@predicate.com

2. **Second Job**

GINIA was founded in 2002 by Cybersecurity Subject Matter Experts (SMEs) who established our core capabilities in Cybersecurity consulting. Since the company's inception, GINIA has expanded its primary services to include: Information Assurance, Research and Development, Management Consulting, Business Intelligence (BI), Data Analytics, and Application Development support services to the Department of Defense (DoD), Department of State (DoS), Department of Homeland Security (DHS), and other top Civilian agencies. Our success can be attributed to selecting the absolute best people, process, and technology for each of our clients.

General

Our company is inquiring for a Junior Information Security Analyst to assist one of our federal clients. This is a great opportunity to join a rapidly expanding and successful team. We are looking for someone who has experience evaluating and developing security programs standards. This is a great opportunity to grow with the company. We offer a competitive salary as well as a robust benefits package including healthcare, life and short term disability insurance, pension program, paid time off (PTO) and federal holidays.

Minimum Requirements:

Must be a U.S. Citizen

0-2 years of cybersecurity experience

Must be able to obtain Public Trust

Bachelor’s degree preferred

Responsibilities/ Preferred Qualifications:

Performs vulnerability/risk analysis of computer systems and applications.

Assists with the Risk Management Framework process, including developing Authorization to Operate packages.

Develops and implements information assurance/security standards and procedures.

Identifies, reports, and resolves security violations.

Provides integration and implementation of the computer system security solution.

Runs and reviews vulnerability scans.

Authors and updates security documentation to include but not limited to: system security plan, contingency plans, and configuration management plans.

Supports the development of all project deliverables which may include, but is not limited to, the System Security Plan, Rules of Engagement, test plans, and security assessment report.

Performs analysis, design, and development of security features for system architectures.

Job Type: Full-time

Benefits:

- Dental insurance
- Health insurance
- Life insurance
- Paid time off
- Parental leave
- Retirement plan
- Vision insurance

Schedule:

- Monday to Friday

  Ability to commute/relocate:
- Suite 220 Alexandria, VA 22312: Reliably commute or planning to relocate before starting work (Preferred)

  Education:
- Bachelor's (Preferred)

  Experience:
- Cybersecurity: 1 year (Preferred)

  Work Location: Hybrid remote in Suite 220 Alexandria, VA 22312

3. **Third Job**

   Leidos Defense Group is looking for a Junior Cybersecurity Analyst to works supporting the AFNCR IT Services program at Joint Base Andrews, MD.

   Job Summary:

   The AFNCR IT Services program provides support services for information systems for Headquarters Air Force (HAF), Air Force District of Washington (AFDW), Office of the Secretary of Defense (OSD), Joint Chiefs of Staff, and other Air Force activities within the AFNCR, missions to include the Pentagon, Joint Base Andrews (JBA), Joint Base Anacostia-Bolling (JBAB), and other locations, leased spaces, and alternate sites. The major support areas required are IT Operations and Maintenance; Plans, Projects, and Engineering (PP&E); and National Military Command Center (NMCC). The senior leaders and national defense missions that are supported require that the AFNCR operations never fail, resulting in a fast-paced, challenging, but also rewarding environment.

   If this sounds like the kind of environment where you can thrive, keep reading!

Leidos Defense Group provides a diverse portfolio of systems, solutions, and services covering land, sea, air, space, and cyberspace for customers worldwide. Solutions for Defense include enterprise and mission IT, large-scale intelligence systems, command and control, geospatial and data analytics, cybersecurity, logistics, training, and intelligence analysis and operations support. Our team is solving the world's toughest security challenges for customers with "can't fail" missions.

To explore and learn more, click here!

Are you ready to make an impact? Begin your journey of a flourishing and meaningful career, share your resume with us today!

Primary Responsibilities:

- Monitoring SEIM dashboard for Alerts.
- Performing analysis of malware provided by lead
- Creating reports of cyber anomalies and slide decks to present to leadership
- Reviewing Kibana Queries
- Reviewing Threat intelligence feeds
- Updating YARA rules
- Assist Lead in detection, mitigation, and response to cyber incidents using a combination of technology solutions and processes, and ensuring security issues are addressed quickly on discovery.
- Assist Lead in investigating computer and information security incidents, conducting computer forensic network and host analysis, intrusion and threat hunting support.
- Assist Lead performing penetration tests to evaluate system security, maintaining proficiency in operation tools, creating countermeasures, and identifying trends in

adversary behaviors and vulnerabilities. Responsible for operational planning in support of training, exercises, operations and coordination of integrated cyber operations by targeting hostile adversary activities and capabilities.

- Interpret, analyze, and report all events and irregularities in accordance with computer network directives; including initiating, responding, and reporting discovered events.
- perform full packet analysis of PCAP to determine indication of true incident or false positive using Wireshark.
- Assist Lead in identifying IOCs, TTPs, and other possible malicious activity using various SIEMs.
- Assist Lead in perform detailed analysis of log data to detect and investigate potential security events.

Basic Qualifications:

- Bachelor's degree and less than 2 years of prior relevant experience (additional years of experience / related DISA customer experience and Cyber courses & certifications may be considered in lieu of degree).
- Experience verifying an Indicator of Compromise (IOC).
- Must possess an active Secret clearance.
- DoD 8570 Compliant certifications to include IAT-II at start.

Preferred Qualifications:

- Air Force customer experience.

- Experience with any of the following tools: Trellix, HBSS, ELK, Security Onion, Ansible, Big Data Platform, ELICSAR.

Pay Range:

Pay Range $53,300.00 - $96,350.00

The Leidos pay range for this job level is a general guideline only and not a guarantee of compensation or salary. Additional factors considered in extending an offer include (but are not limited to) responsibilities of the job, education, experience, knowledge, skills, and abilities, as well as internal equity, alignment with market data, applicable bargaining agreement (if any), or other law.

4. **Fourth Job**

   Entry-Level Security Analyst (Recent Cybersecurity College Grad)

   Location: Rockville, MD

   Duration: 12 Months w/ Option to Extend

   Salary: Negotiable

   Looking for recent Cybersecurity College Graduate with prior experience within a Governance Risk & Compliance or Information Security team, ideally in a contributing role. Additionally, a firm grasp of risk escalation procedures is essential.

   Proficiency in using Office 365 tools, the ability to create and maintain customized

SharePoint lists, and expertise in developing Power Bi visuals, reports, and dashboards are highly advantageous skills.

A foundational understanding of NIST Special Publication 800-53 and the application of security/privacy controls is also anticipated. Demonstrated competence in maintaining risk registers and/or policy exception logs.

System One, and its subsidiaries including Joulé, ALTA IT Services, CM Access, and MOUNTAIN, LTD., are leaders in delivering outsourced services and workforce solutions across North America. We help clients get work done more efficiently and economically, without compromising quality. System One not only serves as a valued partner for our clients, but we offer eligible employees health and welfare benefits coverage options including medical, dental, vision, spending accounts, life insurance, voluntary plans, as well as participation in a 401(k) plan.

System One is an Equal Opportunity Employer. All qualified applicants will receive consideration for employment without regard to race, color, religion, sex (including pregnancy, childbirth, or related medical conditions), sexual orientation, gender identity, age, national origin, disability, family care or medical leave status, genetic information, veteran status, marital status, or any other characteristic protected by applicable federal, state, or local law.

References

Harper, R. (2012). The collection and analysis of job advertisements: A review of research methodology. *Library and Information Research*, *36*(112), 29–54. https://doi.org/10.29173/lirg499

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

Information Security Analysts : Occupational Outlook Handbook: : U.S. Bureau of Labor Statistics. (2019, September 4). Retrieved from Bls.gov website: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-2