Abraham Perez
4/7/2024

Computer Network Defense Analyst and the Usage of Social Science (1005)

Introduction:

In this paper, I will discuss the occupation of a Computer Network Defense Analyst (CND Analyst) and its relation to social science. I will also cover various social science principles that can be applied to this job. There will be a discussion of concepts from my CYSE201S class and how they can be applied to the job as well. There's also the clarification of how this career can connect to society and the marginalized groups that relate to it, as well as the challenges that come with said career. Given these key aspects, let's move into the first section.

Principles:

Starting with social science principles, the first principle that can be applied to this job would be parsimony. The reasoning behind this is that one of the roles of a CND Analyst would be "educating our customers to prevent and eradicate the cyber threats to the Defense Industrial Base, critical infrastructures and U.S. National Security Systems" (Indeed, 2024). This helps demonstrate the relation of parsimony because the principle's goal is to keep explanations as simple as possible, that way the "common man" can understand it. Another principle that can be found would be ethical neutrality. This can be related to a CND Analyst's role of distinguishing benign behavior from normal behavior. The relationship between this role and the principle of ethical neutrality can be seen by having a user adhere to ethical standards when overviewing information, specifically should employers be notified of abnormal behavior in a network. One other principle that relates to a CND Analyst's role is skepticism. A CND Analyst needs to be able to have an "open-minded" mindset when it comes to future challenges and problems,

allowing for multiple perspectives to be used. This relates to skepticism because it shows that the user doesn't take claims at face value and evaluates the claims from different angles.

Key Concepts:

One key concept from class that can relate to a CND Analyst's job is the usage of survey research. As cited in "Leveraging Decision Making in Cyber Security Analysis through Data Cleaning" by Zhong, et al., 2017, albeit it's a challenge, "Given the voluminous monitoring data, cyber security analysts need to identify suspicious network activities to detect potential attacks. As the network monitoring data are generated at a rapid speed and contain a lot of noise, analysts are so bounded by tedious and repetitive data triage tasks that they can hardly concentrate on in-depth analysis for further decision making". This usage of monitoring can relate to the topic of survey research because the analysts are monitoring various data being taken from networks. Another key concept from class is human factors. The previous section discusses how a CND Analyst cooperates with customers, this can relate to human factors because a CND Analyst wants to be able to benefit from both the customer's decisions and their own. The third key concept from class that can be related to a CND Analyst is the usage of social engineering. Not only does a CND Analyst maintain a network, but they also require the skills of a penetration tester, this means being able to gain access to a network through whatever vulnerability. So, they might have to use skills such as social engineering to achieve that goal. An example could be asking simple questions such as "Can I have your user login, I work for IT", even though they may not work for IT. Their goal is to persuade users to give them valuable information to gain access to the network. The final key concept that I can find relatable to a CND Analyst is the topic of risk management. Risk management is the usage of methods of mitigating risks, which

should be one of the core knowledge skills of a CND Analyst, as listed in “Cyber Defense Analyst: CISA” from the Cybersecurity and Infrastructure Security Agency (CISA).

Marginalization:

Setting aside the concepts that relate to a CND Analyst’s job, there’s the primary focus on what specific groups it has an impact on. For starters, there’s the consideration that a CND Analyst is going to help out people in a local area. This can be either a small “mom & pop” store by “updating” their network, or even doing maintenance for a school’s network. The goal of a CND Analyst is to help out as much as possible when it comes to cybersecurity problems. But due to this goal, there comes the choice of who/what is a more important priority. Because at the end of the day, the Analyst is trying to gain profit by fixing/securing things. Another challenge would be how much upkeep a network needs. The reasoning behind this is that if the network is so “corrupted”, that it has to be fully restored, or there might be devices or pieces of equipment that are outdated, etc. It starts to become a hassle and comes down to whether or not the Analyst can do anything. One other challenge that a CND Analyst might face would be how some customers might not be “digitally literate”. Although the Analyst does have the core role of teaching the customer the “goings-on” of a network, there’s also the consideration of how much can you teach said customer without completely confusing them.

Connection to Society:

With the previous section discussing specific groups, there’s also the consideration of how the job of a CND Analyst can connect to society. One such connection would be how a CND Analyst monitors people’s private information, much like a parent would monitor their child’s activity/information. The premise of a CND Analyst is that their job is to protect people’s information and diminish any vulnerabilities that can be exploited. Another connection would be

that with the efforts of a CND Analyst, a community could improve their own accessibility to technology. This could mean a decrease in crime or even an increase in cyber awareness. One other connection would be the value of data privacy. As stated before, a CND Analyst focuses on protecting people's private information, so when both parties have a secure connection for their data, it's a win-win for everyone.

Conclusion:

In this paper, I discussed a CND Analyst's role in society, as well as its relation to my CYSE201S Class with its key concepts and principles. There was also the consideration of what challenges the Analyst might face in the work field. Although there is a discussion of marginalized groups in the paper, a CND Analyst can essentially be helpful in several scenarios. It can almost, in a way, create a diverse useful "work palette". Overall, I hope that this informs you what a CND Analyst does and maybe persuades you to look into other occupations in the cybersecurity field.

Works Cited

Found job on indeed.com https://www.indeed.com/viewjob?tk=1hqaumj40irrn800&jk=5684f4d7b5063263&from=sj&jr=1&ad=-6NYlbfkN0AC5S5KfpcrE62cRuYLg6qW_HWiPjKHP06qk-AGfbwYtAHDG2uSkQtKzzXnrBPKrKuXvElVWilcWRf0NllQqnnQ1aao5KNh_MD-wIQrax6BhRZ9bS1yhVuPfBvIr-IBz9WpCGNJvhOieooPHp0cQVQ0P0v2iTJ47_Axhoc87EFLMtrRMQ7OFb7nhn0NIgtEIV7rL9DugOIMk_Dmugks89QKLpNnYhdHwfS4Rxgy6Tm9tJAySRMwfmKAyuQtgApV_uTB6CEU7mQ4sfhFd-kap8XYS4m00f17eS34Z8vDuCm8fCiLY2b2D8k6k3mXT9qqPZIO4McIRxqFM9nn-gbtxC_2QNni1dm7eUuePZ9Lv1DH3eNGDBKEWqMyWn9SJzx_Pvrz88gQyleX4p2uXqoodSi9RX01eCASNyLf2zhqeecadHtG08MMbzsUyN74VmHdyGTTU7ll2ig5xnT3k7p6jbptULv4iwmvk4bvAuFep5CgW66fdFREt2gio2YoqlY4tmM%3D&advn=2500590964327171&xkcb=SoC76_M3CK1Vt-RymB0PbzkdCdPP&xpse=SoCM6_I3CK2hvaRymx0JbzkdCdPP&xfps=1c0f57f6-e74e-4b1e-814b-93a3d8898d6b&vjs=3&ia_hiring_event=1

CISA. (n.d.). *Cyber Defense Analyst: CISA*. Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/careers/work-rolescyber-defense-analyst

Zhong, C., Liu, H., & Alnusair, A. (2017). *Leveraging Decision Making in Cyber Security Analysis through Data Cleaning.* https://digitalscholarship.tsu.edu/cgi/viewcontent.cgi?article=1022&context=sbaj