Shannon Harris

CYSE 201S

Career Paper

Cyber Threat Intelligence Analyst

A career as a Cyber Threat Intelligence Analyst (CTIA) can be both interesting and rewarding. A Cyber Threat Intelligence Analyst is an individual who collects, analyzes and interprets data on risks and threats to a business or organizations security. The primary goal of a CITA is to understand tactics and different techniques used by attackers to proactively protect organizations and companies. Decision making is a major must have to be successful in this role. The salary for this role is in the range of $70,000-$80,000 on average more advanced levels can be up to $!40,000. (Refati, 2024).

Professionals using Social Sciences Research and Principals

Professionals should learn and adapt how to understand and study the human behavior principle of social science theories. Be able to analyze the way actors think, react and interact. This helps to determine why the actors might be committing cybercrimes. Studies show that analyzing human behavior could factor into issues like susceptibility to phishing scams, decision-making under pressure, and the influence of social norms on cyber security practices. Analyzing social trends creates a better foresight into researchers gathering information on potential risks

and vulnerabilities leading to possible cyberthreats. Sociology is also an important principle depended upon in this career sector. Sociology is beneficial to cyber threat intelligence analyst by way of analyzing social media platforms and group networking connecting and gathering information data online. Understanding user behavior from a cognitive perspective is important to researchers as they relate to how human behaviors are learned and have an impact to cybersecurity. Actors' way of thinking could include the reason of why an actor might hack a person could be from a way of upbringing or a personal attachment toward something that had a negative impact on them. (R, 2016)

Culture, Customs and Cybersecurity

According to the class readings cybersecurity culture is "the knowledge, beliefs, perceptions, attitudes, assumptions, norms and
values of people regarding cybersecurity and how they manifest themselves in people's behavior with information
technologies. (material, 2024). For example, a cyber threat intelligence analyst that are a part of an organization culture would have a better understanding and dedication to what it takes to overall protect and secure that company's data. The responsibility and levels of care would be perceived more personally. A researcher or professional that can relate or analyze cybercriminals culture would know how to evaluate their level of sophistication and how they

operate in terms of what languages they use to communicate. I would say that a CTIA is a part of a culture and develop customs to complete their jobs daily. (material, 2024).

The fact that the cyber world can be so unpredictable makes the role of an CTIA to be a creative problem solver. They must be able to be professional, researcher, and be able to decide swiftly but with accuracy. There is also the communication aspect that is important from a social standpoint. As we learned in the modules Social Sciences are interconnected and parallel within Cybersecurity. As a CTIA having a understanding of all these differences and analyzing them will set you apart from others.

Works Cited

Material, C. (2024, 11 23). Module 9 Social Factors.

R, D. (2016). *Cognitive Theories* . Retrieved from APA PsycNet: https://psycnet.apa.org/record/2015-25841-006

Refati, R. (2024, Feb 26). *Becoming A Cyber Threat Intelligence Analyst* . Retrieved from Threat Intelligence Lab: https://threatintelligencelab.com/cybersecurity-career/becoming-a-cyber-threat-intelligence-analyst-2024/#The_CTI_Analyst_Role