Christian Coleman
Professor Yalpi
Cybersecurity and the Social Sciences
November 20, 2024

The Fusion of Cybersecurity and Social Science

Introduction

The role of a Cyber Threat Intelligence Analyst is very much needed in the world today. These professionals have deep understanding of threats in the cyber world. This is to predict and prevent cyber attacks from occurring through their knowledge of human behavior and social trends. This paper explores the ways Cyber Threat Intelligence Analysts use social science research and principles in their daily life, highlighting the profession's connection to societal impact.

Understanding Human Behavior in Cyber Threats

Cyber Threat Intelligence Analysts need to understand the motivations and intentions of threat actors, and that involves psychological and social aspects. For example, when the behavior of ransomware groups is being analyzed, it requires knowledge of criminology and some psychological science. Attackers mainly use methods through social engineering and phishing to take advantage of the fear and urgency that come with the techniques. Having knowledge of these principles allows analysts to develop effective defenses against these types of threats.

Additionally, political science plays a vital role in analyzing nation-state actors. Recognizing international problems and cultural norms helps Cyber Threat Intelligence Analysts understand the intent and potential of attacks that may come from countries like China, Russia, or Iran. Applying these concepts gives analysts a thorough understanding of the threat environment out there in the world.

Context Through Analysis

Cyber Threat Intelligence Analysts use sociology to help them spot trends in cybercrime within certain demographics and cultures. Social Science helps analysts predict how threat actors may take advantage of social weaknesses, such as disinformation aimed at problematic groups. This type of research can be used by analysts to examine how disinformation can affect voter behavior and spark social unrest during elections.

In addition, analysts can tailor their defense tactics based on their knowledge of how certain cultures work. For example, a phishing scam that targets French workers can pose as higher-ranked officials by taking advantage of the hierarchy set in place by that environment. These sociological insights allow threat intelligence to be very effective in society as a whole.

Protecting Marginalized Groups

Marginalized groups such as low-income individuals or the elderly often face a higher risk of cyber attacks and exploitation. Cyber Threat Intelligence Analysts play a crucial role in identifying scams and frauds that target those groups specifically. For example, financial scams could target people that economically weak, while elderly fraud involves fake tech support calls that exploit their lack of knowledge.

Analysts assists organizations by setting policies in place to safeguard communites that are at risk by seeing the current trends in the attacks. Plus, Cyber Threat Intelligence Analysts advocate for easy access to cybersecurity awareness trainings and resources. This empowers

these less fortunate groups to receive the knowledge that they need to protect themselves from future attacks.

Conclusion

A Cyber Threat Intelligence Analyst's work involves a thorough understanding of social trends, human behavior, and cultural differences, going beyond the technical expertise of the job. These experts used social science concepts to deal with vulnerabilities and biases experienced by the less fortunate groups in addition to fighting cyber threats. Social science's contribution to cybersecurity creates a more secure and welcoming online environment while enhancing public confidence in organizations and technology.

Citations

Goss, A. (2024, June 13). *Day in the life of a senior threat intelligence analyst*. Kraven Security. https://kravensecurity.com/a-day-in-the-life-of-a-senior-threat-intelligence-analyst/

Carpenter, P. (2024, August 12). *Council post: Cybersecurity: What can we learn from the social sciences?*. Forbes. https://www.forbes.com/councils/forbesbusinesscouncil/2022/06/24/cybersecurity-what-can-we-learn-from-the-social-sciences/

National Academies Press. (n.d.). *Read "A decadal survey of the social and behavioral sciences: A research agenda for advancing intelligence analysis" at nap.edu*. 6 Integrating Social and Behavioral Sciences (SBS) Research to Enhance Security in Cyberspace | A Decadal Survey of

the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis | The National Academies Press. https://nap.nationalacademies.org/read/25335/chapter/10