Threat Intelligence Analyst

Tayshon Mott

Old Dominion University

CYSE 201s

Diwakar Yalpi

11/14/2025

Introduction

Cybersecurity has become a crucial part of modern life as individuals, businesses, and governments rely heavily on digital systems. One important role in this field is the Threat Intelligence Analyst, a professional who studies potential cyber threats and helps organizations prepare for and prevent attacks. This paper provides an overview of the threat intelligence career and explains how social science principles, key course concepts, and broader societal issues connect to this profession. It also highlights the impact of cybersecurity on marginalized communities and the role analysts play in protecting essential systems.

Social Science Principles

Social science principles help Threat Intelligence Analysts understand the human behaviors behind cyberattacks. Relativism allows analysts to recognize that motivations for cybercrime differ based on a person's background or environment. Objectivity ensures they evaluate threats without personal bias. Parsimony helps them avoid overcomplicating explanations when analyzing data. Empiricism reinforces the importance of using evidence, such as logs and indicators of compromise, rather than assumptions. Skepticism encourages analysts to question whether data is accurate or misleading. Ethical neutrality prevents moral judgment from interfering with analysis, and determinism supports the idea that human actions follow patterns, which helps analysts predict future threats.

Application of Key Concepts

Key course concepts such as history, maturation, testing, instrumentation, mortality, and regression threats relate to how analysts evaluate data. The history threat appears when global

events influence cyber activity, making it important to determine whether changes are due to outside events. Maturation threats relate to the natural evolution of attackers over time. Testing and instrumentation threats remind analysts that changes in system behavior or tools can affect how threat data is interpreted. Mortality threats occur when important data disappears, such as when attackers delete traces of their activity. Regression to the mean reminds analysts that sudden spikes in threats may naturally settle over time. Understanding these concepts helps analysts avoid misinterpreting cyber patterns and strengthens their ability to identify real risks.

Marginalization

Cybersecurity doesn't impact everyone the same way. Marginalized communities usually face higher risks because they might not have access to good security tools or enough knowledge about staying safe online. These groups are often targeted by scams, fraud, or identity theft. Threat Intelligence Analysts help by spotting threats that affect these communities more and by supporting ways to make security resources easier to access. Having more diverse cybersecurity teams also helps reduce bias in analyzing threats and makes protection better for everyone.

Career Connection to Society

Threat Intelligence Analysts are really important for keeping the systems we all rely on safe, like banks, hospitals, transportation, and government networks. They help stop data breaches, system outages, and big cyberattacks that could cause serious problems for the public. On top of that, they provide information and analysis that help shape cybersecurity policies and guide important decisions. By doing this work, analysts help people trust digital systems and make sure essential services run smoothly and safely.

Conclusion

In conclusion, threat Intelligence Analysts are really important because they help keep digital systems safe and show organizations what's going on behind cyber threats, both technically and when it comes to human behavior. Using social science ideas and the key concepts from class makes it easier for them to make sense of data and guess what attackers might do next. With cybersecurity becoming such a big part of everyday life, these analysts aren't just protecting companies—they're also helping make things safer, fairer, and more trustworthy for everyone who uses technology.

References

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *Journal of Cybersecurity*, 5(1), 1–14.

Kuerbis, B., Dorward, J., & Buchanan, B. (2020). Mapping the evolving relationship between cybersecurity and public policy. *Journal of Cyber Policy*, 5(2), 1–20.

Tanczer, L. M., Lopez-Neira, I., Parkin, S., Patel, T., & Danezis, G. (2018). Gender and IoT research report: The implications of smart technology on women's safety. *UCL STEaPP Research Papers*, 1–41.