

Cyber Threat Intelligence Analyst Career Review

Steven Gills

Old Dominion University

CYSE 201S

Diwakar Yalpi

14 April 2026

Cyber Threat Intelligence Analyst Career Review

In the digital age, security is no longer bound to physical barriers. As society becomes increasingly reliant on interconnecting, digital systems, the vulnerability of these networks has created a new frontier of conflict. At the heart of this battleground is the cybersecurity professional, whose role has evolved from a simple technical troubleshooter to a strategic protector of digital integrity.

A Cyber Threat Intelligence (CTI) Analyst is a cybersecurity professional who focuses not only on how the attacks occur, but who specifically is behind it and why they chose their target. By applying principles from psychology, sociology, and criminology, CTI analysts transform technical data into human centered intelligence (Abraham et al., 2025). They rely heavily on several core social science principles to perform their roles effectively. These principles allow analysts to move beyond the typical indicators of compromise to understand the tactics and techniques of the human actor.

Cyber Threat Intelligence Analysts are responsible for monitoring cyber threats, analyzing attacker behavior, and producing reports to guide security decisions . While technical skills are important, their work heavily depends on psychological principles. For example, analysts study attacker behavior and motivation, which relates to psychological theories of decision-making and rational choice. Understanding why attackers engage in phishing, ransomware, or fraud helps analysts predict future threats (*Cyberpedia Threats Cyberthreat Intelligence What Is Cyber Threat Intelligence (CTI)?*, n.d.). Sociological concepts are also central. Analysts examine how cybercriminal groups operate as social networks, often collaborating in online forums or dark web communities. This reflects concepts such as group behavior and social organization (Abraham et al., 2025). Additionally, analysts must understand

how people within organizations respond to threats, including issues like trust, communication, and organizational culture. Another key concept is risk perception, which explains how individuals and organizations interpret cyber threats (Kapon, 2024). Analysts must translate technical risks into understandable information for decision-makers, influencing how organizations prioritize security actions.

Society at large is increasingly interconnected, but this connectivity is not equal. Social science research has identified a phenomenon known as "cyber poverty," where marginalized groups face higher risks of cybercrime due to limited resources and lower digital literacy (LAZAR, 2024). CTI analysts play a vital role in identifying the specific phishing and social engineering tactics used to exploit these communities, allowing for targeted public awareness campaigns.

The career of a Cyber Threat Intelligence analyst is a hybrid of technical expertise and social science insight. By applying psychological profiling, sociological research, and ethical principles like objectivity, analysts are able to humanize the data they monitor. This perspective is essential for protecting a diverse society where cybercrime disproportionately affects the marginalized. Ultimately, CTI is not just a defense of servers, but a defense of the human behaviors and societal structures that rely on them.

References

- Abraham, C., Belanger, F., & Daultrey, S. (2025, August 29). Promoting research on cyber threat intelligence sharing in ecosystems. *Journal of Cybersecurity*, 11(1), tyaf016. Oxford Academic. <https://doi.org/10.1093/cybsec/tyaf016>
- Cyberpedia Threats Cyberthreat Intelligence What Is Cyber Threat Intelligence (CTI)?* (n.d.). Palo Alto Networks. Retrieved April 14, 2026, from <https://www.paloaltonetworks.com/cyberpedia/what-is-cyberthreat-intelligence-cti>
- Kapon, B. (2024, December 12). *The Role of a Threat Intelligence Analyst*. The Role of a Threat Intelligence Analyst. <https://www.kelacyber.com/blog/the-role-of-a-threat-intelligence-analyst/>
- LAZAR, A. (2024, March 25). *Cyber-poor, target-rich: The crucial role of cybersecurity in nonprofit organizations*. CyberPeace Institute. Retrieved April 14, 2026, from <https://cyberpeaceinstitute.org/news/cyber-poor-target-rich-the-crucial-role-of-cybersecurity-in-nonprofit-organizations/>