Cybersecurity Professional Career: Threat Intelligence Analyst

Joshua Martin

School of Cybersecurity

Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Diwakar Yalpi

April 16, 2026

Introduction

Threat intelligence analysts rely heavily on threat modeling and risk assessment frameworks. These frameworks are linked directly to social science principles. Cybersecurity professionals use these models to help them comprehend human behaviors and evaluate how threats impact both systems and people. These threats impact marginalized groups and society as a whole. Examining how threat modeling and risk assessments are used daily by threat intelligence analysts show that work in this field not only protects systems but also protects people.

Threat Models

Threat intelligence analysts use threat models daily. This process includes identifying and categorizing potential threats. Frameworks such as STRIDE, MITRE ATT&CK, and the Cyber Kill Chain mode provide approaches that help these cybersecurity professionals protect systems and citizens everyday. These structures also allow for these professionals to break down attacks into stages. We used the STRIDE threat modeling approach in our smart city architecture to systematically identify security flaws in domains such as transportation, healthcare and smart home. In addition, we used the MITRE ATT&CK architecture to identify threats and match them to known adversarial tactics and approaches (Ouaissa et al, 2025). Threat intelligence analysts everyday interpret data and turn that data into practical takeaways. On a daily basis, these analysts use these frameworks to assess system architecture and to identify any weak points in the architecture.

Risk Assessments

Risk assessments build on threat modeling. This occurs because threat intelligence analysts evaluate the likelihood and impact of any threats that they identify. Tools such as the

Common Vulnerability Scoring System (CVSS) are used to prioritize which risk demands attention the quickest. The CVSS is important because there are multiple threats daily and knowing which threats should be prioritized is important to the safety of the community. CVSS offers a standardized framework to assess the severity of vulnerabilities based on factors such as impact, exploitability, and environmental conditions (Ouaissa et al, 2025). Analysts use these frameworks to decide whether they should escalate an incident or adjust security.

Interactions with Society

Threat intelligence analysts also interact with society through data that is analyzed. Things such as social media, online forums, and other online sources are all related to intelligence. There are many instances of the use of AI on social media platforms. Threat intelligence analysts analyze content that is put out on social platforms. There are inherent risks in using AI systems, including biased outcomes, privacy violations, psychological harm, facilitation of mass surveillance, and creation of environmental hazards… Undoubtedly, newer forms of risks will continue to emerge and add to the uncertainties of an already complex AI development and deployment process (Rangarajan and Ghatak, 2025). Many people interact with AI on a daily basis and many may not even know that they are. This is extremely dangerous because in many cases data can be stolen by AI. Threat intelligence analysts interact with society everyday while also balancing ethical considerations. Analysts balance intelligence gathering and privacy.

Interaction with Marginalized Groups

Marginalized groups are also heavily thought about everyday by threat intelligence analysts. These analysts play a huge role in communicating any risks to the public. The findings from threat intelligence analysts impact the way that individuals respond to cyber threats.

Knowing how different audiences interpret information is an important thing for these professionals to know. Cybersecurity policy can have a significant impact on society, especially for marginalized groups. For example, policies requiring extensive identity verification of online services may disproportionately affect poor individuals who may not have access to such records… By considering the needs and challenges of marginalized groups, cybersecurity policy analysts can develop policies that protect everyone, not just the privileged few (Huitz, 2024). Everyday threat intelligence analysts have to ensure that information is accessible to everyone and not only individuals who have access to certain records. Marginalized groups are thought about on a daily basis to ensure that they are able to access the information, and to ensure that the information is trusted by them because some may have different levels of trust in larger institutions.

Conclusion

In conclusion, threat intelligence analysts rely heavily on threat modeling and risk assessment frameworks, which are related to social science principles. Having these frameworks ensure that these analysts are able to identify and prioritize threats, handle ethical concerns, and assist with interacting with marginalized groups. Analysts rely on society to understand why these attacks are directed at certain systems and populations. Analysts are able to assess how cyber attacks are distributed unevenly across society and they can see that these often place marginalized groups to a more severe degree. By using threat modeling and risk assessment frameworks, threat intelligence analysts work everyday to ensure the safety and security of society as a whole.

References

Ouaissa, et al (2025) *A framework for cyber threat modeling and risk assessment in smart city environments.* Frontiers in Computer Science

Rangarajan & Ghatak (2025) *STRIFE: A socio-technical framework for threat modeling of AI systems*. Illinois Institute of Technology

Huitz (2024), *The role of Social Science in Cybersecurity Policy Analysis*. Old Dominion University.