Cybersecurity Professional Career Paper: Title of the paper

Student Name: Margaret Yardegar

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Professor Yalpi

Date: November 14th, 2025

A Security Operations Center Analyst is one of the core roles in cybersecurity. While the work includes monitoring alerts, analyzing logs, and responding to incidents, the deeper reality is that SOC Analysts operate at the intersection of technology and human behavior. Cyber threats come from people, target people, and exploit predictable patterns in social systems. Because of that, SOC Analysts depend on social science principles to understand threat motives, victim behaviors, and the broader societal impact of cybercrime. This paper explains how the SOC career uses social science in everyday work, how it connects to concepts learned in class, how it impacts marginalized communities, and how this career interacts with society on a larger level.

SOC Analysts rely heavily on social science because every cyber incident ties back to human behavior. Criminology research helps analysts understand offender motivations, especially when analyzing phishing campaigns, fraud attempts, or social engineering patterns. Psychology explains why people fall for certain attacks and why attackers design messages that provoke fear, urgency, or trust. Sociology becomes important when analysts consider how online communities, cultural beliefs, and social norms influence both cybercrime trends and the spread of misinformation. These social science connections help SOC Analysts predict threats, analyze attacker behavior, and develop more effective defensive strategies (Holt & Bossler, 2021).

Several class concepts align directly with a SOC Analyst's daily work. Social engineering shows how attackers target human vulnerabilities instead of technical ones. Power, identity, and inequality help explain why certain groups are victimized more often. Social structure and group behavior apply to organized cybercrime groups and hacktivist movements. Finally, labeling theory helps explain how people rationalize harmful cyber behavior. These concepts allow SOC Analysts to look beyond the computer and see the social environment

shaping cyber incidents. Understanding these ideas gives analysts a broader lens to interpret threats and protect users more effectively (Wall, 2017).

Cybersecurity does not affect everyone equally. Marginalized communities, including low-income individuals, racial minorities, immigrants, and the elderly, often face higher cyber risks because of limited access to technology education, weaker digital protection, or systemic inequities. SOC Analysts play a key role in protecting these groups, even if indirectly, by securing the platforms and institutions they rely on. Analysts must also consider biases built into algorithms, data collection systems, and law enforcement tools. A thorough understanding of these challenges helps SOC Analysts approach their work responsibly and make decisions that do not unintentionally harm already vulnerable groups (Benjamin, 2019). Recognizing these issues allows SOC Analysts to contribute to more equitable digital environments.

The work of a SOC Analyst influences society because cyber threats disrupt hospitals, schools, banks, government services, and everyday life. When analysts detect an attack early, they prevent financial loss, data exposure, or service interruptions for entire communities. Society also shapes the SOC career because new technologies, political tensions, and cultural behaviors change the threat landscape. For example, rising misinformation, online extremism, and global conflicts all lead to new types of cyberattacks. This creates a constant feedback loop between society and cybersecurity. SOC Analysts must understand social patterns to adapt their work and protect the people who depend on digital systems.

A Security Operations Center Analyst is more than a technical role. It requires deep awareness of human behavior, social structures, and the needs of different communities. This career relies on social science research, psychological insights, and sociological concepts to analyze threats and protect organizations. It also has a meaningful connection to society,

especially to marginalized groups who face greater risks online. By understanding both the human and technical sides of cybersecurity, SOC Analysts help create safer digital spaces and support a more secure society overall.

References

Benjamin, R. (2019). Race after technology: Abolitionist tools for the New Jim Code. Polity Press.

Holt, T. J., & Bossler, A. M. (2021). Cybercrime and digital forensics. Routledge.

Wall, D. (2017). Cybercrime: The transformation of crime in the information age. Polity Press.