Security Operations Center (SOC) Analyst:

Jaden Cooper

Old Dominion University

CYSE201S: Cybersecurity & Social Science

Diwakar Yalpi

11/15/2025

Introduction

I think when people think about cybersecurity, they only know what they see in the movies and shows they watch. Movies and shows like: Mr. Robot, The Matrix, Tron: Ares, and The Amateur, all make cybersecurity look a lot more interesting and cooler. What they don't know is that it is a lot slower and involves more patience, and it also doesn't look as cool as they do in the movies. Or there could be people that think it just involves code, firewalls, or hackers, but cybersecurity is so much more than that. It deals a lot with human behavior, understanding them, and understanding society.

In the future, I really want to be able to work from home or wherever I am in the world. So, the Security Operations Center (SOC) Analyst looked very appealing to me, aligns with my desires, and is a great example of a connection to social science. SOC Analysts monitor networks, detect threats, and respond to suspicious activity, but they also rely heavily on social science principles like psychology, criminology, and sociology to understand cybercriminal behavior and protect users, especially from marginalized communities. In my paper, I will talk about this role and how it connects to what we learn in this class.

Description of the SOC Analyst Role

SOC Analysts are the first line of defense in cybersecurity. They work in Security Operations Centers or remotely, and they monitor real-time security alerts, analyze weird patterns, and anything that looks like it could be a potential threat. They work with other IT teams, management, and higher ups, being law enforcement if it gets to that point. According to the Bureau of Labor Statistics (2024), SOC Analysts are in high demand due to the growing number and sophistication of cyberattacks. This role and career are technical, so SOC Analysts

need to understand human behavior, organizational culture, and societal risks to respond effectively and quickly.

Social Sciences in their Daily Work

SOC Analyst use social science principles a lot in their daily work. There are some criminology theories like Routine Activity that help SOC Analyst understand why the attacks happen and who they will go after. Hackers like to go after people and companies with weak security and if they know there isn't much overlook. SOC Analysts are aware of this and try to create alerts and do everything they can from stopping that.

Psychology is a big part in it too, because you are dealing with a lot of human emotion and behavior. Hackers will try to manipulate people over computers to get into the system easier. Research says human error is the number one reason for breaches and cyber attacks because we are careless when clicking things and we just click away without knowing what we click. SOC Analysts know this need to know when it's a phishing attempt whether it's a phone call, an email, or a suspicious message that exploits fear, urgency, or trust. They are also given training and practice on this and should know when someone is trying to create an opportunity to get in the system.

Organization behavior comes to play here too because when an attack is happening it is easy to get nervous and shut down. SOC Analysts need to react and be able to work calmly which connects to our learnings on social science for group dynamics, stress responses, and communication strategies.

SOC Analysts Interaction with Marginalized Communities and Society

Cyberattacks and breaches don't have the same effect on everyone. Marginalized Communities like families with not as much money, older people, and people that struggle with English are vulnerable to these attacks because they lack knowledge on cybersecurity and may not be able to get the top-notch security measures or tech. SOC Analysts are important to these groups because they monitor threats that could affect them and help design systems for them that are secure and meet everyone's needs.

Conclusion

I really like what SOC Analysts do, and I really hope I can get into this career in the future. It's more than just being a technical specialist, they must understand human behavior, organizational dynamics, and society trends. They must use criminology, psychology, and social science principles, they can anticipate threats, educate users, and protect vulnerable populations. This career is a perfect example and was super easy to write about because of how cybersecurity work is not just about technology but also about people and society. Understanding these connections makes SOC Analysts so important and they help keep the cyber world safe for everyone.

References

U.S. Bureau of Labor Statistics. (2025, August 28). *Information security analysts*. U.S. Bureau of Labor Statistics. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Khan, N. F., Ikram, N., & Saleem, S. (2023, April 22). *Effects of socioeconomic and digital inequalities on cybersecurity in a developing country*. Security journal. https://pmc.ncbi.nlm.nih.gov/articles/PMC10122089/

Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. (2020). *Security operations center: A systematic study and open challenges*. IEEE Access, 8. https://doi.org/10.1109/ACCESS.2020.3045514