Cybersecurity Career Paper: Security Operations Center Analyst

Student Name: Cameron Kim

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Professor Diwakar Yalpi

Date: 14 April 2026

Introduction

A Security Operations Center (SOC) Analysts is a cybersecurity professional position responsible for monitoring a company or organization's networks. SOC Analysts respond to cyber attack incidents, identifying suspicious behavior, and preventing data breaches. They work in real time with event management systems. They also use threat intelligence platforms to find abnormal activity and protect data. The purpose of this paper is to explain how SOC analysts rely on social science research in their everyday work.

Social Science Principles

SOC analysts depend on social sciences because many cybercrimes target human behavior and error rather than technology systems. User behavior is one of the weakest links in cybersecurity, as individuals often make predictable mistakes when interacting with technology (Hadlington). Some examples are clicking on malicious links, using weak passwords, or ignoring security warnings. SOC analysts identify risks and design better defenses from understanding these social science behaviors. Analysts analyze user logs to detect abnormal behavior patterns and compare them to regular patterns.

Application of Key Concepts

Several social science concepts apply to SOC analyst roles, including decision making and identifying differences in behavior. Phishing susceptibility research shows that individuals vary in their ability to detect cyber threats, meaning security awareness is not "one size fits all" (Kleitman). SOC teams use this information to create training programs. SOC analysts also use Security Information and Event Management (SIEM) systems to collect and analyze data across an organization to detect anomalies. These systems rely on behavioral data to detect said

irregularities. SOC analysts comply with HIPAA and GDPR to ensure proper handling of sensitive data.

Marginalization

Individuals in low income communities often have limited access to cybersecurity education, making them more vulnerable to scams, identity theft, and phishing attacks. A lack of proper resources disproportionately affects those communities. Research on phishing susceptibility shows that individual differences impact who is more likely to fall victim to cyberattacks (Kleitman). This means marginalized populations with less digital literacy may face higher risks. There are also concerns about surveillance and privacy. Increased monitoring of people in workplaces or public systems can affect vulnerable populations if not regulated. To address this, the cybersecurity field is working to increase diversity and inclusion in the workforce and improve access to cybersecurity education.

Career Connection to Society

SOC analysts play an important role in protecting society's infrastructure. They help secure hospitals, financial institutions, energy systems, and government networks from cyberattacks. Without their work, society would be at a much greater risk. SOC analysts also ensure compliance of policies and laws by monitoring systems and responding to incidents quickly and effectively. By protecting digital infrastructure, SOC analysts maintain trust in technology. This trust is essential for society because every day users rely on digital systems for every day tasks.

Scholarly Journal Articles

My first source is from Lee Hadlington. Hadlington's research shows that human behavior is one of the most significant factors that attributes to cybercrime. The study explains

how user mistakes and psychological tendencies contribute to breaches. This shows that SOC analysts must understand human behavior, not just technological systems (Hadlington).

My next source is from Kirlappos and Sasse. This article emphasizes that usable security depends on trust and user engagement. It argues that security systems must be designed in a way that users can follow. This supports SOC analysts' role in improving training and designing security systems (Kirlappos and Sasse).

The last source is from Kleitman et al. This study examines differences in phishing susceptibility. It shows that some users are more vulnerable than others due to cognitive and behavioral differences. This helps SOC analysts understand why specific training and behavioral monitoring is necessary in cyber defense (Kleitman).

Conclusion

SOC analysts rely heavily on social science principles to perform their daily responsibilities effectively. Research on human behavior, trust, and decision making plays an important role in understanding cybersecurity risks. These professionals use social science concepts to detect threats, improve user awareness, and strengthen organizational defenses. Additionally, cybersecurity has social implications, such as marginalized communities who may face greater risks due to limited access to resources or education. Overall, cybersecurity is not just a technical field, but also a deeply human centered profession.

Works Cited

Hadlington, Lee. “Human Factors in Cybersecurity: Examining the Link Between User Behavior and Security Outcomes.” *Computers in Human Behavior*, vol. 72, 2017, pp. 65–72. https://www.cell.com/heliyon/fulltext/S2405-8440(17)30998-2?_returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS2405844017309982%3Fshowall%3Dtrue

Kirlappos, Iacovos, and M. Angela Sasse. “What Usable Security Really Means: Trusting and Engaging Users.” Lecture Notes in Computer Science, 2014, pp. 69–78, https://link.springer.com/chapter/10.1007/978-3-319-07620-1_7

Kleitman, Sabina, et al. “It’s the Deceiver and the Receiver: Individual Differences in Phishing Susceptibility and False Positives with Item Profiling.” *PLoS ONE*, vol. 13, no. 10, 26 Oct. 2018, https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0205089