Twaitney Addison
4/13/2026
CYSE 201s
Dr. Jordan Quinn

Cybersecurity Career Professional Paper: Security Operations Center (SOC) Analyst

Introduction

A Security Operations Center (SOC) Analyst is a cybersecurity professional responsible for monitoring, detecting, investigating, and responding to cyber threats in real time. SOC analysts work in high-pressure environments where they analyze security alerts, investigate suspicious activity, and help protect organizations from data breaches and attacks. While this career is highly technical, it also heavily depends on social science concepts such as human behavior, communication patterns, decision-making, and social engineering. In everyday SOC work, understanding people is just as important as understanding technology. This paper examines how SOC analysts rely on social science research and principles, and how those concepts apply to their daily responsibilities, especially in relation to society and marginalized groups.

Social Engineering and Human Behavior in Cybersecurity

One of the biggest ways SOC analysts use social science is through understanding social engineering. Social engineering is when attackers manipulate people into giving up confidential information, often by exploiting trust, fear, or urgency. According to Mitnick and Simon (2002), most successful cyberattacks involve some level of human manipulation rather than purely technical hacking. SOC analysts must

recognize patterns of human behavior in phishing emails, suspicious login attempts, and unusual communication patterns.

Psychology plays a major role in this process. For example, attackers often rely on cognitive biases such as authority bias (people trusting someone who appears to be in charge) or scarcity bias (fear of missing out). SOC analysts are trained to identify these tactics in real time when reviewing alerts or investigating incidents. This shows how cybersecurity is not just technical, but deeply connected to how people think and behave.

Sociology, Risk Perception, and Daily SOC Work

SOC analysts also rely on sociology and risk perception theories when prioritizing threats. Not all alerts are equally dangerous, so analysts must decide what requires immediate attention. This decision-making process is influenced by organizational culture, communication structure, and how risk is perceived within a team.

For example, if multiple users in a company report phishing emails, SOC analysts may escalate the issue faster due to collective behavior patterns. NIST (2011) emphasizes that effective cybersecurity programs depend on understanding both technical systems and human organizational behavior. In daily SOC operations, analysts constantly balance technical data with social context to determine which threats are most serious.

Interaction with Marginalized Groups and Society

SOC analysts also interact with broader society, including marginalized communities, through the systems they protect. Cybersecurity incidents often disproportionately affect vulnerable populations. For example, low-income individuals may be more targeted by phishing scams due to limited access to cybersecurity education. Similarly, marginalized groups may be more impacted when healthcare or government systems experience data breaches.

From a social science perspective, this raises issues of digital inequality. If certain groups are less protected or less informed, they become easier targets for cybercrime. SOC analysts contribute to reducing this gap by identifying widespread threats and helping organizations improve security awareness training. ENISA (2020) highlights that cyber threats increasingly target individuals through psychological manipulation, making public education and awareness essential.

SOC analysts also play a role in protecting sensitive personal data, including information about race, health, financial status, and identity. When breaches occur, marginalized groups may face greater harm such as discrimination or financial instability. This makes the SOC analyst's role not just technical, but socially significant in protecting fairness and privacy.

Communication and Decision-Making in SOC Teams

Another important social science concept in SOC work is communication. Analysts must clearly communicate findings to other cybersecurity professionals, management, and sometimes law enforcement. Miscommunication can lead to delayed responses or failed containment of threats.

Group decision-making theory also applies here. SOC teams often work in shifts and collaborate under pressure, meaning decisions are rarely made alone. Effective teamwork, leadership structure, and clear communication channels are essential for fast and accurate incident response. These concepts come directly from organizational psychology and sociology.

Conclusion

The role of a SOC Analyst demonstrates that cybersecurity is not only about technology but also about people and society. Social science principles such as psychology, sociology, and communication theory are essential in understanding threats, responding to incidents, and protecting organizations. SOC analysts rely on these concepts daily when identifying social engineering attacks, prioritizing risks, and communicating within teams. Additionally, their work has a broader social impact, especially in protecting marginalized groups who are often more vulnerable to cybercrime. Overall, this career shows how deeply connected cybersecurity is to human behavior and social systems.

References

ENISA. (2020). *Cybersecurity culture guidelines: Behavioural aspects of cybersecurity*. European Union Agency for Cybersecurity.

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Wiley.

National Institute of Standards and Technology (NIST). (2011). *Information security handbook: A guide for managers (Special Publication 800-100)*. U.S. Department of Commerce.