Cybersecurity Professional Career Paper: SOC Analyst

Student Name: Melissa Gaskins

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Dr. Jordan Quinn

Date: 04/16/2026

A SOC, Security Operations Center, analyst is an important career in the world of protecting people and systems in cyberspace. According to Chamkar et al., Security Operations Center analysts provide organizations with enhanced security protection to ensure confidentiality, integrity, and availability are efficiently maintained (Chamkar et al., 2023). Cybersecurity is important in the modern world because most of the world's population uses technology daily. Therefore, it is important for cybersecurity professionals to provide security measures to the world's population and organizations who incorporate technology into their lives. This paper will discuss how Security Operations Center analysts use social science principles and concepts while protecting the world of technology.

SOC analysts use many of the social science principles in their daily tasks. One of the most common principles they use is skepticism. According to Module Two, "skepticism is the principle that all claims should be questioned and critically examined rather than accepted at face value" (Slide 15). One of the duties of a SOC analyst is monitoring and responding to cyber threats using tools like SIEM that alert the team to possible suspicious activity. According to Alahmadi et al., false positive alerts are quite common at a Security Operations Center (Alahmadi et al., 2022). Therefore, analysts should be skeptical and not immediately believe that alerts are always accurate. They must investigate the alerts before determining it as a real threat. Another principle used by SOC analysts frequently is empiricism. Module Two explains empiricism as studying behavior from research instead of relying on opinions and hunches. SOC analysts must use real data to determine if a threat is real. According to Alahmadi et al., "analysts… process security alerts based on awareness of regular network activity" and "severity rating" (Alahmadi et al., 2022).

One of the key concepts that SOC analysts use during work is risk assessment. According to Module Eleven, “risk assessment is a systematic process used to identify, analyze and evaluate risks associated with potential threats to an organization” (Slide 10). SOC analysts must review a lot of alerts which may be false positives. Therefore, they must determine which alerts should be investigated first assessing which risks are more impactful to the organization or system (Alahmadi et al., 2022). Another social science concept that SOC analysts use is Rational Choice Theory. Module Eleven defines Rational Choice Theory as “individuals/businesses make choices in their best interest” (Slide 14). Once again, analysts use Rational Choice Theory when deciding which alerts should be investigated first.

Certain marginalized groups are more likely to be targeted by cybercriminals and attacks. According to Ghosh et al., people with lower income and living in rural areas are more vulnerable to cyberattacks. The study found the reasoning behind this is due to “low digital literacy, limited economic advantages, and scarce resources for cybersecurity” (Ghosh et al., 2025). To ensure equal digital protection, analysts and other cybersecurity professionals can spread awareness through cybersecurity training to people with low income and living in rural areas.

In conclusion, Security Operations Center analysts play an important part in cybersecurity by adding a layer of security by protecting systems and organizations and monitoring system logs. They help prevent harmful events such as data breaches and disruption of services (Alahmadi et al., 2022). Overall, SOC analysts contribute to the safety and stability of societal infrastructures by ensuring important assets and systems remain safe in the world of technology.

References

Alahmadi, B., Axon, L., & Martinovic, I. (2022). *99% False Positives: A Qualitative Study of SOC Analysts' Perspectives on Security Alarms*. https://www.usenix.org/system/files/sec22-alahmadi.pdf

Ghosh, A., Sudip Diyasi, & Dey, D. D. (2025). Cybersecurity Literacy Programs for Marginalized Communities: Bridging the Gap in Digital Security a. *ResearchGate*. https://doi.org/10.5281/zenodo.14740268

Samir Achraf Chamkar, Maleh, Y., & Noreddine Gherabi. (2023). SOC Analyst Performance Metrics: Towards an optimal performance model. *EDPACS*, *68*(3), 16–29. https://doi.org/10.1080/07366981.2023.2259046