Profession in Cybersecurity: Cyber Defense Analyst

Author: Clyde Cabico

Introduction

A cybersecurity career entails many avenues, each of which must start on a solid foundation. The foundation of cybersecurity is basic knowledge of information technology. Overlooked is a highly critical aspect of cybersecurity—the contributions of social science. As it is explicitly reiterated time and time, humans are the weakest link in cybersecurity. The professional career of a Cyber Defense Analyst requires not only exceptional knowledge of Information Technology but also insights drawn from Psychology, and Sociology remain crucial disciplines that continually cycle to make this professional career whole. The social science disciplines mentioned are integral to understanding the human element in cybersecurity, addressing user behavior, and mitigating vulnerabilities. Key themes from Module 1 and Module 7 in the course CYSE 201s will be drawn upon—Interdisciplinary approach to cybersecurity, connection to marginalized groups, and the human factors in cybersecurity.

Overview: Cyber Defense Analyst

KSATs refer to Knowledge, Skills, Abilities, and Tasks—core competencies essential for specific roles or industries. I will highlight three KSATs that have a relationship with both Psychology and Sociology, required knowledge and skills for the role of a Cyber Defense Analyst per the Department of Defense *Cyber Workforce Framework* (2020).

KSAT (DoD Cyber Exchange, 2020)

1. [991] Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution)
2. [1069A] Knowledge of general kill chain (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
3. [6900] Knowledge of specific operational impacts of cybersecurity lapses.

These three KSATs mentioned are a few of the many required knowledge, skills, abilities, and tasks that construct the expectations and responsibilities of a Cyber Defense Analyst. A cybersecurity defense analyst, most times referred to as a cyber analyst, is a skilled professional focused on securing networks and IT infrastructure—possessing a deep understanding of cyberattacks, malware, and cybercriminal behavior, proactively working to predict and defend against potential threats (Westen Governors University, n.d.).

Connection: CYSE 201s (Mod 1 &7)

The first KSAT requires understanding various classes of attacks, such as insider threats. This requires knowledge of human behavior and psychology, as analysts must anticipate the motives and actions of individuals within an organization

The second KSAT requires deep familiarity with the general kill chain[1] (Lockheed Martin) which emphasizes the importance of identifying patterns in cybercriminal behavior, a concept with a strong foundation in sociology and psychology—it enables analysts to predict and disrupt malicious activities.

[1] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

The last KSAT requires analysts to recognize the operational impacts of cybersecurity lapses—involving a strong understanding of how breaches affect human systems, such as organizational trust and societal resilience, drawing heavily on knowledge of sociological frameworks.

Societal Impact and Marginalized Groups

Marginalized groups are disproportionately faced with heightened cybersecurity risks due to systematic inequities—in most cases economic and education. Cyber Defense Analysts play a crucial role in addressing these disparities by advocating equitable access to cybersecurity training and resources. In addition, analysts can work to design systems and policies that protect vulnerable populations, reducing the societal impact of breaches.

Conclusion

The role of a Cyber Defense Analyst exemplifies the need for interdisciplinary approaches, bridging technical expertise with insights from psychology and sociology. These perspectives are essential for addressing human vulnerabilities and creating comprehensive and effective cybersecurity solutions.

References

Department of Defense Cyber Exchange. (2020, March 20). Cyber Defense Analyst. https://public.cyber.mil/dcwf-work-role/cyber-defense-analyst/

Lockheed Martin. (n.d.). *Cyber Kill Chain®*. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Westen Governors University. (n.d.). *What does a cybersecurity analyst do?* https://www.wgu.edu/career-guide/information-technology/cybersecurity-analyst-career.html