Cybersecurity Career Paper

Threat Hunter

OLD DOMINION UNIVERISTY

CYSE 201S – Cybersecurity & Social Science

November 12, 2025

By: Ethan Spruill

ODU Honor pledge

"I pledge to support the Honor System of Old Dominion University. I will refrain from any form of academic dishonesty or deception, such as cheating or plagiarism. I am aware that as a member of the academic community it is my responsibility to turn in all suspected violations of the Honor Code. I will report to a hearing if summoned."

INTRODUCTION

Cybersecurity has become one of the most essential fields of work in this modern digital era where large industries rely on cybersecurity experts to protect their data, infrastructure, and defend against new and evolving threats. The specific career I have chosen to investigate is the Threat Hunter, a career that specializes in identifying cyberattacks before they cause damage. This paper examines the Threat Hunter profession and explores how social science principles contribute to their daily responsibilities. It also analyzes how our cybersecurity principles we have learned in lecture contribute to this career, and how their role intersects with marginalized communities. Now let's begin our deeper dive into how Threat Hunters contribute to society through the protection of our digital systems.

Social Science Principles

Threat Hunters combine technical cybersecurity skills with social science insights to be able to understand the human behavior behind cyberattacks. By exploiting predictable behavioral patterns and socio-economic factors rather than using purely technical vulnerabilities it makes it far easier to find where threats may be coming from allowing them to stop it before it ever begins. Modern threat hunting increasingly requires understanding the attacker's intent and motivation as attack techniques continue to evolve and are influenced by human behavior rather than only hacking sophistication [1]. Overall, this means that Threat Hunters analyze patterns in human behavior such as personality theories and cognitive theories so that they can find the holes in the digital system to allow them to prevent these evolving attacks before they ever hit. Along with this psychological and behavioral analysis, threat hunters support organizational awareness efforts by communicating the risks they find to help influence employee behavior to create a human firewall of protection and a culture of security.

Application of Key Concepts

The Threat Hunter career relies heavily on core cybersecurity concepts that we have covered, such as stated above how cognitive and behavioral theories help guide them in interpreting the attacker's decision-making and anticipating attacks before they occur. Another example would be our look into economic theories, which suggest that attackers often select targets that would maximize their financial gains while minimizing their risks, which this in turn changes how a threat hunter would prioritize which systems or departments are most likely to be attacked. Each of these concepts align with the professional methodologies present in our scholarly research documents. Threat hunters collect and analyze cyber threat intelligence through platforms like MISP to map attacker techniques and generate hypotheses based on their observed behaviors [2]. Threat hunters use their behavioral analysis techniques to enact this looking at login patterns, or system changes and how they may align between separate attacker users. This is again reinforced by demonstrating that adversary behavior becomes visible in kernel-level audit logs when analysts recognize patterns, a process very comparable to case-study based profiling [3]. Lastly, Victimization theory also applies to this career as attackers often target users that display vulnerability. Threat Hunters ensure that these vulnerabilities in users is relayed to the organization to teach safer practices in the workplace rather than tear down the users that may unknowingly be creating the entry for attackers. Modern threat hunting combines historical attack data with behavioral analysis to predict future threats and proactively defend against them [1]. By uniting technical evidence with these theories that we have covered in our course, threat hunters can easily stop attacks before they cause organizational instability and help ensure that all users conduct safer practices.

Marginalization

Research overall indicates that marginalized groups such as the elderly tend to have less access to cybersecurity knowledge and resources, which overall increases their vulnerabilities to target digital attacks. While this career focuses primarily on organizational defense, they still need to support a broader understanding of how individuals can lower the risk factors associated with these attacks. As threat hunters analyze these behavioral patterns, they are a key factor in the protection of these marginalized groups through their research as they can relay this information to those who aren't as knowledgeable to allow for their digital literacy to grow and protect themselves when they become targeted. Since threat hunting relies on behavioral data, it becomes very crucial that this data is interpreted both simply and ethically so that populations with lower digital literacy can access the cybersecurity education they need [1].

Career Connection to Society

Threat Hunters play an essential role in protecting major digital systems that modern society depends on in any field that you can think of from healthcare to energy systems. By constantly identifying cyberattacks, they prevent threats that can halt these services and damaging overall public trust with these necessary organizations. Each of our scholarly articles reinforces this societal impact: [1] outlines how evolving attack methods threaten all sectors requiring these specialized personnel to maintain them, [2] demonstrates that threat hunting boosts global security readiness by enabling this early detection of threats that would've effected a wide range of companies, [3] further links threat hunting to public safety by showing that advanced cybercriminals can only be stopped by analyzing these behavioral patterns below the technical system layer. These studies collectively show that threat hunters protect the stability of our digital society.

REFERENCES

[1] Mahboubi, A., Luong, K., Aboutorab, H., Bui, H. T., Jarrad, G., Bahutair, M., Camtepe, S., Pogrebna, G., Ahmed, E., Barry, B., & Gately, H. (2024). *Evolving techniques in cyber threat hunting: A systematic review.* Journal of Network and Computer Applications.

[2] Ammi, M., & Jama, Y. M. (2023). Cyber threat hunting case study using MISP. *Journal of Internet Services and Information Security, 13*(2), 1–29.

[3] Zhang et al. (2022). *A flexible approach for cyber threat hunting based on kernel audit records.* Cybersecurity, 5(11). https://cybersecurity.springeropen.com/articles/10.1186/s42400-022-00111-2