Threat Hunter/ Cyber Threat Intelligence Analyst

Student Name: Jacob E. Moore

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 04/15/2026

Introduction

Here's a more natural, human-sounding version that keeps it strong academically but reads less formally. Cyberattacks are becoming more advanced and happen more often, which means organizations need skilled cybersecurity professionals to stay ahead of them. One career in this field is a Threat Hunter, sometimes called a Cyber Threat Intelligence Analyst. Instead of waiting for alerts to pop up, threat hunters take a more proactive approach by digging through networks, systems, and data to find hidden threats before they cause real damage. This type of work requires not just technical skills, but also strong critical thinking and an understanding of how attackers think and behave. Since cybercrime is driven by human decisions and motivations, social science plays an important role in this career. This paper will look at how threat hunters use social science concepts in their day-to-day work, how their role impacts different groups in society, and why this career is so important in today's digital world.

Social science principles

Threat hunters rely a lot on social science because cybersecurity really comes down to understanding people. Hackers aren't just random systems, they're individuals making choices based on motivation, rewards, pressure, and influence from others. When threat hunters understand why attackers choose certain targets, how scams like social engineering trick people, and how cybercriminal groups operate, it becomes easier to predict and catch attacks early. Psychology plays a big role, especially with things like phishing and insider threats. Threat hunters look for patterns in behavior to spot when something feels off. For example, if an employee suddenly starts downloading large amounts of sensitive data late at night, that might raise a red flag. It's not just about the action itself, but how unusual it is compared to normal behavior. Sociology also matters because a lot of cybercrime happens in groups. Hackers often

work together in online forums, ransomware groups, or dark web communities where reputation and trust are important. By understanding how these groups interact and organize themselves, threat hunters can get a better sense of how attacks are planned and what might be coming next.

Applications of Key Concepts

One important social science concept used in threat hunting is rational choice theory. This idea basically means that people think about risks and rewards before making decisions, including committing crimes. Threat hunters use this way of thinking to understand why attackers go after certain targets. For example, industries like banking or healthcare are often targeted because they hold valuable data, making them more appealing to attackers looking for a big payoff. Another key concept is human-computer interaction, which focuses on how people use technology. This helps threat hunters figure out whether something unusual is actually a threat or just a normal mistake. For instance, someone clicking the wrong link or accessing a file at an odd time might not always mean something malicious is happening. Knowing what typical user behavior looks like helps reduce false alarms and makes detection more accurate. Threat hunters also rely on risk analysis and behavioral analytics to spot anything out of the ordinary. They use tools like SIEM systems, endpoint detection software, and user behavior analytics to connect technical data with human actions. This helps them catch threats that might otherwise go unnoticed by automated systems. On top of that, they have to be careful about legal and ethical boundaries. Monitoring user activity comes with privacy concerns, so threat hunters must follow laws, company policies, and regulations when collecting and analyzing data.

Marginalization

Threat hunters need to understand that cyber risks don't affect everyone equally. Some groups are more likely to be targeted, especially when it comes to things like online harassment, identity theft, doxing, surveillance, and scams. People in minority communities, activists, journalists, and lower-income individuals can be at higher risk, often because they don't always have the same access to cybersecurity tools or education. A big part of a threat hunter's job is helping protect these groups by spotting attacks that are aimed at them and stopping those threats as early as possible. They also help organizations strengthen their systems so they're not accidentally allowing harmful or unfair activity to happen. At the same time, they must be mindful of how their tools work, making sure that behavior-monitoring systems don't wrongly flag or single out certain groups. Cybersecurity as a field is also working toward being more diverse and inclusive. Bringing in people with different backgrounds and experiences helps improve how threats are understood and handled, because it adds more perspectives to the problem.

Career Connection to Society

Threat hunters play a significant role in protecting society by defending critical infrastructure and essential services. Banks, hospitals, government agencies, energy providers, and transportation systems all rely on cybersecurity professionals to prevent devastating attacks. Without threat hunters, sophisticated adversaries may remain undetected inside networks for months, potentially leading to financial loss, service disruptions, or threats to public safety. For example, threat hunters help protect healthcare organizations from ransomware attacks that could delay patient care and endanger lives. Public cybersecurity policy also increasingly depends on professionals in this field. Threat intelligence gathered by analysts informs national defense strategies, regulatory compliance standards, and law enforcement investigations into cybercrime.

Scholarly Journal Articles

Harlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors.

This article demonstrates how psychological and behavioral factors influence cybersecurity risks, supporting the importance of understanding human behavior in threat hunting.

Nurse, J. R. C., et al. (2014). Understanding insider threat: A framework for characterizing attacks.

This source provides insight into insider threat behavior and shows how social science concepts help cybersecurity professionals identify malicious internal actors.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime.

This article explains how criminology theories apply to cyberattacks and supports the use of rational choice and behavioral prediction in threat intelligence.

Conclusion

In the end, being a Threat Hunter or Cyber Threat Intelligence Analyst is about more than just technical skills. It's also about understanding people and how they think. By looking at things like attacker motivation, behavior patterns, and how people are influenced or manipulated, threat hunters get a clearer picture of how cyber threats work. Their role is important not just for protecting companies, but also for helping protect vulnerable groups and the systems society depends on every day. As cyber threats keep changing, using social science alongside technical knowledge will continue to be a key part of staying one step ahead.

References

Harlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. *Heliyon, 3*(7), e00346.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime. *Crime Science, 5*(1), 1–12.

Nurse, J. R. C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G., & Whitty, M. (2014). Understanding insider threat: A framework for characterizing attacks. *IEEE Security and Privacy Workshops*.