

Evaluation of a Thesis & Choice of a Research Topic

Prepared by

ALI MMADI, PhD student-Midocean University





Research Issues (2)

Task 1

INTRODUCTION

For this first task of the module "Research Questions 2", I will proceed with the evaluation of a master's thesis in the field of cybersecurity, and then I will present and justify the choice of my own research topic. My presentation will follow the following structure:

- 1) Presentation and evaluation of the chosen thesis.
- 2) Explanation of my personal research topic.
- 3) And finally, the justification of this choice in relation to my research interests.

The thesis I chose to evaluate is entitled: 'The Impact of Social Engineering Techniques on Cloud Infrastructure Security: A Case Study in the Banking Sector.'



Presentation of the evaluated thesis

This work focuses on a major challenge in modern cybersecurity: human vulnerability. While technical defenses in the Cloud are becoming increasingly sophisticated, social engineering remains a remarkably effective attack vector. The author analyzes different techniques, such as targeted phishing (spear phishing) and identity spoofing (vishing), and assesses their effectiveness against employees of financial institutions using cloud services.

The great strength of this thesis lies in its practical approach, combining a solid literature review with a concrete case study, often including simulated penetration tests. It not only lists the threats but also proposes a framework of awareness measures and security policies to mitigate these risks.

I was particularly struck by this thesis due to the clarity with which it presents the breaking point between technology and the human factor.

appropriate research topic

Research Topic: Evaluation of the Effectiveness of Endpoint Detection and Response (EDR) Solutions Against Advanced Persistent Threats (APT).



Explanation of Clarity and Importance

1. **Clarity:** The topic is precise and well-defined. It is not about studying cybersecurity in general, nor all types of EDR solutions. We are focusing on their specific ability to counter a specific adversary: APTs. The key concepts (EDR, APT) are well established in the literature.**Importance:** This topic is of critical importance for several reasons:**Current Issue:** APTs, often supported by nation-states, represent one of the greatest threats to national security and industrial secrets. They are designed to remain undetected for months or even years.**Technological Relevance:** EDR solutions have become the cornerstone of endpoint defense (servers, workstations)

But are they up to the task against such determined and skilled adversaries? Economic and strategic stakes: A breach in these defenses can lead to massive financial losses, theft of intellectual property, and damage to reputation. Assessing their effectiveness is not an academic question; it is an operational necessity for most large organizations. This topic therefore aims to make a tangible contribution to the field by identifying the strengths and, above all, the potential weaknesses of modern EDR technologies.

Relevance to my interests

2. Relevance to my research interests.

This topic is perfectly aligned with my professional aspirations and intellectual curiosity for three main reasons:

Interest in Threat Hunting: I am fascinated by the proactive investigation process that involves tracking signs of a compromise rather than passively waiting for an alert. Analyzing EDR capabilities is at the core of this discipline.

Passion for technical analysis: I have a strong interest in reverse engineering, malware analysis, and understanding the Tactics, Techniques, and Procedures (TTPs) of hacker groups. Studying how an EDR detects these TTPs is a natural extension of this passion.

Desire to contribute to a rapidly evolving field: The threat and defense landscape is constantly changing.

Delving into this research topic will allow me not only to gain cutting-edge expertise but also, I hope, to produce recommendations that can help practitioners better configure and choose their tools. In summary, this is not just a subject of study for me; it is a field in which I wish to build my career.

Logical presentation of the reasons

The logic that led to this choice is a natural sequence of ideas, which I can summarize as follows: Starting point: The evaluation of the thesis on social engineering enhanced my understanding of human risk. This led me to reflect on other types of threats that an organization must face. Construction of the problem: If human risk can be mitigated through training, how can one defend against an adversary who has already crossed this first barrier, stealthily and with long-term objectives?

APTs are the embodiment of this threat. Identification of the key defensive solution: The last line of technical defense against an APT that has infiltrated the network is often the EDR solution, which monitors endpoint behavior in real time. Summary and questioning: Thus, the central question has become evident: "To what extent is our last line of defense effective against the most sophisticated adversary?" My research topic is the structured formulation of this question. You can see that my choice is not arbitrary. It is the result of a cascading thought process, starting from one threat (social engineering) and leading to another (APTs), by identifying a precise and relevant research need in the current cybersecurity landscape.

conclusion

In conclusion, I presented the evaluation of a thesis on social engineering, which served as a catalyst for defining my own research topic. I proposed to study "The Effectiveness of EDR Solutions Against Advanced Persistent Cyber Threats," a subject that I consider to be clear, important, and perfectly aligned with my research interests, as I have attempted to demonstrate logically. I am now eager to continue this project and take on this exciting challenge.

Bibliographic References

- 1.1. Mandia, J., Likhachev, A., & Amin, K. (2021). *Incident Response & Computer Forensics (4th ed.)*. McGraw Hill.
- 1.2. Chen, P., Desmet, L., & Huygens, C. (2014). A study on advanced persistent threats. In *IFIP International Conference on Communications and Multimedia Security* (pp. 63-72). Springer, Berlin, Heidelberg.
- The MITRE Corporation. (2023). *MITRE ATT&CK Matrix*. <https://attack.mitre.org/>
- 2.1. Chuvakin, A., & Storment, C. (2020). *EDR For Dummies*. John Wiley & Sons.
- 2.2. [Sans.org](https://www.sans.org). (2022). *The CIS Critical Security Controls for Effective Cyber Defense, Version 8*. Center for Internet Security. <https://www.cisecurity.org/controls/cis-controls-list>
- 2.3. Vectra AI. (2023). *The 2023 State of Threat Detection Report*.
- 3.1. Scarfone, K., Souppaya, M., & Cody, A. (2021). *Guide to Cyber Threat Information Sharing (Special Publication 800-150). * National Institute of Standards and Technology (NIST). <https://csrc.nist.gov/pubs/sp/800/150/final>
- 3.2. The MITRE Corporation. (2023). *MITRE D3FEND*. <https://d3fend.mitre.org/>
- 3.3. Payne, B. D., & Lee, R. B. (2020). *The Basics of Cyber Safety: A Hands-On Approach*. Jones & Bartlett Learning.
- 4.1. Gartner. (2023). *Magic Quadrant for Endpoint Protection Platforms*. <https://www.gartner.com/doc/reprints?id=1-2G406OQ&ct=230819&st=sb>



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

