

Development of the Theoretical Framework

Field: Cybersecurity

Prepared by

ALI MMADI, PhD student-Midocean University





Research Issues (2)

Task 2

**Subject: Evaluation of the Effectiveness of
EDR Solutions Against Advanced Persistent
Threats (APT)**

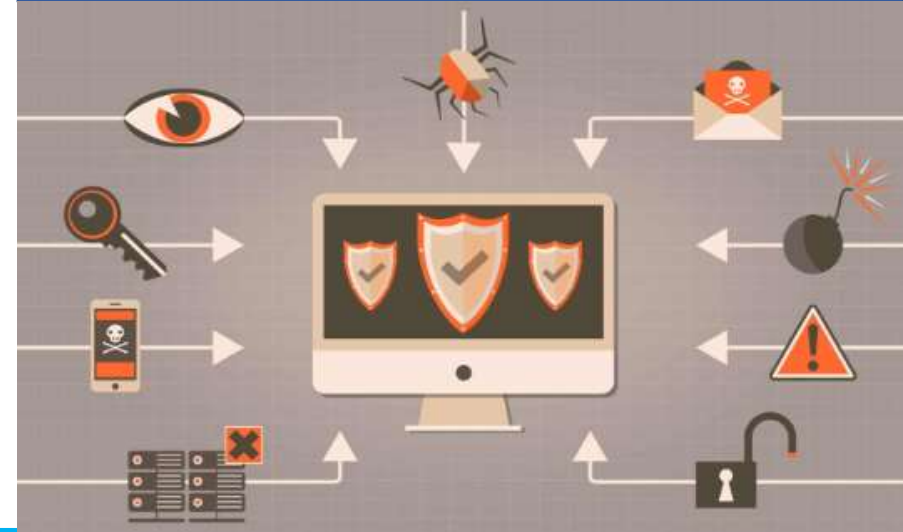


Introduction and Link with Task 1

As part of this second task, I will develop the theoretical framework of my research topic, which is, I recall, 'Evaluating the Effectiveness of EDR Solutions Against Advanced Persistent Cyber Threats.'

This work directly follows the previous task. During the evaluation of the thesis on social engineering, I identified the need to focus on a stealthy and technical threat once the first line of human defense has been bypassed. The theoretical framework that I will present to you today aims precisely to lay the academic and conceptual foundations for understanding and analyzing this threat and the defenses designed to counter it.

Task 1: The Impact of Social Engineering Techniques on Cloud Infrastructure Security: Case Study in the Banking Sector



My presentation will be structured around three main pillars, each corresponding to a key aspect of the literature:

- 1) The threat landscape:** Understanding the APT adversary.
- 2) The defensive ecosystem:** The technological foundations of EDRs.
- 3) The evaluation framework:** How to measure effectiveness in a scientific way.

Pillar 1 - The APT Threat Landscape

The literature agrees on several fundamental characteristics of APTs, well described by authors such as Chen, Desmet & Huygens (2014): their targeted nature, long-term persistence, and high level of sophistication to avoid detection. However, for a study like mine, a simple definition is not enough. An operational model is needed. This is where the MITRE ATT&CK framework becomes the essential source. It is not just a simple glossary; it is a universally adopted library of adversary Tactics, Techniques, and Procedures.

My first theoretical pillar consists of defining and modeling the adversary, that is, Advanced Persistent Cyber Threats.

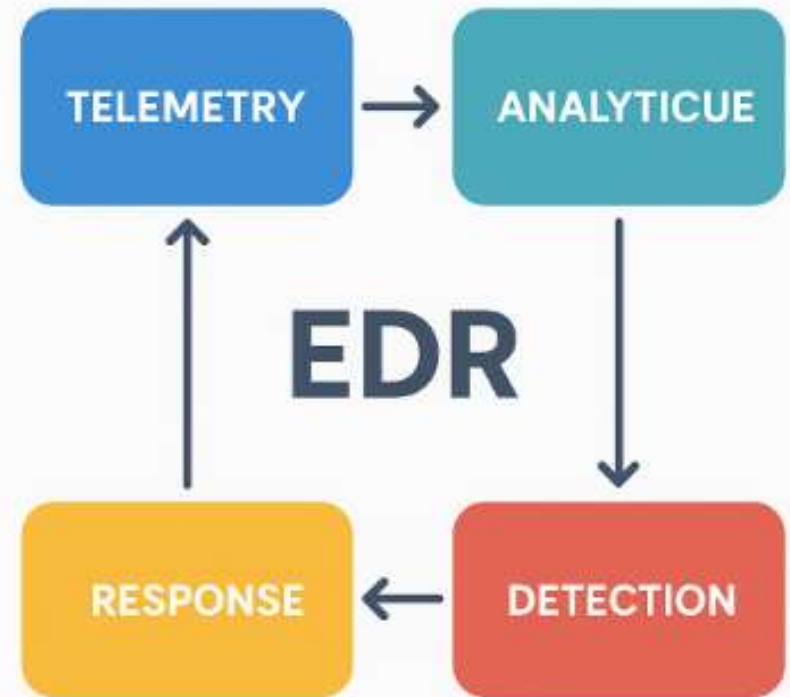
What is the MITRE ATT&CK Framework?



Pillar 2 :The EDR Defensive Ecosystem

The second pillar of my theoretical framework describes defense:

EDR solutions. As Chuvakin explains in "EDR for Dummies," an EDR is not just a simple antivirus. It is a platform built around three key functions, identified in the literature: The collection of rich telemetry on endpoint activity (processes, network, registry). Analytics to turn this data into alerts, using signatures, behavioral analysis, or Machine Learning. Response capabilities to investigate and contain a threat. To frame my evaluation, I need to understand what makes an EDR effective. Here, I turn to best practice frameworks such as the CIS Critical Security Controls.

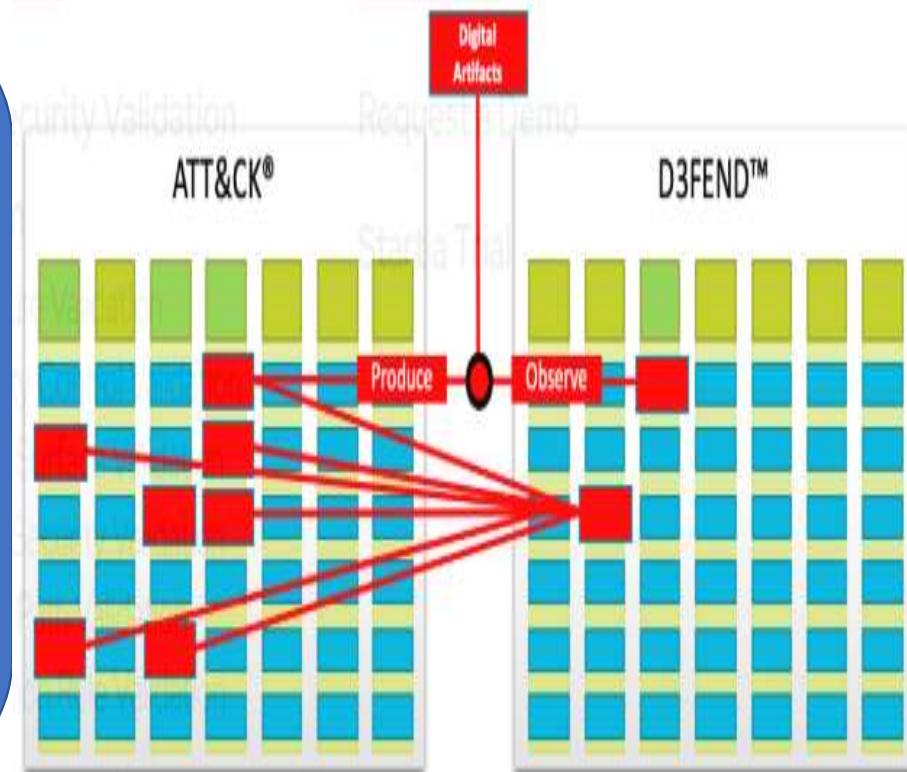


Control 10 on malware monitoring and activity logs precisely defines what an organization must be able to monitor, providing an initial framework for evaluating an EDR's data collection capabilities.

By cross-referencing commercial literature, such as Gartner Magic Quadrant reports, with academic literature, I can identify the main market players (**CrowdStrike, SentinelOne, Microsoft Defender**) and their fundamental architectural differences, which will very likely influence their effectiveness.

Pillar 3 - The Scientific Evaluation Framework

Finally, the third and last pillar is the most critical: how can effectiveness be evaluated in a systematic and reproducible way? This is the central methodological question. To answer it, I cannot rely on opinions alone. I must base myself on solid evaluation frameworks. The MITRE D3FEND framework is an essential theoretical building block here. Designed as the defensive counterpart to ATT&CK, D3FEND maps defense techniques against attack techniques.





Specifically, this allows me to create a direct bridge between my threat modeling and my defense evaluation. For example: ATT&CK Technique "T1078 - Valid Accounts":

Use of compromised legitimate accounts.

D3FEND Countermeasure "User Account Permissions Audit":

Audit of user account permissions. My evaluation protocol will therefore consist of, for each APT technique identified in Pillar 1: Identify the theoretically applicable D3FEND countermeasure. Verify whether the tested EDR implements a function corresponding to this countermeasure. And most importantly, simulate the attack in a controlled test environment, inspired by the methodologies described by NIST in its security testing guides, to observe whether the EDR detects and blocks the activity. This approach, modeled on industry standards, ensures the rigor and objectivity of my future evaluation.

Conclusion

In summary:

Exhaustiveness is ensured through the use of diverse sources: foundational academic articles, standard industry frameworks (MITRE, NIST, CIS), and recent field reports.

The coherence of ideas is maintained through a logical sequence that starts with the threat (APT), moves to defense (EDR), and culminates in an evaluation method (D3FEND/ATT&CK) that systematically links the two. The reliability of sources is a crucial point; I deliberately prioritized authoritative references in the field of cybersecurity, thereby avoiding unverified or purely commercial sources. This theoretical framework does not merely describe the existing situation; it provides an operational roadmap for the upcoming testing phase. It defines what to test, how to test it, and according to which criteria to assess the results. In doing so, it lays a solid foundation for research that is both academically rigorous and practically relevant.

In conclusion, the theoretical framework I have just presented is based on a comprehensive and structured literature review.



Bibliographic References

- 1) The MITRE Corporation. (2023). *MITRE ATT&CK: Design and Philosophy*. Retrieved from https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf
- 2) The MITRE Corporation. (2023). *MITRE D3FEND: A Knowledge Graph of Cybersecurity Countermeasures*. Retrieved from <https://d3fend.mitre.org/>
- 3) National Institute of Standards and Technology (NIST). (2020). **SP 800-160 Vol. 1: Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems**. J. Boyens, C. Smith, A. Bartol, K. Winkler, A. Holbrook, & M. Fallon (Eds.). Gaithersburg, MD, USA: National Institute of Standards and Technology.
- 4) Center for Internet Security (CIS). (2022). *The CIS Critical Security Controls (CIS Controls) v8*. Retrieved from <https://www.cisecurity.org/controls/cis-controls-list>
- 5) 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.
- 6) AV-TEST Institute. (2023). *Independent Tests of Endpoint Detection and Response Solutions*. Retrieved from <https://www.av-test.org/en/>



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

