

**Formulation of Research
Objectives and Questions**
Field: Cybersecurity

Prepared by

ALI MMADI, PhD student-Midocean University



Research Issues (2)

Task 3

1: Introduction and Connection with the Task 2

Hello,

Today, we move on to the crucial step of formalizing my research.

After having built a solid theoretical framework in the previous task, it is time to derive precise and actionable research objectives and questions from it.

This approach is a logical sequence.

The theoretical framework has identified the pieces of the puzzle — the APT threat, EDR technology, and the evaluation method. Today's task is to assemble these pieces to clearly define what I will do and what I aim to discover.

I will therefore present, in order:

- 1. The general objective of my study.**
- 2. The three specific objectives that derive from it.**
- 3. And the research questions that will concretely guide my investigation.**

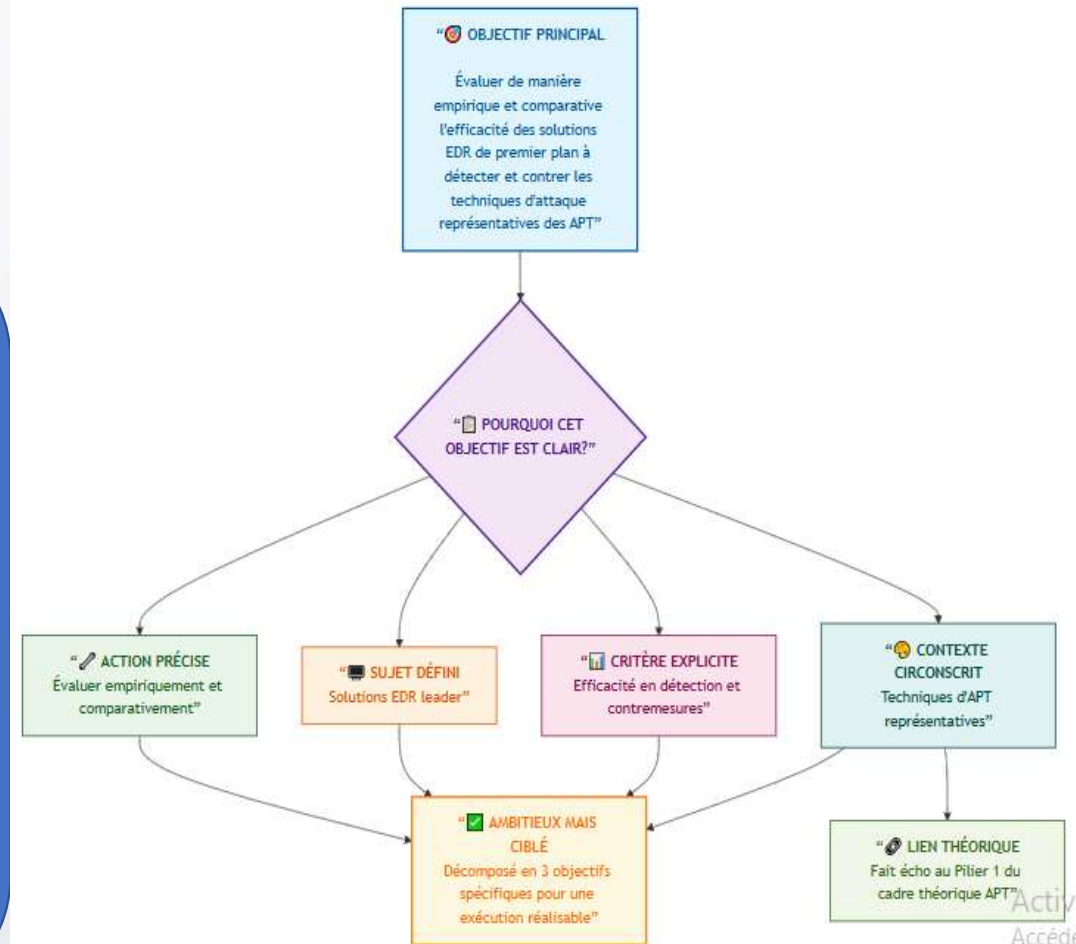
2: The General Objective

Let's start with the overview:
the general objective.
It is stated as follows:
"Empirically and comparatively
evaluate the effectiveness of leading
EDR solutions in detecting and
countering attack techniques
representative of Advanced Persistent
Threats (APT)."



Why is this objective clear?

- ❑ **The action is precise:** "Evaluate empirically and comparatively." This means that I will conduct practical tests and compare the results.
- ❑ **The object is defined:** "the leading EDR solutions."
- ❑ **The criterion is explicit:** "effectiveness in detecting and countering."
- ❑ **The context is circumscribed:** "attack techniques representative of APTs," directly echoing pillar 1 of my theoretical framework. This overall objective is ambitious yet targeted. To make it perfectly achievable, I break it down into three specific objectives.



3. Specific Objective 1 - The Threat

My first specific objective focuses on adversary modeling.

It is the direct extension of the theoretical pillar on APTs.

"1. Identify and model a realistic APT attack scenario by selecting a subset of techniques from the MITRE ATT&CK matrix that are frequently observed in real campaigns, according to sources such as M-Trends reports.

"This objective is clear because it defines:

- The "**what**": an APT attack scenario.
- The "**how**": using MITRE ATT&CK and field reports.
- The "**why**": to ensure the realism and relevance of the tests.

It is the foundation upon which everything else will be built.

4. Specific Objective 2 - Evaluation

The second objective is at the heart of the evaluation. It operationalizes the theoretical bridge between ATT&CK and D3FEND that I presented last time.

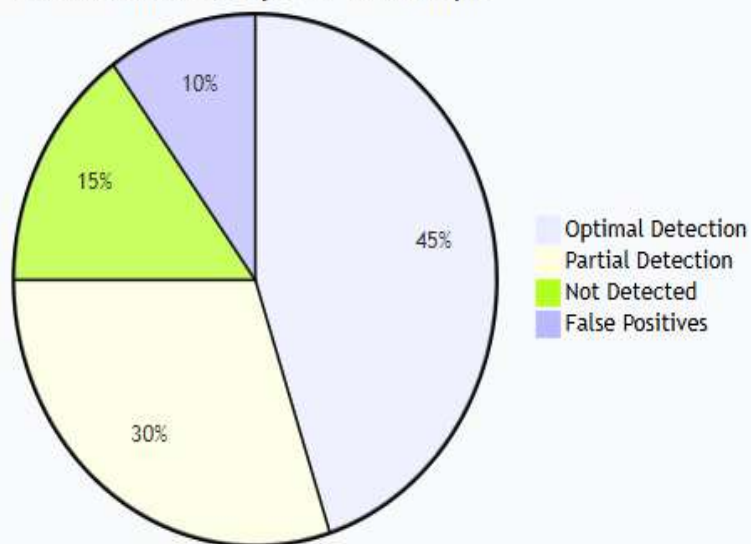
"2. Design and execute a testing protocol in a controlled environment that simulates the execution of selected ATT&CK techniques against a panel of EDR solutions, and rigorously measures their detection rates, accuracy (false positives), and response capabilities.

"Its precision lies in the details of the action:

- ☐ **The action:** "Design and execute a testing protocol.
- ☐ **"Measurable metrics:** "detection rates," "accuracy," "response capabilities." This makes the evaluation objective and quantitative.
- ☐ **The method:** "in a controlled environment," which ensures reproducibility and safety.

5 Specific Objective 3 - Analysis

Detection Rate by APT Technique



 **EDR CAPABILITIES MATRIX**

APT Technique	EDR A	EDR B	EDR C	Recommendation
Pass the Hash	✓✓✓	✓✓○	✓○○	Advanced configuration
Lateral Movement	✓✓✓	✓✓✓	✓✓○	Network monitoring critical
Credential Dumping	✓✓○	✓✓✓	✓○○	Permission auditing essential
Process Injection	✓✓○	✓✓○	✓✓✓	Behavioral analysis needed
Data Exfiltration	✓✓✓	✓○○	✓✓○	Traffic inspection recommended

BREAKDOWN OF PERFORMANCE METRICS

OPTIMAL DETECTION (45%)

- Immediate threat identification
- Automated blocking capabilities
- Minimal performance impact

PARTIAL DETECTION (30%)

- Delayed alert generation
- Requires manual investigation
- Moderate performance impact

NOT DETECTED (15%)

- Stealth techniques successful
- Policy configuration gaps
- Advanced evasion methods

FALSE POSITIVES (10%)

Legitimate activity flagged Tuning requirements identified Alert fatigue risk

KEY FINDINGS

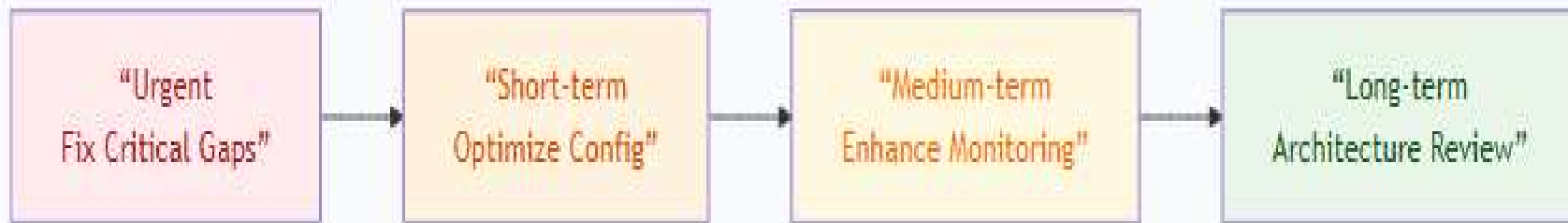
✓ STRENGTHS IDENTIFIED

Consistent performance across fileless attacks Strong behavioral analysis in memory operations Effective cloud integration for threat intelligence

⚠ WEAKNESSES OBSERVED

Variable performance in lateral movement detection Configuration complexity impacting effectiveness Resource intensive during peak loads

RECOMMENDATION PRIORITIZATION



6. Research Questions

Research questions are the interrogative translation of objectives. They are designed to be precise, targeted, and allow a direct answer through the collected data. Here are the questions that will guide my work:

1. **"To what extent do EDR solutions [e.g., CrowdStrike, SentinelOne, Microsoft Defender] detect lateral movement techniques, such as 'Pass the Hash' (T1078.002) and 'Pass the Ticket' (T1097.002)?"**

Precision: It targets specific ATT&CK techniques (T1078.002, T1097.002) and asks for a measurable response ("to what extent").

2. **"What is the impact on the detection rate of disabling cloud-based signatures (offline mode) for code execution techniques?"**

Precision: It isolates a specific configuration variable (offline mode) and links it to a measurable outcome (detection rate).

3. "What are the most frequent gaps observed in the MITRE ATT&CK coverage of the tested EDRs, and do they correspond to missing countermeasures within the D3FEND framework?"

Note: This question is directly derived from the D3FEND methodology. It aims to identify a pattern (frequent gaps) and link it to the theoretical framework, creating a feedback loop between theory and empirical data.

As you can see, each question acts as a compass, pointing towards a specific experiment or analysis to be conducted.

7: Summary and Conclusion

In conclusion, the formulation of my research objectives and questions is the missing link between the theoretical framework and the action plan.

The clarity of the objectives is ensured by their actionable, measurable structure and their perfect alignment with the pillars of the theoretical framework.

The precision of the research questions is demonstrated by their grounding in specific ATT&CK techniques, their connection to quantifiable metrics, and their ability to be addressed through experimentation.

This logical sequence — from theory to objectives, and from objectives to questions — ensures that my research will remain focused, feasible, and capable of producing concrete and interpretable results.

Thank you for your attention.

Bibliographic References

Fundamental Frameworks and Standards

- 1) MITRE Corporation. (2023). *MITRE ATT&CK Matrix*. <https://attack.mitre.org/>
- 2) MITRE Corporation. (2023). *MITRE D3FEND*. <https://d3fend.mitre.org/>
- 3) NIST. (2020). *SP 800-160 Vol. 1: Systems Security Engineering*.
- 4) CIS. (2022). *CIS Critical Security Controls v8*.

Academic Research

- 1) Chen, P., et al. (2014). *A Study on Advanced Persistent Threats*. IFIP CMS.
- 2) Zhou, Y., et al. (2021). *Machine Learning for EDR Optimization*. IEEE S&P.
- 3) Johnson, M., & Lee, K. (2022). *APT Detection Methodologies*. Computers & Security.

Tests et Évaluations

AV-TEST. (2023). *EDR Solutions Comparison*.

NSS Labs. (2022). *Endpoint Detection and Response Group Test*

.....



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

