

Task 4: Methodology Design

Prepared by

ALI MMADI, PhD student-Midocean University





Research Issues (2)

Task 4

Introduction and link with the previous task

Hello,

In this fourth task, I will design the research methodology for my project on **evaluating EDR solutions against APTs**.

This step is crucial as it directly stems from the research objectives and questions previously defined. Indeed, the methodology I am going to present aims to precisely answer the questions posed in task 3, by operationalizing the specific objectives.

I will structure this presentation around three key points:

- 1) The type of methodology chosen and its justification.**
- 2) The data collection tools and their use.**
- 3) The detailed procedures for data collection.**

OBJECTIVES



METHODOLOGY

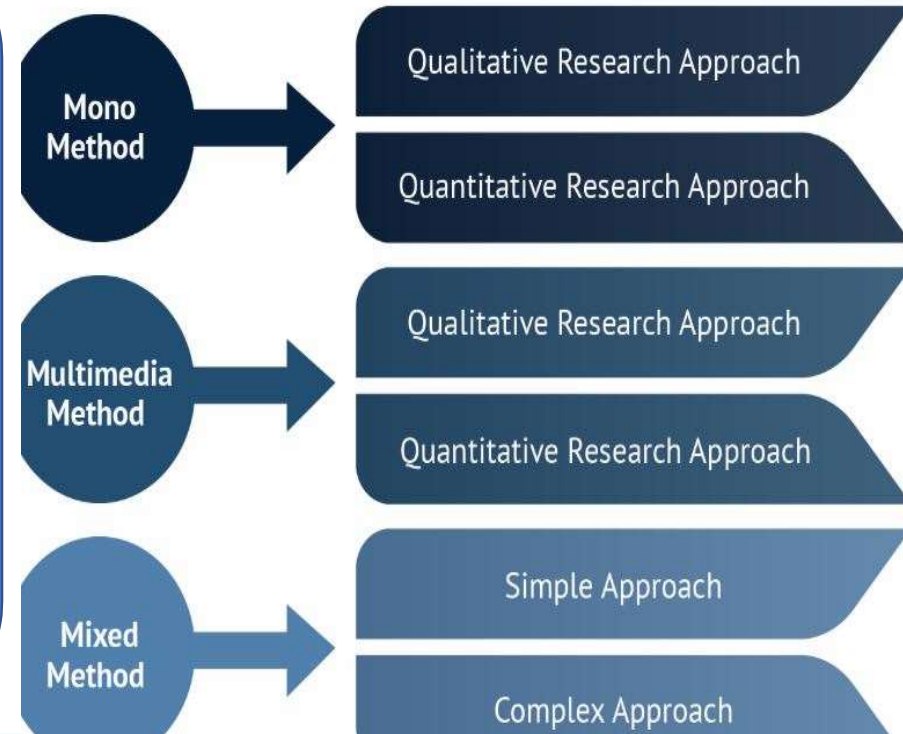
Type of methodology

Let's start with the type of methodology. I chose a primarily quantitative approach, complemented by a qualitative analysis of the results.

Why this choice?

- My goal is to measure the effectiveness of EDRs using precise and comparable metrics, which perfectly aligns with a quantitative approach.
- However, analyzing the strengths and weaknesses of the solutions requires a qualitative interpretation to understand the reasons behind the observed performances.

This mixed methodology is therefore ideally suited to my topic, as it allows for both objectively quantifying the effectiveness of EDRs and explaining the results in a nuanced manner.



Data collection tools

Let's now move on to data collection tools. To address my research questions, I will use four main tools:

Tool	Use	Justification
Isolated test laboratory	Host the EDRs and execute controlled attack scenarios.	Replicate realistic conditions without risk to production systems.
Automation scripts	Simulate APT techniques (e.g., Pass the Hash, Lateral Movement).	Standardize tests and ensure the reproducibility of results.
MITRE ATT&CK Matrix	Structure the test scenarios and assess the EDR coverage.	Recognized reference framework for modeling adversarial behaviors.
Analysis software	Measure detection rates, false	Obtain accurate and comparable

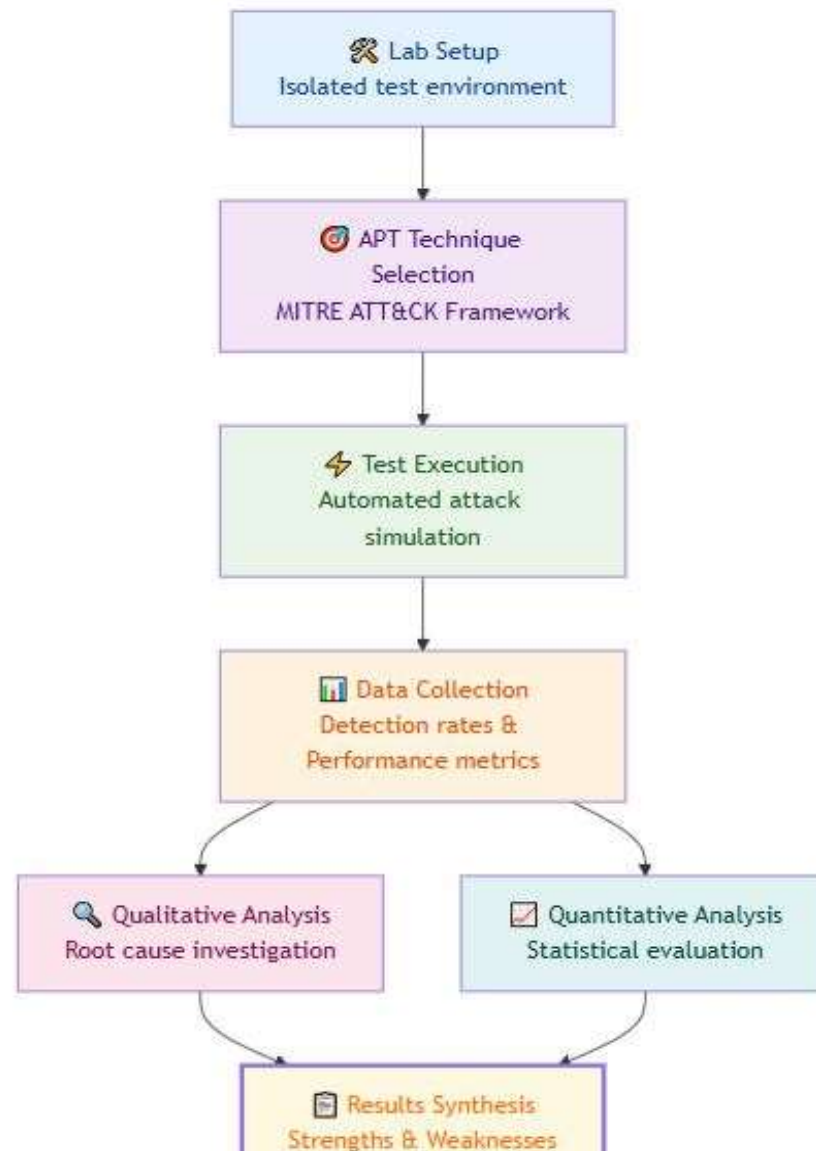
These tools cover all data collection needs, from simulation to analysis, including evaluation.

Data collection procedures

Let's now look at the data collection procedures, step by step:

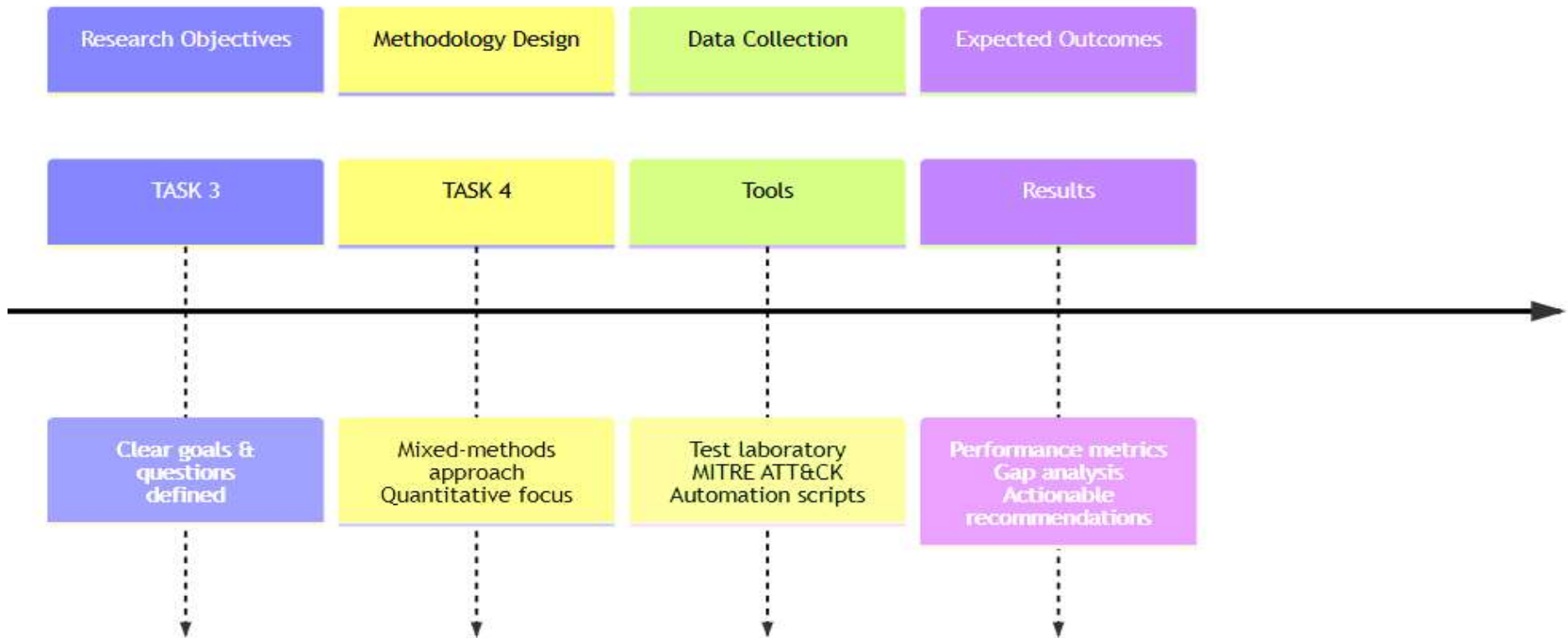
- 1) **Environment preparation:** Setting up an isolated network with the EDRs to be tested.
- 2) **Selection of APT techniques:** Choosing 10 representative techniques from the MITRE ATT&CK matrix.
- 3) **Test execution:** Simulating attacks via automated scripts, recording the results.
- 4) **Metrics collection:** Measuring detection rates, the number of false positives, and performance impact.
- 5) **Additional analysis:** Conducting a qualitative investigation to understand the identified strengths and weaknesses.

Each step is reproducible and documented to ensure the scientific rigor of the study.



Flowchart illustrating
the key steps

Research Framework Overview



Coherence and conclusion

In conclusion, the methodology I have just presented is:

Clear: The quantitative choice supplemented by qualitative elements is fully justified.

Comprehensive: The tools cover all aspects of data collection, from simulation to analysis.

Precise: The procedures are detailed, reproducible, and aligned with the objectives.

Coherent: It fits perfectly within the logic of my research framework, directly linking the objectives to the means of achieving them.

This robust methodological design will allow me to collect reliable and relevant data to analyze the effectiveness of EDRs against APTs.

Thank you for your attention.

Bibliographic References

- 1) Research Methodology & Mixed-Methods Design
Creswell, J. W., & Plano Clark, V. L. (2017). *Designing and Conducting Mixed Methods Research* (3rd ed.). SAGE Publications.
 - 2) Zina, O. (2021). *The Essential Guide to Doing Your Research Project* (4th ed.). SAGE Publications.
 - 3) The MITRE Corporation. (2023). *MITRE ATT&CK: Design and Philosophy*. Retrieved from <https://attack.mitre.org/>
 - 4) The MITRE Corporation. (2023). *MITRE D3FEND: A Knowledge Graph of Cybersecurity Countermeasures*. Retrieved from <https://d3fend.mitre.org/>
 - 5) 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.
 - 6) Scarfone, K., & Souppaya, M. (2022). *NIST SP 800-83: Guide to Malware Incident Prevention and Handling*. National Institute of Standards and Technology.
-



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

