

Task 5: Data Collection

Prepared by

ALI MMADI, PhD student-Midocean University



Research Issues (2)

Task 5

Introduction and link with the previous task

Assalam Anlaikum!!!

Today we are moving on to Task 5, dedicated to data collection. This step is crucial because it represents the practical implementation of the methodology we designed in Task 4. If the methodology was the roadmap, data collection is the journey itself.

My evaluation will focus on the clarity of objectives, the comprehensiveness of methods, the accuracy of the sample, and quality control.



Type of methodology

Let's start with the purpose of the collection. This directly stems from the research questions in Task 3:

Research Question	Data to Collect	Specific Objective
To what extent do EDRs detect lateral movement?	Detection rate, alert logs	Quantifying effectiveness against specific APT techniques
What is the impact of offline mode on detection?	Performance metrics, detection results	Assess resilience without cloud connectivity
What are the gaps in ATT&CK coverage?	Coverage matrix, analysis reports	Identify common weakness patterns

This alignment ensures that each piece of data collected directly serves to answer a specific research question.

Collection and Implementation Methods

Let's move on to the data collection methods. In accordance with the mixed methodology, I will use:

1. Quantitative Methods:

- **Automated tests** using Python/Bash scripts to simulate 10 ATT&CK techniques
- **Metrics collection:** detection rate, response time, resource consumption
- **Tools:** Virtualized lab (VMware), automation scripts, cron jobs

2. Qualitative Methods:

- **Analysis of logs** and alerts generated by EDRs
- **Direct observation** of administration interfaces
- **Evaluation grid** based on the D3FEND framework

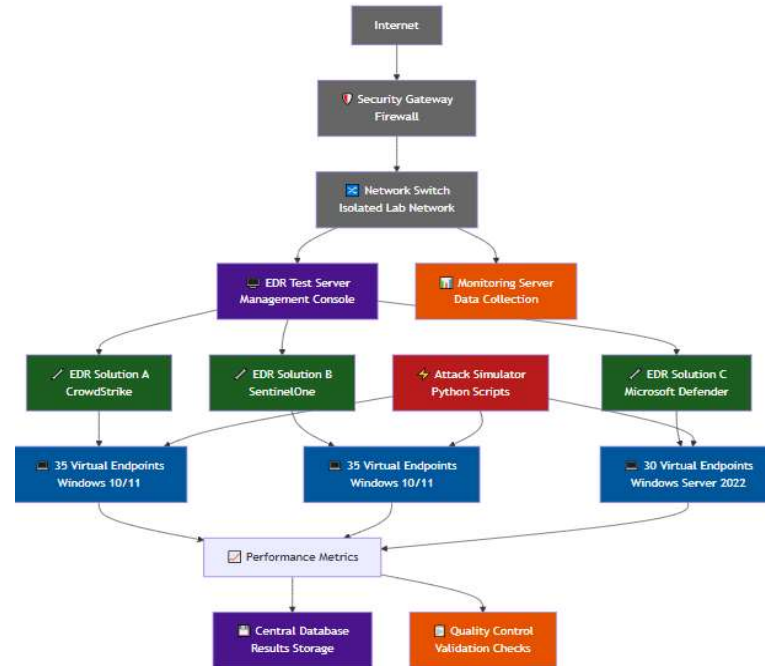
Each test will be repeated 10 times to ensure the reliability of the quantitative data.

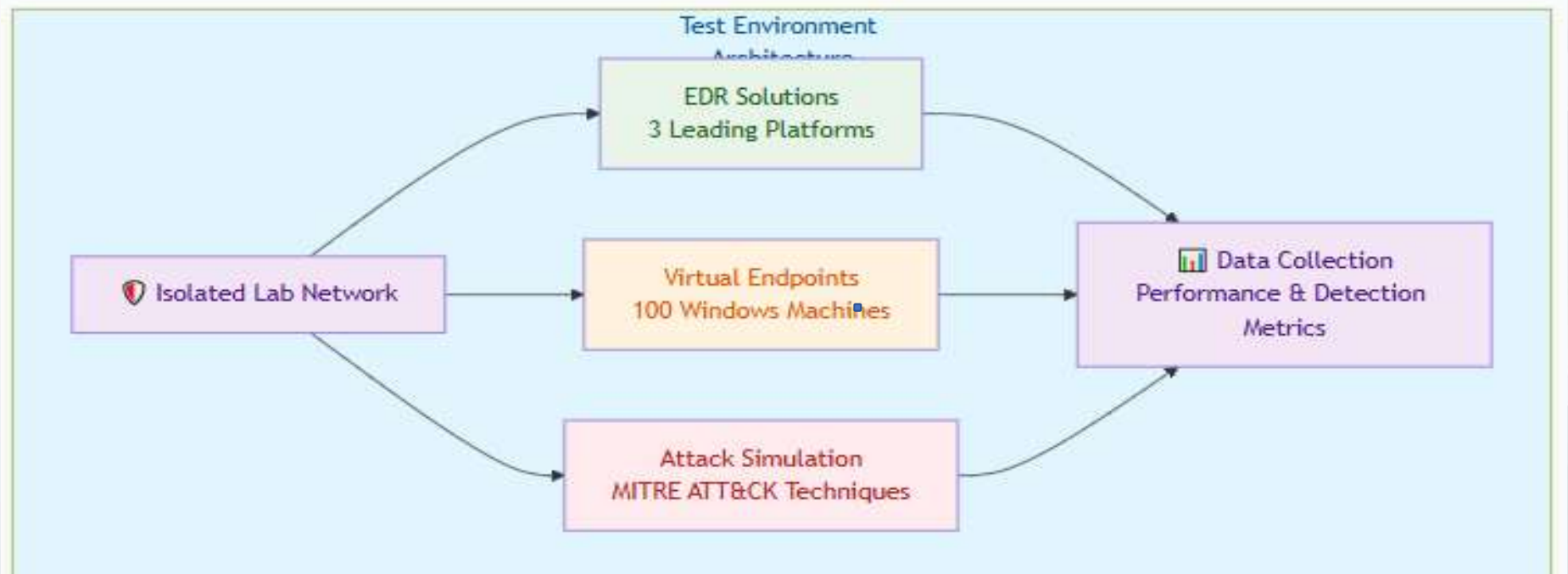
Sample and selection method

The sample is precisely defined:

Sample of EDR Solutions:

- 3 leading solutions selected according to the Gartner 2024 Magic Quadrant
 - market share, advanced feature **Selection criteria:** s, enterprise relevance
- Test Environment: 100 virtual endpoints (Windows 10/11, Windows Server 2022) Standard configurations according to CIS benchmarks Isolated network simulating a typical enterprise environment

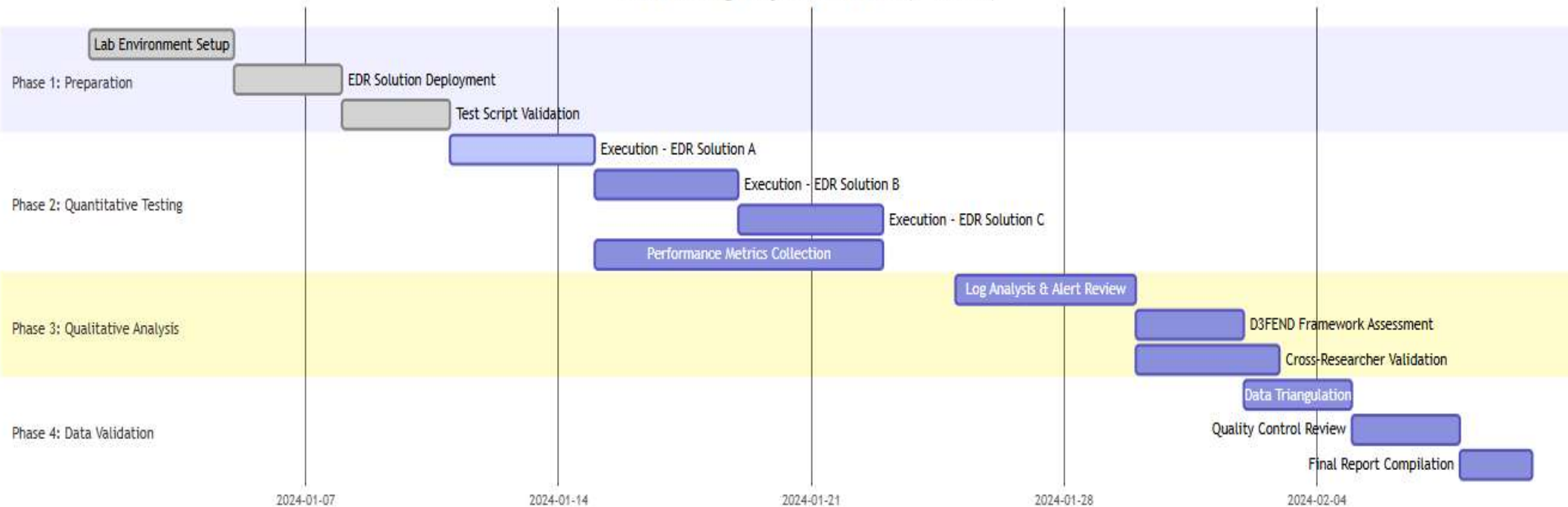




The method is therefore a reasoned sampling based on objective criteria of representativeness.

Schedule and quality control

EDR Testing Project Timeline (4 Weeks)



4-week schedule:

Week 1: Lab setup and EDR deployment

Week 2: Execution of quantitative tests (200 tests in total)

Week 3: Collection of qualitative data and log analysis

Week 4: Data validation and triangulation

Quality Control:

Cross-validation: 2 researchers analyze the same datasets

Experiment log: documentation of each anomaly or observation

Pilot tests: protocol validation on 1 EDR before full deployment

Random checks: 10% of tests repeated to verify consistency

Summary and conclusion

In conclusion, this approach to data collection:

- Aligns perfectly with the research questions and methodology
- Combines quantitative and qualitative methods for a comprehensive view
- Defines a representative sample with clear criteria
- Integrates rigorous quality controls to ensure reliability

This systematic approach ensures that the data collected will be robust, relevant, and directly usable for analysis.

Thank you for your attention.

Bibliographic References

1) Foundational Testing & Evaluation Frameworks

The MITRE Corporation. (2023). *MITRE ATT&CK: Design and Philosophy*. Retrieved from <https://attack.mitre.org/>

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*. 4) J. Boyens, C. Smith, A. Bartol, K. Winkler, A. Holbrook, & M. Fallon (Eds.).

Johnson, C. S., Badger, M. L., Waltermire, D. A., Snyder, J., & Skorupka, C. (2016). *Guide to Cyber Threat Information Sharing* (NIST Special Publication 800-150). National Institute of Standards and Technology.

6) Boss, S., Kirsch, J., & Simon, L. (2022). *Towards a Framework for Evaluating Endpoint Security Solutions*. In *Proceedings of the 2022 ACM on Workshop on Cybersecurity*

7) Research Methodology & Quality Assurance

Creswell, J. W., & Plano Clark, V. L. (2017). *Designing and Conducting Mixed Methods Research* (3rd ed.). SAGE Publication
Practical Implementation & Tools

Sanders, C., & Smith, J. (2018). *Applied Network Security Monitoring: Collection, Detection, and Analysis*. Syngress.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

