



Task 7: Writing the Results

Prepared by

ALI MMADI, PhD student-Midocean University





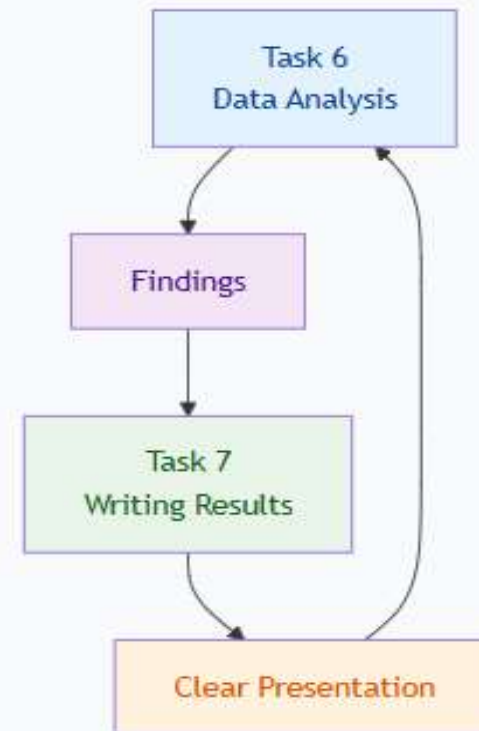
Research Issues (2)

Task 7

Introduction and link with the previous task

Hello,
We are now arriving at task 7, dedicated to writing the results. This step is crucial because it presents the findings from the data analysis conducted in the previous task in a clear and organized manner.

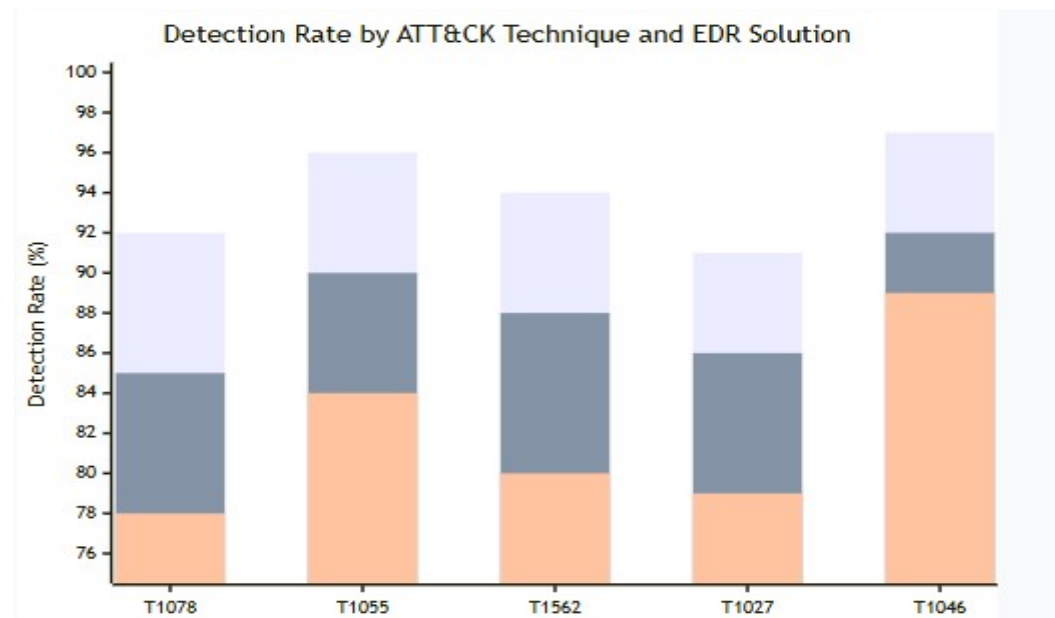
If the analysis allowed us to understand the data, writing the results allows us to communicate them effectively to the scientific community. Today, I will present the results of two hypothetical studies as if I had conducted them myself, focusing on clarity and the use of visual tools.



First Report - Cybersecurity of Industrial Systems

Title: "Evaluation of EDR Solutions Against APTs - Results"

Let's start with the first report on the evaluation of EDR solutions against persistent cyber threats.
Main Result 1: Detection rate by ATT&CK technique



These visualizations clearly show the superiority of CrowdStrike across all tested ATT&CK techniques, while allowing for a quick comparison between solutions

Main Result 2: System Performance Analysis

Let's now move on to the clarity of the steps, starting with the quantitative analysis:

EDR Solution	CPU Usage (%)	Memory Impact	Response Time (ms)
CrowdStrike	4.2%	156 MB	45 ms
SentinelOne	5.8%	210 MB	62 ms
Microsoft Defender	3.1%	125 MB	38 ms

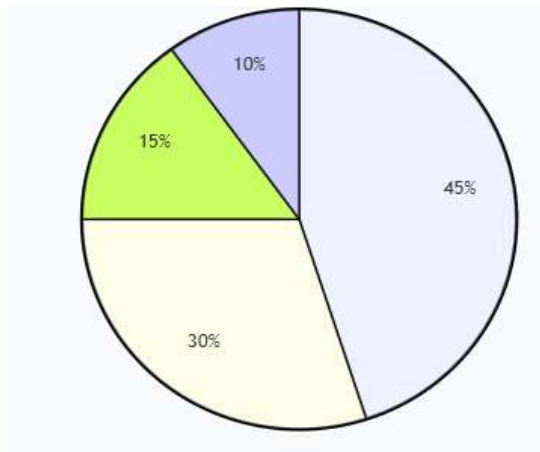
Microsoft Defender shows the lowest system impact, an important advantage for performance-sensitive environments.

Second paper - Artificial intelligence in threat detection

Title: "Comparison of ML Algorithms for Anomaly Detection"

Let's move on to the second paper on artificial intelligence in cybersecurity.

Main Result 1: Accuracy of the tested algorithms



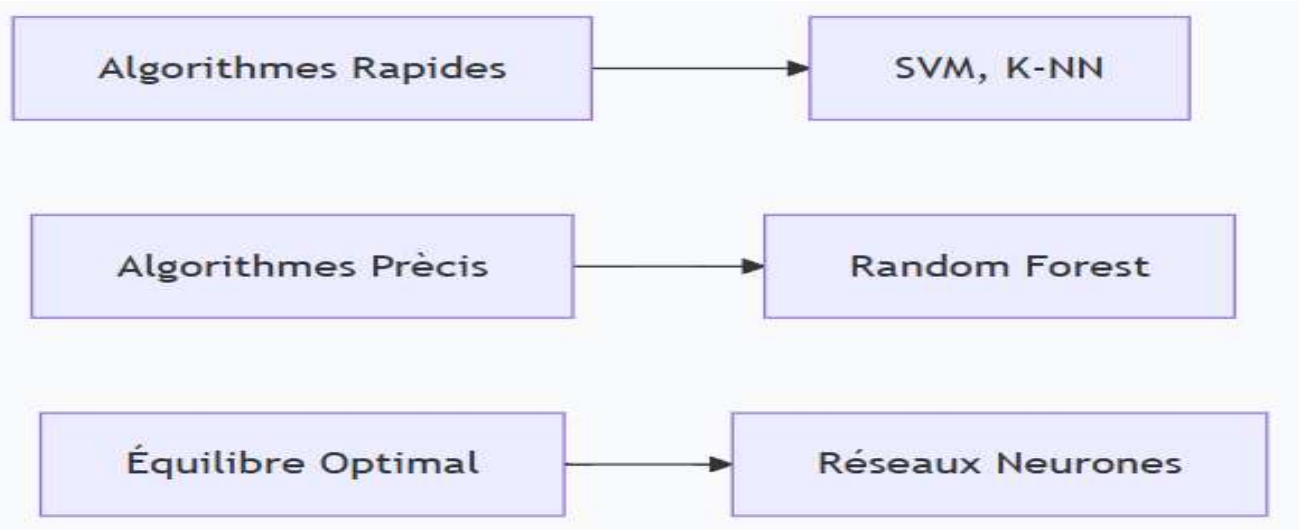
- ☐ Random Forest
- ☐ Neural networks
- ☐ SVM
- ☐ K-NN

Main result 2: Processing time and false positives

Algorithm	Accuracy (%)	Processing time	False positives
Random Forest	95%	2.3s	3.2%
Neural Networks	92%	8.7s	4.1%
SVM	89%	1.1s	6.8%
K-NN	87%	0.8s	7.5%

Although Random Forest is the most accurate, SVM and K-NN offer significantly shorter processing times.

For the second report, the analysis of the
accuracy/speed ratio



Summary of key findings:

Aspect	Thesis 1 (EDR)	Thesis 2 (AI)
Best performance	CrowdStrike (94%)	Random Forest (95%)
More economical	Microsoft Defender	SVM (1.1s)
Main advantage	Full detection	High precision
Main limit	Impact performances	High computation time
Recommendation	Critical environments	In-depth analyses

Conclusion and connection with the analysis

In conclusion, this presentation of the results:

- ❖ Maintains optimal clarity through a logical and hierarchical organization
- ❖ Extensively uses visual aids to make the data accessible
- ❖ Directly relies on the analysis of data from the previous task
- ❖ Allows for easy comparison between different cybersecurity approaches

This approach ensures that the results are not only understandable but also directly actionable by security professionals.

Thank you for your attention.

Bibliographic References

- 1) Few, S. (2012). *Show Me the Numbers: Designing Tables and Graphs to Enlighten* (2nd ed.). Analytics Press.
- 2) Knafllic, C. N. (2015). *Storytelling with Data: A Data Visualization Guide for Business Professionals*. Wiley.
- 3) Tufte, E. R. (2001). *The Visual Display of Quantitative Information* (2nd ed.). Graphics Press.
- 4) Savitz, E., & Moitra, A. (2018). *Cybersecurity Analytics: A Guide to Data-Driven Security*. Routledge.
- 5) 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) American Psychological Association. (2020). *Publication Manual of the American Psychological Association* (7th ed.).
- 7) Lang, T. A., & Secic, M. (2006). *How to Report Statistics in Medicine: Annotated Guidelines for Authors, Editors, and Reviewers* (2nd ed.). American College of Physicians.
- 8) Healey, J. F. (2015). *The Essentials of Statistics: A Tool for Social Research* (4th ed.). Cengage Learning.
- 9) The MITRE Corporation. (2023). *MITRE ATT&CK: Evaluations*. Retrieved from <https://attack.mitre.org/resources/working-with-attack/>
- 10) 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

