

Presentation of a scientific research problem in cybersecurity

Prepared by

ALI MMADI, PhD student - Midocean University



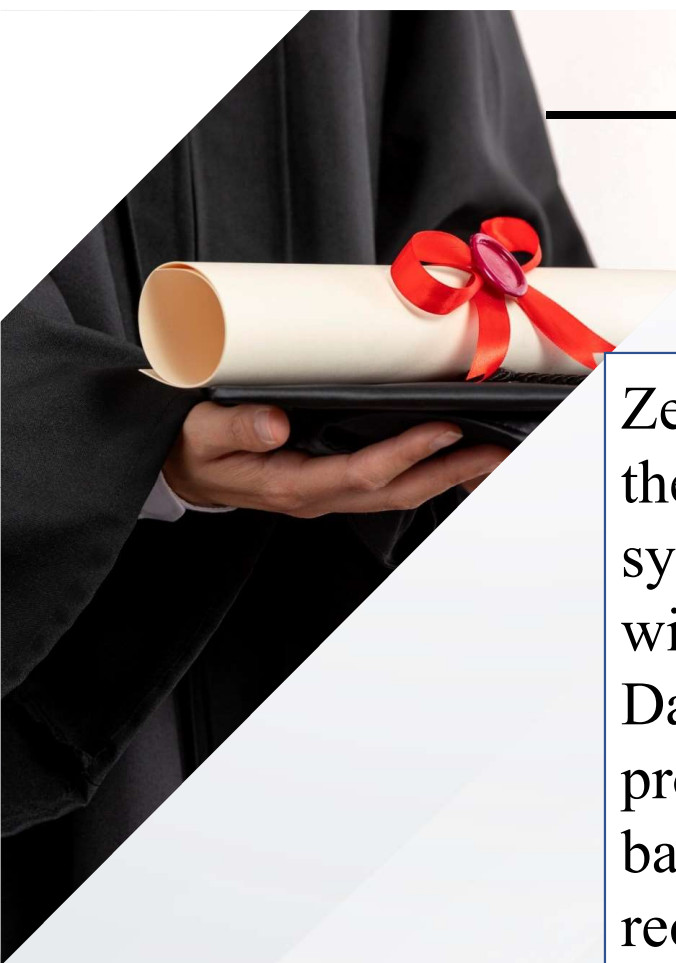
Research Skills 1

Task 4

Chosen scientific research: Use of artificial intelligence to detect Zero-Day attacks in computer networks

INTRODUCTION

I am going to present to you a scientific research problem from a recent study in the field of cybersecurity. This study focuses on the detection of Zero-Day attacks, which are among the most dangerous as they exploit vulnerabilities that are still unknown to systems. The aim here is to show you how a research problem can be formulated, and according to what scientific method the researchers proceeded to define it rigorously.



Context and importance of the subject

Zero-Day attacks are particularly formidable because they are not yet documented or detected by traditional systems. Antivirus, firewalls, or classic IDS often work with known signature databases. But in the case of Zero-Days, there is no existing signature. This observation prompted researchers to consider a smarter solution, based on artificial intelligence and machine learning, to recognize suspicious behaviors without relying on a pre-established database. This issue is crucial for the security of critical infrastructures such as hospitals, banks, or government systems.

Problem formulation

Based on this situation, the researchers formulated the central problem of their study, which I summarize here: How to design a detection system capable of effectively identifying Zero-Day attacks using machine learning methods, despite the lack of known signatures? To arrive at this formulation, they used an inductive approach: First, they observed a frequent phenomenon: current systems fail to detect these invisible attacks. Next, they generalized this observation by asking the question: what is missing in these systems? Finally, they transformed this into a clear and focused research question, concentrating on the possibilities offered by artificial intelligence. This process is fundamental for guiding the subsequent research.

Method used to formulate the problem

Here are the methodical steps they followed to construct this research problem:

- 1) Initial observation: attacks are bypassing current tools.
- 2) Literature review: researchers analyzed what already exists, particularly in the field of machine learning applied to security.
- 3) Delimitation of the study area: they chose to focus solely on Zero-Day attacks.
- 4) Formulation of the central question: they posed the problem in a precise form that is scientifically exploitable.
- 5) Justification of the choice: they explained why this problem is a priority today, especially in an increasingly connected world. This method is scientific, progressive, and compliant with research standards.

CONCLUSION

In conclusion, well phrasing a research problem is an essential step, as it determines the direction, method, and expected results. In this example related to Zero-Day attacks, we see how a concrete observation can lead to a rigorous formulation, following the inductive method. Thank you very much for your attention, and see you very soon for the next video.

List of references

- 1) Wang, W., Sheng, Y., Wang, J., Zeng, X., Ye, X., & Huang, Y. (2017). *HAST-IDS: Learning Hierarchical Spatial-Temporal Features Using Deep Neural Networks to Improve Intrusion Detection*. IEEE Access, 6, 1792–1806.
- 2) Sommer, R., & Paxson, V. (2010). *Outside the Closed World: On Using Machine Learning for Network Intrusion Detection*. IEEE Symposium on Security and Privacy.
- 3) Harang, R. E. (2014). *The Challenges of Zero-Day Detection with Machine Learning*. Journal of Cybersecurity, 1(1), 1-11.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

