



Task 4 Research issues 3
Artificial Intelligence in the Detection of
Cyber Threats in Hybrid Environments

Field:
Cybersecurity

Prepared by

ALI MMADI, PhD student-Midocean University





Research Issues(3)

Task 4

ALI MMADI

PhD student - Midocean University

www.midocean.ae

Introduction

As part of assignment number 4,
I am presenting a report on the latest global developments and trends in the field
of artificial intelligence applied to cybersecurity, particularly in hybrid
environments.



Global context

According to the 2024 IBM Security report, the global average cost of a data breach reached \$4.45 million, an increase of 15% over three years.

Furthermore, the 2024 report from Check Point Software Technologies indicates that cyber attacks have increased by 38% on a global average.

These figures show increasing pressure on organizations, particularly those using hybrid infrastructures combining public and private cloud.

2. First trend: AI and Machine Learning-based Detection

Recent studies show that Deep Learning-based systems achieve detection rates above **95%** in controlled environments.

For example, several studies published in 2023–2024 indicate:

- ☐ Reduction of detection time by **60%**
- ☐ Decrease in false positives up to **35%**
- ☐ Ability to analyze millions of events per second

However, external validity remains limited:

These performances are often achieved in test environments, and not in complex real-world networks.

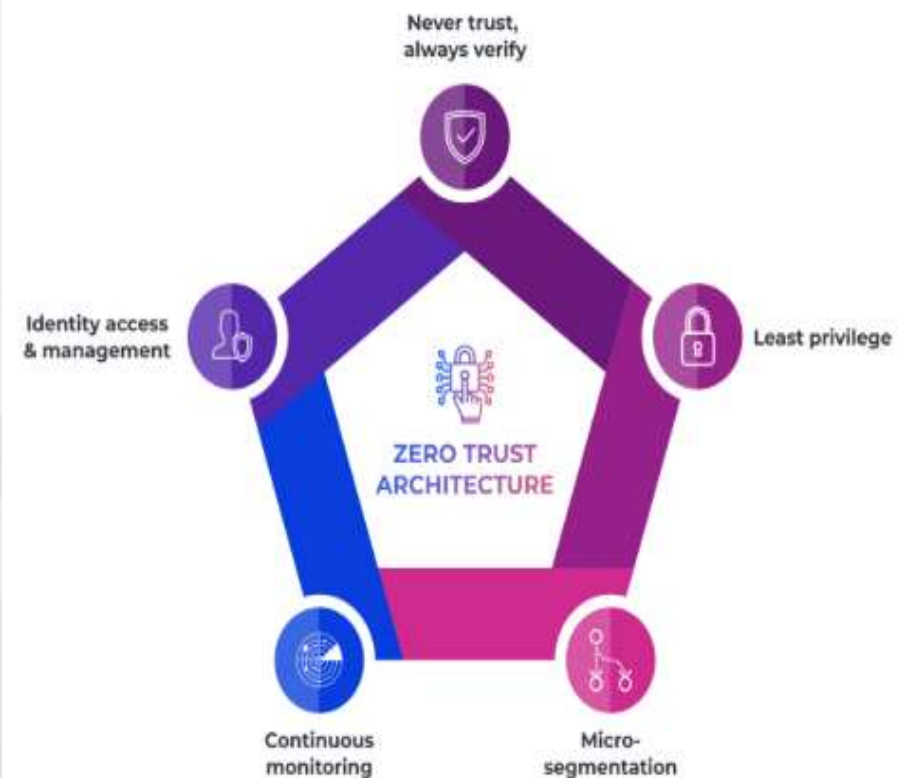
3. Second trend: Zero Trust and dynamic micro-segmentation

According to Gartner (2023), more than **60%** of global companies will gradually adopt a Zero Trust strategy by 2026.

Studies show that micro-segmentation can reduce the lateral spread of attacks by **70% to 80%**.

However, scalability challenges clearly emerge:

- ❖ Identity management complexity
- ❖ Explosion in the number of access rules
- ❖ Need for qualified human resources



4. Third trend: Cyber-resilience and risk-based approach

Recent research shifts the focus from simple prevention to cyber resilience.

The risk-based model includes:

- ☐ **Predictive analysis**
- ☐ **Prioritization of critical assets**
- ☐ **Attack simulation (Red Teaming)**

Organizations using a risk-based approach reduce the financial impact of attacks by an average of 30% according to 2024 industry studies.

5. Emerging challenges

◆ A. External validity

Many studies use public datasets like CICIDS or UNSW-NB15.

However, these datasets do not always reflect the real diversity of current threats.

◆ B. Scalability

AI models require:

- High computing power
- Continuous maintenance
- Model updates

In hybrid environments with limited resources, this poses a strategic challenge.

◆ C. Human factor

2024 reports show that:

- More than 74% of breaches involve human error
- Cloud misconfiguration = major cause of incidents

This means that technology alone is not enough.

6. Recent innovations (2024–2025)

The new research focuses on:

- Explainable AI to reduce opaque decisions
- Intelligent SOAR automation
- Behavioral detection based on adaptive Zero Trust

A strong trend is the integration of generative AI into automatic response systems.

7. Positioning of my future project

In the context of developing countries and resource-limited hybrid infrastructures, a strategic question remains:

How to adapt advanced AI models while controlling costs and human risks?

My research focus could therefore be on:

A hybrid model combining lightweight AI, a risk-based approach, and strengthening human controls.

Conclusion

In conclusion,

Global trends clearly show:

- ✓ A massive adoption of AI
- ✓ A generalization of Zero Trust
- ✓ A transition towards cyber resilience

However, challenges of external validity, scalability, and the human factor remain critical limitations.

Future research must integrate not only technical performance but also the organizational and economic dimension.

Thank you for your attention.

رمضان مبارك

- 1) Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020).
Zero trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology.
<https://doi.org/10.6028/NIST.SP.800-207>
- 2) BM Security. (2024).
Cost of a data breach report 2024. IBM Corporation.
<https://www.ibm.com/reports/data-breach>
- 3) Gartner. (2023).
Predicts 2023: Cybersecurity industry focuses on the human deal. Gartner Research.
- 4) Buczak, A. L., & Guven, E. (2016).
A survey of data mining and machine learning methods for cyber security intrusion detection.
IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.
<https://doi.org/10.1109/COMST.2015.2494502>
- 5) Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016).
A deep learning approach for network intrusion detection system.
In Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (pp. 21–26).
<https://doi.org/10.4108/eai.3-12-2015.2262516>
- 6) Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018).
Toward generating a new intrusion detection dataset and intrusion traffic characterization.
In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP) (pp. 108–116).
<https://doi.org/10.5220/0006639801080116>
- 7) Linkov, I., & Kott, A. (2019).
Fundamental concepts of cyber resilience: Introduction and overview.
IEEE Security & Privacy, 17(4), 72–75.
<https://doi.org/10.1109/MSEC.2019.2925640>
- 8) Zhang, Y., Chen, X., Li, L., & Wong, D. S. (2022).
Artificial intelligence in cloud security: A survey.
IEEE Access, 10, 53487–53506.
<https://doi.org/10.1109/ACCESS.2022.3171803>
- 9) Verizon. (2024).
Data breach investigations report (DBIR) 2024. Verizon Enterprise.
<https://www.verizon.com/business/resources/reports/dbir/>



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

