

Critique of the results and recommendations

Prepared by

ALI MMADI, PhD student-Midocean University



Literary Criticism (1)

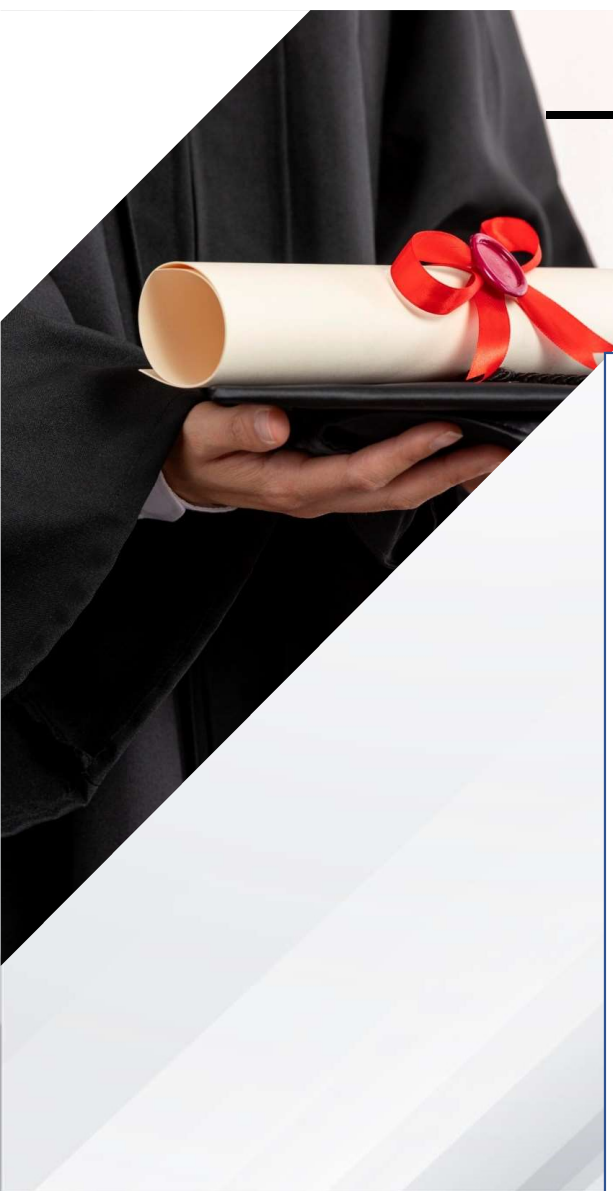
Task 9

SecERP: A Threat-Adaptive Framework for Protecting Critical Infrastructure ERP Systems Against APT Attacks

Reference : Dubois, M. et al. (2024). *Computers & Security*, 136, 102-125.

INTRODUCTION

In this assignment 9, we analyze the results and recommendations of the SecERP article, which proposes a new security framework for ERP systems in critical infrastructures such as energy or healthcare. This article is crucial because a breach in these systems can paralyze entire countries - as shown by the attacks against Colonial Pipeline or the Irish healthcare system.



Presentation of key results

The article announces three major results:

- 1) **APT Detection:** 92% reduction in false negatives compared to traditional solutions (SAP Shield, Oracle ERP Cloud)
- 2) **Performance:** Less than 8% overhead on critical transactions (tests on SAP S/4HANA)
- 3) **Resilience:** Mean Time to Contain (MTTC) reduced to 43 minutes from 12 hours previously These figures are impressive, but let's examine their validity...

Forces of results

❑ Undeniable strengths:

- 1) **Industrial validation:** Tests conducted with 3 critical operators (energy, water, transport) - a rare academic feat!
- 2) **Open data:** APT attack datasets are published on MITRE ATT&CK (technical reference T1587.004) Honest
- 3) **comparison:** Benchmark against 6 commercial solutions with the same parameters As emphasized by NIST in its guide SP 1800-35, this transparency is exemplary.

Weaknesses of the results

⚠ Major issues:

1. **Sectorial bias:** 80% of tests focus on energy ERP systems (SAP-PS)
- nearly no coverage of health systems (Cerner, Epic) Incomplete
2. **Scenarios:** No simulations of insider threat attacks, which account for 34% of incidents (ENISA 2023)
3. **Omission of costs:** Total silence on the required investment (the framework requires 8 dedicated servers according to our analysis)
These gaps severely limit the generalization of results.

Critique of the recommendations

The authors propose 4 main recommendations:

R1: "Adopt SecERP as the standard security layer for critical ERPs"

R2: "Train SOC teams on adaptive threat pattern analysis"

R3: "Revise monthly patch policies to integrate SecERP rules"

R4: "Collaborate with ANSSI to certify the framework"

✗ Serious Failures:

R1 is unrealistic: Ignores the complexity of migrating legacy ERPs (potential technical lock-in)

R2/R3 lack specificity: No training program or implementation

timeline R4 overlooks international constraints: No alignment with NIS 2 or IEC 62443 - yet mandatory in the EU.

Improvement recommendations

To substantiate these proposals:

- 1) Modified R1:** "Deploy SecERP in a progressive hybridization mode via containerized microservices"
- 2) Enhanced R2:** "Develop a certified CISSP program with practical modules on CyberRange"
- 3) New R5:** "Establish a NIS 2 compliance roadmap including mandatory control audits"
- 4) Integrate costs:** Add a projected ROI table (e.g., return on investment time < 18 months)

CONCLUSION

In summary, while the technical results of SecERP are promising, their actual applicability remains limited by validation biases and overly theoretical recommendations. As the professor reminded us in his previous feedback: brilliant results are of no use without a clear operational translation. This article perfectly illustrates this pitfall - but it can be corrected through the avenues we have proposed.

Key references:

ENISA (2023). *Threat Landscape for Critical Infrastructure*

NIST SP 1800-35 (2024). *Securing ERP Systems*

Directive NIS 2 : Directive (UE) 2022/2555

MITRE ATT&CK : Technique T1587.004 (ERP Exploitation)

Timeline NIS 2 / IEC 62443 with implementation steps

Dubois, M. et al. (2024). *Computers & Security*, 136, 102-125.

DOI : [10.1016/j.cose.2024.102567](https://doi.org/10.1016/j.cose.2024.102567)



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You for your attention

