# Title

How can a robot IT-security-expert ensure a more rapid[[1]](#footnote-1) response as a human expert in case of a given[[2]](#footnote-2) incident

Previous version: https://miau.my-x.hu/bprof/2023/thesis04\_a1\_c1.docx

# Abstract

In today's rapidly evolving digital landscape, IT security incidents (like attempts from unauthorized sources to access systems or data, unplanned disruption to a service or denial of service, unauthorized processing or storage of data…c.f. footnote#2) are a constant threat. Effective and or efficient incident response planning is crucial for minimizing the impact of these incidents.

* Problems: The problem addressed is the lack of a systematic (automatable) approach to incident response planning, which often results in ineffective and inefficient responses like weakness in (Preparation, Detection and analysis, Containment, Eradication and Recovery).

* Goals: This research (leading to an application being capable of automating activities which are still here and now activities for human beings) is to provide a methodology (in source code presented) like (One of the most important steps in the incident response process is the detection phase[[3]](#footnote-3)) for optimizing incident response planning in IT security.

* Tasks: Involved include conducting a literature review like (Jason Andress, in The Basics of Information Security (Second Edition), 2014), developing a system model for incident response planning, applying the model to realworld scenarios (like Network Security, Cryptography, Compliance and Operational Security, Application, Data, and Host Security...), and evaluating the results from experts in the field to gather their insights.

Security metrics are measured against certain criteria to quantify[[4]](#footnote-4) the risk of damage or loss as a result of malicious attacks. These metrics are especially important for understanding what areas are open for improvement, what are the most prominent weaknesses[[5]](#footnote-5), and how to properly allocate the cybersecurity budget.

we can measure[[6]](#footnote-6) effectiveness by (Measuring and Improving Detection Accuracy, Understanding the Effectiveness of Automation, Investigating

Permissions and Entitlements, Gauging Attack Surface Awareness)

We can measure efficiency[[7]](#footnote-7) by (Understanding the Role of People in Security, Measuring Process Effectiveness, Evaluating Technology Effectiveness).

And after all this comes the role of the general evaluation[[8]](#footnote-8) or the ideal values that must be followed for evaluation: The Number and Type of Reported Incidents, The Amount of Time to Detect an Incident, The Amount of Time to Resolve An Incident and The Cost Per Incident.

Some books and articles specialized in security breaches and responses to them: [https://www.sciencedirect.com/topics/computer-science/security-incidentresponse](https://www.sciencedirect.com/topics/computer-science/security-incident-response)

You can view books:

1. [https://www.sciencedirect.com/book/9780128007440/the-basics-ofinformation-security](https://www.sciencedirect.com/book/9780128007440/the-basics-of-information-security)
2. [https://www.sciencedirect.com/book/9780124058712/fismacompliance-handbook](https://www.sciencedirect.com/book/9780124058712/fisma-compliance-handbook)

* Targeted groups/customers: Targeted groups/customers: The targeted group for this research (application) is IT professionals (like Cybersecurity, Networks and systems, Software development, Web development…) and organizations (like ASIS&T, IEEE, IIMA, SIAM …) responsible for incident.

* Utilities[[9]](#footnote-9): The proposed solution (application) will be offers a comprehensive and systematic approach to incident response planning that can be applied to various types (like Computer Systems, Servers, Networks, Databases…) of IT systems.

* Discussions: The findings of this study + application will be discussed in detail, including the advantages (like Maintain Trust, Mitigate Damage, Ability to Face Incident Confidently…) and disadvantages (like consider outsourcing your incident response team, education level of the staff…) of different approaches (like Privilege Escalation Attacks, Insider Threat Attacks, Unauthorized Access Attacks …).

* Results[[10]](#footnote-10): The results of this research will be demonstrating the utility of system modeling in improving incident response planning and provide a basis for future research in this area.

* Future: The results of this study will have implications (like rapid response to accidents) for the future of IT-security and provide a foundation for further research (like Cyber security) in this field.

This thesis will address how to respond to a security incident correctly and as quickly as possible.

General evaluation: there are a lot of really good focus points for even more theses. It is important to choose one single and simple focus point for one single author, because it is never possible to automate all the above-mentioned components in one single thesis. It is also good, that we have more and more relevant keywords (c.f. like …). These keywords can be transformed later into attributes…

https://miau.my-x.hu/bprof/2023/thesis04\_a2\_c2.docx

🡨this version is a better version (compared to https://miau.my-x.hu/bprof/2023/thesis04\_a1\_c1.docx).

There is a Hungarian proverb: https://hu.glosbe.com/hu/en/j%C3%B3b%C3%B3l%20is%20meg%C3%A1rt%20a%20sok

It means, we have to focus on one single/simple goal/task/point from now on - and later, we can complete our portfolio...

A (system) model has to simplify the reality. Therefore, too complex systems should always be reduced to components...

This reduction could be executed based on the really existing data assets.

We need data and the potential good goals/problems (having however no data) should be excluded at first.

The next question is: what kind of data do we really have - concerning this complexity?

1. How can be measured the rapidness? [↑](#footnote-ref-1)
2. What is this focused incident? [↑](#footnote-ref-2)
3. THIS IS A REALLY GOOD FOCUS FOR A THESIS! WHAT KIND OF DATA SETS ARE NEEDED FOR AN AUTOMATED DETECTING (RISK-INDEX-ESTIMATION)? [↑](#footnote-ref-3)
4. THIS IS ALSO A REALLY GOOD FOCUS FOR A THESIS! WHAT KIND OF DATA SETS ARE NEEDED FOR AN AUTOMATED DAMAGE-ESTIMATION)? [↑](#footnote-ref-4)
5. AN AUTOMATED SWOT-ANALYSIS WOULD ALSO BE A GOOD FOCUS FOR A THESIS… [↑](#footnote-ref-5)
6. Next step: How – exactly?! (c.f. flowchart) [↑](#footnote-ref-6)
7. Next step: How – exactly?! (c.f. flowchart) [↑](#footnote-ref-7)
8. Next step: How – exactly?! (c.f. flowchart) [↑](#footnote-ref-8)
9. After the decision about one particular goal/task/problem-(package), utilities should be estimated as a numeric value… [↑](#footnote-ref-9)
10. A result should always be an application (and its detailed documentation). [↑](#footnote-ref-10)