# Title

Automation of incident Response Planning[[1]](#footnote-1) in IT Security (AIR-P-ITS)

A = author

C = conductor

# Abstract

In today's rapidly[[2]](#footnote-2) evolving digital landscape, IT security incidents (like …) are a constant[[3]](#footnote-3) threat. Effective and or efficient incident response planning[[4]](#footnote-4) is crucial for minimizing the impact[[5]](#footnote-5) [[6]](#footnote-6)of these incidents.

* Problems: The problem addressed is the lack of a systematic (automatable) approach to incident response planning, which often results in ineffective[[7]](#footnote-7) and inefficient[[8]](#footnote-8) 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) for optimizing[[9]](#footnote-9) incident response planning in IT security
* Tasks: Involved include conducting a literature review[[10]](#footnote-10) like (Jason Andress, in The Basics of Information Security (Second Edition), 2014), developing a system model for incident response planning, applying the model to real-world scenarios (like ...), and evaluating the results from experts in the field to gather their insights.

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: The targeted group for this research (application) is IT professionals (like …) and organizations (like …) responsible for incident response planning.
* Utilities: The proposed solution (application) will be offers a comprehensive and systematic approach to incident response planning that can be applied to various types (like …) of IT systems
* Discussions: The findings of this study + application will be discussed in detail, including the advantages (like …) and disadvantages (like …) of different approaches (like …).
* Results: The results of this research will be demonstrating the utility[[11]](#footnote-11) 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[[12]](#footnote-12) response to accidents) for the future of IT-security and provide a foundation for further research (like Cyber security) in this field.

General interpretation based on CISCO: (https://www.cisco.com/c/en/us/products/security/incident-response-plan.html)

What does a classic incident response plan do?

An incident response plan is a set of instructions to help IT staff detect, respond to, and recover from network security incidents. These types of plans address issues like cybercrime, data loss, and service outages that threaten daily work.

WHAT WILLWE DO? (KEYWORD: AUTOMATION!): An automated incident response plan is a automatically generated set of instructions to help IT staff detect, respond to, and recover from network security incidents. These types of plans address issues like cybercrime, data loss, and service outages that threaten daily work.

\*\*\*

Remark: In case of each “like …”-sign, it is necessary to complete the set of the potential items/examples concerning the particular phenomenon…

(Plural forms of keywords need quasi always a set of examples!)

Decision points:

1. Will lead the basic idea to a manual-driven expert system (c.f. CISCO-definition)? OR
2. Will lead the basic idea to an inductive (data-driven) expert system (c.f. CISCO-definition)? OR
3. (see footnote #12): Is the real goal a source code for speed-increasing concerning some responses?

To-do:

1. Completing the “like-…”-positions
2. Making decisions in case of each decision point

Deadline: ASAP (c.f. general deadline for closing the negotiation phase about title and abstract) – at least till February 03. 24.00 (CET) – c.f. special offer about co-operation with other Students

1. Classic interpretation = e.g., <https://www.cisco.com/c/en/us/products/security/incident-response-plan.html>, BUT we have to automate more and more layers of the manual-driven expertise! [↑](#footnote-ref-1)
2. Is it really a rapid process? c.f. https://trends.google.com/trends/explore?date=all&q=%2Fm%2F0227jd [↑](#footnote-ref-2)
3. A task for later: What kind of evidence are given to proof the correctness of the word „constant”? Is threatening potential not rather a phenomenon with a kind of constant changing? (c.f. fever-curve) [↑](#footnote-ref-3)
4. Benchmark services: e.g., https://www.controlcase.com/incident-management/?utm\_term=&utm\_campaign=Remarketing+-+All+Regions&utm\_source=google&utm\_medium=cpc&hsa\_acc=5046975321&hsa\_cam=17880238693&hsa\_grp=&hsa\_ad=&hsa\_src=x&hsa\_tgt=&hsa\_kw=&hsa\_mt=&hsa\_net=adwords&hsa\_ver=3&gclid=CjwKCAiAuOieBhAIEiwAgjCvcrl0roDGheKIXQfzyZYKddFSvPR5dMIoUtxVCierkrvtiZYqiOr58BoCLqQQAvD\_BwE [↑](#footnote-ref-4)
5. And minimizing the costs = increasing the efficiency through automation [↑](#footnote-ref-5)
6. HOW CAN WE MEASURE THE IMPACT?! 🡨 this is a system modeling challenge as such [↑](#footnote-ref-6)
7. HOW CAN WE MEASURE THE EFFECTIVNESS? 🡨 this is a system modeling challenge as such [↑](#footnote-ref-7)
8. HOW CAN WE MEASURE THE EFFICIENCY? 🡨 this is a system modeling challenge as such [↑](#footnote-ref-8)
9. HOW CAN WE MEASURE THE OPTIMUM VALUES? 🡨 this is a system modeling challenge as such [↑](#footnote-ref-9)
10. The literature should deliver operationalized solution for all footnotes, but especially at least for footnote 6-7-8-9! [↑](#footnote-ref-10)
11. It is obligatory to develop an application. It is not enough to derive e.g., utilities... [↑](#footnote-ref-11)
12. Alternative title: How can a robot IT-security-expert ensure a more rapid response as a human expert in case of a given incident? [↑](#footnote-ref-12)