Title

How can a robot IT-security-expert ensure a more rapid response as a human expert in case of a given incident?

1. Can be measured the rapidness as a security expert by (Mean Time to Detect, Mean Time to Respond, Mean Time to Resolution, Time to Containment, Time to Recovery).

<https://securityscorecard.com/blog/how-to-use-incident-response-metrics>

1. There are some incidents (like Advanced Persistent Threats, Cyber Espionage, Ransomware attacks).

[https://www.techtarget.com/searchsecurity/feature/10-types-of-securityincidents-and-how-to-handle-them](https://www.techtarget.com/searchsecurity/feature/10-types-of-security-incidents-and-how-to-handle-them)

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…) 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 ) the detection phase requires some kind of data(like Network logs, Security events, User behavior data, Vulnerability data ...) 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 the risk of damage (like Assess the extent of the damage, Identify the critical systems and data that were impacted, Determine the cost of recovery) 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 (Strengths, Weaknesses, Opportunities, Threats) we can use SWOT analysis to make things simple:

Strengths:

* Provides a Standard Process for Incident Response. o Protects Sensitive Information. o Helps Respond Quickly and Effectively.

Weaknesses:

* The incident response team lacks authority and visibility in the organization.
* Incident response tools are inadequate, unmanaged, untested or underutilized.

Opportunities:

* Identify opportunities to improve the safety measures in place to reduce the risk of damage.
* Evaluate the possibility of implementing new safety measures, such as new technologies or procedures, that can increase the level of safety and reduce the risk of damage.

Threats:

* Identify external factors that may increase the risk of damage(like Excessive consumption, Abnormal browsing behavior, Anomalies in outbound network traffic), such as new technologies, changing regulations, or emerging risks.
* Evaluate the potential impact of these threats on the safety measures in place and identify steps that can be taken to mitigate their impact.

[https://assets.kpmg.com/content/dam/kpmg/pdf/2016/04/cyber-incidentresponse.pdf](https://assets.kpmg.com/content/dam/kpmg/pdf/2016/04/cyber-incident-response.pdf) With ChatGPT

 And how to properly allocate the cybersecurity budget.

We can measure efficiency by:

* + 1. Resource utilization: This measures the extent to which the resources (such as personnel, technology, and budget) used during the response were used effectively and efficiently.
		2. Automation: This measures the extent to which automation was used during the response and the impact it had on the speed and efficiency of the response.
		3. Incident resolution speed: This measures the speed at which incidents were resolved, from the time they were detected to the time they were fully resolved.
		4. Process improvement: This measures the extent to which the security incident response process has been improved over time, and the impact of those improvements on efficiency.
		5. Repeat incidents: This measures the rate of repeat incidents, indicating the efficiency of the incident response and resolution process in preventing similar incidents from occurring in the future.

we can measure effectiveness by:

* 1. Time to detect: This measures the time it takes to detect a security incident, from the time the incident occurred to the time it was discovered.
	2. Time to contain: This measures the time it takes to contain the security incident; from the time it was discovered to the time it was fully contained.
	3. Time to recover: This measures the time it takes to fully recover from the security incident, from the time it was fully contained to the time normal operations have been fully restored.
	4. Data loss: This measures the extent of data loss as a result of the security incident, including the amount of data lost and the type of data that was lost.
	5. Feedback from stakeholders: This measures the feedback from stakeholders, such as customers, employees, and partners, on the effectiveness of the security incident response and their level of satisfaction with the response.

[https://securityscorecard.com/blog/how-to-use-incident-responsemetrics](https://securityscorecard.com/blog/how-to-use-incident-response-metrics)

And after all this comes the role of the general evaluation or the ideal values that must be followed for evaluation:

1. Time to detect: A commonly accepted standard is to detect a security incident within 24 hours or less.
2. Time to contain: A commonly accepted standard is to contain a security incident within 2-4 hours of detection.
3. Time to recover: A commonly accepted standard is to fully recover from a security incident within 2-7 days, depending on the complexity of the incident and the systems affected.
4. Data loss: The ideal value for data loss is to minimize it as much as possible and to have a robust backup and recovery plan in place.
5. The ideal values for evaluating security incidents will vary depending on the specific organization and its needs. However, there are some general standards and best practices that can be used as a baseline.
6. Financial impact: The ideal value for financial impact is to minimize it as much as possible, through effective incident response, contingency planning, and risk management.
7. Lessons learned: The ideal value for lessons learned is to continuously learn from security incidents, making improvements to the incident response process and implementing new security measures to prevent similar incidents in the future.

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: 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: 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.

There is a large amount of data available concerning the complexity in security incidents. This data can include information on the types of security incidents that have occurred (such as data breaches, cyber-attacks, and network intrusions), the methods used by attackers (such as phishing, malware, and social engineering), the industries and organizations that have been targeted, and the impact of the incidents on businesses and individuals.

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

The above-mentioned URLs are very important (c.f. definition of keywords, demonstrating focus-points, etc.), BUT there are still no single demo databases (e.g., public log-data?!) behind them…

It is necessary to have real data or the be capable generating them… c.f. <https://miau.my-x.hu/miau/296/risk_index_naive_regression_coco.xlsx>

Based an the real and/or generated test data, it is possible to create a demonstration about the entire process of the analytical approach = system model…

Demo: https://miau.my-x.hu/miau/296/risk\_index\_naive\_regression\_coco.xlsx

This level of operational view (of detail-oriented, reproducible demonstration) should be achieved in each thesis in this semester...

So, we will need real and/or generated data assets for such a customized file concerning inductive expert systems, or a parallel logic demonstrated (c.f. manual-driven expert system - <https://miau.my-x.hu/myx-free/ego_en/> 🡨c.f. binary approach in the XLSX-file above-cited)...

The keywords and rules documented/referenced till now are a solid basis for a manual-driven expert system (details asap)...

😊