A Multi-criteria Approach to Improve the Cyber Security Visibility Through Breach Attack Simulations

Antonio Horta[1,3], **Raimir Holanda**[1,2], **Renato Marinho**[1,2]

[1]Morphus labs, Morphus Segurança da Informação
R. Carolina Sucupira, 1368 - Aldeota, Fortaleza - CE, Brazil

[2]University of Fortaleza
Av. Washington Soares, 1321 - Edson Queiroz, Fortaleza - CE, Brazil

[3]Instituto Militar de Engenharia - IME
Praça Gen. Tibúrcio, 80 - Urca, Rio de Janeiro - RJ, Brazil

{ajhorta,rholanda,rmarinho}@morphus.com.br

Abstract. *Cyber threats are increasingly present in our daily lives and represent a great risk for companies. In this sense, organisations run breach attack simulations to generate an action plan and recommendations that must be followed. However, these action plans are the result of the tacit knowledge of specialists. Upon this issue, this research proposes a formal and automatic method to generate prioritized action plans to improve the visibility of the environment. The method proposed here is demonstrated through an experiment, in which the results were consistent and useful for the scenario in which it was tested.*

1. Introduction

Cyber-attacks are increasingly present in our daily lives. Technical reports, conferences, forums and news point out that cyber-attacks are a real threat lately. In an attempt to mitigate this problem, organisations use resources to improve their security postures by improving their security processes in the face of cyber threats and attacks.

In this sense, companies perform assessments, intrusion tests and breach attack simulations (BAS) in an attempt to obtain an action plan to direct their efforts and investments in improving security. The problem is that these action plans are the result of the tacit knowledge of experts, together with the results observed during the respective tests. Based on this issue, this research sees an opportunity to propose a formal and automatic method for prioritizing action plans to increase the detection capacity of the environment, here called visibility.

It was observed in the state of the art that the action plans follow the recommendations of existing frameworks to implement a set of controls. This study intends through multi-criteria decision aid (MCDA) methods and based on results of breach attack simulations tests, establish weights for each of these controls and reach an ordered list of the action plan to be followed by the decision maker. This proposed method is demonstrated through an experiment at the end of this work, in which the results were consistent with the scenario in which it was tested.

For a better understanding of the problem, the proposal and the experiment carried out, this work will present in the following sections, the works related to the topic,

followed by a theoretical foundation on cyber threats, security frameworks and methods of multi-criteria decision-making. Afterwards, all the steps of the proposed method will be described, followed by a practical experiment made with a dataset of the result of the breach attack simulations performed and finally the analysis of the results.

2. Related Work

As a consequence of the evolving and emerging cyber security threats, researchers have been developing various works that propose approaches to cyber security analysis. Security metrics, for instance, have been proposed in [Ramos et al. 2019] to the construction and maintenance of more secure systems. To address these issues, this work proposes three security metrics: trust probability, damage level and data security level.

The paper [Mylrea et al. 2018] demonstrates how the Insider Threat cyber security Framework (ITCF) web tool and methodology includes over 30 cyber security best practices to help organisations identify, protect, detect, respond and recover to sophisticated insider threats and vulnerabilities. The paper tests the efficacy of this approach and helps validate and verify ITCF's capabilities and features through various insider attacks use-cases. In realization of their goals, ITCF: provides an easy to use rapid assessment tool to perform an insider threat self-assessment; determines the current insider threat cyber security posture; defines investment based goals to achieve a target state; connects the cyber security posture with business processes, functions, and continuity; and finally, helps develop plans to answer critical organizational cyber security questions.

Machine learning and big data techniques are applied in [Zolanvari et al. 2019] for analyzing and securing the Internet of Things (IoT) technology. The paper runs a cyber-vulnerability assessment and discusses the utilization of machine learning in countering these susceptibilities. Finally, the paper discusses a case study, which includes details of a real-world testbed that was built to conduct cyber-attacks and to design an intrusion detection system (IDS).

The authors in [Shinde and Ardhapurkar 2016] aims to elucidate various techniques used in vulnerability assessment and penetration testing (VAPT), making cyber security awareness at various levels of an organisation for adoption of required up-to-date security measures by the organisation to stay protected from various cyber-attacks.

Also, based on penetration test approach, the paper presented in [Stiawan 2017] intends to identify the latest types of attacks attempted to the primary security system, enhancing the existing security system and build more effective defense systems. The paper analyzes cyber-attack techniques as well as the anatomy of penetration test in order to assist security officers to perform appropriate self-security assessment on their network systems.

However despite the number of papers published on cyber security analysis, few of them have been focusing on visibility gaps. In this specific context, the authors in [Gourisetti et al. 2019] have been developing a framework and a software application called the cyber security vulnerability mitigation framework through empirical paradigm (CyFEr). In this research, a prioritized gap analysis (PGA) involves a hierarchical execution of various steps. Finally, the CyFEr determines the top-ranking solution, which is identified as the cyber security path to achieve desired maturity.

The present paper focuses not on vulnerabilities, but on visibility gaps of the security infrastructure, such as, endpoints (antivirus), SIEM (Security Information and Event Management) and SOC (Security Operation Center) and unlike previous works, it proposes a formal and automatic method to generate prioritized action plans.

3. Modeling Cyber Threats

Organisations around the world are providing enormous effort to secure their data. They are using various types of tools and techniques to keep the business running, while adversaries are trying to breach security and send malicious software to access valuable data. Proper utilisation of attack modelling techniques provide advance planning, which can be implemented rapidly during an ongoing attack event. In this paper, we used the MITRE ATT&CK as a framework to map the different threats behaviour into tactics, techniques and procedures and to figure out the threat kill chain.

Information systems are exposed to different types of security risks. The sources of security risks are different, and can originate from inside or outside of information system facility, and can be intentional or unintentional. The precise calculation of loses caused by such incidents is often not possible because a number of small scale incidents are never detected, or detected with a significant time delay, a part of incidents are interpreted as an accidental mistake, and all that results with an underestimation of the risks. Currently, common types of threats are: ransomware, advanced persistent threat attacks, distributed denial-of-service attacks, phishing, botnets, viruses and worms.

3.1. MITRE ATT&CK Framework

MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cyber security product and service community. In the current version, MITRE ATT&CK has three matrices: Enterprise, Mobile and ICS (Industrial Control System). Each matrix represents the relationship between tactics, techniques, and sub-techniques and contains a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack life cycle and the platforms they are known to target. In addition to procedures, MITRE ATT&CK provides mitigation and detection procedures for each technique. Mitigations are recommendations of how defenders should apply to reduce the chance of being successfully targeted by the corresponding technique and detection are ways to detect an intrusion using the technique [MITRE 2022].

3.2. NIST

The NIST framework is based on existing standards, guidelines, and practices for organisations to better manage and reduce cyber security risks. In addition to helping organisations manage and reduce risks, it was designed to foster risk and cyber security management communications amongst both internal and external organisational stakeholders.The cyber security framework consists of three main components: the core, implementation tiers, and profiles. The framework Core provides a set of desired cyber security activities and outcomes using common language that is easy to understand. The Core guides organisations in managing and reducing their cyber security risks in a way that complements

an organisation's existing cyber security and risk management processes. The five Functions included in the framework Core are: *identify*, *protect*, *detect*, *respond* and *recover* [NIST 2022].

3.3. CIS

The SysAdmin, Audit, Network, Security (SANS) Institute has defined the CIS controls (formerly known as Critical Security Controls) as a set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. Currently in version 8, the CIS controls combines and consolidates the CIS controls by activities, rather than by who manages the devices. Physical devices, fixed boundaries, and discrete islands of security implementation are less important; this is reflected in version 8 through revised terminology and grouping of safeguards, resulting in 20 different Controls [SANS 2022].

3.4. ISACA COBIT

The COBIT (Control Objectives for Information and related Technology) is a framework that has been developed to support the management and governance of enterprise IT. In the latest version, COBIT 2019, there are 6 governance system principles and 40 processes that support the governance and management objectives [De Haes et al. 2020]. Also, COBIT defines the components to build and sustain a governance system such as processes, organisational structures, policies and procedures, flows of information, culture and behaviors, skills and infrastructure, establishing the factors that must be considered by the organisation to build a better governance system.

3.5. Breach Attack Simulations

Changes in the current infrastructure like update or insertion the new devices can compromise the security environment. In this sense, breach attack simulations can play a critical role in protecting key organisational assets by simulating likely attack tactics and techniques across the infrastructure and providing the identification of eventual gaps of visibility. Breach and attack simulations are therefore an advanced security testing method. These simulations identify vulnerabilities in security environments by mimicking the likely attack patterns and techniques used by malicious actors. A breach attack simulation can simulate malware attacks on endpoints, data exfiltration, malware attacks and sophisticated APT (Advanced Persistent Threat) [Shahid et al. 2022] attacks that move laterally through a network, targeting the most valuable assets.

4. Benchmarks for Threats

As observed in the related works and for the development of a research that compares a certain state of visibility of a company obtained by breach attack simulations, it is necessary that there are reference indicators to which these results can be compared. For this reason, based on public data from the ATT&CK framework, some indicators were calculated to be used in the prioritization process proposed in this research.

4.1. Indexes and Metrics

The following indicators were calculated and consolidated based on data extracted directly and dynamically from the ATT&CK framework through the

security knowledge discovery method proposed in the research: cyber threat hunting through automated hypothesis and multi-criteria decision making [Horta Neto and Fernandes Pereira dos Santos 2020]. The indicators presented in Table 1 consolidate the techniques and sub-techniques found in the intrusion-set, tools and groups categories of the ATT&CK framework. Table 1 is organized into 3 columns, in which the *Index* column represents the index code, the *description* column presents the name of the index and which category it belongs to and, finally, the *Items* column represents the number of techniques and sub-techniques found from a recursive process within these categories until reaching the technique or sub-technique of each intrusion-set, malware and tools within the ATT&CK framework.

Table 1. Indexes calculated for comparison purposes

Index	Description	Items
TGi	Techniques in Groups Index	455
TMi	Techniques in Malware Index	346
TTi	Techniques in Tools Index	201
TRi	Techniques in Ransomware Index	183
TCi	Techniques in Custom Index	-

$*$ indexes consolidated using ATT&CK version 11.0

In the case of the last two indices in Table 1, the TRi is related to the techniques found in ransomware and it was consolidated based on the presence of the word *ransomware* found within the descriptions of the ATT&CK. It is important to say that this specific category is not present on the ATT&CK. On the other hand, the TCi is an index that can be configured according to a group of techniques defined by the decision maker.

All indices are presented as an ordered list of the techniques most frequent in the groups, malware, ransomware and tools categories. Based on this ranking, Table 2 presents the top 10 ATT&CK's techniques used by each category.

Table 2. Ranking of top 10 techniques most used by threats

	TGi	TMi	TTi	TRi
1º	T1105	T1105	T1105	T1486
2º	T1082	T1082	T1016	T1106
3º	T1027	T1027	T1083	T1083
4º	T1083	T1071.001	T1027	T1027
5º	T1059.003	T1059.003	T1071.001	T1490
6º	T1071.001	T1083	T1082	T1082
7º	T1057	T1057	T1003.001	T1059.003
8º	T1547.001	T1070.004	T1059.001	T1562.001
9º	T1070.004	T1140	T1018	T1489
10º	T1016	T1016	T1049, T1057, T1569.002	T1057

5. Multi-Criteria Decision Aid Methods

Multi-criteria decision methods comes from the area of Operations Research, in which it presents several methods for solving decision making problems. MCDA methods are used

to solve three types of problems [Zopounidis and Doumpos 2002]: *choice*, *ranking* and *classification*. According the generalised framework for multi-criteria method selection [Watróbski et al. 2019], for each type of problem involving aspects of decision making, there are specific methods to be used.

The prioritization of cyber threats is considered a *ranking* problem, where the application of an MCDA method results in a ranking of alternatives to be prioritized. Among the *ranking* methods, the best known are [Sałabun et al. 2020]: *weighted product model* (WPM), *weighted sum model* (WSM), *weighted aggregated sum product assessment* (WASPAS), *preference ranking organization method for enrichment of evaluations* (PROMETHEE II), *technique for order preference by similarity to an ideal solution* (TOPSIS), *višekriterijumska optimizacija i kompromisno rješenje* (VIKOR) and *elimination et choix traduisant la realité* (ELECTRE II).

5.1. Methods for Determining Weights

The weighting of criteria is a key element of the multi-criteria decision analysis that in the case of the MCDA methods mentioned above, each criterion receives a weight that will be a determinant of the decision-making processes used in the experiments of this study.

There are several ways for determining weights, which can be determined manually according to the preferences and judgment of decision makers or using methods and functions designed for this purpose, for example: analytic hierarchy process (AHP) [Saaty 2008], simple aggregation of preferences expressed by ordinal vectors group decision making (SAPEVO-M) [Gomes et al. 2020], best-worst method (BWM)[Rezaei 2015] and the ranked attribute weights [Barron and Barrett 1996] for weighting the criteria or alternatives.

5.2. Methods and Applications

The ranking methods mentioned above have stages, specificities and applications defined by their respective authors. In general, these MCDA methods have input parameters, such as, alternatives, criteria and weights to achieve the result of the problem.

The TOPSIS and VIKOR [Opricovic and Tzeng 2004] methods calculate the closeness to the ideal solution using an aggregating function defined for this purpose. In which, the VIKOR uses linear normalization to eliminate the units of the criterion functions, while TOPSIS uses vector normalization. Conversely, there is WASPAS, a simple method, which combines the WPM and WSM [Chakraborty et al. 2015] methods for adding and multiplying weights, capable of providing more accurate results compared to the two methods alone.

Finally, the PROMETHEE [Brans et al. 1986] method is a multi-criteria analysis method that uses as a basis the outranking concept introduced by the ELECTRE method. Similarly, ELECTRE II [Roy and Bertier 1971] is based on the construction of one or more resilience relationships, performing a pairwise comparison with the use of discordance and concordance matrices to make recommendations to the ranking problems.

6. Prioritizing Actions to Improve the Detection

As can be seen in Figure 1, the method proposed in this research aims to obtain, through the results of a breach attack simulation, a list of recommendations to increase visibility

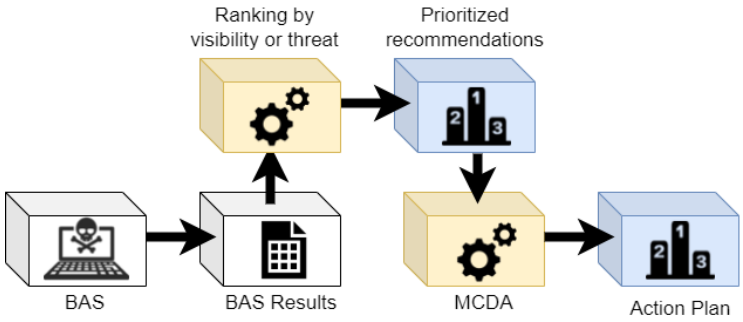

Figure 1. Prioritizing process based in BAS results and MCDA methods

in relation to cyber threats, or recommendations for one or a specific group of threats. Once this list of recommendations is reached, the method make a action plan prioritizing the control items presented in Table 3, directly related with ATT&CK's techniques to

Table 3. Cross-referencing control items between frameworks

Nº Tech. in ATT&CK v8.2	CIS Controls	NIST CSF	ISACA COBIT 19
1	1.1	ID.AM-1, PR.DS-3	BAI09
4	2.1	ID.AM-2	BAI09
4	2.4	DE.CM-7	BAI09
11	3.1	PR.IP-6	APO14, DSS06
8	3.2	ID.AM-5	APO14
58	3.3	PR.AC-4	DSS05
20	3.1	PR.DS-2	DSS05
12	3.11	PR.DS-1	DSS05, DSS06
209	4.1	PR.IP-1	APO13, BAI06, BAI10
51	4.2	PR.IP-1	BAI10
25	7.1	ID.RA-1	DSS05
25	7.2	ID.RA-1	EDM03, APO12
24	7.5	DE.CM-8	DSS05
35	7.6	ID.RA-5, PR.IP-12	DSS05
8	8.2	PR.PT-1, DE.AE-3	DSS03
1	9.1	PR.IP-1	APO10
7	9.2	PR.AC-5	DSS05
9	9.6	DE.CM-7, PR.AC-5	DSS05
4	9.7	DE.CM-4	DSS05
7	10.1	DE.CM-4	APO13, DSS05
7	10.2	DE.CM-4	DSS05
11	11.1	PR.IP-9, ID.SC-5	APO14
45	12.2	PR.AC-5	APO01, APO03
21	13.7	DE.CM-1	DSS05
25	14.1	ID.AM-6, ID.GV-1, PR.AT-1	BAI08
17	14.2	PR.AT-1	DSS05
3	14.5	PR.AT-1	DSS06
3	14.9	PR.AT-1, PR.AT-2, PR.AT-4, PR.AT-5	APO01
16	16.1	PR.IP-1	BAI01, BAI11
3	16.2	RS.AN-5	DSS03
3	16.3	RS.AN-1	DSS03
3	16.4	ID.AM-2	EDM03

be implemented, using a MCDA method chosen by the decision maker. Such control items can be: MITRE ATT&CK's data sources into techniques, NIST Common Security Framework, CIS or ISACA COBIT.

The method proposed here consists of carrying out steps that, from the import of the BAS results, generate a list of recommendations to increase the security posture based on the visibility observed in the BAS exercise and, later, an action plan with the items of control prioritized by a MCDA method chosen to be implemented.

6.1. The Input from BAS

This method starts with inputting the BAS results organized into a spreadsheet that follows the format shown in Table 4

Table 4. Input spreadsheet format

enterprise	campaign	platform	attack_version	tactic_id	technique_id	not_detected	intelligence	network	endpoint	siem	soc
Enterprise X	1	Windows	1.1	TA0007	T1135	3			1		
Enterprise Y	1	Windows	1.1	TA0005	T1562.001	23			2		1
...	...	...	...	...	...	...	...	...	...	...	...

* The data presented are random and intended to demonstrate the schema of the table

The input spreadsheet presented in Table 4 is organized in 12 columns according to the following descriptions: **enterprise**) refers to the name of the company or institution where the BAS was carried out; **campaign**) is an identifier that groups BAS tests in a given company into campaigns or groups that the decision maker sees sense in specifying; **platform**) is the operating system of the machine on which the BAS was run; **attack_version**) indicates the version of ATT&CK used in BAS; **tactic_id**) denotes the code of the tactic used at that time of the BAS; **technique_id**) refers to the MITRE ATT&CK; **not_detected**) gathers the number of attacks executed that were not detected during the BAS; **intelligence**) indicates how many attacks were identified by the threat intelligence team; **network**) refers to attacks identified by network devices such as firewalls, intrusion detection etc; **endpoint**) are the attacks identified directly on the endpoint, such as antivirus and event detection responses; **siem**) are the attacks detected through security information event management and finally; **soc**) which refers to attacks during BAS that were detected by the security operations team.

6.2. Prioritizing Recommendations

Therefore, to arrive at an ordered list of recommendations to increase security posture based on visibility, it is necessary to calculate the detection index, according to the formula 1, where: D_i denotes the column **detected** by the sum of **intelligence** (i) + **network** (n) + **endpoint** (e) + **siem** (s) + **soc** (o) and **total** column is the sum of the **detected** and **not_detected** columns.

$$\frac{D_i}{\sum total_i}, \text{ for } D_i = i_i + n_i + e_i + s_i + o_i \quad (1)$$

The result of applying the formula 1, result in a spreadsheet with an ascending order that represents the ATT&CK techniques that were less detected during the BAS.

In addition to the ordering by less detected technique, it is possible to generate an ordering of recommendations based on some specific threat group by comparing the BAS results with the indices presented in the Tables 1 and 2. In the case of, for example, choosing TRi from Table 2, the BAS result would be filtered only for the techniques that appear in TRi and would be placed in the same order of TRi, already calculated as the TOP 10 most found techniques in Ransomware.

6.3. Action Plan with MCDA

In Table 5, the recommendations being ordered according to the established priority, that is, visibility or some specific set of threats. For each of the recommendations, there are numerous control items, such as the columns: data source, CIS Info, NIST CSF and ISACA COBIT 19, correlated with each ATT&CK technique by the *CIS Security Navigator*.[1]

Table 5. Output spreadsheet of recommendations ordered by worst visibility

priority	detected	total	detection_index	technique	detection	kill_chain_phases	data_source	CIS Info	NIST CSF	ISACA COBIT 19
Best $\xleftarrow[visibility]{}$ Worst	0	20	0	T1082	System and network discovery techniques normally ...	discovery	[DS0002, DS0003 DS0004]	[4.2, 4.4, ... 13.4, 13.8]	[PR.IP-1, ID.RA-5, ... PR.AC-5, DE.CM-1]	[BAI10, APO13, ... APO01, APO03]
	3	26	0,1	T1562.001	Monitor processes and ...	defense_evasion	[DS0002, DS0005 DS0006]	[3.3, 4.7, ... 6.2, 6.8]	[PR.AC-4, PR.AC-1, ... PR.IP-11, PR.AC-4]	[DSS05]
	...	...	...	...	...	...	...	...	...	...

The data presented are random and intended to demonstrate the schema of the table

The action plan is precisely an ordered list of these control items that will be issued to the decision maker. Modeling this problem in a MCDA method perspective, this research considers as alternatives, each of these control items and as criteria, the ATT&CK techniques. The values of the decision matrix will be filled with the detection indexes of the crossing of each technique with each control item or with 1 if control item there is not in technique, as can be seen in Table 6.

[1] https://www.cisecurity.org/controls/cis-controls-navigator/

Table 6. Decision Matrix

High $\xrightarrow{\text{ranked attribute weights}}$ Low			
CIS Info	**T1222**	**T1082**	**...**
4.2	1	0,115385	...
7.6	1	0,0201	...
...	...	...	...

6.4. The Weight of the Criteria

Regardless of the MCDA method chosen, it is necessary to establish its weights. In the case of this proposal, the weights were established by the *ranked attribute weights* [Barron and Barrett 1996] method, since it has a simple application, adequate to the problem being treated and does not require interaction from the decision maker. Since there is an ordered list of recommendations by techniques from previous step, the techniques in the decision matrix are placed in this order, it means in visibility or threat priority. Therefore, the weights are established from the first to the last technique, leaving only the application of some MCDA method to reach the action plan of the desired control items as can be seen in Table 6.

7. The Experiment

In the experiment accomplished, data from a BAS campaign were used with a sampling of 8 Windows platform hosts and 27 techniques of MITRE ATT&CK grouped into 467 malicious behaviors. For the execution of the attack emulation of this campaign, the Caldera[2] platform was used, in which, at the end of each execution, all the observations in logs were registered if each attack was identified, blocked, detected, responded or not. All this information was manually consolidated, resulting in the input spreadsheet[3] that follows the schema presented in Table 4.

Firstly, formula 1 was applied and it was possible to obtain the heat map (Figure 2) of the visibility of the tested environment, based on the techniques that were identified or not.

This heat map has a scale that goes from green to red. The techniques in red indicate those that had a low detection or were not detected, in contrast to the green ones, which are the opposite. Through this heat map, the decision maker can follow the recommendations giving priority to the items that are in red.

Analogous to visibility, it is also possible to generate a heat map, referring to the techniques that most appear in groups, malware, ransomware or tools, through the direct comparison of the indices shown in Table 1. Figure 3 is the resulting heat map using the TMi index based on the BAS results. This heat map presents the techniques most used by malware, those that pose a greater risk of being exploited.

In the execution of this first step, in which the output table is obtained, as shown in Table 5, it is necessary to generate an action plan with the control items according to preferences and that make sense for the tested environment. Additionally, as can be seen

[2] `https://caldera.MITRE.org`

[3] `https://filedropper.com/d/s/RlR17eWq9Pvts3hwW4azxE1TgFeu4V`

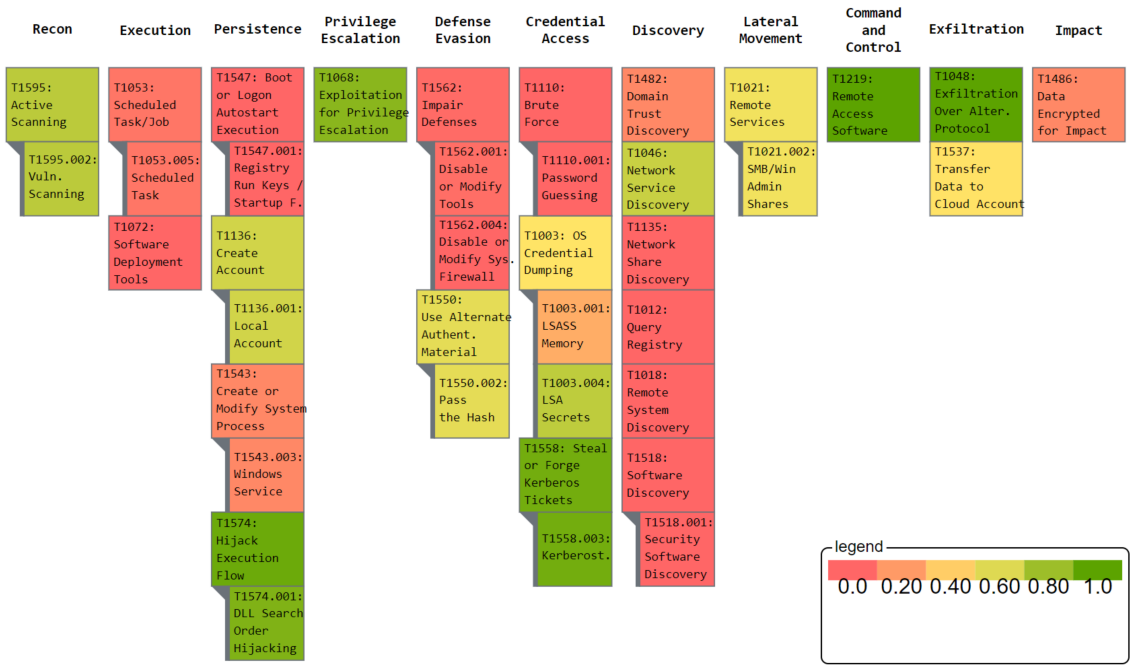

Figure 2. Heat map of visibility

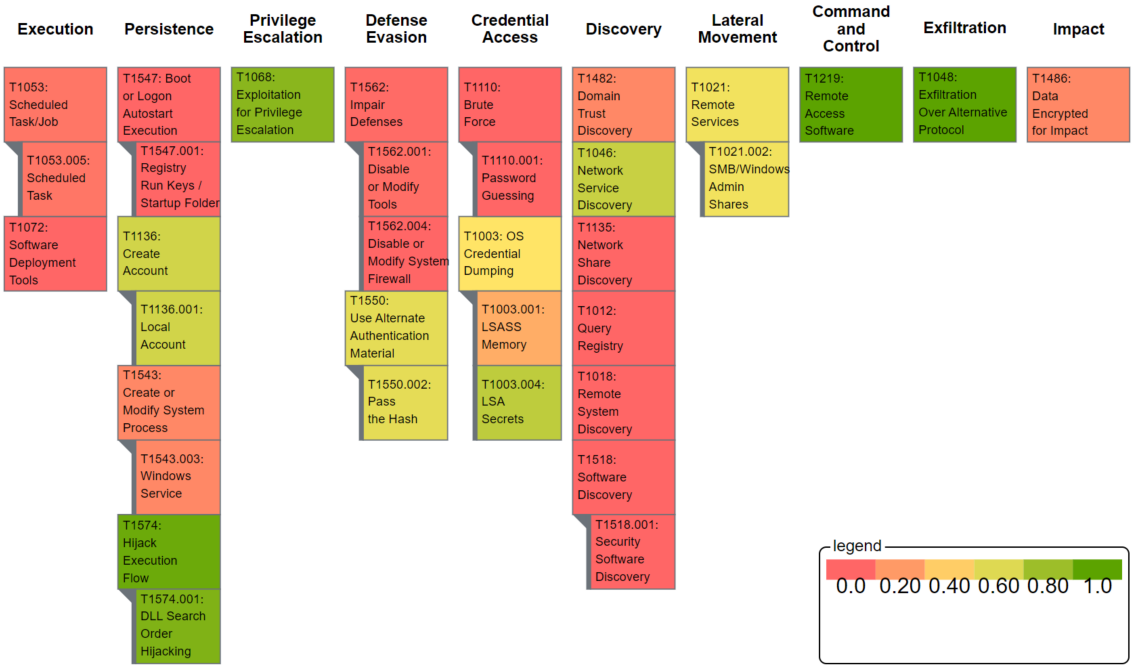

Figure 3. Heat map of visibility by TMi

in Table 3, the control items are correlated with each other through the various MITRE ATT&CK's techniques. Therefore, with the list of recommendations generated and the techniques ordered according to visibility or specific threat, this experiment applies a MCDA method to generate an action plan with the control items to be implemented. It is important to note that the choice of a MCDA method for sorting is necessary, as the control items presented in the output table (e.g. Table 5) are grouped and mixed among

all the recommendations that were generated.

It is then up to the decision maker to choose which MCDA method will be used to generate his action plan. In this experiment, with the objective of making a proof of concept, we selected the methods: TOPSIS, ELECTRE II and WASPAS because they are very popular and represent different perspectives for decision making. Therefore, these methods were applied according to the decision matrix format explained in Table 6 to generate action plans based on CIS controls, which, when executed, resulted in Table 7 which is a consolidation of the spreadsheet[4] output generated at the end of the experiment.

Table 7. CIS controls prioritized by 3 diferent MCDA methods

#	TOPSIS	WASPAS	ELECTRE	#	TOPSIS	WASPAS	ELECTRE
1º	4.1	4.1	4.1	**29º**	18.2	16.1	16.1
2º	4.7	18.2	11.2	**30º**	11.1	4.7	4.7
3º	4.10	11.2	11.3	**31º**	11.2	16.8	4.10
4º	5.2	11.3	11.4	**32º**	11.3	4.10	5.2
5º	6.3	11.4	11.5	**33º**	11.4	5.2	6.3
6º	6.4	11.5	4.2	**34º**	11.5	6.3	6.4
7º	6.5	4.2	4.5	**35º**	4.2	6.4	6.5
8º	3.1	4.5	6.1	**36º**	4.5	6.5	3.1
9º	5.3	6.1	6.2	**37º**	6.1	3.1	5.3
10º	5.4	6.2	13.4	**38º**	6.2	5.3	5.4
11º	5.5	13.4	7.1	**39º**	13.4	5.4	5.5
12º	6.8	7.1	7.2	**40º**	7.1	5.5	6.8
13º	2.5	7.2	7.3	**41º**	7.2	6.8	13.8
14º	2.6	7.3	18.2	**42º**	7.3	2.5	2.5
15º	16.13	7.4	11.1	**43º**	7.4	2.6	16.8
16º	18.3	7.5	7.4	**44º**	7.5	16.13	2.6
17º	18.5	10.5	7.5	**45º**	10.5	18.3	16.13
18º	3.12	3.3	10.5	**46º**	3.3	18.5	18.3
19º	4.4	9.2	3.3	**47º**	9.2	3.12	18.5
20º	4.8	14.1	9.2	**48º**	14.1	4.4	3.12
21º	7.6	14.3	14.1	**49º**	14.3	4.8	4.4
22º	7.7	16.1	14.3	**50º**	16.1	7.6	4.8
23º	12.2	16.9	16.1	**51º**	16.9	7.7	7.6
24º	12.8	9.3	16.9	**52º**	9.3	12.2	7.7
25º	13.3	5.1	9.3	**53º**	5.1	12.8	12.2
26º	13.8	14.9	5.1	**54º**	14.9	13.3	12.8
27º	16.8	15.7	14.9	**55º**	15.7	13.8	13.3
28º	16.1	11.1	15.7	**56º**	8.3	8.3	8.3

As can be seen in Table 7, each of the methods ordered the CIS controls according to their perspectives, however, the first and last positions are unanimous for the 3 methods. Furthermore, if we take as a reference only the sections (the integer number of the CIS) it is possible to notice that the WASPAS and ELECTRE II methods have some similarity and, on the other hand, TOPSIS contrasts with them.

[4] https://filedropper.com/d/s/7Aor2LPsjYj0U6fJiKV91mYVPr2KLy

8. Conclusions and Future Work

As can be seen, this research deals with a relevant topic in the context of cyber security, more specifically to increase the security posture based on the observations and results of breach attack simulations. The method proposed here, which uses the results of BAS exercises, proved to be robust and capable of producing coherent recommendations with a prioritized action plan according to the analyzed context. The heat maps presented proved to be useful tools for the decision maker to understand which points need more attention, as well as to assess the detection capacity of their environment.

In the experiment presented, 3 MCDA methods were used with the purpose of carrying out the proof of concept of the method, and not to evaluate the performance or results of each one, since the decision of which method should be used is up to the decision maker to choose the one that best meets your needs. Regarding the results obtained in the experiment, it was observed, based on the environment used, that there was convergence of the poles formed by the first and last controls between the 3 methods. This indicates that for this case, the first control item must be treated with priority and all others must be considered before the last one.

Finally, understanding that the choice of a more adequate method is a complex task for the decision maker, we observe as opportunities for future work, the development of an adaptation of the ensemble methods in the area of artificial intelligence for the use of multiple MCDA methods and obtaining of a single action plan selected by this ensemble.

References

Barron, F. H. and Barrett, B. E. (1996). Decision quality using ranked attribute weights. *Management science*, 42(11):1515–1523.

Brans, J.-P., Vincke, P., and Mareschal, B. (1986). How to select and how to rank projects: The promethee method. *European journal of operational research*, 24(2):228–238.

Chakraborty, S., Zavadskas, E. K., and Antucheviciene, J. (2015). Applications of waspas method as a multi-criteria decision-making tool. *Economic Computation and Economic Cybernetics Studies and Research*, 49(1):5–22.

De Haes, S., Van Grembergen, W., Joshi, A., and Huygh, T. (2020). Cobit as a framework for enterprise governance of it. In *Enterprise governance of information technology*, pages 125–162. Springer.

Gomes, C. F. S., Santos, M. d., Teixeira, L. F. H. d. S. d. B., Sanseverino, A. M., and Barcelos, M. R. d. S. (2020). Sapevo-m: a group multicriteria ordinal ranking method. *Pesquisa Operacional*, 40.

Gourisetti, S. N. G., Mylrea, M., and Patangia, H. (2019). Cybersecurity vulnerability mitigation framework through empirical paradigm (cyfer): Prioritized gap analysis. *IEEE Systems Journal*, 14(2):1897–1908.

Horta Neto, A. J. and Fernandes Pereira dos Santos, A. (2020). Cyber threat hunting through automated hypothesis and multi-criteria decision making. In *2020 IEEE International Conference on Big Data (Big Data)*, pages 1823–1830.

MITRE (2022). Mitre att&ck. `https://attack.mitre.org`. (Accessed on 05/26/2022).

Mylrea, M., Gourisetti, S. N. G., Larimer, C., and Noonan, C. (2018). Insider threat cybersecurity framework webtool & methodology: Defending against complex cyber-physical threats. In *2018 IEEE Security and Privacy Workshops (SPW)*, pages 207–216. IEEE.

NIST (2022). National institute of standards and technology. `https://nist.gov`. (Accessed on 05/26/2022).

Opricovic, S. and Tzeng, G.-H. (2004). Compromise solution by mcdm methods: A comparative analysis of vikor and topsis. *European journal of operational research*, 156(2):445–455.

Ramos, A., Milfont, R. T., Holanda Filho, R., and Rodrigues, J. J. (2019). Enabling online quantitative security analysis in 6lowpan networks. *IEEE Internet of Things Journal*, 6(3):5631–5638.

Rezaei, J. (2015). Best-worst multi-criteria decision-making method. *Omega*, 53:49–57.

Roy, B. and Bertier, P. (1971). *La méthode ELECTRE II: une méthode de classement en prédence de critères multiples*.

Saaty, T. L. (2008). Decision making with the analytic hierarchy process. *International journal of services sciences*, 1(1):83–98.

Sałabun, W., Watróbski, J., and Shekhovtsov, A. (2020). Are mcda methods benchmarkable? a comparative study of topsis, vikor, copras, and promethee ii methods. *Symmetry*, 12(9):1549.

SANS (2022). Sysadmin, audit, network, security. `https://www.sans.org`. (Accessed on 05/25/2022).

Shahid, W. B., Aslam, B., Abbas, H., Khalid, S. B., and Afzal, H. (2022). An enhanced deep learning based framework for web attacks detection, mitigation and attacker profiling. *Journal of Network and Computer Applications*, 198:103270.

Shinde, P. S. and Ardhapurkar, S. B. (2016). Cyber security analysis using vulnerability assessment and penetration testing. In *2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)*, pages 1–5. IEEE.

Stiawan, D. (2017). Cyber-attack penetration test and vulnerability analysis. *International Journal of Online and Biomedical Engineering*.

Watróbski, J., Jankowski, J., Ziemba, P., Karczmarczyk, A., and Zioło, M. (2019). Generalised framework for multi-criteria method selection. *Omega*, 86:107–124.

Zolanvari, M., Teixeira, M. A., Gupta, L., Khan, K. M., and Jain, R. (2019). Machine learning-based network vulnerability analysis of industrial internet of things. *IEEE Internet of Things Journal*, 6(4):6822–6834.

Zopounidis, C. and Doumpos, M. (2002). Multicriteria classification and sorting methods: A literature review. *European Journal of Operational Research*, 138(2):229–246.