Employing PDDL Plan to Recommend Security Controls against Cyberattacks

Afaq Inayat, Matheus Saueressig, Muriel Figueredo Franco, Eder John Scheid, Lisandro Zambenedetti Granville

Abstract Cybersecurity is a constantly evolving field that could benefit most from the introduction of Artificial intelligence (AI). AI offers cybersecurity opportunities, for example, to improve attack modeling, prediction, and response. A promising field of research is AI planning, which involves the automated generation of action sequences to achieve specific goals. For example, in a logistic scenario, the goal could be *satisfy a location*, while in a vulnerability scenario, the goal can be defined as *account credential is compromised*). In this paper, we introduce an AI-based approach that uses the Planning Domain Definition Language (PDDL) to model the behavior of cyberattacks, specifically phishing and ransomware. Using an AI planner, we generate detailed attack steps and classify them into standard attack lifecycle phases, including reconnaissance, weaponization, delivery, exploitation, installation, and command & control. The classification is used to propose security controls that align with industrial frameworks such as the NIST Cybersecurity Framework and ISO 27001. The approach was evaluated using a scenario of a phishing attack, highlighting the effectiveness of the classifying attack steps and providing the countermeasures with compliance to *de facto* standards. The results highlight the potential of our approach to AI planning to provide a structured and proactive methodology to map and understand the behavior of cyberattacks and provide recommendations for specific protections according to compliance demands.

1 Introduction

Cybersecurity in the era of AI provides opportunities such as the detection of attack patterns and incident response [1]. A promising subfield within AI is AI planning [3], which involves the automated generation of strategies or action sequences to achieve specific goals and has shown the potential to improve cybersecurity plan-

Institute of Informatics (INF) – Federal University of Rio Grande do Sul (UFRGS)
Porto Alegre, Brazil
E-mail: {afaq.inayat|msaueressig|mffranco|ejscheid|granville}@inf.ufrgs.br

ning and management by modeling attack patterns and identifying potential attack paths [15]. With the help of AI planning, organizations can respond more quickly and allocate resources more effectively.

AI planning has been applied in several cybersecurity fields, such as penetration testing and incident response [4]. Organizations face difficulties in proactively identifying the vulnerability and understanding the attack. AI planning helps in decision making [27] and serves as an ally by providing an attack path, helping to understand the attack landscape, enabling organizations to allocate resources and provide defense proactively.

In addition to AI planning, selecting and prioritizing appropriate countermeasures to address cyberattacks is one of the major challenges in cybersecurity [21]. This task is often complex and requires a deep understanding of the attack landscape and available security controls. Recommender systems are gaining importance in this context, helping in decision-making in cybersecurity [12].

Research conducted in the field of cybersecurity applications has shown that AI planning can utilize the PDDL to effectively model various attack patterns [26] [5]. Although AI planning helps identify potential attack paths, that is essential in cybersecurity. This provides a comprehensive view of adversaries infiltrating the system and can better anticipate and defend against the attack. Identification of attack steps is significant for additional support in determining priority and selecting the most appropriate countermeasures [22]. Choosing the right control against cyberattacks is not always a trivial task. This is where recommender systems play a crucial role in supporting the user through the decision-making process.

Recommender systems can help operators prioritize relevant information and improve decision-making processes, making it easier for operators to implement the appropriate controls. [8] designed MENTOR, a tool that provides recommendations to end-users and network operators about the appropriate protection service in particular scenarios. Likewise, [2] proposes a tool to help analysts filter out anomalies and latent risks by developing a recommendation system based on collaborative filtering and expert knowledge, which generates ratings of the worst cases along with the best available recommendations.

Although AI planning and recommender systems have advanced, cybersecurity remains a critical challenge, requiring solutions to proactively address the attack by providing countermeasures and ensuring safety and security.

In this paper, we present the PDDL-based approach to model the attack and leverage the AI planner to generate the attack steps. The generated steps will then be classified according to the standard attack lifecycle, such as reconnaissance, weaponization, delivery, exploitation, installation, and command and control. Based on these classifications, we offer recommendations for security controls aligned with industry frameworks such as the NIST cybersecurity framework and ISO 27001, ensuring a more comprehensive and proactive cybersecurity posture.

The remainder of the paper is organized as follows. Section II covers the related work. Section III describes the approach, Section IV details the evaluation of the work, and Section V concludes the work and present future work.

2 Related Work

In this section, we will focus on two perspectives, i.e., AI planning using PDDL and the recommender systems. We will briefly discuss a few works that will explore these perspectives.

2.1 AI Planning

AI planning in cybersecurity is beneficial because it improves how security experts analyze, study, and understand cyberattacks. Prior work in applying AI planning in cybersecurity applications provides evidence for using PDDL in various cybersecurity scenarios.

In [26], the author proposed an automatic attack path discovery method using PDDL by creating a manageable device reachability graph partitioning approach to help the AI planner find attack paths faster. In [4], developed a prototype system that automates the cyber incidence response system using the AI planning technique. Their work focuses on False Data Injection Attacks (FDIA) against the smart grid. In [25] developed an AI planning system for automated red teaming, which helps build attack discovery and response mechanisms.

Using AI planning [5] proposed an AI planner to generate an attack tree for the adversarial strategies that can compromise critical infrastructure systems. The attack model is presented in [23] using PDDL to automatically generate an attack path for the penetration testing scenarios and validate these attacks by executing the corresponding action, including an exploit against the real targeted network. The paper[14] proposes an AI planning tool to automate security planning and management for mitigating ransomware attacks.

The author [15] leverages AI planning to develop a framework using PDDL to address security vulnerabilities in cloud computing, focusing on access control misconfiguration. The author of [16] presents an approach in cybersecurity training by integrating AI planning techniques, specifically using a PDDL symbolic logic engine, with reinforcement learning. Similarly, in [19], the author explores the application of AI planning techniques to enhance cybersecurity by introducing a practical approach to verify the correctness and completeness of formal functional specifications, which are essential for identifying potential vulnerabilities.

2.2 Recommender Systems

Recommender systems are used in many fields like E-commerce, Online Advertisement, Netflix, and YouTube [6], but there are also opportunities to use recommender systems in cybersecurity, such as to recommend protections based on business demands [8] and select cost-effective protections against specific threats [7]. The recommender system proposed in [11] is designed to track vulnerabilities. It utilizes automated techniques to identify the smallest possible collection of software vulner-

abilities and promptly warns enterprises. The recommender system employs natural language processing, fuzzy matching, and machine learning techniques to minimize the manual labor required for matching software product vulnerabilities. In [12], the recommender system is designed for incident response, leveraging network monitoring tools and security frameworks to address security threats such as ransomware and lateral movement of attackers. The system utilizes network traffic analysis, vulnerability assessments, and insights about the local environment to create profiles for the devices within a network, thereby adding support to the incident handlers in decision-making.

In [24] present a method for building an attack graph to identify potential attack paths in a maritime supply chain infrastructure and then utilizing a recommender system to make the prediction about the future attack steps within the network based on the identified attack paths. In [20], the digital twin (DT) based method is proposed to enhance cyber-physical system security. The DT uses real-time data for anomaly detection in the physical layer and employs an attack graph model for network security analysis, providing risk assessments and recommending targeted security measures. The author [13] developed a web-based system that identifies hardware-based vulnerabilities and provides the user with appropriate recommendations on specific situations to improve cybersecurity.

While AI planning and recommender systems are discussed individually, there is no research on combining these two approaches to provide comprehensive solutions for cybersecurity. The gap in the literature highlights the need for not only modeling attacks using PDDL but also showing the need for a recommender system for security control based on the provided action steps.

3 Approach

The proposed approach models cyberattack using AI planning, providing a structured understanding of the attack steps and corresponding control recommendations. Figure 1 shows the approach, including its components and relationships. The approach starts with the PDDL description, which is composed of two files, *i.e.,* domain and problem, and these files describe the actions, precondition, and goal condition of cyberattack as shown in Figure 1. The planner takes the input of the PDDL description to generate the output plan. The planner output attack steps are classified according to the attack lifecycle, *i.e.,* reconnaissance, weaponization, delivery, exploitation, installation, and command and control. We utilize the OpenAI API to classify the attack steps. It helps accurately classify and identify patterns in the attack steps. Based on this result, the recommendations for security control are provided, and the recommendations are built on pre-existing frameworks such as the NIST Cybersecurity Framework and ISO/IEC 27001. The classification of the attack steps and controls at each phase of the attack lifecycle improves overall cybersecurity strategy.

Aligning the attack steps and the controls from the industry framework, such as NIST and ISO, to the standard attack lifecycle ensures a more comprehensive and

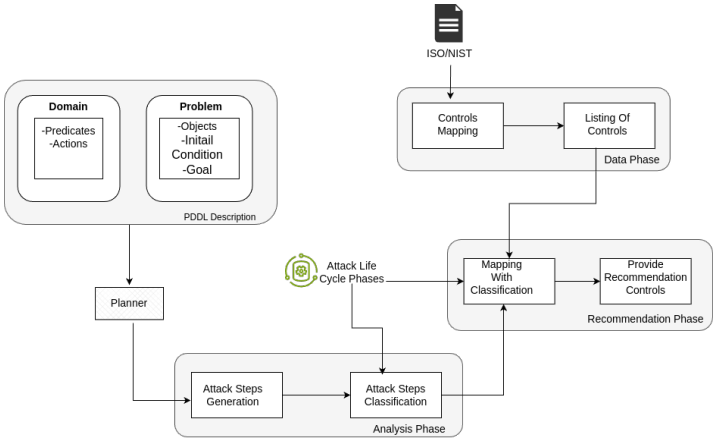

Fig. 1 The Proposed Approach

proactive cybersecurity posture. It also ensures that the recommendations provided are not only proactive but also aligned with industry best practices. The detailed explanation of each phase is as follows:

3.1 PDDL Description

Recent advancements in PDDL have led to its adoption in a wide range of fields (*e.g.,* penetration testing, security assessment, robot mapping, urban planning, and traffic control) [17]. PDDL is a standardized language designed to express planning problems in AI. PDDL description is comprised of two main components: the domain and the problem. The details of both are given below.

PDDL Domain is a high-level description of a set of problems and the corresponding actions and constraints involved. In the PPDL domain, we specify the requirements (such as strips, typing, and equality). The domain stores preconditions, post-conditions, and cause-effect relationships in a sequence of actions that represent an attack. Figure 2 shows the preconditions and effects of the two different actions. The action in the PDDL domain describes a scenario where an entity performs a task. Before the action can occur, the preconditions ensure that the entities involved are valid. Once the action is executed, the system updates to reflect that the task has been completed.

The precondition section inside the action ”user-visits-site” specifies the conditions that must be true for the action to be applicable or executable (*i.e.,* :precondition (and (user ?User) (software ?Browser) (browser ?Browser) (site ?Site))). In precondition, ”and” is a logical conjunction, meaning all conditions inside must be true. In other words, before the user can visit a site, the user must be valid, the browser must be software and a valid browser, and the site must be valid site. The

```
(:action user-visits-site
:parameters (?User ?Browser ?Site)
:precondition (and (user ?User)
(software ?Browser)
(browser ?Browser) (site ?Site))
:effect (and (use-software
?Browser)
(user-visits-site ?User ?Site)))
```

```
(:action gain-write-access

:parameters (?attacker ?bucket)
:precondition (s3-bucket ?bucket)

:effect (has-write-access ?attacker
?bucket))
```

Fig. 2 PDDL Representation of Actions for Two Different Domains

effect describes changes in the system after the action has occurred. The planner will only accept a domain if it supports all the requirements mentioned on the domain.

PDDL problem contains an initial state, a set of predicates that are set to true initially, and a goal state, a set of predicates that may or may not be true with the actions defined in the domain. The objects section starts with the list of specific objects (or instances) that exist in a scenario. In the PDDL, the problem goal section defines the desired state or conditions that the planner should aim to achieve. The goal state denotes the desired final state of the world for the given attack.

Planner takes PDDL description as an input. The output of the planner is a plan, that is, a sequence of actions that takes the agent from the initial state to the goal state. AI planners have the advantage of requiring no data or datasets to train. Instead, an entity within a domain is modeled, describing the relevant features of an environment, the goals, constraints, and the actions available to the entity. The PDDL planner aims to solve a PDDL problem by finding a plan that satisfies it.

3.2 Analysis Phase

The planner takes the input of the PDDL description to generate the output plan, which is the attack steps that lead to the compilation of the goal. The analysis phase is the second phase of the solution, and the attack steps are used as input for the analysis phase as an attack step generation. These generated attack steps move to the classification part, where each step will be classified according to the attack lifecycle, such as reconnaissance, weaponization, delivery, exploitation, installation, and command and control.

The attacks go through the described phases in a variant of degrees. This ensures that we do a structured analysis of how an attack occurs, seen from the view of attackers. We utilize the OpenAI API to classify the attack steps. It helps accurately classify and identify patterns in the attack steps. For example, if the attacker gathers information about the user by sending a malicious email, it indicates that the attacker is gathering information about the user, which means the attacker is in the reconnaissance phase of the attack lifecycle.

The attack occurs in multiple steps in which the attacker guides the user on his own way to get access to the system. All of the generated steps will be classified based on the standard attack lifecycle. In the analysis phase, classifying the attack

steps according to the standard attack lifecycle is important because it provides a structured understanding of the attack progression. This structured approach helps the security analyst to better understand the attack flow, which makes it easier to recognize the vulnerabilities in the system. It also helps develop countermeasures that can disrupt the attack at various stages.

3.3 Data Phase

In this phase, we use well-known, widely recognized, and easily available controls, specifically the NIST Cybersecurity Framework and ISO 27001 controls framework. Both of the frameworks are internationally recognized. By utilizing these frameworks, we ensure that our approach aligns with the best practices, ensuring coverage of key security aspects like risk management and response planning.

Each framework contains a robust set of controls to mitigate various threat scenarios. Both frameworks are well-established; they provide a trusted base for developing our cybersecurity controls. By aligning our approach with NIST and ISO 27001, we aim for a robust and well-rounded security framework.

In our approach, we mapped controls that are common in both frameworks. It will allow us to draw on the strengths of both frameworks while maintaining simplicity and coherence in our control implementation. After completing this mapping, we prioritize the specific controls most relevant to malware threats. This selection process strengthens our security posture and simplifies the integration of controls, making the implementation more efficient and effective.

3.4 Recommendation

In the recommended phase, we begin by compiling a list of controls that are common to both of the security control frameworks. This initial compilation serves as a foundation for our security strategy. Once the list is established, we categorize these controls according to the standard attack lifecycle. The lifecycle includes phases such as reconnaissance, weaponization, delivery, exploitation, installation, command, and control. This classification of controls according to the attack lifecycle allows us to align our security measures with the specific phases of an attack.

For example, controls related to user training and awareness might be particularly relevant during the reconnaissance phase when attackers gather information about the target. By mapping controls to the attack phases, we can ensure that our recommendations are proactive and strategically focused on mitigation at each lifecycle step. This proactive approach allows us to enhance our ability to mitigate risk at each step of the attack lifecycle.

4 Evaluation

The implementation of our solution used in the evaluation and examples of usage are publicly available at `https://github.com/afaqinayat/PDDL-Implementation`. To evaluate the proposed approach, we started by focusing on generating attack steps using an AI planner. We run two different planners in our experiment: the Metric-ff planner and the Fast Downward [10],[9]. The Metric-ff planner gives a simple output without too much detailed information, while the Fast Downward gives the output with additional details (*e.g.*, plan cost, memory, and expended states) and provides an optimal output plan. After the planner's decision, we use PDDL as a language to create the domain and problem file for the planner, where the actions, preconditions, and goal conditions tailored to the cyberattack are defined. These files are described as a *.pddl* file and served as the foundation for generating the attack steps.

The planners run the *.pddl* files (domain and problem files) to automate solutions for planning problems. Both the planners were executed in the Linux environment. Once the planner is executed, it produces a series of steps that show the transition from the initial state to the final goal state, thus highlighting each action a malicious attacker would take. For example, Figure 3 presents a visualization of the steps involved in the S3 ransomware attack [18]. The identification of these steps is crucial as they provide information on how an attacker progresses, and this information is valuable as it helps identify attack patterns. The generated plan steps also provide insights into the different stages of the attack lifecycle, which can be simple or complex, thus facilitating risks and vulnerability assessments.

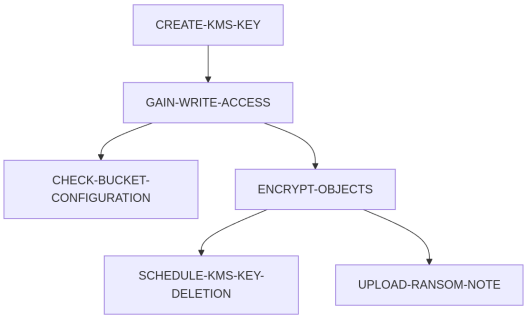

Fig. 3 Steps of the S3 Ransomware Attack

The Metric-ff planner is a straightforward, relaxed planning and hill-climbing search approach that gives a sample output plan without any other detailed information. Fast Downward planner uses heuristics and various search enhancements, which give us detailed information like plan cost, expanded states and total time, and many other information. One of the benefits of using Fast Downward is that it gives us the opportunity to test our domain and solve problems with different types of searches. we check the four searches such as *astar(blind())*, *astar(hmax())*, *astar(lmcut())* and *eager_greedy([ff()])* with two different scenerio separately (*ie.,*

phishing and ransomware attacks). Each offers different levels of efficiency and complexity; among them, the *lmcut* generally provides the advanced heuristic, most efficient and best performance due to its more informed search guides while *eager_greedy* selects actions that seem immediately promising to find the quick solution. It does not guarantee optimal solutions but is typically faster for finding feasible solutions. The plan cost remains the same for specific scenarios, but the value of the expended states and total time are changing. Table 1 shows the different search results of the phishing attack.

Table 1 Different Searches Details

No.	Search Name	Plan Cost	Expended States	Peak Memory (KB)	Total Time (s)
01	astar(blind())	10	31	10224	0.001973
02	astar(hmax())	10	23	10224	0.001891
03	astar(lmcut())	10	11	10224	0.001946
04	eager_greedy([ff()])	10	11	10224	0.002042

Next, we moved to the classification of the attack steps into the various stages of the attack lifecycle. First, we tried a keyword-matching approach to categorize each step. The keyword-based approach was not effective and often failed to appropriately categorize certain plan steps, as it failed to account for the full context of the action and its meaning. This limitation was apparent when steps involved minor differences in terminology. To address this, we integrate OpenAI API, which enhances the classification process; the code snippet in Listing 1 illustrates how we set the query used by OpenAI API. The code query is used by the function classify_action, which uses OpenAI API to classify a list of actions into phases of the attack lifecycle. The OpenAI API leverages advanced natural language processing (NLP) techniques that go beyond keyword matching. It has the capability of understanding the context and semantics behind each attack step, ensuring that the classification more accurately aligns with the stages of the attack lifecycle. This approach not only enhanced the accuracy of classification but also provided a scalable solution.

Listing 1 Message to OpenAI API

```
...
        messages=[
            {
                "role": "user",
                "content": f"Classify each cyber action in
                the following:{action_name} in most relevant one
                category from this cyberattack life cycle
                list: {category}. In output i want dictionary of
                the all the actions like x: 'y', here x is the
                index of action and y is classification
                result from given list",
            }
...
```

The final phase of our work focuses on the recommender system that mapped the set of controls to the classified attack steps controls that focus on malware prevention. The controls are derived from established frameworks such as NIST CSF and

Table 2 Recommended Controls for Different Attack Phases

Killchain Phase	Control	Company	Price	Efficacy
Delivery	Malware Protection	Trend Micro	$40 - $69.90/year	High
		Kaspersky Lab	$69.90/year	High
Exploitation	Malware Protection	McAfee	$399/year	High
		CrowdStrike	$99.99/device/year	High
Exploitation	Human Security Awareness	SANS Institute	$1279/year	High
		Cybrary	$660/year	High
Installation	Malware Protection	Fortinet	$69.90/year	High
		Trend Micro	$40 - $69.90/year	High
Installation	Event Logging	Splunk	$1800/GB/day	High
		IBM QRadar	$10400/year	High
Act on Objective	Malware Protection	Trend Micro	$40 - $69.90/year	High
		McAfee	$399/year	High
Act on Objective	Human Security Awareness	D3 Security	$727/year	Medium
		Global Learning Systems	$711/year	Medium

ISO 27001; both are widely recognized in the field of cybersecurity. These controls are also mapped with the stages of the attack lifecycle to ensure that they are relevant and effective in addressing potential vulnerability at each stage. Additional information for each control, like cost, provider company, and efficacy, are critical factors for decision-making for security operations, and the CyberDB website is utilized to get these details. Table 2 shows a snippet of the recommended controls output for the example of the phishing attack; the steps generated by the planner are classified as follows *Delivery, Delivery, Delivery, Exploitation, Installation, Weaponization, Installation, Exploitation, Act on Objective*. The full table with the full output of the recommender system can be found in a PDF in the paper repository. Such detailed information like cost and efficacy helps in making informed decisions when selecting appropriate security measures. For example, the control human security awareness recommends for exploitation and action in objective phases with different efficacy. By offering recommendations that are based on the specific stage of the attack life cycle, the recommender system enhances the decision-making process, making it easier for administrators to prioritize actions that will provide an effective defense against the cyber attack. This improves the overall security posture by providing actionable insights.

5 Conclusions and Future Work

In conclusion, we employed the PDDL and have demonstrated the efficacy of AI planning to model and anticipate cyberattacks. By using an AI planner, we can generate the attack steps, allowing us to identify and classify each phase of the cyberattack, ranging from reconnaissance to command and control. This structured approach not only aids in understanding the attack lifecycle but also facilitates the identification of critical points where intervention can be most effective. In other

words, we can say that it empowers the organization to proactively mitigate risks and deploy countermeasures.

The usage of a recommender system further strengthens the proposed approach. Based on that, security teams can make informed decisions by providing tailored recommendations based on the identified attack path. Combining AI planning and recommender systems has the potential to improve cybersecurity by proactively identifying vulnerabilities and tailoring defense strategies.

Future work involves expanding the PDDL to various attack scenarios and the integration of recommendation systems for protection. Also, additional quantitative evaluations have to be conducted, and further AI techniques can be explored (*e.g.*, supervised and unsupervised learning) for the recommendation of effective protections that encompass specific compliance and business demands. Furthermore, generative AI benefits have to be explored more in-depth, thus verifying the accuracy of different frameworks and tools for cybersecurity scenarios.

Acknowledgements

This work was partially supported by the São Paulo Research Foundation (FAPESP) under grant number 2020/05152-7, the PROFISSA project, and is part of CNPq process 316662/2021-6. It is also part of the INCT of Intelligent Communications Networks and the Internet of Things (ICoNIoT), funded by CNPq (proc. 405940/2022-0) and the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) Finance Code 88887.954253/2024-00.

References

1. A. O. Adewusi, U. I. Okoli, T. Olorunsogo, E. Adaga, D. O. Daraojimba, O. C. Obi: Artificial intelligence in cybersecurity: Protecting national infrastructure: A usa. World Journal of Advanced Research and Reviews **21**, 2263–2275, 2024
2. C. Ayala, K. Jimenez, E. Loza-Aguirre, R. O. Andrade: A hybrid recommender system for cybersecurity based on a rating approach. In: Advances in Security, Networks, and Internet of Things: Proceedings from SAM'20, ICWN'20, ICOMP'20, and ESCS'20. Springer, 2021, pp. 397–409
3. S. Castellanos, M. C. Alvarez-Herault, P. Lalanda: Decision support tool for the development of power distribution networks based on ai planning. In: 27th International Conference on Electricity Distribution (CIRED 2023). Vol. 2023. Rome, Italy, 2023, pp. 1425–1429
4. T. Choi, R. K. Ko, T. Saha, J. Scarsbrook, A. M. Koay, S. Wang, W. Zhang, C. St Clair: Plan2defend: Ai planning for cybersecurity in smart grids. 2021 IEEE PES Innovative Smart Grid Technologies-Asia (ISGT Asia) pp. 1–5, 2021
5. G. Falco, A. Viswanathan, C. Caldera, H. Shrobe: A master attack methodology for an ai-based automated attack planner for smart cities. IEEE Access **6**, 48360–48373, 2018
6. L. Ferreira, D. C. Silva, M. U. Itzazelaia: Recommender systems in cybersecurity. Knowledge and Information Systems **65**(12), 5523–5559, 2023

7. M. Franco, E. Sula, B. Rodrigues, E. Scheid, B. Stiller: ProtectDDoS: A Platform for Trustworthy Offering and Recommendation of Protections. In: Economics of Grids, Clouds, Systems, and Services. Springer, Izola, Slovenia, September 2020
8. M. F. Franco, B. Rodrigues, B. Stiller: Mentor: the design and evaluation of a protection services recommender system. In: 2019 15th international conference on network and service management (CNSM). IEEE, Halifax, Canada, 2019, pp. 1–7
9. M. Helmert: The fast downward planning system. Journal of Artificial Intelligence Research **26**, 191–246, 2006
10. J. Hoffmann: The metric-ff planning system: Translating"ignoring delete lists"to numeric state variables. Journal of artificial intelligence research **20**, 291–341, 2003
11. P. Huff, K. McClanahan, T. Le, Q. Li: A recommender system for tracking vulnerabilities. In: Proceedings of the 16th International Conference on Availability, Reliability and Security, 2021, pp. 1–7
12. M. Husák: Towards a data-driven recommender system for handling ransomware and similar incidents. In: 2021 IEEE International Conference on Intelligence and Security Informatics (ISI). IEEE, San Antonio, Texas USA, 2021, pp. 1–6
13. M. Iavich, G. Iashvili, R. Odarchenko, S. Gnatyuk, A. Gagnidze: Developing security recommender system using content-based filtering mechanisms. In: International Scientific-Practical Conference" Information Technology for Education, Science and Technics". Springer, Cherkasy, Ukraine, 2022, pp. 619–634
14. A. Inayat, M. F. Franco, E. J. Scheid, L. Z. Granville: Security management using planning domain definition language: A case for ransomware mitigation. In: Anais da XX Escola Regional de Redes de Computadores. SBC, Port Alegera, Brazil, 2023, pp. 31–36
15. M. Kazdagli, M. Tiwari, A. Kumar: Leveraging ai planning for detecting cloud security vulnerabilities. arXiv preprint arXiv:2402.10985 , 2024
16. R. Kerr, S. Ding, L. Li, A. Taylor: Accelerating autonomous cyber operations: A symbolic logic planner guided reinforcement learning approach. In: 2024 International Conference on Computing, Networking and Communications (ICNC). Big Island, Hawaii, USA, 2024, pp. 641–647
17. M. Khalaf, L. Peters, K. Waedt: Modeling security controls and system assets as autonomous planning tasks. INFORMATIK 2022, 2022
18. R. S. Labs: S3 ransomware: Part 1-attack vector, 2024, `https://rhinosecuritylabs.com/aws/s3-ransomware-part-1-attack-vector/`, accessed: 2024-12-12
19. X. Lou, K. Waedt, Y. Gao, I. B. Zid, V. Watson: Combining artificial intelligence planning advantages to assist preliminary formal analysis on industrial control system cybersecurity vulnerabilities. In: 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI). Gheorghe Asachi Technical University of Iasi, Romania, 2018, pp. 1–8
20. J. Ma, Y. Guo, C. Fang, Q. Zhang: Digital-twin-based cps anomaly diagnosis and security defense countermeasure recommendation. IEEE Internet of Things Journal , 2024
21. F. Mizrak, G. R. Akkartal: Prioritizing cybersecurity initiatives in aviation: A dematel-qsfs methodology. Heliyon **10**(16), 2024
22. P. Nespoli, F. Gomez Marmol, J. Maestre Vidal: Battling against cyberattacks: Towards pre-standardization of countermeasures. Cluster Computing **24**, 57–81, 2021
23. J. L. Obes, C. Sarraute, G. Richarte: Attack planning in the real world. arXiv preprint arXiv:1306.4044 , 2013
24. N. Polatidis, E. Pimenidis, M. Pavlidis, S. Papastergiou, H. Mouratidis: From product recommendation to cyber-attack prediction: Generating attack graphs and predicting future attacks. Evolving Systems **11**, 479–490, 2020
25. B. M. Reinstadler: AI attack planning for emulated networks. Ph.D. thesis, Massachusetts Institute of Technology, 2021
26. Z. Wang, Y. Zhang, Z. Liu, X. Wei, Y. Chen, B. Wang: An automatic planning-based attack path discovery approach from it to ot networks. Security and Communication Networks **2021**(1), 1444182, 2021
27. E. Zouave, M. Bruce, K. Colde, M. Jaitner, I. Rodhe, T. Gustafsson: Artificially intelligent cyberattacks. Stockholm: Totalförsvarets forskningsinstitut FOI , 2020