Analysis and Forecasting of Vulnerabilities with AI for Decision Support

Roman Graf
Deloitte Consulting GmbH
Vienna, Austria
e-mail: rgraf@deloitte.at

Artūrs Lavrenovs
University of Latvia
Riga, Latvia
e-mail: arturs.lavrenovs@lu.lv

***Abstract*—In this article, we address questions, such as: How to structure, analyze, and forecast the development of vulnerabilities in the constantly changing world around us? What threat landscape have we experienced in the past, and which attack vectors are most important at the moment? How to adapt to the coming cyberspace threats? We aim to help politicians, decision-makers, industry, lawyers, and technological pioneers adapt their defenses when the rules of the game are constantly evolving. Protecting organizations against the increasing number of cyber-attacks has become as crucial as it is complicated. To be effective in identifying and defeating such attacks, cyber analysts require novel threat modelling methodologies based on AI techniques that can automatically recommend protection measures for current and future periods. We propose a custom, simple, explainable on-site approach to recommend the most significant threats. Our goal is to provide a solution that could extract vulnerability features from the CVE database, find related correlations in a fast and scalable way, and automate recommendations, reducing the number of manual research activities and increasing the organization's security.**

***Keywords*—Vulnerabilities analysis, AI, cybersecurity.**

I. Introduction

The challenge of identifying, prioritizing, and patching known software vulnerabilities has been a continuous task for cyber defenders for years. To improve vulnerability mitigation procedures, cyber defenders need an expert system that can accurately perform decision support regarding vulnerability severity, relevance, and likelihood of exploitation, being able to adapt to information published after the initial disclosure. The proposed decision support method can reduce the amount of effort required to address critical vulnerabilities. The presented technique addresses challenges posed by the constant evolution of technologies, threats, cyber-attack vectors, and ways of formulating and coordinating security experts' responses. Discussing the security implications of attack vectors without knowing their severity is impractical.

This is an attempt to facilitate the management of security measures. Effective threat analysis models based on proven security standards, such as NIST[1], ISO-27001[2], etc., prevent or reduce the most significant risks. To better understand the risk severity and to improve threat model accuracy, we developed a novel AI method, which returns the expected risk severities that are most significant for recommendation decisions. We employed collaborative filtering and predictive analysis methods to get recommendations. Using this method, we further improved the accuracy of a threat model with a better understanding of the risks. Based on a well-known CVE database, using AI methods, we calculate recommendations for protection measures for the next period. Compared to the first version of our method [3], where we used exploit DB [4] as a main source for vulnerabilities, in the second version, we moved to the CVE database [5], which has several advantages, such as a more complete and structured content. These recommendations are based on the attack vector developments in previous time periods. Such recommendations will provide decision support for cybersecurity experts on risk estimation and budget planning for their risk models. The presented technique comprises attack vector extraction, feature composition, analysis of attack profiles, and recommendations for matching profiles and missing security measures to plan the organization's security posture.

II. Related Work

One of the most developed existing vulnerability scoring systems is the Exploit Prediction Scoring System (EPPS) [6]. It is a data-driven exploit scoring system that produces scores for all known vulnerabilities, which is freely available, and which adapts to new information, providing crowd-sourced expertise. This system attempts to predict the probability of vulnerability exploitation for the next 30 days and thus may be prioritized for remediation. Compared to this approach, we try to predict potential attack vectors based on the analysis of historical development of vulnerabilities and not based on the existence of exploit code. Additionally, our main goal is decision support and not a scoring of vulnerability. Another approach to forecasting the volume of CVEs [7] employs initial correlation analysis and diligently crafted statistical features such as CVSS score. Our approach is different, since we apply another type of classification by attack vectors, based on a custom taxonomy model. A brief overview of related approaches for the application of recommendation systems in the cybersecurity domain is given in [8]. These

https://doi.org/10.51408/csit2025_36

systems [9] use algorithms to identify patterns within data and apply them to various problems, such as predicting individuals' future responses to actions and performing pattern analysis on objects of interest. A recommender system in this research is defined as one that uses active information-filtering techniques to exploit past user behavior to suggest information tailored to an end user's goals. The working paper [10] defines recommender systems as a key application for mapping the Intelligence Cycle and Human Language Technology. The research additionally states that in the cyber domain, recommender systems are used for generating prioritized lists for defense actions [11], detecting insider threats [12], monitoring network security [13], and expediting other analyses [14]. In contrast to the referenced research, our approach also employs recommender systems for defense actions, but we additionally employ the power of the pentesting expertise and use an exploits database and knowledge of the historical development of attack vectors, combined with up-to-date market studies, to set up defense actions.

Multiple researchers are developing an automated technology [15] that addresses a range of cybersecurity challenges from product recommendation to cyber-attack prediction. A recommendation system is utilized to make predictions about future attack steps within the network to classify, predict, and prevent attacks. Our approach instead analyzes attack vectors and their historical development and infers required protection measures against future threats.

None of the discussed approaches provides recommendations for risk modeling in terms of security standards and penetration testing background in a feasible way.

III. Recommendation Workflow

The workflow process is depicted on the left side (Figure 1) and is composed of two parts. One process is shown in the middle and describes a recommendation of additional risks, and the second part, presented on the right side, is a prediction of potential risks. For both parts, the same data is used, which is aggregated from different sources, such as publicly available or custom exploit databases, studies, and threat intelligence tools, and from domain experts, who are vendors, antimalware producers, SOC or CERT experts. The main query workflow execution begins with the extraction of, e.g., exploit database data (see Step 1 in Figure 1 on the left side) and parsing of the extracted content for feature extraction and their normalization in Step 2. The most important risks for an organization are defined in Step 3. The reasoning for such a definition can be based on the existing organization's risk model, the threat landscape in a particular country, and the SOC team's statistics.

For the computation of the features, we employ a proprietary-developed parsing method. Through extracted features, we obtain quarterly risk profiles broken down into attack vectors. It is also possible to additionally extend the model knowledge base by additional sources and attack vectors. In the next step, we search the model by previously defined organizational risk profile using the "Manhattan distance" collaborative filtering method, find a similar profile, and complete the organizational risk profile with additional attack vectors (Step 4), distributing additional risks proportionally. Additionally, we can employ the "Slope One" prediction method [16] to predict probably the most important additional risks and calculate them similarly in the organizational risk profile (Step 5). The resulting organizational risk profile is then composed of the fixed part of initial risks coming from the ISMS risk model and from calculated recommended risks distributed proportionally to the fixed part of the profile (Step 6). Finally, we calculate the resulting needed security measures, mapping them from the ISMS mitigation plan and current Security studies (Step 7).

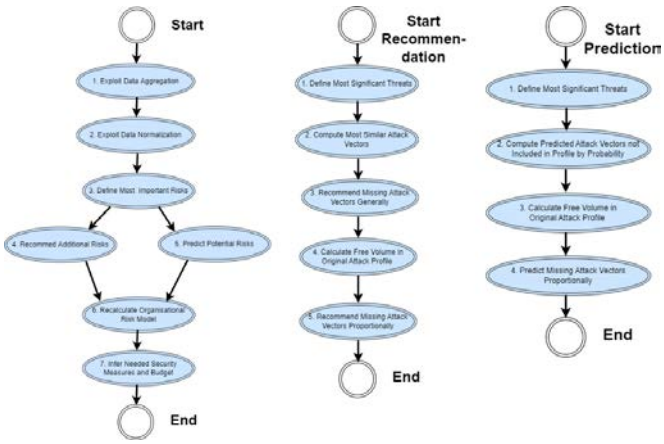

Fig. 1: The workflow for feature extraction and recommendation of attack vectors using the AI approach

Since the data is not subject to grade inflation (no different scales for different profiles), experimental data is not sparse, and data is dense (almost all attributes are filled with non-zero values), we selected the Manhattan distance algorithm in Formula 1 to calculate profile similarity [16].

$$M = | x_1 - x_2 | + |y_1 - y_2| \quad (1)$$

A simple and high-performing item-based "Slope One" prediction algorithm is a way to fine-tune our collaborative filtering approach and produce more accurate recommendations efficiently. Using implicit ratings, we observe the development of the threat landscape over time. The main step in this method is to compute deviations. The average deviation between timestamp *i* and timestamp *j* is represented in Formula 2:

$$dev_{i,j} = \sum_{u \in S_{i,j}(X)} \frac{u_j - u_i}{card(S_{i,j}(X))} \quad (2)$$

where $S_{i,j}(X)$ is the timestamp (quarters) set in the entire set *X* of all ratings that have scored both quarter *i* and quarter *j*. The $u_j - u_i$ numerator is the quarters' rating difference for particular items (attack vectors).

The suggested approach can be accomplished with a rule-based expert system [17]. Such a recommendation engine will provide decision support for cybersecurity experts on risk estimation and budget planning for their risk models. A rule-based expert system can facilitate the selection of protection measures for different attack vectors based on recommendations from different data sources and considering other potential impacts, rules, and policies.

IV. Experimental Evaluation

A. Evaluation data set

For the experimental dataset with ground truth labels, we extracted exploits and organized them by quarters. For each quarter, we calculated the number of exploits per attack vector. Attack vectors are used as a key in a dictionary later. Additionally, we normalized the data and excluded outdated or outstanding data. With time, we noticed that “exploit-db” database activity had dropped in the last months and for version 2 of our approach, which we called VAFES (Vulnerability Analysis and Forecasting Expert System), we selected a more stable and actively supported CVE database [38] with over 1,8 million of entries (see Figure 2) and used this data for further steps. We also extended the number of analyzed attack vector types. We created our attack vector types taxonomy, and in Figure 2 we demonstrate analysis results for the last 3 years sorted by different parameters, such as attack vector, time, assigner, vendor, severity, and problem type description.

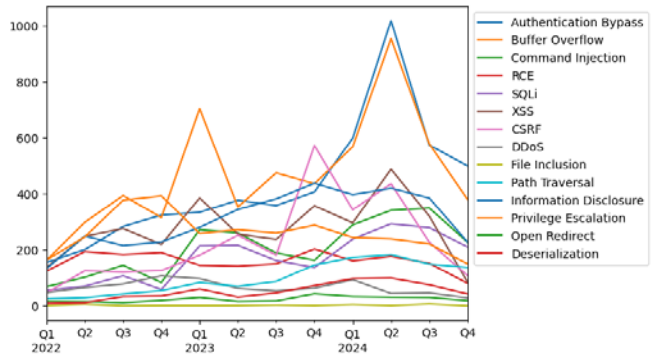

Fig. 2: The distribution of most significant attack vectors over the last 3 years using CVE source

The analysis of the most significant attack vectors shows that problem types in the original database are not properly normalized and require this step to proceed with the analysis. For example, we see CWE-79 addressing the XSS attack vector is included 5 times due to slightly different syntax in the problem type field.

B. Experimental results and interpretation

As a use case for the experiment, we assume that we are a CISO of an example organization, who is tasked to perform a risk analysis according to the cybersecurity standards and to plan and budget protection measures for the next period, “the year 2025, quarter 1”. The organization maintains a defense procurement portal. An expert analyzes the architecture and processes of the organization. From the documentation and organizational SOC team, they know that there are known weaknesses in the authentication process, a remote code execution vulnerability was reported in the last Web pentesting, and the Web application has a connection to the database. These three attack vectors are also defined in an organizational risk model created using the ISO2k standard.

Based on aggregated information and organization specificity, the expert creates a request to recommender “{'Authentication Bypass':0.15,'RCE':0.2,'SQLi':0.1}”, including the mentioned three attack vectors with respective weighting (in the range 0.0 to 1.0, where 1.0 is the maximum value for all attack vectors per quarter) for key “2025Q1” as shown in Figure 3. The recommender responds with a vector of the nearest risk profiles, whereas a lower distance value means that this profile is the nearest. For the given request, the nearest profile is “2024Q4” with a distance value of 0.078. When we analyze the nearest profile in more detail, we see the weights of each attack vector. “Authentication Bypass” is weighted by 0.228, which means this risk takes about 23% of the total risk at that time (fourth quarter of the year 2024). “Buffer Overflow” takes about 0.174% and so on. And finally, an expert gets a recommendation on how to extend his initial profile based on recommender analysis. Recommender suggests completing the query risk profile with additional attack vectors: ('XSS',0.038), ('Command Injection',0.104), ('Priv.Esc.',0.068), etc.

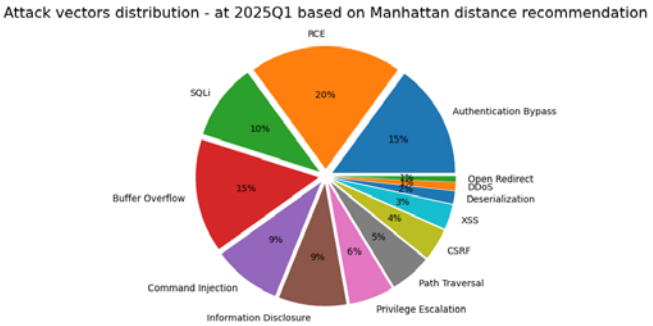

Fig. 3: This figure visualizes the final recommended risk profile for the requested period Q1 of the year 2025

The final recommended risk profile depicted in Figure 3 for the requested period Q1 of the year 2025 consists of an original fixed part (“Authentication Bypass”, “RCE”, and “SQLi”) and of a recommended part (“Command Injection”, “File Inclusion”, “Buffer Overflow”, “Path Traversal”, etc.). The recommended part is distributed over the non-fixed volume proportionally to the recommended splitting. The predicted profile was calculated similarly according to the workflow in Figure 1. This approach facilitates the weighting step for the expert. Finally, expert maps identified risks to the protection measures. After the mapping expert summarizes the required protection measures and splits the budget accordingly.

C. Expert System for Decision Support

An expert system for decision support demonstrates an example of an application of the Rule Engine for a particular scenario. Rule engines should support rules, facts, priority, mutual exclusion, preconditions, and other important aspects of decision-making. In Figure 4 on the left side, we have a set of facts D1-D12, and then actions or outcomes that result from a set of rules D13-D17. Having defined a cybersecurity strategy, including risk management, prediction, and recommendations for threat development and implementation of required mitigation measures, we consider scenarios when a cyber incident or new vulnerability is reported to a Security expert. Assume that the organization’s security feed expert was informed about the spreading elevation of privilege vulnerability in Veeam Agent for Microsoft Windows Software.

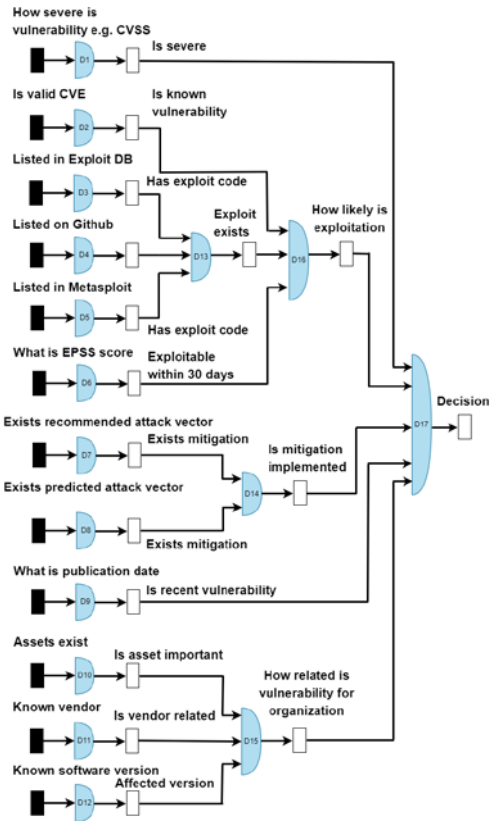

Fig. 4: An example selection of forward rule chaining for vulnerability analysis

Manually or using prepared scripts expert checks if this vulnerability is already listed as CVE, assesses which severity it can have, validates whether his organization has related assets and matching software, and researches the EPSS score, which predicts the likelihood of exploits in the wild, and if an exploit already exists to estimate the probability of attack. In the asset database expert finds that Veeam Agent software is employed in the organization and currently has version 6.1.2.134. There is already a CVE-2024-29853 for that https://nvd.nist.gov/vuln/detail/CVE-2024-29853 with a high severity 7.8 and CVSS score CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H. By analyzing the impact of this vulnerability, the expert understands that it allows for local privilege escalation, but an attacker needs additional conditions to perform the attack. The EPSS score for this vulnerability is 0.00043, which means that the exploitation probability in the next 30 days is quite low. The expert provides collected facts as input to the expert system, which facilitates decision-making for further actions based on predefined rules. The expert system provides an output that it is a quite recent known vulnerability of high severity, listed in CVE repositories without a known exploit with low exploitation expectation. The organization has important assets of the related vendor, but not the vulnerable software version. Recommended and predicted threats are already addressed with respective mitigation measures for the given vulnerability. No further actions are required. This decision saves the organization's potential expenses e.g., forensic investigation to understand if vulnerability could already be exploited, analysis of attack vectors, and definition of mitigation measures, because in this case, it is already done.

V. Conclusion

In this work, we have presented an automated approach to recommend protection measures for establishing a threat model using AI methods. The suggested expert system can significantly improve remediation strategies. We have combined expertise gathered during the information security assessments and pentesting projects with the power of the AI approach for decision support. The main contribution of this work is a real-time automatic solution that can recommend protection measures in a fast and effective way based on a large number of labeled attack vectors in order to facilitate an organization's threat model creation and cybersecurity budget planning. The presented method employs a domain expert knowledge base collected from domain experts to assess up-to-date risks and attack vectors. The proposed method has been experimentally evaluated, and it has shown that it is both practical and effective.

References

[1] NIST Cyber Security Framework. [Online]. Available: https://www.nist.gov/cyberframework.

[2] Information Security Management System. [Online]. Available: https://www.iso.org/standard/27001.

[3] Analysis and forecasting of exploits with AI. [Online]. Available: https://cyberchess.lv/, *CyberStory*, Beta Hall, 15:30-16:00.

[4] Exploit Database [Online]. Available: https://www.exploit-db.com/.

[5] CVEProject [Online]. Available: https://github.com/CVEProject/cvelistV5/.

[6] É. Leverett, M. Rhode and A. Wedgbury, "Vulnerability Forecasting: Theory and Practice", *Digit. Threat.*, Res.Pract. 3,4, Article: 42, 27 pages, 2022. https://doi.org/10.1145/3492328

[7] J. Jacobs, S. Romanosky, O. Suciu, B. Edwards and A. Sarabi, "Enhancing Vulnerability Prioritization: Data-Driven Exploit Predictions with Community-Driven Insights", 2023. https://arxiv.org/abs/2302.14172

[8] V. N. Gadepally, B. J. Hancock, K. B. Greenfield, J. P. Campbell, W. M. Campbell and A. I. Reuther, "Recommender Systems for the Department of Defense and Intelligence Community", *LINCOLN LABORATORY JOURNAL*, vol. 22-1, pp. 74-89, 2016.

[9] G. Adomavicius and A. Tuzhilin, "Toward the Next Generation of Recommender Systems: A Survey of the State-of-the-Art and Possible Extensions", *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, no. 6, 2005, pp. 734–749.

[10] S. Bailey, "The Intelligence Cycle and Human Language Technology", *HLT Return on Investment Working Group, internal document*, 2015.

[11] K.B. Lyons, "A Recommender System in the Cyber Defense Domain", master's thesis AFIT-ENG-14-M-49, *Air Force Institute of Technology Graduate School of Engineering and Management*, Wright-Patterson Air Force Base, 2014.

[12] P. Thompson, "Weak Models for Insider Threat Detection", *Proceedings of SPIE, vol. 5403: Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense*, pp. 40–48, 2004.

[13] T. A. Lewis, "An Artificial Neural Network-Based Decision Support System for Integrated Network Security", *master's thesis AFIT-ENG-T-14-S-09, Air Force Institute of Technology Graduate School of Engineering and Management, Wright-Patterson Air Force Base*, 2014.

[14] C. J. Wood, "What Friends Are For: Collaborative Intelligence Analysis and Search", *master's thesis, Naval Postgrad. School*, 2014.

[15] N. Polatidis, E. Pimenidis, M. Pavlidis, H. Mouratidis, "Recommender Systems Meeting Security: From Product Recommendation to Cyber-Attack Prediction", *Engineering Applications of Neural Networks EANN*, vol. 744, pp. 508-519, Springer, 2017. https://doi.org/10.1007/978-3-319-65172-9_43

[16] R. Zacharski, "A Programmer's Guide to Data Mining", 2015. [Online]. Available: http://guidetodatamining.com/

[17] R. Graf, L. A. Kaplan and R. King, "Neural Network-Based Technique for Android Smartphone Applications Classification," *11th International Conference on Cyber Conflict*, Tallinn, Estonia, pp. 1-17, 2019. doi:10.23919/CYCON.2019.8757162.