UNIVERSITY POLITEHNICA OF BUCUREȘTI FACULTY OF AUTOMATIC CONTROL AND COMPUTERS

PhD Thesis

in Computer Science, Information Technology and System Engineering

System and method for reducing the attack surface and optimizing the response to cyber-security incidents

Author:

Ing. Cristian Săndescu

Supervisor:

Prof. dr. ing. Răzvan-Victor Rughiniș

Bucharest

2022

Contents

List of Figures

List of Tables

1 Introduction

1.1 Overview

In order to respond to the challenge of cyber threats, the cyber security industry is constantly forced to innovate in order to develop new mechanisms to ensure the continuous monitoring and defense of information systems. This task is all the more complex as the emergence of new technologies that amplify the risk of exploitation by malicious actors increases.

In a competitive free market, the success of software products and services depends on their speed. Although beneficial, this feature of the free market, and in particular of the IT industry, has an unintended consequence: exposure to cyber-attacks. Technical vulnerabilities resulting from the pressure of the business environment on rapid technical implementation create risks of exploitation and material or intellectual loss. Thus, the field of cybersecurity provides an answer to the current paradigm of the development of IT solutions characterized by exponential speed and complexity. This response refers to the development of techniques and systems to reduce the risk of exploitation of cyber vulnerabilities.

Both the state of affairs and the estimates of cybersecurity experts show that technological advancement is creating a complex IT environment in which the means of exploiting cyber vulnerabilities are becoming increasingly sophisticated, fast and efficient. An analysis of the costs of exploiting cyber vulnerabilities in 2015 illustrates annual costs of € 300 billion [1]. A 2016 descriptive analysis of a cyberattack dataset shows that the minimum cost of a cyberattack is € 200,000 [2]. It follows that the means to reduce the risk of exploiting cyber vulnerabilities are key to avoiding costs.

The average time required to identify and fix a security breach is 287 days, and 53% of organizations are unaware of the attack, all the while, according to the latest Ponemon study, IBM [3]. Teams working in cyber security operations centers (SOCs) are overwhelmed by the average number of 11,000 alerts per day they have to respond to, putting the current cyber security industry at a deficit of 2.7 million professionals - ISC2 [4]. In the above context, influenced by the changes imposed by the pandemic, the number of ransomware attacks

increased 13 times in the first half of 2021, compared to the same period in 2020, according to the Trend Micro report [5].

There are two approaches to reducing the risks of exploiting cyber vulnerabilities in IT infrastructures. First of all, it is a reactive approach that requires a real-time response to attempts to exploit cyber vulnerabilities. The second approach focuses on proactivity and involves addressing vulnerabilities prior to actual exploitation. It follows that risk mitigation through the second approach (proactive approach) is an ongoing process that has as its main foundation the operation of prioritizing the cyber vulnerabilities identified in an IT infrastructure. In other words, the proactive approach involves the ongoing monitoring of a cyber infrastructure in order to identify and prioritize cyber vulnerabilities to address them before operation.

The proactive approach to cybersecurity involves a number of precautionary measures taken to reduce the risk of exploiting cyber vulnerabilities. These measures focus on reducing the risk of exploitation by prioritizing actions to address weaknesses in a cyber infrastructure. This prioritization process is performed by quantifying the risk associated with an exposure by reference to a number of parameters.

A first type of parameters proposed in this thesis refers to the internal parameters. The internal parameters used in the proactive approach to cyber risk reduction can be defined in terms of variables that represent the features of the system to be protected. The process by which these variables are used as a benchmark in prioritizing existing vulnerabilities is based on a method of risk assessment that emphasizes the impact that the exploitation of a vulnerability has on the infrastructure concerned. This method emphasizes the organizational context of the infrastructure to be protected.

The second type of proposed parameters refers to external parameters. External parameters used in the proactive approach to cyber risk reduction can be defined in terms of variables that represent the dynamics of the external environment of a cyber infrastructure. In this case, the focus is on the likelihood of exploiting a cyber vulnerability given the motivations, objectives and capabilities of the agents who intend to exploit the system to be protected.

Therefore, this thesis presents a series of empirical studies conducted in order to develop the components of a system of proactive reduction of the risk of cyber threats. The proposed

system aims to quantify internal and external parameters in order to prioritize the cyber vulnerabilities of an information system. Thus, the proposed system is intended to receive as input a number of internal and external parameters that characterize a cyber infrastructure and to provide as an output a list of cyber vulnerabilities prioritized according to the risk of exploitation. Figure 1 provides a graphical representation of the system.

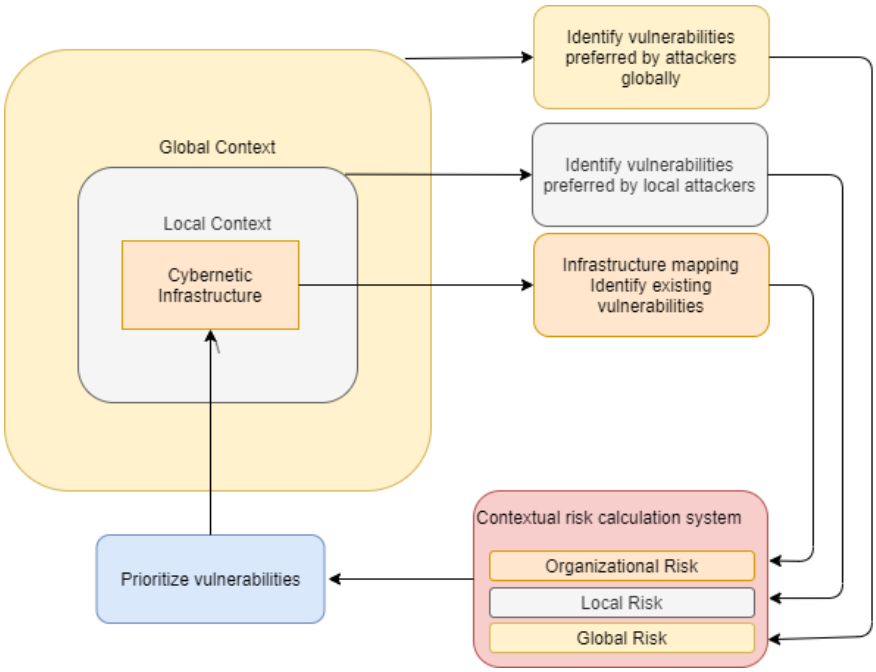

Figure 1. Overview of the proposed system.

1.2 Thesis Outline

The thesis is organized in five main sections. The next section presents the theoretical aspects that act as a foundation for the empirical studies developed in the next section. Theoretical aspects related to the techniques and models used in the research process are presented. These cover natural language processing methods, honeypot systems and security vulnerability risk assessment methods. Each of the mentioned sections facilitates the presentation of the results of the empirical studies. Each empirical study presents one of the three components presented in Figure 1: the model for early identification of cyber security vulnerabilities, the model for optimizing the response to cyber-attacks using "Honeypot" systems, and the model for integrated calculation of contextual risk to reduce cyber-attack surface. Three empirical

studies are presented aimed at developing the modules needed to design, implement and evaluate the performance of the proposed models.

The first empirical study describes the implementation and results of an early vulnerability identification system. Its results demonstrate the feasibility of developing machine learning models based on the understanding of natural language that would allow the early detection of new vulnerabilities, as well as the reduction of detection time for SecOps teams. The study aims to quantify global external parameters taken from open sources such as specialized news platforms and social networks where research communities such as Twitter are present. The associated section 3.1 presents the results of the implementation of a system based on natural language processing and machine learning algorithms that allows the quantification of global attack trends from OSINT data, while the theoretical aspects used are presented in Section 2.1 of this document.

The section associated with the second empirical study presents the results of the design, implementation and evaluation of the performance of an innovative "honeypot" system called Hunt. This system involves the development of an agent architecture developed to map in detail the cyber infrastructure that is to be protected in order to obtain the necessary data for the development of a honeypot system that allows the analysis of local attack tendencies of malicious actors - the agent of camouflage. The second component is represented by the attacker profiling subsystem using elements from game theory. This section also presents the results of implementing a honeypot system for a real cyber infrastructure, by testing the system camouflaged between the pages of a real web application. Unlike traditional honeypot systems, the proposed system uses two new components: a camouflage system, and an attacker gamification system. Such an approach requires simulating the environment to be protected and attracting real attackers to understand their attack strategies and targets. Section 2.2 develops in detail the theoretical aspects of a honeypot approach in this regard, while section 3.2 presents the way of working and the results of the study.

The third empirical study describes the implementation and results of an algorithm for calculating the organizational contextual risk of a cyber infrastructure. It aims to quantify internal and external parameters in order to prioritize the identified cyber vulnerabilities to reduce the noise level at the level of a complex infrastructure. Section 3.3 associated with this empirical study presents the results of implementing an algorithm and a vulnerability prioritization system developed to analyze the cyber infrastructure to be protected and the

results of the methodology used to reduce the attack surface of the organization by SecOps teams effectively. The elements of theory used in this study are presented in detail in section 2.3 of this thesis.

Together, the results of the three empirical studies allow the opening of a discussion section presenting the limitations and opportunities for integration in order to implement a system to ensure the efficiency of processes in operational security centers, targeting the two basic areas of their functioning. This section is followed by a section summarizing the results and conclusions of each of the studies along with subsequent optimization possibilities.

2 Theoretical Aspects

This section describes the theoretical aspects relevant to the implementation of the proposed system. Thus, theoretical aspects related to early detection using natural language processing techniques, aspects related to honeypot systems and aspects related to the contextual risk of exploiting a cyber vulnerability are discussed.

2.1 Early detection using natural language processing techniques

Natural language processing is a key component in developing a system for estimating the global contextual risk of exploiting a cyber vulnerability. Therefore, this section describes various techniques and procedures for implementing and optimizing an algorithm to process open source data in order to identify information about cyber vulnerabilities.

First, the processes of the Spacy natural language processing sequence are described [6]. For each process, different implementation and optimization techniques are analyzed in relation to the information identified in works such as: Jurafsky and Martin [7], Pulford [8], Nair and Hinton [9], Bouchard [10], Shore and Johnson [11].], Kingma and Ba [12], Gal and Ghahramani [13], Honnibal and Johnson [14].

Additionally, text classification techniques and procedures are analyzed using machine learning algorithms proposed by Zhang [15], Rennie, et al. [16], McCallum and Nigam [17], Vryniotis [18]., Nigam, et al. [19], Cortes and Vapnik [20], Platt [21], Wu, et al. [22], Crammer and Singer [23], Mola [24], Quinlan [25], Breiman [26], Dumais [27], Mikolov, et al. [28], Pennington, et al. [29], Landauer, et al. [30], Zhila, et al. [31], DeepLizard [32], Ognjanovski [33], Ruder [34], Brownlee [35], Senior, et al. [36], Sumit [37], Jacovi, et al. [38], Zhang, et al. [39], De Mulder, et al. [40], Hochreiter and Schmidhuber [41], Sherstinsky [42], Bahdanau, et al. [43], Su and Kuo [44], Vaswani, et al. [45], Horev [46] and others.

This section therefore manages to provide an overview of the existing means by which it is possible to develop a system for the early detection of cyber vulnerabilities through natural language processing techniques.

2.2 Optimizing cyber-attack responses using honeypot systems

The external environment of a cyber infrastructure is composed of the local environment and the global environment. Each type of environment brings with it a different type of exploitation risk. Local risk refers to trends in cyber-attacks that target primarily a specific cyber infrastructure. While computing based on organizational contextual risk allows vulnerabilities to be prioritized by the importance of components and the likelihood of exploitation given their susceptibility to attacks, profiling attackers allows vulnerabilities to be prioritized by attack types and targets preferred by malicious actors.

In this sense, the theoretical aspects discussed in this section allow the identification of directions for implementing a modular system for assessing the local contextual risk of exploiting cyber vulnerabilities in an IT infrastructure in order to optimize responses to cyber-attacks. Thus, this section begins with the use of works such as those proposed by Spitzner [47], Pouget, et al. [48], Barnett [49], Livshitz [50] and HoneynetProject [51] to define three important concepts: honeypot, honeynet and honeytoken.

Further, this section starts from the synthesis proposed by Nawrocki, et al. [52] to analyze existing honeypot systems. In this sense, the systems proposed by Portokalidis, et al. [53], Sharma and Sran [54], HiHatProject [55], Zhuge, et al. [56], TheHoneynetProject [57], Oosterhof [58], Provos [59], Rapid7 [60] and Osquery [61]. The analysis of the above systems therefore allows the identification of benchmarks in order to implement the local contextual risk assessment system for the exploitation of a cyber vulnerability and the optimization of responses.

Obtaining data from a honeypot further addresses issues such as the need for information of "blue teams" and the need to identify indicators to prevent zero-day vulnerabilities. A honeypot system thus manages to expose the unknown weaknesses in a cyber infrastructure for the teams responsible for remediation. Moreover, the information obtained by such a system can be quantified and used in calculating the operational risk of the various components of a cyber infrastructure.

2.3 Contextual risk of exploiting a cyber vulnerability

Defining the contextual risk of exploiting cyber vulnerabilities is part of the broader discussion of the difference between a proactive and reactive approach to cyber security. A study by FireEye shows that almost half (42%) of exploits of cyber vulnerabilities are made after the release of a version of the target software that treats that vulnerability [62]. This shows that an appropriate process of prioritizing cyber vulnerabilities - which involves calculating the risk of exploitation - can significantly reduce the losses caused by cyber-attacks.

Cyber security risk assessment procedures are methodologies for targeting vulnerabilities identified in an IT infrastructure. Most existing risk assessment procedures use a standardized system for assessing common vulnerabilities called CVSS [63]. This system is the result of efforts to centralize all identified cyber vulnerabilities and annotate them with an impact score. Thus, the monitoring systems for cyber threats have the function of identifying and quantifying the risk of vulnerabilities in a cyber infrastructure based on the standardized CVSS system.

Although effective, the approach based on the standardized CVSS system raises a major issue in terms of ensuring cyber security. This approach based on international databases tends to ignore the context of cyber infrastructure. In this regard, approaches can be identified that propose the inclusion of additional parameters that take into account contextual aspects of cyber infrastructure.

Furthermore, this section describes various theoretical and empirical approaches identified from the literature review that propose different methods for calculating the risk of exploiting cyber vulnerabilities using information additional to the CVSS system. Thus, solutions such as those described by Joh and Malaiya [64], Singh, et al. [65], Rapid7 [66] and Secureworks [67] which take into account variables within the cyber infrastructure to calculate the risk of exploiting cyber vulnerabilities. Hence the first type of contextual risk defined in terms of organizational contextual risk, which allows the prioritization of vulnerabilities in relation to the importance of infrastructure components and the probability of exploitation given their susceptibility to attacks.

Based on the observations made by Chen, et al. [68], a second type of contextual risk of exploiting cyber vulnerabilities is proposed that considers variables from the external

environment of the cyber infrastructure. The external environment of a cyber infrastructure is composed of the local environment and the global environment. Each type of environment brings with it a different type of exploitation risk. Local risk refers to trends in cyber-attacks that target primarily a specific cyber infrastructure. While scoring based on organizational contextual risk allows vulnerabilities to be prioritized in terms of the importance of components and the likelihood of exploitation given their susceptibility to attacks, local risk scoring allows vulnerabilities to be prioritized according to the types and targets of attack preferred by malicious actors.

Unlike contextual risk scoring, local scoring uses parameters external to the infrastructure to prioritize identified vulnerabilities. Such an approach requires simulating the environment to be protected and attracting real attackers to understand their attack strategies and targets. Thus, the section develops in detail the theoretical aspects of a honeypot approach. In summary, the proactive contextual approach in mitigating the risk of exploiting cyber vulnerabilities in an IT infrastructure in relation to the organizational context can be improved by analyzing local external attack trends.

The global external environment of a cyber infrastructure has the same characteristics as the local environment but on a larger scale. Thus, the risk associated with this environment, the global risk, refers to the trends in cyber-attacks that mainly target a common component of cyber infrastructures. In other words, global risk involves a quantification of the popularity of exploiting a global vulnerability.

An alternative to quantifying the global contextual risk of exploiting cyber vulnerabilities is to use OSINT (Open-Source Intelligence) methods. In this regard, this section documents articles from the literature such as those written by Hayes and Cappa [69], Horawalavithana, et al. [70], Hobbs [71], Andrew, et al. [72], Rosa, et al. [73] and Day, et al. [74]. Also described are various technical implementations of OSINT data processing algorithms such as those proposed by Chen, et al. [75], Mittal, et al. [76], Sabottke, et al. [77], Dionysius, et al. [78], Abdullah, et al. [79], Zhou, et al. [80], Liao, et al. [81], Husari, et al. [82], Tavabi, et al. [83] and Deliu, et al. [84].

3 Empirical Studies

In order to develop the system proposed in Figure 1, the implementation of three complementary modules is targeted. It is primarily about developing a system that allows for the early detection of cyber vulnerabilities in open data sources ("EVE"). Secondly, it is a system that allows the optimization of the response to cyber-attacks through a honeypot architecture ("HUNT"). Thirdly, it is an integrated system for calculating the contextual cyber risk to reduce the area of attack ('CRS').

The first system consists of a natural language processing model that allows the identification of cyber vulnerabilities from open data sources such as websites and the Twitter platform. This system allows the automation of the process of identifying an existing strategy for the exploitation of cyber vulnerabilities and the identification of new cyber vulnerabilities. Thus, cyber vulnerabilities preferred by global attackers can be identified.

The second system consists of a cyber infrastructure scanning agent and a model for developing a honeypot replication of the infrastructure. The purpose of this system is to replicate the cyber infrastructure in order to expose it to cyber-attacks and to identify the vulnerabilities preferred by local attackers. The section dedicated to this system presents the agent's implementation efforts in a real infrastructure as well as the implementation efforts of a honeypot system.

The latest proposed system has as its components a component for mapping cyber infrastructure and a component for identifying and assessing cyber vulnerabilities. Together, the two components allow the implementation of an organizational contextual risk calculation system. As part of the implementation of this system in a real cyber infrastructure, a methodology for calculating organizational contextual risk has been developed.

In the following lines are presented in turn the efforts of the three empirical studies that aimed to implement the systems presented above.

3.1 Early detection of vulnerabilities in open data sources ("EVE")

The modular global contextual risk estimation system involves the use of natural language processing techniques through machine learning and natural language processing technologies in order to identify cyber vulnerabilities from open data sources. The innovative character of the proposed solution is given by the system processing sequence that merges data from two OSINT type sources: posts from the Twitter platform and specialized articles.

For the development of the proposed system, a series of data sets were used. The first data set used is a corpus of 1000 cyber security articles extracted mainly from The Hacker News and supplemented with articles from Threat Post, Ars Technica and Security Affairs. The second set of data is a total of 3,100 tweets from Twitter communities, in which sharing knowledge about new cyber vulnerabilities is a common practice. Additionally, a new untagged dataset was created by automatic retrieval from specialized websites. The new corpus was extracted from 20 specialized websites and contained 65.8 million tokens and a vocabulary of 63,000 words. The last data set is the usability assessments applied to a convenience sample of 20 individuals.

Figure 2 shows an overview of the proposed system, developed following the efforts presented in the laboratory activity [85, 86]. For the text analysis, prediction and classification component, a number of approaches based on machine learning and natural language processing techniques were used. Thus, the first two data sets were used to implement text analysis modules in Twitter articles and posts. Furthermore, the following data set was used to implement an interpretable model of data analysis, prediction and classification. Finally, the last data set was used to evaluate the user interface of the proposed system.

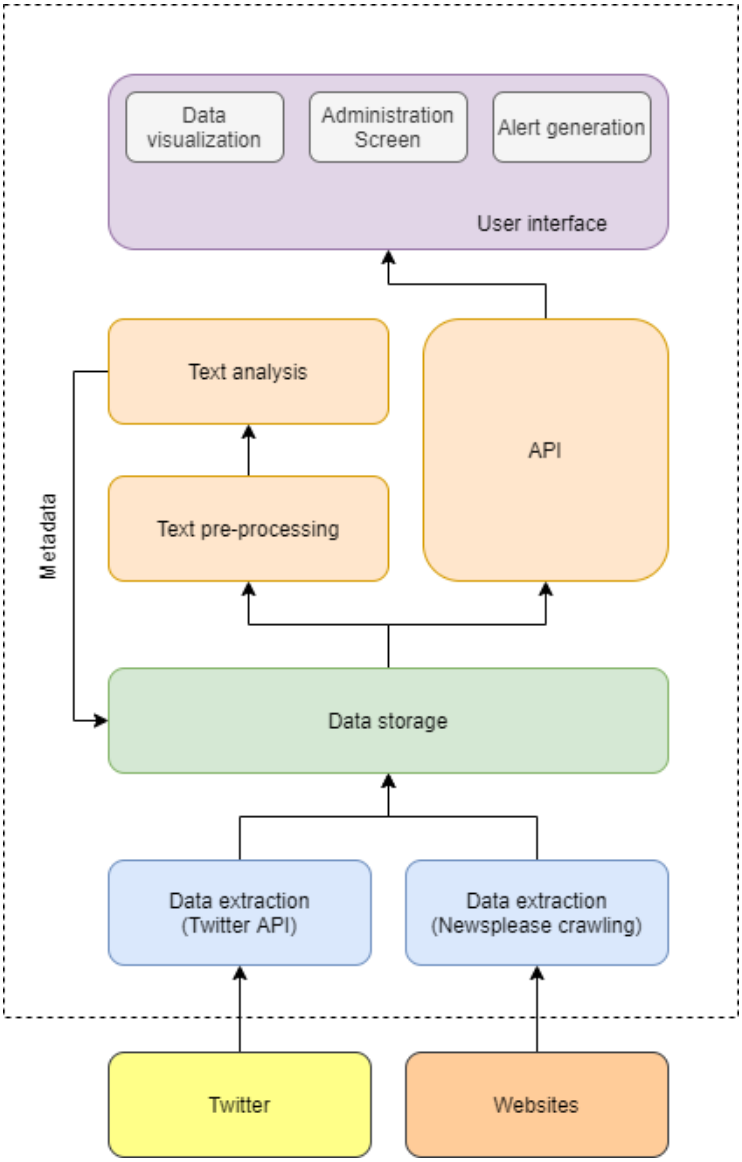

Figure 2. Early vulnerability identification system architecture.

The results in Table 1 show that the BERT classification method has a slightly better overall performance in terms of accuracy (85.50%) than SVM, while MNB has a considerably lower performance.

Table 1. Evaluation of implementation alternatives for the news-based analysis module.

Model	**Min.**	**Max.**	**Mean**
SVM	**83.00**	87.00	85.05
MNB	72.50	81.50	76.60
BERT	82.50	**88.00**	**85.50**

Regarding the algorithm for detecting cyber vulnerabilities that uses only data from web platforms specialized in posting news in the field of cyber security, the proposed prototype obtains an average accuracy of 85.5%. The results obtained for other similar solutions vary between 90% and 95% [80-82]. However, in Table 2 it is shown that when considering specialized articles contained in the posts on the Twitter platform, but also of certain metrics such as the number of appreciations and distributions, an accuracy is obtained approximately equal to the best identified in the literature.

Table 2. Evaluation of implementation alternatives for the news-based module in Twitter posts.

Model	**Accuracy (text only)**	**Accuracy (text + likes + retweets)**
BERT	93.33%	93.97%
SVM	90.96%	90.97%
CNN	**93.97%**	**94.96%**

The results in Table 3 show the performance obtained by the trained models only on the tweet texts used; as such, the available text has been reduced to a maximum length of 144 characters. Here, too, the BERT model has better performance than the others with an accuracy of 92.31%, surpassing the CNN model by about 1%..

Table 3. Evaluating implementation alternatives for the module based on Twitter posts.

Model	**Accuracy (tweet text only)**	**Accuracy (text + likes + retweets)**
BERT	**91.91%**	**92.39%**
SVM	75.90%	76.06%
CNN	90.80%	91.28%

Regarding the algorithm for detecting cyber vulnerabilities that uses data exclusively from the Twitter platform, the proposed prototype obtains an accuracy of 92.39%. These results exceed the standard of the identified existing algorithms whose accuracy varies between 45% and 92% [75-78].

In Table 4, the results of the different implementation alternatives developed for the development of an interpretable model can be seen. The first model (MNB) provided a benchmark for comparing the results, which is an interpretable model. The following models

involved either the exclusive use of the automatically collected aggregated data set or the adjustment of the annotated item data set. The third model involved the addition of an interpretability component that allows the explanation of classification results through prototypes (exemplary articles for text classes).

Table 4. Performance of interpretable models.

Model	Accuracy	Precision	Recall	Score F2	Interpretable
MNB	0.84	**0.92**	0.62	0.66	Yes
Longformer (no fine-tunning)	**0.87**	0.76	0.95	0.90	No
Longformer (with fine-tuning)	0.86	0.73	**0.98**	**0.92**	No
Longformer + ProSeNet	**0.87**	0.78	0.91	0.88	Yes

Additionally, a usability analysis of the system's graphical interface was performed. The original contribution in this regard refers to the use of the graphical interface layout as an object of evaluation, in order to obtain early feedback. According to the proposed evaluation method, the graphical interface could be labeled as any of the following: superfluous, neutral, too task-oriented, too self-oriented, task-oriented or desired. According to the AttrackDiff evaluation method, the layout can be labeled as task-oriented. Moreover, the usability assessment method made it possible to identify opportunities to improve the user interface. The figure below shows an example screen in the GUI.

.

Figure 3. Screen example from the graphical interface of the global contextual risk estimation system.

3.2 Optimizing the response to cyber-attacks using honeypot systems ("HUNT")

This section presents the implementation of a system that aims to calculate the local contextual risk of exploiting a cyber vulnerability. The proposed approach aims to create an agent-type architecture and to create a honeypot-type architecture capable of simulating a virtual environment, distracting the attackers of that virtual environment as well as collecting information on the means of attack used.

The first data set used to evaluate the implementation contains information collected through the scanning agent developed within an infrastructure comprising 12 devices. For each device, the scan agent was able to obtain information about the application names, their descriptions, identification numbers, installation date, language, local package, code type, component vendor, component version, and other details such as connected ports. Of these, the evaluation was performed by reference to the component name, version, component description, and associated port for a device. The choice of these dimensions was made by reference to the minimum standard of information needed to infer cyber vulnerabilities in the infrastructure.

The second data set is the response of an application load balancer (ALB) to scanning mechanisms such as Nikto, Nmap and DIRB. A total of 317,709 packets were sent to the ALB component to identify its effectiveness in redirecting suspicious traffic to the developed honeypot system. Thus, positive or negative detection of suspicious traffic was reported along with the number of packets for each mechanism.

The third data set is obtained after performing an experiment in which the performance of the honeypot system was evaluated. The data obtained refer to the number of packets sent within 24 hours by cyber attackers, a unique identifier for attackers, the country of origin of the attack and the level of vulnerability of the system reached by honeypot attackers. In addition, these results were compared with the results of a traditional honeypot system developed in order to obtain a benchmark.

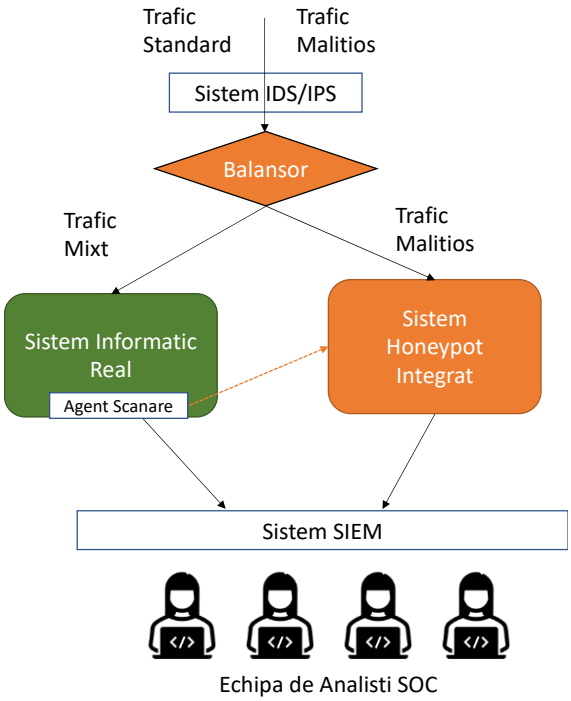

Figure 4. The architecture of the HUNT honeypot system integrated by the load balancer

To evaluate the proposed system, the results of the agent's application on a real cyber infrastructure, the load balancer results in the case of a honeypot system implemented on a website and the honeypot results within 24 hours in front of cyber attackers are analyzed in turn.

Following the implementation of the agent in a cyber infrastructure, a number of data were obtained such as: application data, driver data, firewall data, hardware data, installed feature data, process data, user data, network data, operating system data, packet data, and more. Table 5 shows a sample of data extracted from a single device of an infrastructure. Data such as those in Table 5 can be used to create a honeypot system that simulates the infrastructure to be protected. The developed agent folds both for the subsequent implementation of the honeypot system and for obtaining additional information for the cyber infrastructure analysis system. In this regard, the agent may provide additional information for the calculation of organizational contextual risk.

Table 5. Sample data collected by the agent.

Application	Version	Description	Port
Microsoft Windows Operating System	10.0.17763.1	Distributed File System Replication	49913
Microsoft Windows Operating System	10.0.17763.719	Domain Name System (DNS) Server	49700
Microsoft Windows Operating System	10.0.17763.1	Spooler SubSystem App	49677
Microsoft Windows Operating System	10.0.17763.1	Local Security Authority Process	49675
Microsoft Windows Operating System	10.0.17763.1	Local Security Authority Process	49674
Microsoft Windows Operating System	10.0.17763.1	Local Security Authority Process	49668
Microsoft Windows Operating System	10.0.17763.1	Host Process for Windows Services	49667
Microsoft Windows Operating System	10.0.17763.1	Host Process for Windows Services	49666
Microsoft Windows Operating System	10.0.17763.1	Host Process for Windows Services	49665
Microsoft (R) Windows (R) Operating System	10.0.17763.1	Microsoft.ActiveDirectory.WebServices	9389
Microsoft Windows Operating System	10.0.17763.1	Host Process for Windows Services	3389
Microsoft Windows Operating System	10.0.17763.1	Local Security Authority Process	3269
Microsoft Windows Operating System	10.0.17763.1	Local Security Authority Process	3268
Microsoft Windows Operating System	10.0.17763.1	Local Security Authority Process	636
Microsoft Windows Operating System	10.0.17763.1	Host Process for Windows Services	593
Microsoft Windows Operating System	10.0.17763.1	Local Security Authority Process	464
Apache HTTP Server	2.4.47	Apache HTTP Server	443
Microsoft Windows Operating System	10.0.17763.1	Local Security Authority Process	389
Microsoft Windows Operating System	10.0.17763.1	Host Process for Windows Services	135
Microsoft Windows Operating System	10.0.17763.1	Local Security Authority Process	88
Apache HTTP Server	2.4.47	Apache HTTP Server	80
Microsoft Windows Operating System	10.0.17763.719	Domain Name System (DNS) Server	53

Furthermore, the results of the application of suspicious traffic routing via Nikto, Nmap and DIRB to the load balancer component are summarized. As can be seen in Table 6, indicators related to the number of packets sent, the size of the traffic generated, the number of

responses that returned the 404 error, as well as the detection of suspicious port-level traffic by load balancer were measured.

Table 6. Traffic redirected to the honeypot by the Load Balancer component.

Mechanism	**No. sent packages**	**Nr. 404 answers**	**Port Detection**	**Redirected to Honeypot**
Nikto (123)	2340	978	Negative	Positive
Nikto (ade)	2123	900	Negative	Positive
Nikto (4890)	2000	874	Negative	Positive
Nikto (567)	1988	850	Negative	Positive
Nmap (TCP)	1005	-	Positive	Positive
Nmap (Stealth)	1004	-	Positive	Positive
Nmap (Fin)	1009	-	Positive	Positive
Nmap (Null)	1007	-	Positive	Positive
Nmap (UDP)	1008	-	Positive	Positive
Nmap (UDP)	1006	-	Positive	Positive
Nmap (X-mas)	1004	-	Positive	Positive
DIRB (imp)	120321	60594	Positive	Positive
DIRB (nerec)	50344	12456	Negative	Positive
DIRB (404)	120321	60594	Positive	Positive
DIRB (IM)	11229	56789	Positive	Positive
Total	317,709	142,924	N/A	N/A

Finally, the results obtained by the honeypot system developed for the same website are presented. As can be seen in Table 7, information on attackers and the level of vulnerability reached in the honeypot system is illustrated. These results show that the developed system is 4.4 times more performant than a traditional honeypot system.

Table 7. Hunt system attacker statistics measured over 24h.

Id Atacator	Nr Pachete Trimise	IP Atacator	Tara Atacator	Nivel Atins
THA1	73,492	121.235.179.x	China	L2
THA2	45,334	195.82.150.x	Ucraina	L2
THA3	39,975	159.75.52.x	China	L2
THA4	25,648	109.195.179.x	Rusia	L1
THA5	16,811	35.232.230.x	USA	N/A
THA6	16,654	161.35.59.x	USA	L1
THA7	13,543	221.158.220.x	Korea de Nord	N/A
THA8	11,582	213.142.159.x	Turcia	L1
THA9	10,902	89.216.121.x	Serbia	L1
THA10	7,503	49.85.59.x	China	L1
THA11	7,326	178.63.41.x	Germania	N/A
THA12	7,219	77.47.247.	Ucraina	N/A
THA13	5,998	178.172.137.x	Belarus	N/A
THA14	5,863	124.244.3.x	Hong Kong	N/A
THA15	5,694	94.103.91.x	Rusia	N/A
THA16	5,869	185.156.43.x	Ucraina	L3
THA17	5,728	52.42.115.x	USA	N/A
THA18	4,619	201.163.247.x	Mexic	N/A
THA19	2,802	15.229.2.x	Brazilia	N/A
THA20	2,661	89.137.217.x	Romania	N/A
THA21	2,487	175.24.114.x	China	N/A

These results confirm the development of the components needed to implement a honeypot system as a constituent part of a system to reduce the risk of exploiting cyber vulnerabilities of an IT infrastructure. Unlike similar agent-based scanning solutions [53-61], the proposed system is distinguished by its superior ability to reproduce the targeted infrastructure, given the plausibility of replicating elements based on data collected by the agent.

3.3 Integrated Contextual Risk Reduction System ("CRS")

In order to implement a system for calculating the organizational contextual risk of exploiting cyber vulnerabilities in an IT infrastructure, the development of a component for continuous monitoring of a cyber infrastructure and the development of a methodology for calculating the contextual score of identified vulnerabilities are aimed. This choice was motivated by laboratory research [89, 90]

External (eg Nmap) and internal scanning means (based on a virtual machine installed in the target infrastructure) have been implemented for the development of continuous monitoring components. A set of data obtained from internal and external scanning processes on a real cyber infrastructure was used to develop the methodology. The data set contains 133 inputs that represent devices identified by the scanning means. For each device, a number of features were collected, such as: product name, version, cpe ID number, operating system type, port, transport protocol, and url. CVE and CVSS international vulnerability indexing systems have also been used to identify cyber vulnerabilities. In total, 63 cyber vulnerabilities present in the analyzed system were identified.

In addition, data were collected on the impact of each component on the cyber infrastructure. This data was entered by the cyber infrastructure manager through a specially developed visual interface. Furthermore, a number of information about the degree of exposure of the devices was inferred in relation to the information obtained through internal and external scanning. Details of the methodology used to infer this data are provided in a later section. Figure 5 shows the system architecture.

.

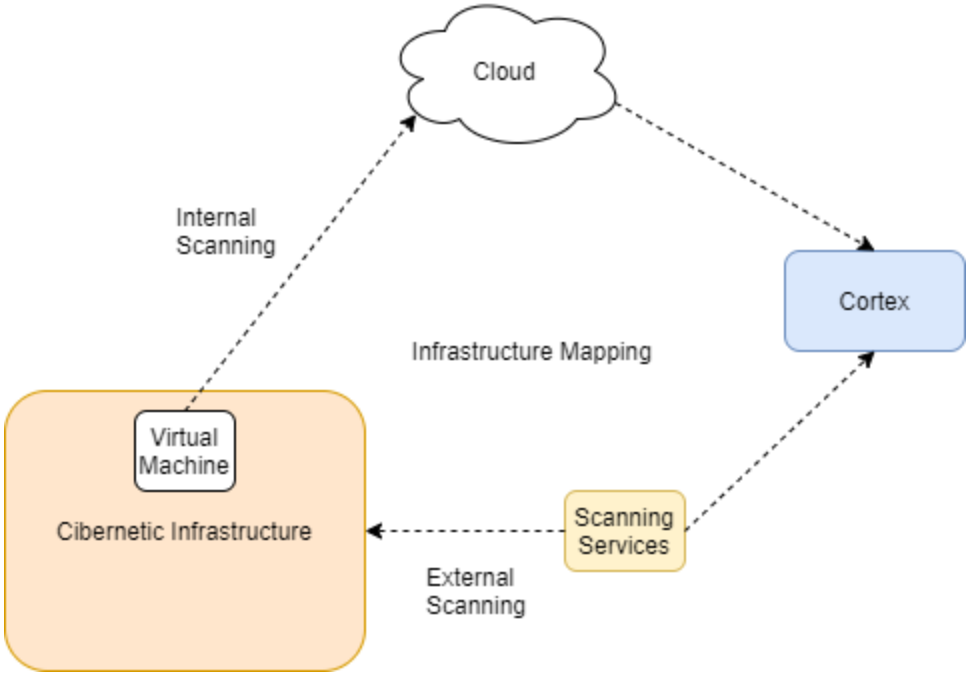

Figure 5. The architecture of the cyber infrastructure analysis system.

External and internal scanning tools allow the collection of data on cyber infrastructure and the identification of cyber vulnerabilities. The "Cortex" component allows the use of extracted data to calculate the organizational contextual risk score. To this end, a procedure for assessing the individual risk of each device in relation to the CVSS system has been implemented. After applying the individual risk rating procedure, the system calculates the contextual risk score for each device. The contextual risk score of a device is composed of the degree of exposure of the device in relation to the ease of access to the Internet (ZE), the probability of exploitation given the existence of a made public strategy (ES) and the degree of exposure of the device to the type of users. human or computational access to the system (EU). The formula below shows the three elements (ZE, ES, EU) and the associated weights (PZ, PE, PU).

$$CRS = PZ * ZE + PE * ES + PU * UE$$

This formula allows the quantification of the organizational contextual risk in relation to the susceptibility of the components to cyber-attacks. The associated weights are presented in Table 8 and were assigned by a decision based on the consensus of the cybersecurity experts involved in the project.

Table 8. Device context punctuation.

ZE		UE	
Context type ZE	Score	Context type UE	Score
Internet	100	Servers & Users	100
WAN	60	Users only	60
Isolated Users	40	Servers only	40
Isolated Servers	20	No access	0
Offline	0		

Furthermore, a formula has been developed that also considers the importance of devices for organizational processes in relation to the data provided by the network administrator. Thus, the final formula considers the individual risk score based on CVSS, the contextual risk score described above (CRS) and the impact that the operation of the device would have on the business (BI). In the formula below, the three elements (CVSS, BI and CRS) are presented together with the corresponding weights (PC, PB and PS), whose value is determined empirically.

$$ORS = PC * CVSS + PB * BI + PS * CRS$$

Table 9 shows a sample of the results obtained by applying the contextual risk calculation formulas. IP and DNS data have been anonymized. The table also includes the scores for the constituent elements of each formula. For the example below, the weights PZ (0.3), PE (0.5) and PU (0.2) but also PC (0.5), PB (0.25), and PS (0.25) were used.

Table 9. The results of the application of the formula for calculating the contextual risk of the organization on a sample with identified cyber vulnerabilities.

CVE	IP/DNS	CVSS	ZE	UE	ES	CRS	BI	ORS
CVE-2018-20148	Anonymized	98	100	100	100	100	55	87.75
CVE-2017-14723	Anonymized	98	100	100	100	100	55	87.75
CVE-2017-16510	Anonymized	98	100	100	100	100	55	87.75
CVE-2020-11984	Anonymized	98	100	100	100	100	55	87.75
CVE-2019-0398	Anonymized	88	100	100	50	75	100	87.75
CVE-2015-4603	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-4073	Anonymized	98	100	100	100	100	50	86.5
CVE-2015-6834	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-4072	Anonymized	98	100	100	100	100	50	86.5
CVE-2015-6835	Anonymized	98	100	100	100	100	50	86.5
CVE-2015-4599	Anonymized	98	100	100	100	100	50	86.5

CVE-2014-9912	Anonymized	98	100	100	100	100	50	86.5
CVE-2015-4600	Anonymized	98	100	100	100	100	50	86.5
CVE-2015-4602	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-4071	Anonymized	98	100	100	100	100	50	86.5
CVE-2015-4603	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-4073	Anonymized	98	100	100	100	100	50	86.5
CVE-2015-6834	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-4072	Anonymized	98	100	100	100	100	50	86.5
CVE-2015-4599	Anonymized	98	100	100	100	100	50	86.5
CVE-2015-4600	Anonymized	98	100	100	100	100	50	86.5
CVE-2015-4602	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-4071	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-7127	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-6288	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-6290	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-5771	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-2554	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-4538	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-9137	Anonymized	98	100	100	100	100	50	86.5
CVE-2019-9641	Anonymized	98	100	100	100	100	50	86.5

As can be seen, the contextual risk calculation formula (CRS) allows the differentiation of a CVE as being less urgent, from a contextual point of view, which is then transposed into the final operating risk calculation formula. It can also be seen that the organizational contextual operational risk (ORS) calculation formula allows a better prioritization of the identified cyber vulnerabilities in the cyber infrastructure than the CVSS score.

The empirical study described in this section brings in addition to similar solutions such as Nextpose [66] or the methods proposed by Joh and Malaiya [64] and Singh, et al. [65] presented in the dedicated section of Chapter 2.1, a prioritization based on factors in addition to those in international databases such as CVSS. It is primarily a matter of introducing a parameter that indicates the importance of the device for carrying out the activity of the organization, therefore, and the importance of fixing the vulnerabilities identified on this device. It is also about inferring certain parameters from the data obtained by scanning from outside and inside the network.

4 Discussion

This section discusses the integration opportunities of the three systems developed through the empirical studies presented. The EVE (3.1) and CRS (3.3) systems aim to improve the formula for calculating contextual risk by taking into account external parameters. The cyber security vulnerability early identification system offers the possibility to improve the formula for calculating the organizational contextual risk of exploiting a vulnerability. For example, the exploit score (ES) parameter involves identifying the existence of a means of exploiting cyber vulnerabilities. Early identification of cyber vulnerabilities can identify the existence of an exploitation strategy given the mention of vulnerability in the online community. Moreover, the related score can thus obtain values between 1 and 100, not being limited only to the existence or non-existence of the knowledge of the system managers regarding the strategies for exploiting cyber vulnerabilities.

An integration between the Hunt (3.2) and EVE (3.1) systems can be designed in a two-way way, so that the Honeypot component transmits to the early identification module new attack vectors unknown until then, and the early vulnerability identification component transmits to the module CTF from Hunt new emerging vulnerability, which it should integrate into the profiling flow of attackers. In the same way, we can consider the integration between Hunt (3.2) and CRS (3.3) opportune, in which case the contextual risk calculation system can provide the CTF component of Hunt with the list of vulnerabilities of the most important systems to expose them to exploitation. attackers who are able to exploit them. At the same time, I emphasize the importance of data transfer between EVE (3.1), Hunt (3.2) and CRS (3.3) systems to SIEM / SOAR systems used in the day-to-day activities of SecOps teams for analysis and response to security incidents.

Last but not least, the identification of new types of internal and external parameters can lead to the identification of new approaches for the integration of the three systems. In conclusion, this thesis presents the studies carried out to reduce the attack surface and optimize the response to cyber security incidents in complex infrastructures for teams in operational security centers (SOC), but also the opportunities for integration between the components described above.

5 Conclusions and further developments

This thesis presents the research efforts we have made in order to develop the components of an integrated system for streamlining the processes of operational security centers (SOC) by reducing the attack area and optimizing the response to incidents in complex IT infrastructures. Such a system responds to the problems of scaling operational security teams (SecOps), which are characterized by exponential speed and complexity, and which bring with them an increased exposure to cyber risks. In this sense, the innovative solutions proposed in the 3 studies offer methods for early identification of new vulnerabilities, optimization of the response to cyber-attacks using modern honeypot systems, and prioritization of known cyber vulnerabilities to reduce the attack surface. The results of the studies promise to streamline the operation of operational security centers. Moreover, further developments aim at improving the performance of the proposed systems and integrating them into a unitary system.

5.1 Original Contributions

Regarding the original contributions presented in this thesis, the following are listed:

• CO1: Design, development and testing of two automated natural language processing models for early identification of cyber vulnerabilities using open data sources.

• CO2. Development and testing of an interpretable automatic model for natural language processing to explain the results obtained.

• CO3: Design and implementation of an innovative methodology for assessing the usability of graphical interfaces of cybersecurity web applications.

• CO4: Design, development and testing of a honeypot computer system with the ability to camouflage in the real infrastructure of an organization.

• CO5: Design, implementation and testing of the impact of a method of profiling attackers in honeypot systems using game theory.

• CO6: Design and testing of a method and an algorithm to quantify the contextual risk of exploiting cyber vulnerabilities in a complex IT infrastructure based on external and internal metadata.

5.2 Publications

Grigorescu, O., **Săndescu, C**., & Rughiniş, R. (2016, September). CODA footprint continuous security management platform. In *2016 15th RoEduNet Conference: Networking in Education and Research* (pp. 1-5). Bucharest:IEEE.

Săndescu, C., Rughinis, R., & Grigorescu, O. (2017). Hunt: Using honeytokens to understand and influence the execution of an attack. In *The International Scientific Conference eLearning and Software for Education* (Vol. 1, p. 511). Bucharest:" Carol I" National Defence University.

Iorga, D., Corlătescu, D., Grigorescu, O., **Săndescu, C**., Dascălu, M., & Rughiniş, R. (2020, December). Early Detection of Vulnerabilities from News Websites using Machine Learning Models. In *2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)* (pp. 1-6). Bucharest:IEEE.

Radu, R., **Săndescu, C.**, Grigorescu, O., & Rughiniş, R. (2020, December). Analyzing Risk Evaluation Frameworks and Risk Assessment Methods. In *2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)* (pp. 1-6). IEEE.

Grigorescu, O., **Săndescu, C**., & Caba, A. (2020, December). Web Application Honeypot Published in the Wild. In *2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)* (pp. 1-6). Bucharest:IEEE.

Iorga, D., Corlatescu, D. G., Grigorescu, O., **Săndescu, C**., Dascalu, M., & Rughinis, R. (2021, May). Yggdrasil—Early Detection of Cybernetic Vulnerabilities from Twitter. In *2021 23rd International Conference on Control Systems and Computer Science (CSCS)* (pp. 463-468). Bucharest:IEEE.

Frode de la Foret, P., Ruseti, S., **Săndescu**, C., Dascalu, M., & Travadel, S. (2021). Interpretable Identification of Cybersecurity Vulnerabilities from News Articles. In Int. Conf. on Recent Advances in Natural Language Processing (RANLP 2021) (pp. 428-436). Varna, Bulgaria (Online): ACL.

Iorga, D., Grigorescu, O., Predoiu, M., **Săndescu**, C., Dascalu, M., & Rughinis, R. (2021). Early Usability Evaluation to Enhance User Interfaces – A Use Case on the Yggdrasil

Cybersecurity Mockup –. In International Conference on Human-Computer Interaction (RoCHI2021). (pp.103-111) Bucharest, Romania (Online): MatrixRom.

Săndescu C., Dinișor A., Vlădescu C-V, Grigorescu O., Corlătescu D., Dascălu M., Rughiniș R. (in press) Extracting Exploits and Attack Vectors from cybersecurity news using NLP. In *Buletin Ştiinţific Universitatea Politehnica din Bucureşti*

Babalau I, Corlatescu D.,Grigorescu O., **Săndescu C**., Dascălui, M. (in press) Severity Prediction of Software Vulnerabilities based on their Text Description In 2021 International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC 2021), Timișoara, România (Online)

Vlădescu C., Dinișor M-A, Grigorescu O., Corlătescu D., **Săndescu C**., Dascălu M. (in press) What are the Latest Cybersecurity Trends? A Case Study Grounded in Language Models In 2021 International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC 2021), Timișoara, România (Online)

6 References

[1] J. Armin, B. Thompson, D. Ariu, G. Giacinto, F. Roli, and P. Kijewski, "2020 cybercrime economic costs: No measure no solution," in *2015 10th International Conference on Availability, Reliability and Security*, Toulouse, 2015, pp. 701-710.

[2] S. Romanosky, "Examining the costs and causes of cyber incidents," *Journal of Cybersecurity*, vol. 2, pp. 121-135, 2016.

[3] Ponemon IBM, "*Cost of Data Breach Report 2021*", 2021. [Online]. Available: https://www.ibm.com/security/data-breach [Accessed: February, 2022]

[4] The International Information System Security Certification Consortium, "*A Resilient Cybersecurity Profession Charts the Path Forward*", 2021. [Online]. Available: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx [Accessed: February, 2022]

[5] Trend Micro, "*Attacks Surge in 1H 2021 as Trend Micro Blocks 41 Billion Cyber Threats*", 2021. [Online]. Available: https://newsroom.trendmicro.com/2021-09-14-Attacks-Surge-in-1H-2021-as-Trend-Micro-Blocks-41-Billion-Cyber-Threats [Accessed: February, 2022]

[6] Spacy, "*Language Processing Pipelines*", n.d. [Online]. Available: https://spacy.io/usage/processing-pipelines. [Accessed: September 2021]

[7] D. Jurafsky and J. Martin, "*Speech and Language Processing* ", 2020. [Online]. Available: https://web.stanford.edu/~jurafsky/slp3/. [Accessed: June 2020]

[8] G. Pulford, "The Viterbi algorithm," in *IEEE Seminar on Target Tracking: Algorithms and Applications*, Enschede, 2006, pp. 53-65.

[9] V. Nair and G. E. Hinton, "Rectified linear units improve restricted boltzmann machines," in *Proceedings of the 27 th International Conference on Machine Learning*, Haifa, 2010.

[10] G. Bouchard, "Efficient bounds for the softmax function, applications to inference in hybrid models," in *Presentation at the Workshop for Approximate Bayesian Inference in Continuous/Hybrid Systems at NIPS-07*, Hilton, 2007.

[11] J. Shore and R. Johnson, "Axiomatic derivation of the principle of maximum entropy and the principle of minimum cross-entropy," *IEEE Transactions on information theory*, vol. 26, pp. 26-37, 1980.

[12] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," *arXiv preprint arXiv:1412.6980*, 2014.

[13] Y. Gal and Z. Ghahramani, "A theoretically grounded application of dropout in recurrent neural networks," *Advances in neural information processing systems*, vol. 29, pp. 1019-1027, 2016.

[14] M. Honnibal and M. Johnson, "An improved non-monotonic transition system for dependency parsing," in *Proceedings of the 2015 conference on empirical methods in natural language processing*, Lisabon, 2015, pp. 1373-1378.

[15] H. Zhang, "The Optimality of Naive Bayes," presented at the FLAIRS2004 Conference, Canada, 2004.

[16] J. D. Rennie, L. Shih, J. Teevan, and D. R. Karger, "Tackling the poor assumptions of naive bayes text classifiers," in *Proceedings of the 20th international conference on machine learning (ICML-03)*, Washington, 2003, pp. 616-623.

[17] A. McCallum and K. Nigam, "A comparison of event models for naive bayes text classification," in *AAAI-98 workshop on learning for text categorization*, Madison, 1998, pp. 41-48.

[18] V. Vryniotis, "*Machine Learning Blog & Software Development News*", 2013. [Online]. Available: https://blog.datumbox.com/machine-learning-tutorial-the-max-entropy-text-classifier/. [Accessed: June 2021]
[19] K. Nigam, J. Lafferty, and A. McCallum, "Using maximum entropy for text classification," in *IJCAI-99 workshop on machine learning for information filtering*, 1999, pp. 61-67.
[20] C. Cortes and V. Vapnik, "Support-vector networks," *Machine learning,* vol. 20, pp. 273-297, 1995.
[21] J. Platt, "Probabilistic outputs for support vector machines and comparisons to regularized likelihood methods," *Advances in large margin classifiers,* vol. 10, pp. 61-74, 1999.
[22] T.-F. Wu, C.-J. Lin, and R. C. Weng, "Probability estimates for multi-class classification by pairwise coupling," *Journal of Machine Learning Research,* vol. 5, pp. 975-1005, 2004.
[23] K. Crammer and Y. Singer, "On the algorithmic implementation of multiclass kernel-based vector machines," *Journal of machine learning research,* vol. 2, pp. 265-292, 2001.
[24] F. Mola, "Classification and regression trees software and new developments," in *Advances in Data Science and Classification*, ed Rome: Springer, 1998, pp. 311-318.
[25] J. R. Quinlan, *C4. 5: programs for machine learning*. California: Elsevier, 2014.
[26] L. Breiman, "Random forests," *Machine learning,* vol. 45, pp. 5-32, 2001.
[27] S. T. Dumais, "Latent semantic analysis," *Annual review of information science and technology,* vol. 38, pp. 188-230, 2004.
[28] T. Mikolov, K. Chen, G. Corrado, and J. Dean, "Efficient estimation of word representations in vector space," *arXiv preprint arXiv:1301.3781*, 2013.
[29] J. Pennington, R. Socher, and C. D. Manning, "Glove: Global vectors for word representation," in *Proceedings of the 2014 conference on empirical methods in natural language processing (EMNLP)*, 2014, pp. 1532-1543.
[30] T. K. Landauer, P. W. Foltz, and D. Laham, "An introduction to latent semantic analysis," *Discourse processes,* vol. 25, pp. 259-284, 1998.
[31] A. Zhila, W.-t. Yih, C. Meek, G. Zweig, and T. Mikolov, "Combining heterogeneous models for measuring relational similarity," in *Proceedings of the 2013 conference of the North American chapter of the association for computational linguistics: Human language technologies*, Atlanta, 2013, pp. 1000-1009.
[32] DeepLizard, "*Machine Learning & Deep Learning Fundamentals*", n.d. [Online]. Available: https://deeplizard.com/learn/video/gZmobeGL0Yg. [Accessed: July 2021]
[33] G. Ognjanovski, "*Everything you need to know about Neural Networks and Backpropagation — Machine Learning Easy and Fun*", 2019. [Online]. Available: https://towardsdatascience.com/everything-you-need-to-know-about-neural-networks-and-backpropagation-machine-learning-made-easy-e5285bc2be3a. [Accessed: July 2019]
[34] S. Ruder, "*An overview of gradient descent optimization algorithms*", 2016. [Online]. Available: https://ruder.io/optimizing-gradient-descent/. [Accessed: July 2021]
[35] J. Brownlee, "*Understand the Impact of Learning Rate on Neural Network Performance*", 2020. [Online]. Available:

https://machinelearningmastery.com/understand-the-dynamics-of-learning-rate-on-deep-learning-neural-networks/. [Accessed: July 2021]
[36] A. Senior, G. Heigold, M. a. Ranzato, and K. Yang, "An empirical study of learning rates in deep neural networks for speech recognition," in *2013 IEEE international conference on acoustics, speech and signal processing*, Vancouver, 2013, pp. 6724-6728.
[37] S. Sumit, "*A Comprehensive Guide to Convolutional Neural Networks—the ELI5 way*", 2018. [Online]. Available: https://towardsdatascience.com/a-comprehensive-guide-to-convolutional-neural-networks-the-eli5-way-3bd2b1164a53. [Accessed: July 2021]
[38] A. Jacovi, O. S. Shalom, and Y. Goldberg, "Understanding convolutional neural networks for text classification," *arXiv preprint arXiv:1809.08037*, 2018.
[39] X. Zhang, J. Zhao, and Y. LeCun, "Character-level convolutional networks for text classification," *Advances in neural information processing systems*, vol. 28, pp. 649-657, 2015.
[40] W. De Mulder, S. Bethard, and M.-F. Moens, "A survey on the application of recurrent neural networks to statistical language modeling," *Computer Speech & Language*, vol. 30, pp. 61-98, 2015.
[41] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural computation*, vol. 9, pp. 1735-1780, 1997.
[42] A. Sherstinsky, "Fundamentals of recurrent neural network (RNN) and long short-term memory (LSTM) network," *Physica D: Nonlinear Phenomena*, vol. 404, p. 132306, 2020.
[43] D. Bahdanau, K. Cho, and Y. Bengio, "Neural machine translation by jointly learning to align and translate," *arXiv preprint arXiv:1409.0473*, 2014.
[44] Y. Su and C.-C. J. Kuo, "On extended long short-term memory and dependent bidirectional recurrent neural network," *Neurocomputing*, vol. 356, pp. 151-161, 2019.
[45] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, L. Kaiser, and I. Polosukhin, "Attention is all you need," *arXiv preprint arXiv:1706.03762*, 2017.
[46] R. Horev, "*BERT Explained: State of the art language model for NLP*", 2018. [Online]. Available: https://towardsdatascience.com/bert-explained-state-of-the-art-language-model-for-nlp-f8b21a9b6270. [Accessed: July 2021]
[47] L. Spitzner, "*Honeytokens: The Other Honeypot*", 2020. [Online]. Available: https://bit.ly/2Ue1QTZ. [Accessed: June 2021]
[48] F. Pouget, M. Dacier, and H. Debar, "White paper: honeypot, honeynet, honeytoken: terminological issues," *Rapport technique EURECOM*, vol. 1275, p. 09, 2003.
[49] R. Barnett, "*Monitoring VMare Honeypot*", 2002. [Online]. Available: http://honeypots.sourceforge.net/monitoring_vmware_honeypots.html. [Accessed: June 2021]
[50] I. Livshitz, "*Low, Medium and High Interaction Honeypot Security | Guardicore*", 2019. [Online]. Available: https://www.guardicore.com/blog/high-interaction-honeypot-versus-low-interaction-honeypot-comparison/. [Accessed: June 2021]
[51] HoneynetProject, "*Know Your Enemy: Defining Virtual Honeynets*", 2002. [Online]. Available: https://ivanlef0u.fr/repo/madchat/reseau/defense/DefiningVirtualHoneynets.pdf. [Accessed: June 2021]

[52] M. Nawrocki, M. Wählisch, T. C. Schmidt, C. Keil, and J. Schönfelder, "A survey on honeypot software and data analysis," *arXiv preprint arXiv:1608.06249,* 2016.
[53] G. Portokalidis, A. Slowinska, and H. Bos, "Argos: an emulator for fingerprinting zero-day attacks for advertised honeypots with automatic signature generation," *ACM SIGOPS Operating Systems Review,* vol. 40, pp. 15-27, 2006.
[54] N. Sharma and S. S. Sran, "Detection of threats in Honeynet using Honeywall," *International Journal on Computer Science and Engineering,* vol. 3, pp. 3332-3336, 2011.
[55] HiHatProject, "*High Interaction Honeypot Analysis Tool*", 2007. [Online]. Available: https://sourceforge.net/projects/hihat/. [Accessed: August 2021]
[56] J.-w. Zhuge, X.-h. Han, Y.-l. Zhou, C.-y. Song, J.-p. Guo, and W. Zou, "HoneyBow: An automated malware collection tool based on the high-interaction honeypot principle," *JOURNAL-CHINA INSTITUTE OF COMMUNICATIONS,* vol. 28, p. 8, 2007.
[57] TheHoneynetProject, "*Know your Enemy: Sebek2*", 2003. [Online]. Available: http://web.mit.edu/6.857/OldStuff/Fall03/handouts/sebek.pdf. [Accessed: August 2021]
[58] M. Oosterhof, "*Cowrie*", 2014. [Online]. Available: https://cowrie.readthedocs.io/en/latest/README.html. [Accessed: August 2021]
[59] N. Provos, "*Developments of the Honeyd VIrtual Honeypot*", 2008. [Online]. Available: http://www.honeyd.org/. [Accessed: August 2021]
[60] Rapid7, "*InsightVM*", n.d. [Online]. Available: https://www.rapid7.com/products/insightvm/. [Accessed: June 2021]
[61] Osquery, "*Osquery Honeypot*", n.d. [Online]. Available: https://osquery.io/. [Accessed: August 2021]
[62] FireEye, "*Think Fast: Time Between Disclosure, Patch Release and VulnerabilityExploitation — Intelligence for Vulnerability Management, Part Two*", 2021. [Online]. Available: https://www.fireeye.com/blog/threat-research/2020/04/time-between-disclosure-patch-release-and-vulnerability-exploitation.html. [Accessed: June 2021]
[63] FIRST, "*Common Vulnerability Scoring System SIG*", 2005. [Online]. Available: https://www.first.org/cvss/. [Accessed: September 2021]
[64] H. Joh and Y. K. Malaiya, "A framework for software security risk evaluation using the vulnerability lifecycle and cvss metrics," in *Proc. International Workshop on Risk and Trust in Extended Enterprises,* California, 2010, pp. 430-434.
[65] U. K. Singh, C. Joshi, and N. Gaud, "Information security assessment by quantifying risk level of network vulnerabilities," *International Journal of Computer Applications,* vol. 156, pp. 37-44, 2016.
[66] Rapid7, "*Nexpose Vulnerability Scanner*", n.d. [Online]. Available: https://www.rapid7.com/products/nexpose/. [Accessed: August 2021]
[67] Secureworks, "*Taegis*", n.d. [Online]. Available: https://www.secureworks.com/products/taegis/xdr. [Accessed: August 2021]
[68] Y.-Z. Chen, Z.-G. Huang, S. Xu, and Y.-C. Lai, "Spatiotemporal patterns and predictability of cyberattacks," *PloS one,* vol. 10, p. e0124472, 2015.
[69] D. R. Hayes and F. Cappa, "Open-source intelligence for risk assessment," *Business Horizons,* vol. 61, pp. 689-697, 2018.
[70] S. Horawalavithana, A. Bhattacharjee, R. Liu, N. Choudhury, L. O. Hall, and A. Iamnitchi, "Mentions of security vulnerabilities on reddit, twitter and github," in

IEEE/WIC/ACM International Conference on Web Intelligence, Melbourne, 2019, pp. 200-207.

[71] C. Hobbs, Moran, M., Salisbury, D, *Open Source Intelligence in the Twenty-First Century - New Approaches and Opportunities*. London: Palgrave Macmillan, 2021.

[72] C. Andrew, R. J. Aldrich, and W. K. Wark, *Secret intelligence: A reader*. London: Routledge, 2009.

[73] L. Rosa, M. Freitas, S. Mazo, E. Monteiro, T. Cruz, and P. Simões, "A comprehensive security analysis of a scada protocol: From OSINT to Mitigation," *IEEE Access*, vol. 7, pp. 42156-42168, 2019.

[74] T. Day, H. Gibson, and S. Ramwell, "Fusion of OSINT and non-OSINT data," in *Open Source Intelligence Investigation*, ed Cham: Springer, 2016, pp. 133-152.

[75] H. Chen, R. Liu, N. Park, and V. Subrahmanian, "Using twitter to predict when vulnerabilities will be exploited," in *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, New York, 2019, pp. 3143-3152.

[76] S. Mittal, P. K. Das, V. Mulwad, A. Joshi, and T. Finin, "CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities," in *2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, 2016, pp. 860–867.

[77] C. Sabottke, O. Suciu, and T. Dumitraș, "Vulnerability disclosure in the age of social media: Exploiting twitter for predicting real-world exploits," in *24th USENIX Security Symposium USENIX Security 15*, Washington, 2015, pp. 1041-1056.

[78] N. Dionísio, F. Alves, P. M. Ferreira, and A. Bessani, "Cyberthreat detection from twitter using deep neural networks," in *2019 International Joint Conference on Neural Networks (IJCNN)*, Budapest, 2019, pp. 1-8.

[79] M. S. Abdullah, A. Zainal, M. A. Maarof, and M. N. Kassim, "Cyber-attack features for detecting cyber threat incidents from online news," in *2018 Cyber Resilience Conference (CRC)*, Malaysia, 2018, pp. 1-4.

[80] S. Zhou, Z. Long, L. Tan, and H. Guo, "Automatic identification of indicators of compromise using neural-based sequence labelling," *arXiv preprint arXiv:1810.10156*, 2018.

[81] X. Liao, K. Yuan, X. Wang, Z. Li, L. Xing, and R. Beyah, "Acing the ioc game: Toward automatic discovery and analysis of open-source cyber threat intelligence," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Viena, 2016, pp. 755-766.

[82] G. Husari, E. Al-Shaer, M. Ahmed, B. Chu, and X. Niu, "Ttpdrill: Automatic and accurate extraction of threat actions from unstructured text of cti sources," in *Proceedings of the 33rd Annual Computer Security Applications Conference*, New York, 2017, pp. 103-115.

[83] N. Tavabi, P. Goyal, M. Almukaynizi, P. Shakarian, and K. Lerman, "Darkembed: Exploit prediction with neural language models," in *Proceedings of the AAAI Conference on Artificial Intelligence*, New Orelans, 2018.

[84] I. Deliu, C. Leichter, and K. Franke, "Extracting cyber threat intelligence from hacker forums: Support vector machines versus convolutional neural networks," in *2017 IEEE International Conference on Big Data (Big Data)*, Boston, 2017, pp. 3648-3656.

[85] D. Iorga, D. Corlătescu, O. Grigorescu, C. Săndescu, M. Dascălu, and R. Rughiniş, "Early Detection of Vulnerabilities from News Websites using Machine

Learning Models," in *2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, Bucharest, 2020, pp. 1-6.
[86] D. Iorga, D.-G. Corlatescu, O. Grigorescu, C. Sandescu, M. Dascalu, and R. Rughinis, "Yggdrasil—Early Detection of Cybernetic Vulnerabilities from Twitter," in *2021 23rd International Conference on Control Systems and Computer Science (CSCS)*, Bucharest, 2021, pp. 463-468.
[87] O. Grigorescu, C. Săndescu, and A. Caba, "Web Application Honeypot Published in the Wild," in *2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, Bucharest, 2020, pp. 1-6.
[88] C. Săndescu, R. Rughinis, and O. Grigorescu, "Hunt: Using honeytokens to understand and influence the execution of an attack," in *The International Scientific Conference eLearning and Software for Education*, Bucharest, 2017, p. 511.
[89] O. Grigorescu, C. Săndescu, and R. Rughiniş, "CODA footprint continuous security management platform," in *2016 15th RoEduNet Conference: Networking in Education and Research*, Bucharest, 2016, pp. 1-5.
[90] R. Radu, C. Săndescu, O. Grigorescu, and R. Rughiniş, "Analyzing Risk Evaluation Frameworks and Risk Assessment Methods," in *2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, Bucharest, 2020, pp. 1-6.