Școala Doctorală Interdisciplinară
Facultatea de Inginerie Electrică și Știința Calculatoarelor
Departamentul de Electronică și Calculatoare

Doctorand Lucian Florin Ilca

Detecția și răspunsul automatizat la amenințări de securitate cibernetică

Detection and Automated Response to Cybersecurity Threats

SUMMARY

Scientific Supervisor
Prof. Dr. Ing. Petre Lucian Ogruţan

Brașov, 2024

Table of Contents

LIST OF ABBREVIATIONS AND ACRONYMS

Alin.	Aliniat
Art.	Articol
AI (eng.)	Inteligența artificială (Artificial Intelligence)
API (eng.)	Interfață de Programare a Aplicațiilor (Application Programming Interface)
APT (eng.)	Amenințare Persistentă Avansată (Advanced Persistent Threat)
AV (eng.)	Antivirus
BIOS (eng.)	Sistemul de Intrare/Ieșire de Bază (Basic Input Output System)
Buffer (eng.)	Zonă temporară de stocare a datelor, utilizat pentru a gestiona diferențele de viteză sau de capacitate de procesare între emițătorul și receptorul de date
CDN (eng.)	Content Delivery Network (Rețea de Livrare a Conținutului)
CIA (eng.)	Confidențialitate, Integritate și Disponibilitate (Confidentiality, Integrity and Availability)
CERT (eng.)	Echipă Răspuns la Urgențe Cibernetice (Computer Emergency Response Teams)
CTI (eng.)	Informații privind Amenințările Cibernetice (Cyber Threat Intelligence)
CSMA/CD (eng.)	Acces multiplu cu detectare a coliziunilor și detecție a purtătoarei (Carrier-sense multiple access with collision detection)
CPU (eng.)	Unitate Centrală de Procesare (Central Processing Unit)
CSRF (eng.)	Falsificare de cereri între site-uri (Cross-Site Request Forgery - CSRF)
CVE (eng.)	Vulnerabilități și Expuneri Comune (Common Vulnerabilities and Exposures)
DDoS (eng.)	Serviciu Distribuit de Negare a Disponibilității (Distributed Denial of Service - DDoS)
DFIR (eng.)	Investigații Digitale și Răspuns la Incidente (Digital Forensics and Incident Response)
Eng.	Traducere în engleză
ENISA (eng.)	Agenția Uniunii Europene pentru Securitatea Cibernetică
GDPR (eng.)	Regulamentul General privind Protecția Datelor (General Data Protection Regulation)

Hash – ing (eng.)	Proces de conversie a datelor de orice dimensiune într-o valoare de lungime fixă prin intermediul unei funcții hash
HTTPS (eng.)	Protocolul de Transfer de Hipertext Securizat (Hyper Text Transfer Protocol Secure)
HIDS (eng.)	Sistem de Detectare a Intruziunilor pentru Gazdă (Host Intrusion Detection System)
IDS (eng.)	Sistem de Detectare a Intruziunilor (Intrusion Detection System)
IAM (eng.)	Managementul Identității și Accesului (Identity and Access Management)
IoC (eng.)	Indicatori de Compromitere (Indicators of Compromise)
KNN (eng.)	K Cei Mai Apropiați Vecini (K-Nearest Neighbors)
Malware (eng.)	Program răuvoitor / Secvență răuvoitoare
MDR (eng.)	Detectare și Răspuns la Amenințări Gestionat (Managed Detection and Response)
NSM (eng.)	Monitorizarea Securității Rețelei (Network Security Monitoring)
Open-Source (eng.)	Program informatic care are codul său sursă disponibil public și poate fi utilizat, modificat și distribuit de către oricine
Offset	Distanță între 2 poziții sau locații într-un set de date sau într-o structură de date
RF (eng.)	Pădure Aleatoare (Random Forest)
Software (eng.)	Program, aplicație informatică
Softmax (eng.)	Funcția Softmax (Softmax Function)
SOC (eng.)	Centru de Operațiuni de Securitate (Security Operations Center)
SOAR (eng.)	Orchestare, Automatizare și Răspuns la Securitate (Security Orchestration, Automation, and Response)
SIEM (eng.)	Managementul Informațiilor și Evenimentelor de Securitate (Security Information and Event Management)
SVM (eng.)	Mașini cu Vectori de Suport (Support Vector Machines)
Threat Intelligence (eng.)	Intelligence privind amenințările cibernetice (Cyber Threat Intelligence)
UTM (eng.)	Gestionarea Unificată a Amenințărilor (Unified Threat Management)
Vulnerability Management (eng.)	Managementul Vulnerabilităților
VPN (eng.)	Rețea Privată Virtuală (Virtual Private Network)
WWW	World wide web

LIST OF FIGURES

1 INTRODUCTION

1.1 OVERVIEW

In a context marked by the accelerated evolution of technology and global connectivity, the intensive use of the internet, interaction on social media platforms, and the transfer of information between users have undergone a profound transformation that has significantly influenced the field of information security. This dynamic is stimulated by the proliferation of connected devices, smart devices from phones to household appliances, strengthening society's dependence on technology more than ever. In this light, the interest and efforts dedicated to cybersecurity have seen notable ascension, driven by the necessity to protect critical infrastructures and personal data. In this regard, initiatives and regulations proposed by institutions such as the European Union Agency for Cybersecurity (ENISA) underline the imperative of an active and comprehensive approach in the face of contemporary cybersecurity challenges, highlighting fundamental objectives and suggesting the consolidation of cybersecurity, a field at the intersection of technology, business environment, and political sphere.

The main approach consists in identifying the deficiencies and vulnerabilities of electronic systems and implementing specific solutions for preventing, alerting, and counteracting zero-day attacks (a previously unknown security vulnerability that can be exploited by attackers before it is detected and remedied) and advanced persistent threats (APT - complex attacks that penetrate networks without being detected, aiming for data theft or long-term system surveillance/espionage). The discussion extends to the vulnerabilities of computer systems and their considerable impact on personal and institutional economies. This doctoral thesis aims to address the latest threats, vulnerabilities, and attacks, focusing on innovation and developing protection strategies adapted to the contemporary cyber landscape.

Research objectives include:

a) Optimizing existing learning algorithms and classifying malicious sequences through the proposed methodology to achieve much better accuracy and precision compared to current implementations presented in specialized articles;

b) Developing a prototype (software) for automating and responding to incidents, detecting malicious code sequences using free resources, employing a flexible and scalable software architecture that can be identified and installed in any infrastructure/environment, and managing cyber threats in a simplified, automated, and rapid manner;

c) Implementing and developing detailed security procedures that include both attacks and defenses to assess the risk level in a company/institution to improve data security;

d) Developing machine learning methods used for identifying malicious software sequences and experimentally identifying algorithms with optimal performance for cybersecurity scenarios.

This work brings an innovative contribution to the field of cybersecurity, unique in presenting an automated incident response system. The system is entirely created using free resources and is designed in a modular framework, making it flexible and scalable. This approach has not been explored in existing works, thus offering an original and efficient solution for

managing cyber threats. "Defense in depth" or layered security is a cybersecurity strategy that uses multiple products, policies, and practices to protect the network, infrastructure, resources, and IT properties of an organization/company. It is based on multi-level security solutions: physical, technical, and administrative, to prevent attackers from reaching protected resources.

In Figure 1, the security measures implemented and analyzed in the doctoral research are presented, as well as the measures that were not included in the project. The components colored in blue represent the security measures that have been implemented and analyzed in detail in the doctoral thesis. These include web application security, data loss prevention, multifactor authentication, update management, security testing, file integrity monitoring, etc. On the other hand, elements highlighted in red indicate the security measures that were not included in this work, such as VoIP protection, virtual private network (VPN), database monitoring, or wireless network security. These were excluded because they exceed the main scope of the research, which focuses on automating the management and correlation of responses to cybersecurity incidents and improving and identifying security issues through social engineering, source code analysis of various software used or developed by the company, and purple team exercises.

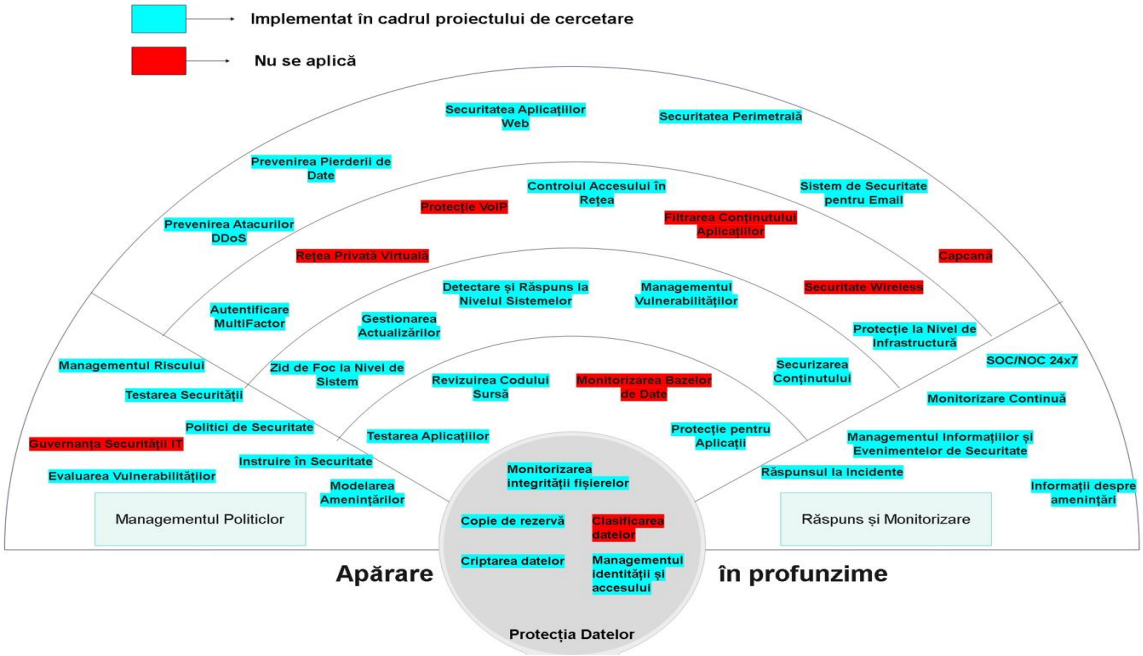

Figura 1 Concept of layered security

1.2 JUSTIFICATION OF THE RESEARCH: THE OPPORTUNITY AND RELEVANCE OF THE RESEARCH TOPIC

Malicious sequences (malware) are intrusive programs that perform unauthorized and harmful activities within systems. They can be easily introduced into any computer system, generating significant disruptions and damage. Malicious sequences constitute a serious and predominant threat, attracting attention in the field of digital sciences.

The system structure provides for the implementation of both manual and automated processes and procedures designed to identify zero-day threats (previously unknown software vulnerabilities

discovered by attackers) and using the system for efficient and rapid response to security incidents. The research is structured into three main phases:

The first phase of the research focused on collecting and analyzing information from bibliographic sources, market exploration, and evaluating current trends to identify the limitations of existing detection systems (such as antivirus solutions offered by top manufacturers like Bitdefender, CrowdStrike, Kaspersky) following specific objectives:

a) Examining the specialized literature to evaluate different methods and strategies for detecting malicious code sequences, establishing the necessary parameters for developing an efficient system for real-time detection of illegitimate software;

b) Conducting a detailed market analysis to define the system requirements, applying conceptual and contextual methods for collecting and examining relevant data;

c) Designing an advanced system capable of analyzing the behavioral characteristics of malicious code sequences and operating mechanisms by implementing machine learning algorithms. This phase lays the foundation for the further development of a tool capable of effectively responding to cybersecurity challenges, optimizing the detection and response process in the face of digital threats.

The second phase was dedicated to the construction, design, implementation, and evaluation of the proposed system for identifying and analyzing malicious code sequences, with the following specific objectives:

a) Developing, configuring, and putting into operation a validated prototype/system under laboratory conditions using proprietary hardware resources to detect malicious code sequences using free (open-source) resources to facilitate the activity of cybersecurity specialists in incident management and conducting investigations;

b) Implementing and developing an original methodology for automatic file backup (the process of copying and archiving data from computer systems to be able to recover them in case of data loss due to technical failures, cyber-attacks, human errors, or other incidents);

c) Implementing and developing an original methodology for identity and access management (IAM - a framework of policies and technologies that ensures the proper management of digital identities and controls user access to an organization's resources and data) to strengthen infrastructure security by applying multiple access control checks;

d) Conducting extensive tests to evaluate the proposed system and gather relevant data for the final analysis of the developed system/prototype. Three testing scenarios were executed to identify suspicious behaviors, verify the model's ability to recognize and counteract attacks, and obtain specific results in response to incidents. This essential phase confirms the system's adaptability and efficiency in the context of the diversity of cyber threats, highlighting the significant contribution of the research to the field of computer security.

The third phase consisted of evaluating computer security using offensive security procedures to identify vulnerabilities with the help of detailed methodologies and procedures presented in specialized articles:

a) Evaluating incident response using social engineering with PhaaS (phishing as a service - an online fraud methodology by which attackers aim to access confidential information such as usernames and passwords by sending electronic messages that mimic reliability but are actually fabricated) to test the effectiveness of cyber-attack prevention and evaluate incident management;

b) Strengthening security through collaborative exercises (purple-team/tabletop exercises) in which defensive security teams (blue team - Security Operations) and offensive security teams (red team - Penetration Testers) work together to improve an organization's security measures;

c) Remedying vulnerabilities in software programs using source code analysis of the tested applications/systems.

2 ANALYSIS OF THE CURRENT STATE

2.1 COMPUTER SECURITY AND THE IMPORTANCE OF CYBER-ATTACKS

In the context of the digital age, security represents a fundamental pillar for the protection of data and essential infrastructures. In this context, cyber-attacks have intensified, underlining the continuous need for innovation and adaptability in the field of information security. A thorough understanding of the characteristics and impact of malicious code sequences is important for developing effective defense solutions, such as implementing a modular, scalable, unified security system designed to manage and monitor threats.

According to the Control Objectives for Information and Related Technologies (COBIT), optimizing information management and information technology is vital for the prosperity and success of organizations in a globalized information society. Among the decisive factors are the increasing dependence on information and the computer systems that manage it, the rising vulnerabilities, significant costs of technology investments, and the capacity of technologies to profoundly reconfigure organizations and business practices.

In conclusion, cyber-attacks represent a persistent and evolving threat in the current technological context.

2.2 TYPES OF CYBER-ATTACKS

Malicious code sequences constitute a broad class of programs designed to execute harmful or unauthorized operations on computer systems. This classification includes a variety of malicious software categories, including computer viruses, worms, trojans, spyware, adware, and ransomware. The field of cybersecurity, being in continuous dynamics, witnesses the unceasing emergence of new types of computer threats. Computer viruses are characterized by an intrinsic capacity for self-replication and spreading, often infiltrating computer systems without the user's warning or consent.

2.3 APPLICATION OF MACHINE LEARNING TECHNOLOGIES IN DETECTING MALICIOUS SEQUENCES

In the contemporary era, artificial intelligence algorithms have the capability to take over a significant portion of human tasks. Machine learning and artificial intelligence technologies resort to algorithms and statistics to develop programs and decision-making processes, leveraging data sets without requiring direct human intervention. A notable example in this context is the anti-spam system, which operates autonomously, eliminating the need for manual rule configuration due to the application of machine learning algorithms.

2.4 DEFINITIONS AND TYPOLOGIES USED IN MACHINE LEARNING

Machine learning constitutes an essential discipline within artificial intelligence that offers systems the ability to acquire knowledge and improve from experience, eliminating the need for explicit programming. This branch focuses on developing computer applications capable of processing data and autonomously extracting features. Its importance in the field of cybersecurity is indisputable, given the facilitation of developing algorithms and analytical models that can identify and evaluate potentially dangerous behaviors and patterns within complex infrastructures. An illustrative case of this applicability is the implementation of machine learning algorithms for identifying anomalies in network traffic dynamics.

In Chapter 3, a machine learning model is presented using supervised learning algorithms for classifying records based on the type of malicious sequence, using labeled data sets. The following classification models were used:

- Decision Tree (DT)
- Random Forest (RF)
- Support Vector Machine (SVM)
- Naive Bayes (NB)
- K-Nearest Neighbors (KNN)

For optimizing the performance of machine learning models, hyperparameters were adjusted and implemented. These hyperparameters are predetermined variables set by the researcher and should not be confused with model parameters, which are automatically determined by the algorithm and are involved in predicting results based on the input data. Hyperparameters are parameters that are not directly learned by a machine model but are used to control the machine learning process. They can influence the performance and behavior of the machine learning algorithm, such as learning rate, regularization, and model architecture. Examples of hyperparameters include the learning rate, the number of layers or neurons in a neural network, and values for regularization.

2.5 CATEGORIES OF MALICIOUS PROGRAMS

A computer virus or malicious program represents a specific form of program and malicious sequence characterized by its ability to self-replicate and attach to other uninfected files, often targeting executable applications. This self-replicating ability allows the virus to spread unnoticed within a computer system. Although viruses can perform operations similar to trojans and other types of malicious software/sequences, they are distinguished by their unique method of propagation and should not be confused with other categories. File viruses represent a common class of computer viruses that tend to attach to or incorporate into executable files. Once such a file is opened or executed, the virus activates, initiating the replication process and possibly performing other suspicious activities. However, it should be noted that data files containing

macros or other forms of executable code, such as Microsoft Office documents, can also be vulnerable to infections.

Malicious sequences or programs represent a wide spectrum of dangerous computer codes that illegitimately access information within computer systems without the explicit consent of users. These IT entities aim to undermine the integrity, confidentiality, and availability of IT networks, distributing harmful sequences within the affected network or systems infrastructure. In the current era, characterized by a significant expansion of the internet, society faces major challenges in the field of cybersecurity, exacerbated by the presence of these illegal software. On the current digital scene, we encounter unauthorized actors such as hackers labeled as "black hats," who are experts in identifying and exploiting the weaknesses of computer systems, often pursuing illegal purposes that differ from ethical hackers who work to protect computer systems and people.

Thus, the essential difference between malicious (sequences) programs and legitimate ones lies in: Comparing authentic and unauthorized functionalities and identifying security risks within sophisticated applications can represent a case study. In conclusion, a clear distinction can be observed between the intentions and actions of malicious and legitimate sequences:

Malicious sequences such as RansomX and the use of CryptCreateHash functions in a malicious context illustrate how malicious sequences exploit system functions to cause harm. RansomX, for example, creates execution methods to stop processes considered unwanted by its authors, using cryptographic functions to encrypt user data, which can lead to data loss or ransom demands.

Legitimate sequences, on the other hand, use functions such as CryptCreateHash and NetServerGetInfo in a legitimate context, demonstrating how the same technologies can be used for constructive purposes. CryptCreateHash is essential for ensuring data integrity and secure authentication, while NetServerGetInfo can be used for efficient network resource management and system state monitoring.

2.6 PRESENTATION OF CURRENT SECURITY SYSTEMS

his subsection offers a thorough examination of current cybersecurity systems, emphasizing innovative technologies and advanced solutions applied in protecting IT infrastructures. The architectures and security mechanisms implemented in both software and hardware equipment are analyzed to identify, prevent, and neutralize cyber threats. Additionally, contemporary trends in developing security systems are discussed, including the adoption of artificial intelligence and machine learning algorithms for evaluating unusual behaviors and identifying potential threats.

In the last five years, OPSWAT (a major company in the field of cybersecurity) has accumulated and disseminated monthly reports on the market distribution of antivirus solutions dedicated to Windows operating systems. The company indicates that its information comes from over 30,000 systems belonging to both corporate environments and individual users who have opted for installing free antivirus applications offered by OPSWAT. According to the latest report issued at the end of October 2023, Symantec ranks as the leader in the antivirus solutions market with a market share of 13.56%, followed closely by ESET with 12.84% and McAfee with 12.21%.

These statistics provide valuable insight into the effectiveness of different antivirus solution providers in the context of Windows systems, constituting a tool for evaluating and choosing these products in the field of cybersecurity.

2.7 EVOLUTION OF MALICIOUS SEQUENCE DETECTION

The evolution of threat detection techniques can be likened to an arms race against malware creators. When antivirus solution providers implement new methods for detecting malicious programs, malware authors develop new methods to pass their code undetected by detection algorithms. This continuous dynamic leads to a constant evolution in techniques both in the field of cybersecurity and in the development of malicious programs.

3 ANALYSIS AND CLASSIFICATION OF MALICIOUS SEQUENCES USING MACHINE LEARNING ALGORITHMS

3.1 PROPOSED METHODOLOGY

Chapter 3 begins with the development of a machine learning model for detecting and classifying malicious sequences using a data set provided by an international academic community, using the Python programming language along with the Scikit-learn library, which includes an extensive diversity of specific algorithms for developing the software used in generating results based on the proposed data set. For graphical representation of the obtained results, the Matplotlib library was used, and for performing complex mathematical calculations, NumPy was used.

To optimize the results, a universal confusion matrix was used, which is an instrumental table in evaluating the accuracy of a classification algorithm. This matrix highlights how often observations are correctly or incorrectly classified by comparing the actual categories with those predicted by the model. Analyzing the confusion matrix allows an accurate assessment of the algorithm's efficiency and the identification of potential errors or weaknesses.

To calculate performance metrics, the "confusion matrix" function offered by the Scikit-learn library was used. This library also provides specialized functions that facilitate the direct calculation of indicators such as precision score (measures the proportion of correct positive identifications out of the total positive identifications), recall score (indicates the proportion of correct positive identifications relative to the total real positive cases), and accuracy score (reflects the percentage of correct predictions out of the total cases). Thus, to increase the efficiency and accuracy of model evaluation, it was decided to use these specific functions.

Additionally, the precision, accuracy, and recall rates were determined for 55 different random states, followed by the calculation of the mean of each metric. To provide a consistent model evaluation in various testing scenarios, the variance of each mean was also calculated. This methodology facilitated model improvement by identifying and reactively adjusting to new variants of malicious code sequences, as well as fine-tuning hyperparameters for overall performance optimization.

3.2 DEVELOPING THE CLASSIFICATION MODEL

The data set is designed to test methods for detecting malicious sequences hidden in memory. The data set was created to represent a real-world situation as faithfully as possible. This data set (MalMem) uses the debugging mode for the memory dump process to avoid the dumping process appearing in memory dumps. Data examination involved analyzing the characteristics of the data set consisting of 57 columns indicating whether each record is legitimate or malicious. Information regarding the number of non-null records, mean value, standard deviation, minimum and maximum value, and the corresponding percentile was investigated. Of the 57 characteristics,

the most relevant used for improving and training the model for classifying and detecting malicious sequences, as well as developing the algorithm for enriching the data set, are listed in the table below. These characteristics are extracted from document files with extensions/formats such as (.pdf, .doc, .docx, .pptx, .ppt, .csv) analyzed through an isolated environment (sandbox) using dynamic file analysis in Cuckoo Sandbox, an isolated testing environment.

3.3 Results Obtained

The initial phase of the study involved identifying the specific data categories of each element in the data set and detecting missing values to ensure the coherence and validity of subsequent investigations. This verification was carried out by analyzing the proportion of actual values to the overall size of the data set, facilitating the prompt identification of columns that require interventions to complete the missing data.

Next, the correlation coefficient, essential in evaluating the association between different variables in the data set, was calculated. The correlation quantifies how two variables fluctuate concomitantly. The value of the correlation coefficient ranges from -1 to 1, where 1 indicates a complete positive correlation (meaning that when one variable increases, the other variable increases similarly), 0 denotes no correlation, and -1 reflects an absolute negative correlation (meaning that when one variable increases, the other variable decreases inversely).
All graphs presented subsequently are from the software developed specifically to classify and analyze the data set.

3.4 Conclusions and Original Contributions

In this chapter of the thesis, the development and evaluation of an innovative methodology along with specialized software for classifying and detecting malicious code sequences using machine learning techniques were presented. A software prototype was developed with the primary objective of improving the existing data set.

4 DEFENSIVE SECURITY - DETECTION AND AUTOMATED RESPONSE TO CYBERSECURITY THREATS

4.1 AUTOMATING THE RESPONSE TO CYBER THREATS

The purpose of this section is to develop and implement a fully functional system for monitoring, detecting, and protecting against malicious code sequences using free (open-source) software to function as a modern, scalable, free system used for incident response and network security, developed to support the IT department staff within a company/institution for security investigations. The incident response system is automated to analyze specific alerts, helping the specialist/designated person to track and remediate them.
The result of this project is a fully functional and scalable open-source prototype system developed in a stable research environment using modules such as SIEM (Security Information and Event Management), IAM (Identity and Access Management), threat intelligence, threat hunting, DFIR (Digital Forensics and Incident Response), vulnerability management, SOAR (Security Orchestration Automation and Response), network security module, using firewall systems, and data backup.

4.2 COMPARISON OF THE PROPOSED SYSTEM WITH CURRENT INCIDENT MANAGEMENT SYSTEMS

The evaluation of current incident management systems addresses an analysis of how organizations identify, respond to, and recover from security incidents. This evaluation is essential as cyber threats become increasingly sophisticated, and the ability to effectively manage these incidents can make the difference between a rapid and effective response and one that leaves the organization vulnerable to additional attacks or significant losses. The evaluation of current incident management systems highlights the importance of an integrated approach that includes well-established procedures and an organizational culture that prioritizes cybersecurity.

4.3 DEVELOPING AND IMPLEMENTING THE SYSTEM FOR INCIDENT RESPONSE AND DETECTION OF MALICIOUS SEQUENCES

In the current era, we witness a remarkable proliferation of information technologies that permeate all fields of human activity. By integrating existing technologies and developing new customized components, the aim is to achieve an autonomous solution capable of responding to increasingly complex challenges in the field of cybersecurity, thus contributing to improving the security level for all users and entities adopting this approach. The proposed system was configured using Docker technology, which facilitates virtualization and flexible deployment in various infrastructures, whether Cloud or On-Premise. Except for Cuckoo Sandbox, whose integration using Docker faces major technical challenges being considered almost impossible, all system components have been optimized to operate in a secure environment.

4.4 RESULTS AND OBSERVATIONS

To analyze and test the presented solution, malicious code sequences from the real environment targeting active networks and services were used. A virtual environment that allows the controlled execution of these illegitimate sequences for testing/validation purposes using common services such as Domain Name Service (DNS) or Simple Mail Transfer Protocol (SMTP) was used. Malicious code sequence samples were procured from open sources, including specialized internet sites hosting these illegitimate samples and personal GitHub pages or educational institutes offering such samples for academic purposes. The authenticity and validity of these samples were verified using the system designed in this research. Online databases renowned such as Malware Bazaar or Malware Hash Registry.

4.5 CONCLUZII ȘI CONTRIBUȚII ORIGINALE

As cyber threats become more sophisticated and disruptive, the importance of an active and well-coordinated approach to incident response becomes crucial. Incident response teams play an essential role in protecting organizations against cyber-attacks and other security incidents by quickly detecting threats, limiting the impact of incidents, and restoring normal operations as quickly as possible. The success of these efforts depends on the clarity of roles, efficient processes, and effective communication, as well as the use of advanced technologies for security data analysis. To strengthen the support provided to security teams in the precise and efficient identification of malicious sequences, this chapter details the development of an advanced system designed to enhance detection, protection, and incident management capabilities. Significant contributions of this system to the field of computer security are also highlighted.

5 OFFENSIVE SECURITY: PROCEDURES FOR TESTING COMPUTER SYSTEM SECURITY

5.1 EVALUATING INCIDENT RESPONSE USING SOCIAL ENGINEERING

Using an original methodology and a system developed for this type of testing, the simulation of phishing attacks in controlled conditions is facilitated, providing organizations the opportunity to evaluate how well their employees are prepared to face such threats and the effectiveness of the adopted response strategies. In a real scenario, to demonstrate the efficiency of the proposed system, an authentic (real) phishing campaign was organized, involving the collection of significant data and respective metrics. The obtained results were subsequently analyzed in detail. The established objectives include:

Designing and implementing a system capable of integrating various free tools, thus facilitating the efficient execution of phishing campaigns and the collection of statistics;

Executing a phishing campaign that simulates advanced attack scenarios. The comparative analysis of the results provided an insight into the effectiveness of different types of phishing, their impact on the targeted organization, and the associated risk level, based on the success rates of previous campaigns; Regarding the delivery procedure of the malicious payload, a free open-source phishing and cybersecurity testing platform was used. This platform allows organizations to create and send phishing campaigns to assess their employees' level of cybersecurity awareness .

Research Results:

During the official phishing campaign, conducted between May 14 and 17, 2021, the following advanced performance metrics were recorded:
Total number of emails sent: 16,185
Emails opened by recipients: 456
Link clicks included: 314
Personal data submissions by recipients: 272
Upon calculating the campaign's success rate, defined as the percentage of personal data submissions relative to the number of opened emails, a performance index of 59.65% was found. This figure illustrates the campaign's effectiveness in persuading recipients to disclose personal information, thus highlighting behavioral vulnerabilities in information security. Employees who interacted with the phishing email, marking it as opened, were included in intensive awareness campaigns to emphasize the importance of vigilance against phishing attacks.

5.2 SECURING SYSTEMS THROUGH JOINT EXERCISE PROCEDURES

These joint exercises are known as cyber-crisis exercises or purple-team exercises. These exercises aim to correlate attacks (carried out in real-time by the Red Team - the attackers) and detect malicious sequences with the help of the Blue Team. The proposed collaboration methods are tested and compared in a controlled environment. The purple team concept in offensive and defensive security refers to a set of methods, processes, or activities that aim to foster collaboration between Red and Blue Teams to form a comprehensive security operations team.
A proprietary methodology or the ATT&CK® purple team methodology can be used (usually, a methodology/procedure is established by the security operations team manager, the offensive security manager, and the chief information security officer). Computer systems rely heavily on data security, the process of transforming best practices into a secure environment using necessary processes/procedures.

5.3 REMEDIATION OF VULNERABILITIES THROUGH SOURCE CODE ANALYSIS

Vulnerabilities present in the source code of applications can be exploited by malicious actors, leading to data breaches, financial losses, and reputational damage to organizations. A proactive approach to addressing these vulnerabilities through static source code analysis is essential for a secure software development lifecycle (SSDLC).
Source Code Analysis (SCA) focuses on identifying security vulnerabilities at the code level written by developers. The primary objective is to detect and remediate flaws that could be exploited for malicious purposes. This process can be carried out manually, through source code review, or automated using Static Application Security Testing (SAST) tools. SAST tools, such as SonarQube, Fortify, and Checkmarx, are the most well-known and widely used software for this purpose.

6 FINAL CONCLUSIONS. ORIGINAL CONTRIBUTIONS. PUBLISHED WORKS AND FUTURE RESEARCH DIRECTIONS

6.1 FINAL CONCLUSIONS

In the current technological context, characterized by the rapid evolution of cyber threats and the growing complexity of IT systems, the research presented in this thesis has made significant advancements in the field of cybersecurity. The development and implementation of advanced systems for detecting and responding to cyber threats have proven to be effective in enhancing the security posture of organizations.

6.2 ORIGINAL CONTRIBUTIONS

Developed and implemented an original system for data protection and Identity and Access Management (IAM);

Implemented a scalable backup solution capable of protecting both system and user data;

Created an advanced system for security incident management and malicious code analysis, integrating various open-source specialized software for effective identification and counteraction of security incidents;

Implemented solutions for collecting, storing, and analyzing event logs from various sources (desktop systems, servers, applications, etc.), identifying suspicious behaviors in real-time;

Developed a system for incident response evaluation, including the generation of homograph domain names and integration of open-source phishing applications into a system named PhaaS (Phishing as a Service);

Optimized Security Information and Event Management (SIEM) for rigorous analysis and quick intervention, offering an integrated perspective and active protection measures against threats;

Correlated events generated by Sysmon with MITRE ATT&CK identifiers to better understand attacker tactics, facilitating the detection and investigation of suspicious activities;

Implemented and configured FleetDM and osquery-defense-kit for advanced system management and monitoring, detecting outdated libraries and potential security issues;

Integrated Velociraptor and Watcher platforms to improve incident response, enhancing the effectiveness of threat detection and reaction;

Implemented a solution for monitoring infrastructure performance and status, facilitating prompt identification of issues and resource optimization;

Integrated CrowdSec with MISP and OpenCTI for the use of collective intelligence in real-time attack identification and blocking, collecting and distributing threat data;

Contributed to the development of the network security module, combining Suricata, Zeek, Arkime, and Rita to enhance network security monitoring and threat detection at OSI levels 2 and 3 (Data Link Layer and Network Layer);

Developed a solution for automatic analysis of email attachments using MINI.io, OwnCloud/Nirvashare, and Cuckoo Sandbox, to prevent email communication compromise;

Improved system interoperability and scalability, efficiently managing security incidents and protecting against cyber threats;

Developed a procedure for securing the source code of an application, exemplified in an international project detailed in the subchapter: Remediating Vulnerabilities through Source Code Analysis;

Created procedures for raising awareness among employees and students about cyber threats using a real phishing test;

Developed a procedure for a cyber-crisis exercise, improving cooperation between red and blue teams and optimizing incident and vulnerability management.

6.3 PUBLISHED PAPERS

Most of the studies and practical experiments conducted during the doctoral studies have been published in international journals with impact factors or presented at international conferences and included in the conference proceedings, indexed by ISI Web of Science. Thus, the developed information has been validated by several research groups, and the content of the thesis has been significantly improved based on the feedback received before the articles were published.

The following publications have been achieved in the field of the thesis:

A. Publications in Journals with Impact Factors Indexed by ISI Web of Science:

Lucian Florin Ilca, Ogruţan Petre Lucian, Titus Constantin Balan (2023). "Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response", Sensors, https://doi.org/10.3390/s23156757

B. Publications in SpringerLink Conference Proceedings Indexed by ISI Web of Science (or Pending Indexing) and BDI:

Lucian Florin Ilca, Titus Constantin Balan (2022). Purple Team Security Assessment of Firmware Vulnerabilities. In: Auer, M.E., Bhimavaram, K.R., Yue, XG. (eds) Online Engineering and Society 4.0. REV 2021. Lecture Notes in Networks and Systems, vol 298. Springer, Cham. https://doi.org/10.1007/978-3-030-82529-4_36

Lucian Florin Ilca, Titus Constantin Balan, "Phishing as a Service Campaign using IDN Homograph Attack," 2021 International Aegean Conference on Electrical Machines and Power Electronics (ACEMP) & 2021 International Conference on Optimization of Electrical

and Electronic Equipment (OPTIM), Brasov, Romania, 2021, pp. 338-344, doi: https://doi.org/10.1109/OPTIM-ACEMP50812.2021.9590028

Lucian Florin Ilca, Titus Constantin Balan, "Windows Communication Foundation Penetration Testing Methodology," 2021 16th International Conference on Engineering of Modern Electric Systems (EMES), Oradea, Romania, 2021, pp. 1-4, doi: https://doi.org/10.1109/EMES52337.2021.9484145

Lucian Florin Ilca, Titus Constantin Balan, "Vulnerability Remediation in ICS Infrastructure Based on Source Code Analysis," 2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet), Bucharest, Romania, 2020, pp. 1-6, doi: https://doi.org/10.1109/RoEduNet51892.2020.9324845

BIBLIOGRAPHY

[1] Y. Li și Q. Liu, „A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments”, *Energy Rep.*, vol. 7, pp. 8176–8186, nov. 2021, doi: 10.1016/j.egyr.2021.08.126.

[2] M. Dunn Cavelty și M. Smeets, „Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority”, *J. Eur. Public Policy*, vol. 30, nr. 7, pp. 1330–1352, iul. 2023, doi: 10.1080/13501763.2023.2173274.

[3] M. Botacin, F. Ceschin, R. Sun, D. Oliveira, și A. Grégio, „Challenges and pitfalls in malware research”, *Comput. Secur.*, vol. 106, p. 102287, iul. 2021, doi: 10.1016/j.cose.2021.102287.

[4] M. T. Rahman *et al.*, „Defense-in-depth: A recipe for logic locking to prevail”, *Integration*, vol. 72, pp. 39–57, mai 2020, doi: 10.1016/j.vlsi.2019.12.007.

[5] M. Alenezi, H. Alabdulrazzaq, A. Alshaher, și M. Alkharang, „Evolution of Malware Threats and Techniques: A Review”, *Int. J. Commun. Netw. Inf. Secur.*, vol. 12, p. 326, dec. 2020, doi: 10.17762/ijcnis.v12i3.4723.

[6] „The Development of the Open Machine-Learning-Based Anti-Spam (Open-MaLBAS) | IEEE Journals & Magazine | IEEE Xplore”. Data accesării: 27 mai 2024. [Online]. Disponibil la: https://ieeexplore.ieee.org/abstract/document/9565223

[7] D. Sulistyowati, F. Handayani, și Y. Suryanto, „Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS”, *JOIV Int. J. Inform. Vis.*, vol. 4, nr. 4, pp. 225–230, dec. 2020, doi: 10.30630/joiv.4.4.482.

[8] „Improvise, Adapt, Overcome: Dynamic Resiliency Against Unknown Attack Vectors in Microgrid Cybersecurity Games | IEEE Journals & Magazine | IEEE Xplore”. Data accesării: 27 mai 2024. [Online]. Disponibil la: https://ieeexplore.ieee.org/abstract/document/10458886

[9] „Cybersecurity data science: an overview from machine learning perspective | Journal of Big Data”. Data accesării: 28 mai 2024. [Online]. Disponibil la: https://link.springer.com/article/10.1186/s40537-020-00318-5

[10] S. Schmitz-Berndt, „Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive”, *J. Cybersecurity*, vol. 9, nr. 1, p. tyad009, ian. 2023, doi: 10.1093/cybsec/tyad009.

[11] „Windows Anti-malware Market Share Report”, OPSWAT. Data accesării: 28 mai 2024. [Online]. Disponibil la: https://www.opswat.com/resources/reports/windows-anti-malware-market-share

[12] A. Sharma, B. B. Gupta, A. K. Singh, și V. K. Saraswat, „Orchestration of APT malware evasive manoeuvers employed for eluding anti-virus and sandbox defense”, *Comput. Secur.*, vol. 115, p. 102627, apr. 2022, doi: 10.1016/j.cose.2022.102627.

[13] N. Fleury, T. Dubrunquez, și I. Alouani, „PDF-Malware: An Overview on Threats, Detection and Evasion Attacks”. arXiv, 27 iulie 2021. doi: 10.48550/arXiv.2107.12873.

[14] V. Shah, „Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats”, *Rev. Espanola Doc. Cient.*, vol. 15, nr. 4, Art. nr. 4, 2021, Data accesării: 27 mai 2024. [Online]. Disponibil la: https://redc.revistas-csic.com/index.php/Jorunal/article/view/156

[15] J. E. van Engelen și H. H. Hoos, „A survey on semi-supervised learning”, *Mach. Learn.*, vol. 109, nr. 2, pp. 373–440, feb. 2020, doi: 10.1007/s10994-019-05855-6.

[16] „Adversarial Machine Learning in the Context of Network Security: Challenges and Solutions | Journal of Computational Intelligence and Robotics”. Data accesării: 28 mai 2024. [Online]. Disponibil la: https://thesciencebrigade.com/jcir/article/view/118

[17] „MalMem Dataset”. Canadian Institute for Cybersecurity. Data accesării: 5 iunie 2023. [Online]. Disponibil la: https://www.unb.ca/cic/datasets/malmem-2022.html

[18] D. Smith, S. Khorsandroo, și K. Roy, „Supervised and Unsupervised Learning Techniques Utilizing Malware Datasets”, în *2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC)*, feb. 2023, pp. 1–7. doi: 10.1109/ICAIC57335.2023.10044169.

[19] H. Liu, C. Zhong, A. Alnusair, și S. R. Islam, „FAIXID: A Framework for Enhancing AI Explainability of Intrusion Detection Results Using Data Cleaning Techniques”, *J. Netw. Syst. Manag.*, vol. 29, nr. 4, p. 40, mai 2021, doi: 10.1007/s10922-021-09606-8.

[20] B. Charbuty și A. Abdulazeez, „Classification Based on Decision Tree Algorithm for Machine Learning”, *J. Appl. Sci. Technol. Trends*, vol. 2, nr. 01, Art. nr. 01, mar. 2021, doi: 10.38094/jastt20165.

[21] C. Catalano, A. Chezzi, M. Angelelli, și F. Tommasi, „Deceiving AI-based malware detection through polymorphic attacks”, *Comput. Ind.*, vol. 143, p. 103751, dec. 2022, doi: 10.1016/j.compind.2022.103751.

[22] C. Condruţ, „COMPARATIVE ANALYSIS OF STRATEGIC CYBER SECURITY FOCUS AREAS – UNITED KINGDOM, ESTONIA, ROMANIA”, *Romanian Intell. Stud. Rev.*, nr. 1(29), pp. 33–61, 2023, Data accesării: 27 mai 2024. [Online]. Disponibil la: https://www.ceeol.com/search/article-detail?id=1161050

[23] „Sensors | Free Full-Text | Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response”. Data accesării: 27 mai 2024. [Online]. Disponibil la: https://www.mdpi.com/1424-8220/23/15/6757

[24] R. Cordeiro de Amorim și C. D. Lopez Ruiz, „Identifying meaningful clusters in malware data”, *Expert Syst. Appl.*, vol. 177, p. 114971, sep. 2021, doi: 10.1016/j.eswa.2021.114971.

[25] A. Diaz, A. T. Sherman, și A. Joshi, „Phishing in an academic community: A study of user susceptibility and behavior”, *Cryptologia*, vol. 44, nr. 1, pp. 53–67, ian. 2020, doi: 10.1080/01611194.2019.1623343.

[26] „Phishing as a Service Campaign using IDN Homograph Attack | IEEE Conference Publication | IEEE Xplore”. Data accesării: 27 mai 2024. [Online]. Disponibil la: https://ieeexplore.ieee.org/abstract/document/9590028

[27] L. F. Ilca și T. Balan, „Purple Team Security Assessment of Firmware Vulnerabilities”, în *Online Engineering and Society 4.0*, M. E. Auer, K. R. Bhimavaram, și X.-G. Yue, Ed., Cham: Springer International Publishing, 2022, pp. 370–379. doi: 10.1007/978-3-030-82529-4_36.

[28] C. Dale, „Red, Blue and Purple Teams: Combining Your Security Capabilities for the Best Outcome”.

[29] „Enterprise Purple Teaming: An Exploratory Qualitative Study - ProQuest”. Data accesării: 28 mai 2024. [Online]. Disponibil la: https://www.proquest.com/openview/3149b511b3b11ba9d4d866de4e4aacae/1?pq-origsite=gscholar&cbl=18750&diss=y

[30] „Vulnerability Remediation in ICS Infrastructure Based on Source Code Analysis | IEEE Conference Publication | IEEE Xplore”. Data accesării: 27 mai 2024. [Online]. Disponibil la: https://ieeexplore.ieee.org/abstract/document/9324845

[31] M. Phelps, „The role of the private sector in counter-terrorism: a scoping review of the literature on emergency responses to terrorism”, *Secur. J.*, vol. 34, nr. 4, pp. 599–620, dec. 2021, doi: 10.1057/s41284-020-00250-6.

[32] „Validation of Firmware Security using Fuzzing and Penetration Methodologies | IEEE Conference Publication | IEEE Xplore”. Data accesării: 28 mai 2024. [Online]. Disponibil la: https://ieeexplore.ieee.org/abstract/document/10126524

[33] S. A. Afaq, M. S. Husain, A. Bello, și H. Sadia, „A Critical Analysis of Cyber Threats and Their Global Impact”, în *Computational Intelligent Security in Wireless Communications*, CRC Press, 2023.