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

REZUMAT

Conducător ştiinţific
Prof. Dr. Ing. Petre Lucian Ogruţan

Brașov, 2024

Cuprins

LISTA DE ABREVIERI ȘI ACRONIME

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

LISTA FIGURILOR

LISTA TABELELOR

1 INTRODUCERE

1.1 PREZENTARE GENERALĂ

Într-un context marcat de evoluția accelerată a tehnologiei și a conectivității globale, utilizarea intensivă a internetului, interacțiunea pe platformele de socializare și transferul de informații între utilizatori au cunoscut o transformare profundă ce au influențat semnificativ domeniul securității informaționale. Această dinamică este stimulată de proliferarea dispozitivelor conectate, dispozitive inteligente, de la telefoane la electrocasnice, consolidând dependența societății de tehnologie, mai accentuată ca oricând. În această lumină, interesul și eforturile dedicate securității cibernetice au cunoscut o ascensiune notabilă, determinate de necesitatea protejării infrastructurilor critice și a datelor personale. În acest sens, inițiativele și reglementările propuse de instituții precum Agenția Europeană pentru Securitatea Datelor (ENISA) subliniază imperativul unei abordări active și comprehensive în fața provocărilor securității cibernetice contemporane, a evidențiat obiective fundamentale și a sugerat consolidarea securității cibernetice, un domeniu la intersecția dintre tehnologie, mediul de afaceri și sfera politică [1].

Abordarea principală constă în identificarea deficiențelor și vulnerabilităților sistemelor electronice și în implementarea soluțiilor specifice pentru prevenirea, alertarea și contracararea atacurilor de tip zero-day (eng. zero-day - vulnerabilitate de securitate anterior necunoscută, care poate fi exploatată de atacatori înainte de a fi detectată și remediată) și a amenințărilor avansate persistente (eng. Advanced Persistent Threats - APT, atacuri complexe care pătrund în rețele fără a fi detectate, având ca scop furtul de date sau supravegherea / spionajul sistemelor pe termen lung). Discuția se extinde asupra vulnerabilităților sistemelor informatice și impactului lor considerabil asupra economiei personale și instituționale. Această teză de doctorat se angajează să abordeze amenințările, vulnerabilitățile și atacurile de ultima oră punând accent pe inovație și pe dezvoltarea de strategii de protecție adaptate la peisajul cibernetic contemporan [2]. Obiectivele cercetării includ:

a) Optimizarea algoritmilor de învățare și clasificarea secvențelor răuvoitoare existente prin metodologia propusă pentru a obține o acuratețe și precizie mult mai bună față de implementările curente, prezentate în articolele de specialitate;

b) Dezvoltarea unui prototip (software) pentru automatizarea și răspunsul la incidente, având rolul în depistarea secvențelor de cod răuvoitoare, utilizând resurse gratuite folosind o arhitectură software flexibilă și scalabilă ce poate identifica și poate fi instalată în orice infrastructură/mediu și gestionează amenințările cibernetice într-un mod simplificat, automat și rapid;

c) Implementarea și dezvoltarea procedurilor de securitate detaliate care includ atât atacuri cât și apărări cu scopul de a evalua nivelul de risc într-o companie/instituție cu scopul de a îmbunătăți securitatea datelor;

d) Dezvoltarea metodelor de învățare automată folosite pentru identificarea secvențelor software răuvoitoare și identificarea experimentală a algoritmilor cu performanțe optime pentru scenarii de securitate cibernetică.

Această lucrare aduce o contribuție inovatoare în domeniul securității cibernetice unică prin prezentarea unui sistem automatizat de răspuns la incidente de securitate. Sistemul este creat în întregime utilizând resurse gratuite și este conceput într-un cadru modular, ceea ce îl face flexibil și scalabil. Această abordare nu a fost explorată în lucrările existente, oferind astfel o soluție originală și eficientă pentru gestionarea amenințărilor cibernetice [3].

„Defense in depth” sau securitatea stratificată este o strategie de securitate cibernetică care utilizează mai multe produse, politici și practici pentru a proteja rețeaua, infrastructura, resursele și proprietățile informatice ale unei organizații/companii. Aceasta se bazează pe soluții de securitate la mai multe niveluri: fizic, tehnic și administrativ, pentru a împiedica atacatorii să ajungă la resursele protejate [4].

În Figura 1 se prezintă măsurile de securitate implementate și analizate în cadrul cercetării doctorale, precum și măsurile care nu au fost incluse în proiect. Componentele colorate în albastru reprezintă măsurile de securitate care au fost implementate și analizate în detaliu în cadrul tezei de doctorat. Printre acestea se numără securitatea aplicațiilor web, prevenirea pierderii de date, autentificarea multifactor, gestionarea actualizărilor, testarea securității, monitorizarea integrității fișierelor, etc. Pe de altă parte, elementele evidențiate în roșu indică măsurile de securitate care nu au fost incluse în cadrul acestei lucrări, cum ar fi protecția VoIP, rețeaua privată virtuală (VPN), monitorizarea bazelor de date sau securitatea rețelelor wireless. Acestea au fost excluse deoarece depășesc scopul principal al cercetării, care se concentrează pe automatizarea, gestionarea și corelarea răspunsurilor la incidentele de securitate cibernetică, precum și pe îmbunătățirea și identificarea problemelor de securitate prin intermediul ingineriei sociale, al analizei codului sursă al diferitelor software-uri utilizate sau dezvoltate de companie și al exercițiilor de tip echipă mov.

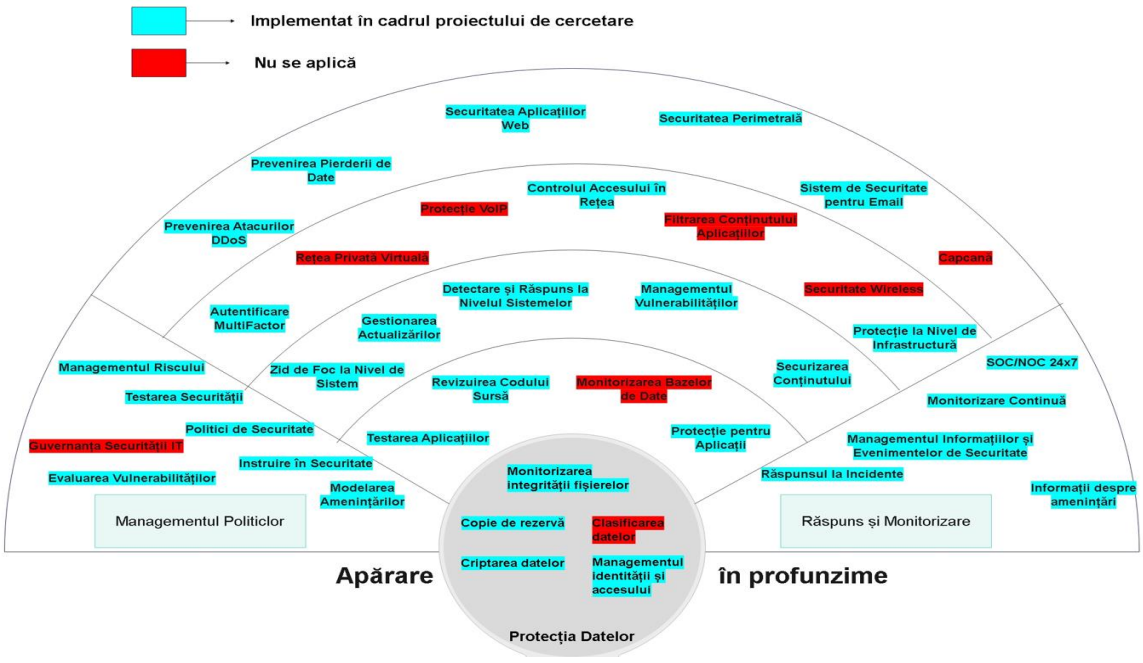


Figura 1 Prezintă conceptul de securitate stratificată.

1.2 JUSTIFICAREA CERCETĂRII, OPORTUNITATEA ȘI ACTUALITATEA TEMEI DE CERCETARE

Secvențele răuvoitoare (eng. malware) reprezintă programele intruzive care desfășoară activități neautorizate și dăunătoare în cadrul sistemelor. Acestea pot fi introduse cu ușurință în orice sistem informatic, generând perturbări și daune semnificative. Secvențele răuvoitoare constituie o amenințare serioasă și preponderentă, atrăgând atenția în domeniul științelor digitale.

Structura sistemului prevede implementarea unor procese și proceduri, atât manuale cât și automatizate, concepute pentru a identifica amenințări de tip zero-day (eng. zero-day - vulnerabilități software necunoscute de producător la momentul descoperirii lor de către atacatori) și folosirea sistemului pentru răspunsul eficient și rapid la incidente de securitate. **Cercetarea este structurată în 3 faze principale:**

Prima etapă a cercetării s-a concentrat pe colectarea și analiza informațiilor din surse bibliografice, explorarea pieței și evaluarea tendințelor actuale pentru a identifica limitările sistemelor de detecție existente (cum ar fi soluțiile antivirus oferite de producători de top precum Bitdefender, CrowdStrike, Kaspersky), urmărind obiective specifice [5]:

a) Examinarea literaturii de specialitate pentru a evalua diferite metode și strategii de detectare a secvențelor de cod rău-intenționate, stabilind astfel parametrii necesari dezvoltării unui sistem eficient pentru detectarea software-ului nelegitim în timp real;

b) Realizarea unei analize detaliate a pieței cu scopul de a defini cerințele sistemului propus, aplicând metode conceptuale și contextuale pentru colectarea și examinarea datelor relevante;

c) Proiectarea unui sistem avansat capabil să analizeze caracteristicile comportamentale ale secvențelor de cod rău-intenționate și mecanismele de funcționare, prin implementarea algoritmilor de învățare automată. Această fază pune bazele pentru dezvoltarea ulterioară a unui instrument capabil să răspundă eficient provocărilor securității cibernetice optimizând procesul de detectare și răspuns în fața amenințărilor digitale.

A doua etapă a fost dedicată construcției, proiectării, implementării și evaluării sistemului propus pentru identificarea și analiza secvențelor de cod rău-intenționate, având următoarele obiectivele specifice [6]:

a) Dezvoltarea, configurarea și punerea în funcțiune a unui sistem/prototip validat în condiții de laborator, folosind resurse hardware proprii, pentru depistarea secvențelor de cod rău-intenționate, utilizând resurse gratuite (open-source), pentru a facilita activitatea specialiștilor în securitate cibernetică în managementul incidentelor și desfășurarea investigațiilor;

b) Implementarea și dezvoltarea unei metodologii originale pentru salvarea automată a fișierelor (eng. Backup-ul reprezintă procesul de copiere și arhivare a datelor din sistemele informatice pentru a le putea recupera în cazul unei pierderi de date, fie din cauza unor defecțiuni tehnice, atacuri cibernetice, erori umane sau alte incidente)

c) Implementarea și dezvoltarea unei metodologii originale pentru managementul identității și a accesului (eng. IAM - reprezintă un cadru de politici și tehnologii care asigură gestionarea adecvată a identităților digitale și controlează accesul utilizatorilor la resursele și

datele unei organizații) cu scopul de a întări securitatea infrastructurii prin aplicarea controalelor multiple de verificare a accesului;

d) Executarea unor teste ample pentru a evalua sistemul propus și a acumula date relevante pentru analiza finală a sistemului/prototipului dezvoltat.

Au fost executate 3 scenarii de testare pentru a identifica comportamente suspecte și a verifica capacitatea modelului de a recunoaște și contracara atacurile și pentru a obține rezultate specifice răspunsului la incidente.

Această etapă esențială confirmă adaptabilitatea și eficiența sistemului în contextul diversității amenințărilor cibernetice, subliniind contribuția semnificativă a cercetării la domeniul securității informatice.

A treia etapă a constat în evaluarea securității informatice, cu ajutorul procedurilor de securitate ofensivă, având rolul de identificare a vulnerabilităților cu ajutorul metodologiilor și a procedurilor detaliate în articolele de specialitate:

a) Evaluarea răspunsului la incidente cu ajutorul ingineriei sociale folosind PhaaS (eng. phishing as a service - o metodologie de fraudă online prin care atacatorii își propun să acceseze informații confidențiale, precum numele de utilizator și parole, expedierea de mesaje electronice care mimează fiabilitatea, însă sunt în realitate fabricate) pentru testarea eficacității prevenirii atacurilor cibernetice și evaluarea gestionării incidentelor de securitate;
b) Consolidarea securității cu ajutorul exercițiilor prin colaborare (eng. purple-team / table top exercises) în care echipele de securitate defensivă (eng. blue team - Security Operations) și echipele de securitate ofensivă (eng. red team - Penetration Testers) lucrează împreună pentru a îmbunătăți măsurile de securitate ale unei organizații;
c) Remedierea vulnerabilităților în programele software folosind analiza codului sursă a aplicațiilor/sistemelor testate.

2 ANALIZA STADIULUI ACTUAL

2.1 SECURITATEA INFORMATICĂ ȘI IMPORTANȚA ATACURILOR INFORMATICE

În contextul erei digitale, securitatea reprezintă un pilon fundamental pentru protecția datelor și a infrastructurilor esențiale. În acest context, atacurile informatice s-au intensificat, subliniind necesitatea continuă de inovare și adaptabilitate în domeniul securității informaționale. O înțelegere amănunțită a caracteristicilor și impactului secvențelor de cod rău-intenționate este importantă pentru elaborarea soluțiilor de apărare eficace, precum implementarea unui sistem modular, scalabil unificat de securitate, destinate gestionării și monitorizării amenințărilor.

Conform Obiectivelor de Control pentru Informații și Tehnologii conexe (COBIT), optimizarea gestiunii informațiilor și a tehnologiilor informaționale este vitală pentru prosperitatea și succesul organizațiilor într-o societate globalizată a informației. Printre factorii decisivi se numără dependența crescândă de informații și de sistemele informatice care le gestionează, vulnerabilitățile în ascensiune, costurile semnificative ale investițiilor în tehnologie, precum și capacitatea tehnologiilor de a reconfigura profund organizațiile și practicile de afaceri [7].

În concluzie, atacurile cibernetice reprezintă o amenințare persistentă și în evoluție în contextul tehnologic actual.

2.2 TIPURI DE ATACURI INFORMATICE

Secvențele de cod rău intenționate constituie o clasă extinsă de programe proiectate să execute operațiuni dăunătoare sau neautorizate asupra sistemelor informatice. Această clasificare include o varietate de categorii de software rău intenționat, incluzând viruși informatici, viermi, troieni, programe de spionaj (eng. spyware), programe de generare a reclamelor nesolicitate (eng. adware) și programe de tip răscumpărare (eng. ransomware). Domeniul securității cibernetice, aflându-se într-o dinamică continuă, asistă la apariția neîntreruptă a noilor tipologii de amenințări informatice. Virușii informatici se caracterizează printr-o capacitate intrinsecă de auto-replicare și răspândire, adesea infiltrându-se în sistemele informatice fără avertismentul sau acordul utilizatorilor [8].

2.3 APLICAREA TEHNOLOGIILOR DE ÎNVĂȚARE AUTOMATĂ ÎN DETECTAREA SECVENȚELOR RĂUVOITOARE

În era contemporană, algoritmii de inteligență artificială au capacitatea de a prelua o porțiune semnificativă din atribuțiile umane. Tehnologiile bazate pe învățare automată și inteligența artificială recurg la algoritmi și statistici pentru elaborarea programelor și proceselor decizionale, valorificând seturile de date fără a solicita intervenția directă umană. Un exemplu notabil în acest context îl constituie sistemul anti-spam (eng. antispam - mecanism destinat

reducerii volumului de corespondență electronică nesolicitată, contribuind la optimizarea eficienței și securității comunicării electronice), care funcționează autonom, eliminând necesitatea configurării manuale a regulilor datorită aplicării algoritmilor de învățare automată.

2.4 DEFINIȚII ȘI TIPOLOGII FOLOSITE ÎN ÎNVĂȚAREA AUTOMATĂ

Învățarea automată constituie o disciplină esențială în cadrul inteligenței artificiale, care oferă sistemelor capacitatea de a acumula cunoștințe și de a se îmbunătăți din experiență, eliminând necesitatea programării explicite. Această ramură se axează pe elaborarea de aplicații informatice capabile de a procesa datele și de a extrage caracteristicile autonom. Importanța sa în domeniul securității cibernetice este incontestabilă, având în vedere facilitarea elaborării algoritmilor și a modelelor analitice care pot identifica și evalua comportamentele și tiparele potențial periculoase din infrastructurile complexe. Un caz ilustrativ al acestei aplicabilități îl reprezintă implementarea algoritmilor de învățare automată pentru identificarea anomaliilor în dinamica traficului de rețea [9].

- Învățare supervizată unde algoritmul extrage modele predictive dintr-un set de date etichetat, cu scopul de a estima răspunsurile corecte pentru intrări noi. Învățarea supervizată se divide în 2 aplicații majore:

  a) Clasificare - aceasta implică distingerea și categorisirea informațiilor dintr-un set de date în diverse clase sau etichete predefinite.

  b) Regresie - se referă la identificarea unei funcții de mapare care corelează variabilele independente cu o variabilă dependentă continuă, având rolul de a calcula probabilitățile bazate pe datele disponibile.
- Învățare nesupervizată algoritmul analizează un set de date neetichetat, încercând să detecteze structura intrinsecă sau relațiile dintre punctele de date prin recunoașterea caracteristicilor, aparițiilor și modelelor latente;
- Învățare prin consolidare modelul este instruit să acționeze într-un mediu specific, optimizându-și comportamentul prin efectuarea de acțiuni și observarea consecințelor acestora.

În Capitolul 3 este prezentat un model de învățare automată, folosindu-se algoritmi din învățarea supervizată pentru clasificarea înregistrărilor în funcție de tipul de secvență răuvoitoare și au fost folosite seturi de date etichetate. Au fost utilizate următoarele modele de clasificare:

- *Arbore de decizie (eng. Decision Tree - DT)*
- *Pădure aleatoare (eng. Random Forest - RF)*
- *Mașină de vectori suport (eng. Support Vector Machine - SVM)*
- *Naive Bayes (eng. - NB)*
- *Vecini cei mai apropiați (eng. K-Nearest Neighbours - KNN)*

Pentru optimizarea performanței modelelor de învățare automată s-au ajustat și implementat hiper-parametri. Acești hiper-parametri constituie variabile prestabilite de către cercetător și nu trebuie confundați cu parametrii modelului, care sunt determinați în mod automat de algoritm și sunt implicați în anticiparea rezultatelor pe baza informațiilor introduse.

Hiperparametrii sunt parametrii care nu sunt direct învățați de modelul unei mașini, ci sunt utilizați pentru controlul procesului de învățare automată. Aceștia pot influența performanța și comportamentul algoritmului de învățare automată, cum ar fi viteza de învățare, regularizarea și arhitectura modelului. Exemple de Hiperparametrii includ rata de învățare, numărul de straturi sau neuroni într-o rețea neurală și valorile pentru regularizare.

2.5 CATEGORII DE PROGRAME RĂUVOITOARE

Un virus informatic sau program răuvoitor reprezintă o formă specifică de program și secvență răuvoitoare care se caracterizează prin capacitatea sa de auto-replicare și de atașare la alte fișiere neinfectate, adesea, țintind în mod frecvent aplicațiile executabile. Această capacitate de auto-replicare permite virusului să se diseminеze neobservat în cadrul unui sistem informatic. Deși virușii pot executa operațiuni similare cailor troieni și altor tipuri de software / secvențe răuvoitoare, ele se disting prin metoda lor unică de propagare și nu ar trebui confundate cu alte categorii. Virușii de fișiere reprezintă o clasă comună de viruși informatici, tind să se atașeze sau să se încorporeze în fișierele executabile. Odată ce un astfel de fișier este deschis sau executat, virusul se activează, inițiind procesul de replicare și posibil de a efectua alte activități suspecte.. Totuși, trebuie menționat că fișierele de date care conțin macro-uri sau alte forme de cod executabil, cum ar fi documentele Microsoft Office, pot fi de asemenea vulnerabile la infecții.

Secvențele sau programele rău intenționate reprezintă un spectru extins de coduri informatice periculoase care accesează ilegitim informațiile din cadrul sistemelor informatice, fără consimțământul explicit al utilizatorilor. Aceste entități informatice vizează subminarea integrității, confidențialității și disponibilității rețelelor informatice, distribuind secvențe nocive în infrastructura rețelei sau a sistemelor afectate. În era actuală, caracterizată de o expansiune semnificativă a internetului, societatea se confruntă cu provocări majore în domeniul securității cibernetice, exacerbate de prezența acestor software-uri ilegale. Pe scena digitală actuală, întâlnim actori neautorizați, precum hackerii etichetați drept ,,pălării negre" (eng. Black Hat), care sunt experți în identificarea și exploatarea punctelor slabe ale sistemelor informatice, urmărind adesea scopuri ilegale, care se diferențiază de cei cu pălării albe, hackerii etici care lucrează pentru a proteja sistemele informatice și oamenii [10]. Astfel, diferența esențială între programele (secvențele) răuvoitoare și cele legitime constă în:

Comparația dintre funcționalitățile autentice și cele neautorizate, precum și identificarea riscurilor de securitate în cadrul aplicațiilor sofisticate poate reprezenta un studiu de caz. În concluzie, se poate observa o distincție clară între intențiile și acțiunile secvențelor răuvoitoare și cele legitime:

Secvențe răuvoitoare, precum *RansomX* și utilizarea funcțiilor *CryptCreateHash* în context răuvoitor, ilustrează modul în care secvențele răuvoitoare exploatează funcțiile sistemului pentru a cauza daune. *RansomX*, de exemplu, creează metode de execuție pentru a opri procese considerate de autorii săi ca fiind nedorite utilizând funcții criptografice pentru criptarea datelor utilizatorilor, ceea ce poate duce la pierderea datelor sau la cereri de răscumpărare.

Secvențele legitime pe de altă parte folosesc funcții cum ar fi *CryptCreateHash* și *NetServerGetInfo*, într-un context legitim, demonstrează cum aceleași tehnologii pot fi utilizate pentru scopuri constructive. *CryptCreateHash*, esențială pentru asigurarea integrității datelor și autentificarea securizată, în timp ce *NetServerGetInfo* poate fi folosită pentru gestionarea eficientă a resurselor de rețea și pentru monitorizarea stării sistemelor.

2.6 PREZENTAREA SISTEMELOR DE SECURITATE ACTUALE

Acest subcapitol oferă o examinare minuțioasă a sistemelor de securitate cibernetică actuale, punând accent pe tehnologiile inovatoare și soluțiile avansate aplicate în protecția infrastructurilor informatice. Sunt analizate arhitecturile și mecanismele de securitate implementate atât în echipamentele software, cât și în cele hardware, cu scopul de a identifica, preveni și neutraliza amenințările cibernetice. În plus, se discută tendințele contemporane în dezvoltarea sistemelor de securitate, inclusiv adoptarea inteligenței artificiale și a algoritmilor de învățare automată pentru evaluarea comportamentelor neobișnuite și identificarea potențialelor amenințări.

În ultimii cinci ani, OPSWAT (companie importantă în domeniul securității cibernetice) a acumulat și diseminat rapoarte lunare privind distribuția pe piață a soluțiilor antivirus dedicate sistemelor de operare Windows. Compania indică faptul că informațiile sale provin de la peste 30.000 de sisteme aparținând atât mediului corporativ, cât și utilizatorilor individuali, care au optat pentru instalarea aplicațiilor antivirus gratuite oferite de compania OPSWAT. Potrivit ultimului raport, emis la finalul lunii Octombrie 2023, Symantec se poziționează ca lider pe piața soluțiilor antivirus, având o cotă de piață de 13,56%, urmat îndeaproape de ESET cu 12,84% și McAfee cu 12,21%. Aceste statistici oferă o perspectivă valoroasă asupra eficienței diferiților furnizori de soluții antivirus în contextul sistemelor Windows, constituind un instrument pentru evaluarea și alegerea adecvată a acestor produse în domeniul securității cibernetice.

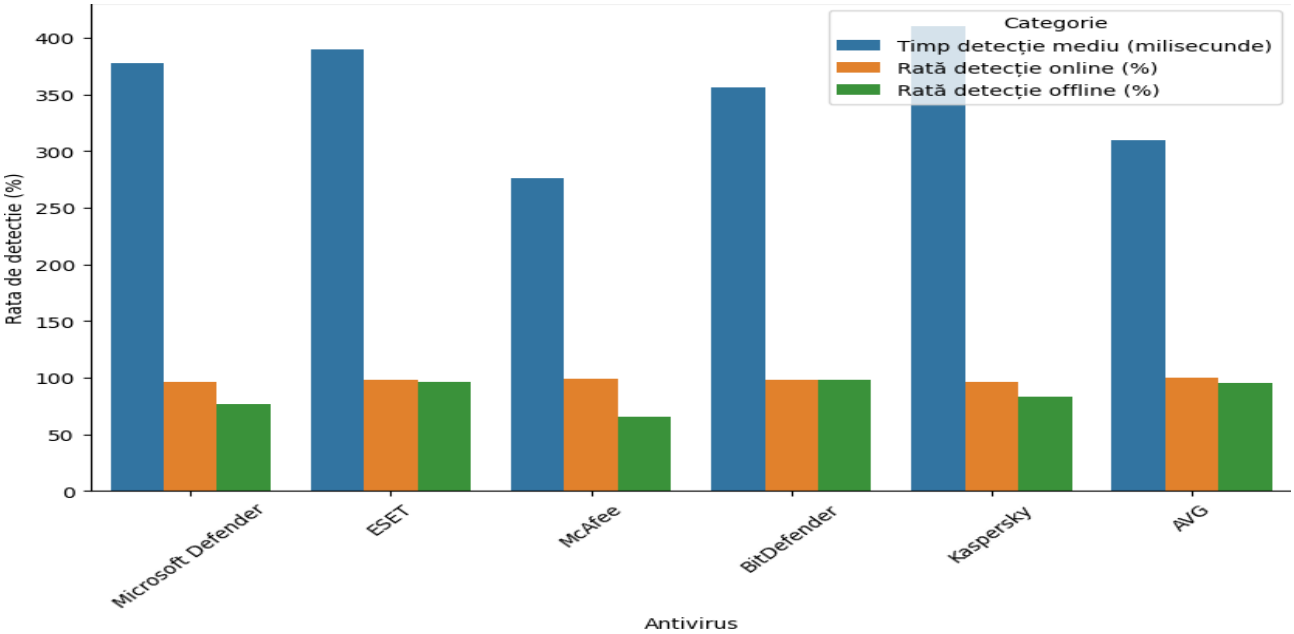


Figura 2 Date privind eficacitatea software-urilor antivirus în anul 2023.

În cadrul Figurii 20 prezentată anterior, sunt evidențiate programele antivirus dezvoltate de companiile Symantec, SentinelOne și McAfee, care au fost recunoscute drept cele mai răspândite și utilizate soluții antivirus pentru platforma Windows în prezent. Această constatare se bazează pe datele privind utilizarea acestora colectate de către furnizorul de software de securitate pentru întreprinderi, OPSWAT [11].

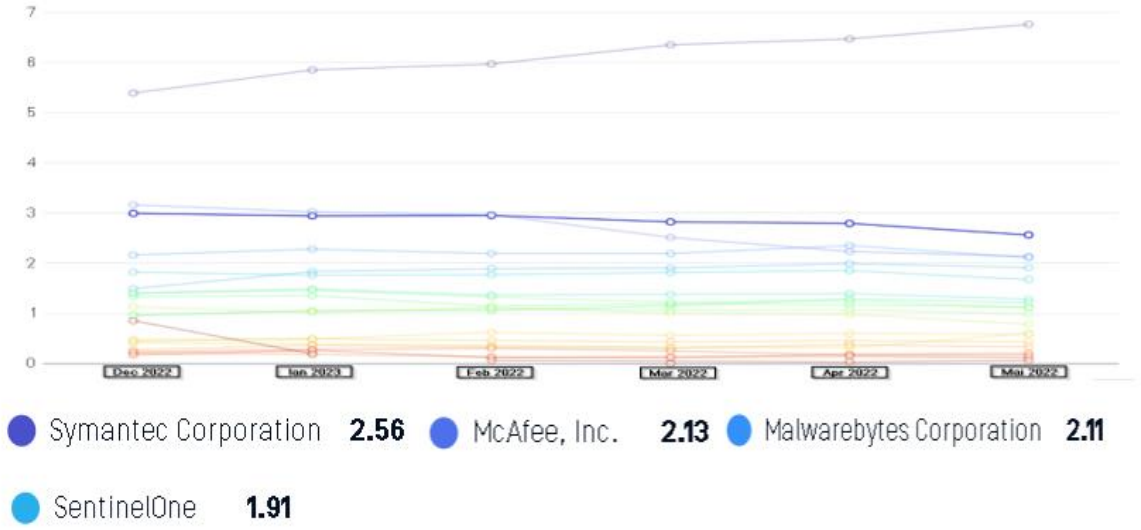


Figura 3 Topul produselor antivirus în 2023 bazat pe studiul OPSWAT.

2.7 EVOLUȚIA DETECTĂRII SECVENȚELOR RĂUVOITOARE

Evoluția tehnicilor de detectare a amenințărilor se poate asemăna cu o cursă de înarmare împotriva creatorilor de programe răuvoitoare. Când furnizorii de soluții antivirus implementează metode noi pentru detectarea programelor răuvoitoare, autorii de programe răuvoitoare dezvoltă noi metode pentru a trece codul lor nedetectat de algoritmii de detectare. Această dinamică continuă duce la o evoluție constantă în tehnici atât în domeniul securității cibernetice, cât și în cel al dezvoltării programelor răuvoitoare.

a) Detectarea bazată pe semnături se fundamentează pe compararea conținutului unui program cu un depozit de expresii regulate pre-învățate, extrase din secvențe răuvoitoare. Procesul de extragere, stocare și distribuire a acestor șiruri de caractere necesită efort și timp semnificativ din partea umană. Cercetătorii de la Symantec, un lider în dezvoltarea soluțiilor antivirus, au subliniat lentitudinea și susceptibilitatea la erori a utilizării semnăturilor. În prezentarea cercetării asupra unui sistem automatizat de extragere a semnăturilor, autorii au raportat o reducere semnificativă a timpului necesar pentru generarea semnăturilor, de peste 1000 de minute (peste 19 ore), aplicat unui set de date de 46.120 de probe.

b) Sistemele de detecție bazate pe anomalii clasifică comportamentele considerate tipice pentru un fișier sau sistem, iar orice deviații de la acestea sunt considerate anomalii. O fază de instruire creează un model al comportamentului sau structurii tipice a fișierului sau sistemului. Faza de monitorizare detectează deviațiile față de liniile de bază stabilite în timpul instruirii. De exemplu, un fișier PDF infectat ar putea diferi semnificativ de structura tipică sau așteptată a unui fișier PDF legitim.

c) Analiza statică constituie un proces esențial în domeniul securității cibernetice, având drept scop extragerea de informații din codul unui program potențial răuvoitor, fără a-l executa. Această metodologie se distinge prin siguranța sa comparativ cu analiza dinamică, deoarece, evită rularea efectivă a codului răuvoitor..

d) Analiza dinamică este un pilon decisiv în cadrul cercetărilor avansate în securitate cibernetică ce implică evaluarea minuțioasă a unui program potențial răuvoitor prin executarea și monitorizarea activității acestuia în timp real.

Analiza dinamică de bază se concentrează pe observarea comportamentelor elementare, cum ar fi: *crearea de procese, activitățile de fișiere sau modificările din regiștrii*. În schimb, analiza dinamică avansată presupune o examinare detaliată a stării interne a programului răuvoitor în timpul execuției. Această abordare utilizează tehnici sofisticate de depanare pentru a investiga codul pas cu pas și pentru a efectua inspecții interne detaliate. Prin aceasta, comportamentele dăunătoare sunt expuse, iar orice cod ascuns prin ambalare este dezvăluit. Elemente precum *identitatea programului, apelurile de funcții, analiza parametrilor și fluxul de informații* sunt analizate meticulos. *Bibliotecile dinamice, procesele și activitățile de fișiere* sunt, de asemenea, examinate [12].

Tehnicile de evadare utilizate de secvențele răuvoitoare sunt proiectate pentru a ocoli mecanismele de securitate și de a împiedica analiza codului răuvoitor. Aceste metode se bazează pe complexitatea algoritmilor și comportamentelor, având drept scop mascarea activității răuvoitoare și menținerea persistenței în sistemul infectat. Exemplele de evadare includ ascunderea codului, polimorfismul, inserarea de cod aleator (non-operații), schimbarea de regiștrii, schimbarea ordinii instrucțiunilor, înlocuirea instrucțiunilor, transpunerea codului sursă, integrarea codului sursă [13]. Mai jos sunt prezentate principalele tehnici de evaziune/ascundere folosite astăzi în prezent de către atacatori și dezvoltatorii programelor rău-intenționate:

a) Ascunderea codului, cunoscută sub denumirea de ascundere sau (eng. obfuscation), constituie o strategie complexă în domeniul securității cibernetice, utilizată pentru a complica procesul de detectare a secvențelor răuvoitoare.

b) Transpunerea codului reordonează sau mută secvențele de cod binar și folosește instrucțiuni necondiționate sau condiționate pentru a reconfigura fluxul de execuție al programului original.

c) Integrarea codului cu o secvență răuvoitoare este extrem de sofisticată deoarece secvența răuvoitoare descompune inițial programul țintă în componente mai mici și apoi adaugă modificări la acestea, cu scopul de a recompune ulterior codul încorporat, creând astfel un nou fișier.

d) Schimbarea ordinii instrucțiunilor unde secvența de instrucțiuni este rearanjată aleatoriu în scopul de a genera variații ale secvenței binare a codului în cadrul multiplelor instanțe ale aceluiași program răuvoitor.

e) Schimbarea instrucțiunilor ce sunt înlocuite cu altele echivalente, în care toate instrucțiunile date au aceeași funcționalitate, și anume, setarea registrului EAX (eng. EAX - Registrul EAX este un registru de 32 de biți utilizat în arhitectura x86 (RAX pentru 64 de biți) pentru a stoca date și rezultate intermediare în timpul execuției programului) la valoarea 0.

f) Injecția codului de non-operație (NOP) un cod de non-operație (NOP) sled, cunoscut și sub denumirea de tunel NOP, reprezintă o secvență lungă de instrucțiuni, adesea inclusă într-un set de instrucțiuni răuvoitoare (eng. shellcode), ca parte a unei tehnici sau a unui program special conceput pentru a exploata o vulnerabilitate specifică.

g) Polimorfism - Primul program răuvoitor polimorfic a fost dezvoltat de Mark Washbrun în anul 1990 și a fost numit Virusul 1260. Polimorfismul reprezintă o tehnică sofisticată de camuflare utilizată de programele răuvoitoare în scopul generării unui număr aparent nelimitat de noi variante distincte ale secvențelor răuvoitoare, cu intenția de a face dificilă analiza și detectarea acestora.

3 ANALIZA ȘI CLASIFICAREA SECVENȚELOR RĂUVOITOARE FOLOSIND ALGORITMI DE ÎNVĂȚARE AUTOMATĂ

3.1 METODOLOGIA PROPUSĂ

Capitolul 3 începe cu dezvoltarea unui model de învățare automată în vederea detectării și clasificării secvențelor răuvoitoare, utilizând un set de date furnizat de o comunitatea academică internațională folosind limbajul de programare Python împreună cu biblioteca Scikit-learn (eng. Scikit-learn - o bibliotecă de învățare automată pentru Python), care include o diversitate extensivă de algoritmi specifici domeniului menționat pentru dezvoltarea software-ului folosit în generarea rezultatelor bazat pe setul de date propus. Pentru reprezentarea grafică a rezultatelor obținute, s-a apelat la biblioteca Matplotlib (eng. Matplotlib - o bibliotecă de creare de grafice pentru Python), iar pentru efectuarea calculelor matematice cu o complexitate ridicată s-a utilizat NumPy (eng. NumPy - o bibliotecă pentru limbajul de programare Python, ce adaugă suport pentru matrici și structuri de date multidimensionale, împreună cu o colecție de funcții matematice pentru a opera cu aceste structuri de date).

În vederea optimizării rezultatelor, s-a folosit o matrice de confuzie universală (eng. confusion matrix - un instrument pentru evaluarea performanței algoritmilor de clasificare), care constituie un tabel instrumental în evaluarea preciziei unui algoritm de clasificare. Această matrice evidențiază cât de frecvent observațiile sunt clasificate corect sau incorect, comparând categoriile reale cu cele prezise de model. Analiza matricei de confuzie permite o evaluare acurată a eficienței algoritmului și identificarea potențialelor erori sau puncte slabe [14].

Pentru calcularea metricilor de performanță, s-a recurs la utilizarea funcției „confusion matrix”, oferită de biblioteca Scikit-learn. Această bibliotecă pune la dispoziție, de asemenea, funcții specializate care facilitează calculul direct al unor indicatori precum scorul de precizie (eng. precision score - măsoară proporția identificărilor corecte pozitive din totalul identificărilor pozitive), rata de detectare (eng. recall score - indică proporția identificărilor corecte pozitive raportată la totalul cazurilor pozitive reale) și scorul de acuratețe (eng. accuracy score - reflectă procentul de predicții corecte din totalul cazurilor). Astfel, pentru a crește eficiența și acuratețea evaluării modelului, s-a decis folosirea acestor funcții specifice.

Adițional, s-a procedat la determinarea preciziei, acurateței și ratei de detectare pentru 55 de stări aleatorii diferite, urmată de calculul mediei fiecărei metrici. Pentru a oferi o evaluare consistentă a modelului în diverse scenarii de testare, s-a calculat și varianța fiecărei medii. Această metodologie a facilitat îmbunătățirea modelului prin identificarea și ajustarea reactivă la noile variante de secvențe de cod rău intenționate, precum și prin finisarea hiperparametrilor pentru optimizarea performanței generale [15].

3.2 DEZVOLTAREA MODELULUI DE CLASIFICARE

Setul de date este proiectat pentru a testa metodele de detectare a secvențelor răuvoitoare ascunse în memorie. Setul de date a fost creat pentru a reprezenta cât mai fidel posibil o situație din lumea reală. Acest set de date (MalMem) utilizează modul de depanare pentru procesul de descărcare al memoriei pentru a evita ca procesul de descărcare să apară în descărcările de memorie [16].

Examinarea datelor a implicat analiza caracteristicilor din setul de date, constând în 57 de coloane care indică dacă fiecare înregistrare este legitimă sau răuvoitoare. Au fost investigate informațiile referitoare la numărul de înregistrări nenule, valoarea medie, deviația standard, valoarea minimă și maximă, precum și percentila corespunzătoare. Din cele 57 de caracteristici, în tabelul de mai jos sunt enumerate cele mai relevante, utilizate atât pentru îmbunătățirea și antrenarea modelului în scopul clasificării și detectării secvențelor răuvoitoare, cât și pentru dezvoltarea algoritmului destinat îmbogățirii setului de date. Aceste caracteristici sunt extrase din fișiere de tip document cu extensii / formate de fișier precum *(.pdf, .doc, .docx, .pptx, .ppt, .csv*), fiind analizate prin intermediul unui mediu izolat (sandbox) prin analiza dinamică a fișierelor în Cuckoo Sandbox, un mediu izolat de testare [17].

Tabelul 1 - Caracteristicile setului de date.

Tipul	Lista de caracteristici	Descriere
Process View	pslist psscan session thrdproc	pslist - Lista de procese în cadrul sistemului de operare psscan - Scanarea proceselor în cadrul memoriei pentru a detecta procese ascunse sau terminate session - Sesiunea în cadrul căreia rulează procesele în sistemul de operare thrdproc - Procesul responsabil pentru gestionarea firelor de execuție în cadrul sistemului de operare
Handles	File Port Event Thread Section	File - Resursa asociată unui fișier pe sistemul de operare Port - Interfață de comunicare utilizată pentru transferul de date între dispozitive sau programe Event - Semnalizator utilizat pentru sincronizarea proceselor sau pentru semnalarea evenimentelor în sistemul de operare Thread - Unitate de execuție a unui proces, responsabilă pentru execuția codului în cadrul acestuia Section - Zonă de memorie utilizată pentru stocarea și organizarea datelor și codului executabil în cadrul unui proces
Apihooks	Psscan Pslist Thrdproc Session	Psscan - Scanarea proceselor pentru a identifica informații și relații între ele în cadrul sistemului de operare Pslist - Listă care prezintă procesele active în sistemul de operare, inclusiv informații detaliate despre fiecare proces

		Thrdproc - Procesul care gestionează firele de execuție în cadrul sistemului de operare, monitorizând și controlând fluxul acestora Session - Sesiunea de lucru sau mediul în care se desfășoară o serie de activități sau procese pe un sistem de operare
Malfind	commitCharge uniqueInjections	CommitCharge - Cantitatea totală de memorie virtuală angajată în modul de lucru actual al sistemului de operare UniqueInjections - Numărul total de injecții unice identificate în cadrul sistemului de operare
Ldrmodule	avgMissingFromInit avgMissingFromLoad avgMissingFromMem	avgMissingFromInit - Media cantității de module care lipsesc din lista de inițializare a sistemului de operare avgMissingFromLoad - Media cantității de module care lipsesc din lista de încărcare a sistemului de operare avgMissingFromMem - Media cantității de module care lipsesc din memoria sistemului de operare

3.3 REZULTATE OBȚINUTE

Faza inițială a studiului a implicat identificarea categoriilor de date specifice fiecărui element al setului de date și detectarea absențelor de valori, pentru a asigura coerența și validitatea investigației ulterioare. Această verificare s-a desfășurat prin analiza proporției valorilor efective față de dimensiunea globală a setului de date, facilitând astfel identificarea promptă a coloanelor ce necesită intervenții pentru completarea datelor deficitare [18].

Apoi, s-a calculat coeficientul de corelație, esențial în evaluarea asocierii între diferitele variabile ale setului de date. Corelația cuantifică modul în care 2 variabile fluctuează concomitent.. Valoarea coeficientului de corelație se încadrează în intervalul -1 până la 1, unde 1 indică o corelație pozitivă integrală (însemnând că, la creșterea unei variabile, cealaltă variabilă crește în mod similar), 0 denotă lipsa oricărei corelații, iar -1 reflectă o corelație negativă absolută (adică, creșterea unei variabile este invers proporțională cu evoluția celeilalte).

Toate graficele prezentate în continuare provin din software-ul dezvoltat special pentru a clasifica și a analiza setul de date [19].

Aceste grafice subliniază importanța fiecărei caracteristici, utilizând coeficientul de corelație pentru evaluare. Acest coeficient cuantifică intensitatea și direcția relației liniare dintre 2 variabile, fiind utilizat pentru a estima cât de strâns sunt legate fiecare caracteristică în parte de variabila țintă sau de alte caracteristici. De exemplu, pentru prima matrice, la a patra (4) interogare, valoarea coeficientului de corelație este de 0,74, indicând o asociere puternică, în timp ce valoarea medie a coeficientului de corelație în setul de date este de 0,38, sugerând o asociere moderată [20].

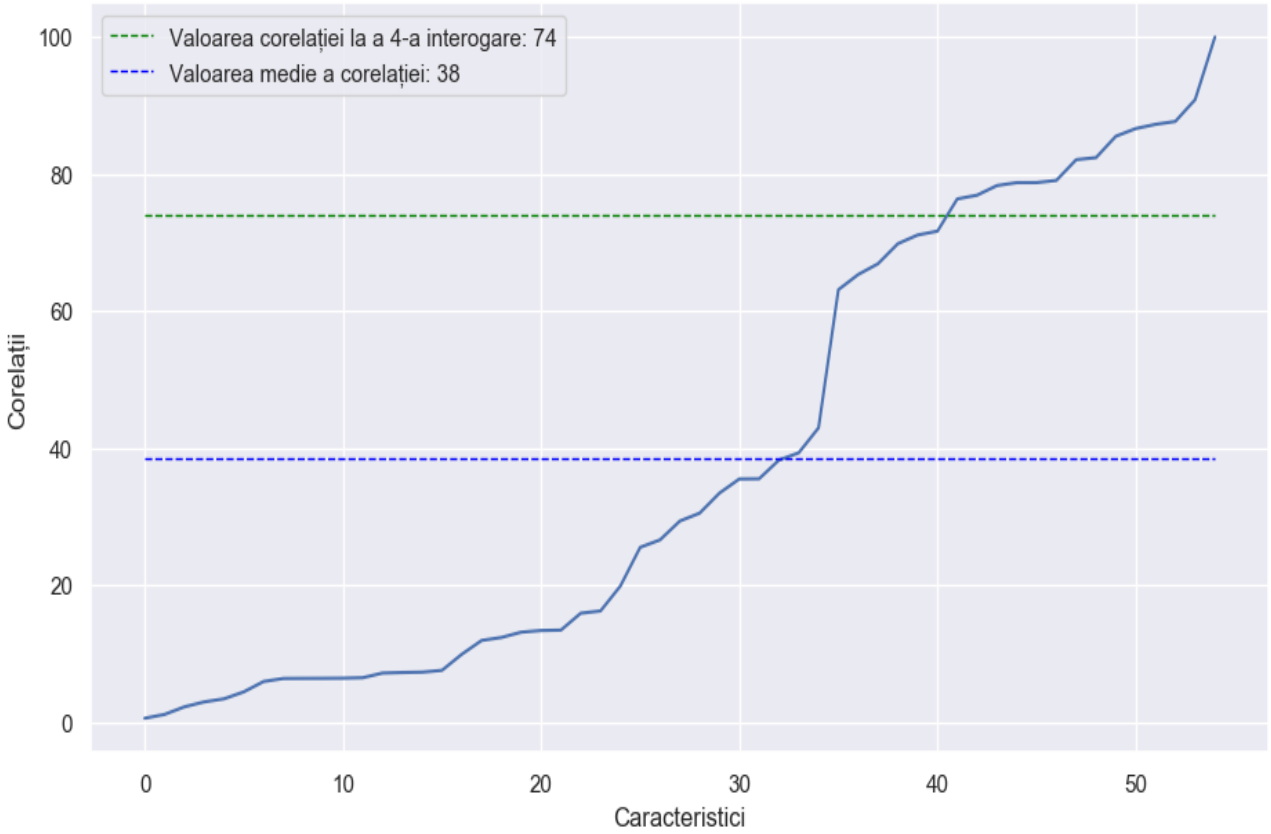


Figura 4 Graficul de corelație.

În plus, valorile atipice ale caracteristicilor pot influența semnificativ acuratețea unui model, după cum se poate observă în Figura 4. O metodă eficientă pentru minimizarea impactului valorilor atipice constă în aplicarea tehnicilor de trucare a distribuției valorilor, prin eliminarea celor care se situează în afara limitelor definite de setul de date al doilea și al treilea. Această abordare contribuie la îmbunătățirea robusteții modelului prin reducerea distorsiunilor cauzate de valorile extrem de neobișnuite, asigurând o analiză mai precisă și mai reprezentativă a setului de date (Figura 5). Prin intermediul graficelor de dispersie, diagramele de cutie sau histogramele, se pot vizualiza distribuția și variația caracteristicilor în contextul variabilei de interes, evidențiind astfel factorii cheie care contribuie la predicțiile modelului. Această abordare facilitează, de asemenea, detectarea posibilelor anomalii sau a valorilor atipice care ar putea distorsiona rezultatele analizei, permițând ajustări metodologice care îmbunătățesc acuratețea și fiabilitatea modelului.

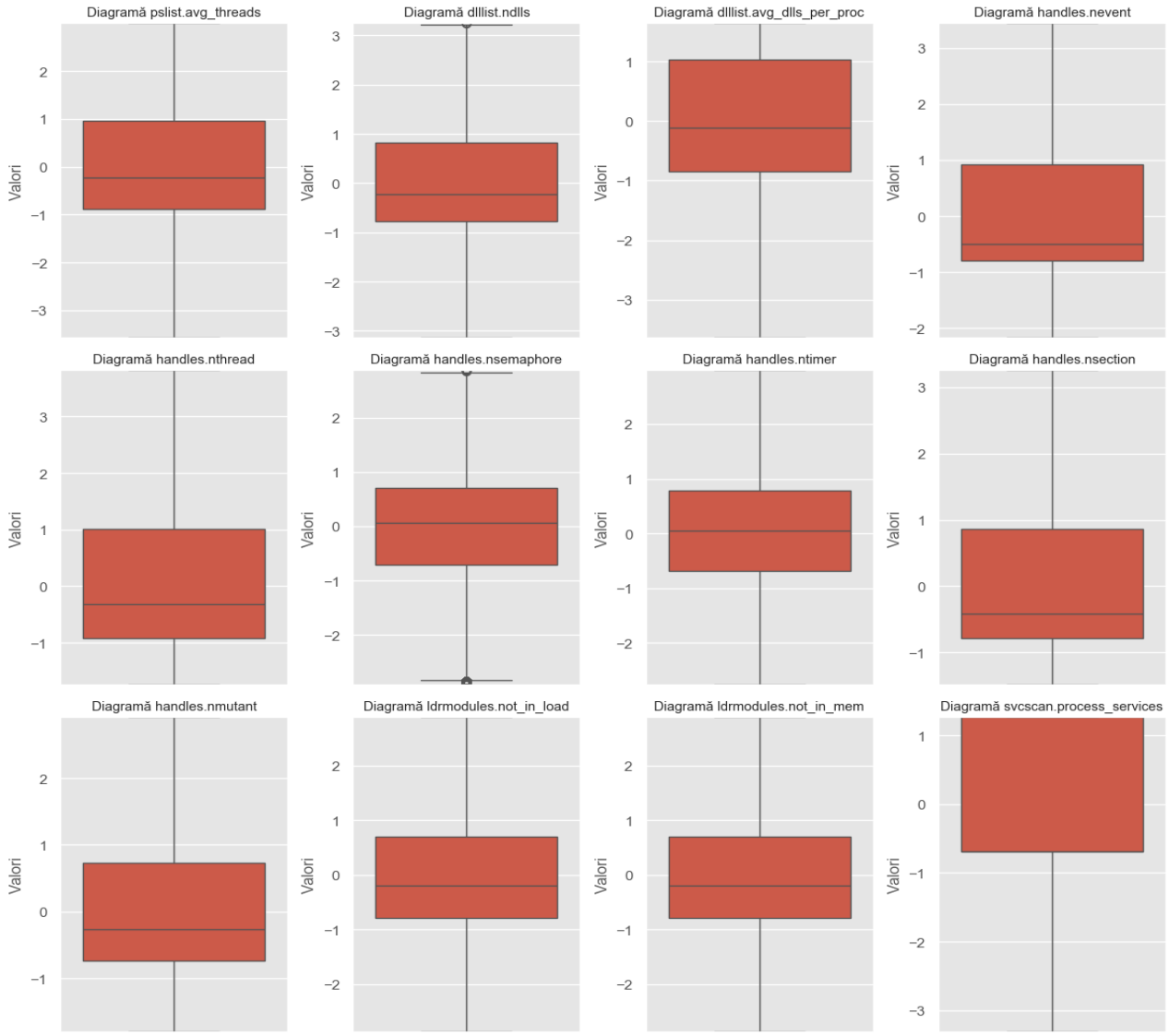


Figura 5 Diagrame specifice pentru caracteristicile selectate cu axe Y individuale.

De asemenea, analiza vizuală a distribuției caracteristicii etichetei țintă (Figura 6) în raport cu diversele caracteristici ale setului de date poate scoate în evidență relațiile de corelație și modelele de asociere existente. Această tehnică permite identificarea tendințelor și a legăturilor semnificative dintre variabila dependentă și variabilele independente, oferind astfel o perspectivă detaliată asupra modului în care diferitele caracteristici influențează comportamentul etichetei țintă.

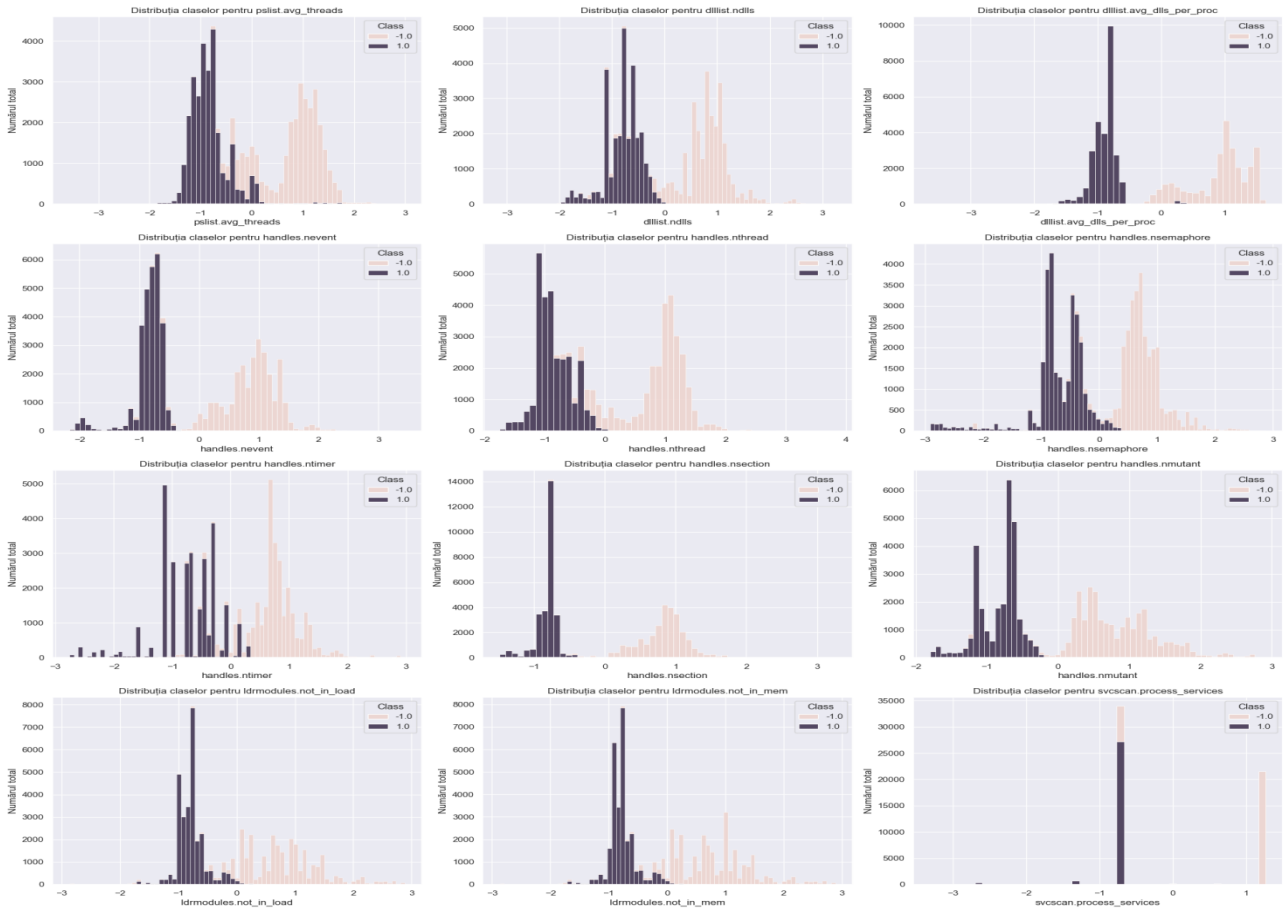


Figura 6 Distribuția caracteristicii etichetei țintă.

Scopul principal al modelului prezentat constă în evaluarea unui anumit ansamblu de valori, caracteristice ce reflectă activitatea rău-intenționată. Această evaluare se realizează eficient printr-o clasificare binară, care utilizează caracteristica „*Clasă*” (*activitate rău-intenționată sau benignă*) ca etichetă țintă. O investigație suplimentară poate fi efectuată pentru a pune caracteristicile în „*Categoria 1*” sau „*Categoria 2*” utilizând un model de clasificare multi-clasă, în scopul efectuării unor determinări mai detaliate, bazate pe categoria specifică a amenințării. *Modelele examinate pentru acest test și set de date includ:*

- Gaussian Bayes Naiv
- K-Vecini Cei Mai Apropiați
- Mașină cu Suport
- Arbore de Decizie
- Pădure Aleatoare

Scalarea Min-Max este aplicată pentru a normaliza valorile caracteristicilor într-un interval de la 0 la 1, menținând în același timp distribuția datelor (analog cu StandardScaler, utilizat anterior). Acest interval este bun pentru algoritmi precum *K-Vecini Cei Mai Apropiați*, care sunt sensibili la variațiile de distanță și nu gestionează eficient valorile negative. Datele sunt segmentate în 2 categorii: un set de antrenament, folosit pentru construirea modelului, și un set de test, utilizat pentru evaluarea performanței. Principala metrică de evaluare este acuratețea [21].

3.4 OPTIMIZAREA ALGORITMILOR DE ÎNVĂȚARE EXISTENȚI PRIN METODA PROPUSĂ

KNN

Această configurație a parametrilor explorează diferite opțiuni pentru numărul de vecini, tipurile de ponderare a voturilor și metricile de distanță, pentru a găsi cea mai bună configurație pentru modelul K-Nearest Neighbors. Modelul cel mai optim a fost detectat folosind funcția *GridSearch:* (KNNClassifier(metric='euclidian', n_neighbors=1)).

Naive Bayes Gaussian

Prin utilizarea *„var_smoothing": np.logspace(0,-9, num=100),* se specifică o secvență de 100 de valori logaritmice între 1 și 10^-9 pentru adăugarea de variație. Această abordare asigură că variația adăugată este suficient de mică pentru a nu distorsiona semnificativ estimările probabilităților, dar suficient de mare pentru a evita cazurile de probabilități zero.

Arborii de decizie

S-a folosit configurația parametrilor pentru căutarea în grilă „*GridSearch*" pentru evaluarea și ajustarea clasificatorului de arbori de decizie (*DecisionTreeClassifier*). A fost identificat cea mai bună combinație pentru clasificatorul de arbori de decizie. S-a determinat parametrul „*criterion*" ca fiind model optim. Acesta specifică modul în care calitatea împărțirii este măsurată, iar „*max_depth*" controlează adâncimea maximă a arborelui. În acest caz, arborele nu va avea mai mult de 9 niveluri de decizie.

Pădure Aleatoare

Configurația modelului RandomForest este definită cu *30 de estimatori* și o *adâncime maximă de 9 nivele* pentru fiecare arbore.

Maşina de Vectori de Suport

Efectuând o căutare de tip grilă „*GridSearchCV*" pe modelul SVM s-a constatat configurația cu cea mai bună performanță ca fiind *LinearSVC(C=0.0001, max_iter=10),* unde *parametrul C* controlează regularizarea, fiind un factor de penalizare pentru erorile de clasificare si *parametrul max_iter* specifică numărul maxim de iterații pentru convergența algoritmului de optimizare. În cazul dat, *max_iter=10* indică că algoritmul se oprește după 10 iterații.

3.5 CONCLUZII ȘI CONTRIBUȚII ORIGINALE

În acest capitol al tezei s-au prezentat dezvoltarea și evaluarea unei metodologii inovative, împreună cu un software specializat pentru clasificarea și detectarea secvențelor de cod rău intenționat, utilizând tehnici de învățare automată. S-a realizat un prototip software având ca obiectiv principal îmbunătățirea setului de date existent.

Ansamblul de date conceput pentru a evalua eficacitatea metodelor de detectare a acestor secvențe camuflate cu ajutorul analizei memoriei RAM (acest lucru implică căutarea de modele suspecte de comportament în cadrul proceselor în execuție, identificarea manipulărilor neautorizate ale datelor sau descoperirea activităților neobișnuite care pot indica prezența codului rău-intenționat) a fost elaborat astfel încât să reflecte cât mai fidel posibil scenarii din lumea reală, utilizând tipuri de software rău-intenționat frecvent întâlnite.

Pentru a mări acuratețea reprezentării comportamentului utilizatorului mediu în timpul unui atac, procesul de obținere a copiei a întregului conținut al memoriei utilizează modul de depanare (*din engleză, debug mode*), evitând astfel înregistrarea procesului de obținere a copiei memoriei în cadrul proceselor propriu-zise.

Printre contribuțiile esențiale ale cercetării din acest capitol, se identifică următoarele:

© Elaborarea unei metodologii de îmbunătățire a setului de date. A fost dezvoltată o abordare sistematică pentru îmbunătățire datelor existente, prin aplicarea tehnicilor de pre-procesare avansate, cum ar fi *„normalizarea prin scalarea Min-Max”* sau folosirea *„GridSearch*”. Aceasta a permis o analiză mai precisă și a îmbunătățit capacitatea de predicție a modelelor de învățare automată;

© Dezvoltarea unui software folosit pentru detecția secvențelor de cod răuvoitoare utilizând algoritmi de învățare automată, cum ar fi Gaussian Bayes Naiv, K-Vecini Cei Mai Apropiați, Mașina de Suport Vectorial, Arborele de Decizie și Pădurea Aleatoare. De asemenea**,** s-a demonstrat o eficacitate sporită în identificarea și clasificarea activităților potențial dăunătoare, în comparație cu abordările prezentate în alte lucrări de specialitate;

© Obținerea unor rezultate mai bune în comparație cu unele lucrări publicate.

Validarea rezultatelor

Rezultatele cercetării au fost diseminate, supuse unui proces de verificare și validate prin publicarea în articolele științifice enumerate mai jos:

- 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

Analiza detaliată, susținută de utilizarea matricei de confuzie a oferit o perspectivă clară asupra performanței reale a diferiților algoritmi testați, evidențiind eficacitatea acestora în detectarea precisă a amenințărilor informatice. În plus, cu ajutorul acestui studiu, s-a reușit identificarea provocărilor specifice legate de detectarea secvențelor de cod nelegitime. Comparativ cu alte metode de detectare, eficiența acestei abordări se distinge prin: *rata superioară de detectare, complexitatea redusă și eficiența în utilizarea resurselor de memorie*, poziționându-se astfel ca o

soluție avansată în combaterea amenințărilor cibernetice. Această analiză profundă subliniază importanța adaptării continue a tehnicilor de detectare la evoluția constantă a tacticilor adoptate de agenții rău-intenționați, asigurând protecția eficientă a datelor și a infrastructurilor critice. Rezultatele obținute, comparațiile efectuate și analiza detaliată a performanței sunt prezentate în **Figura 7**, **Figura 8** precum și în **Tabelul 2**:

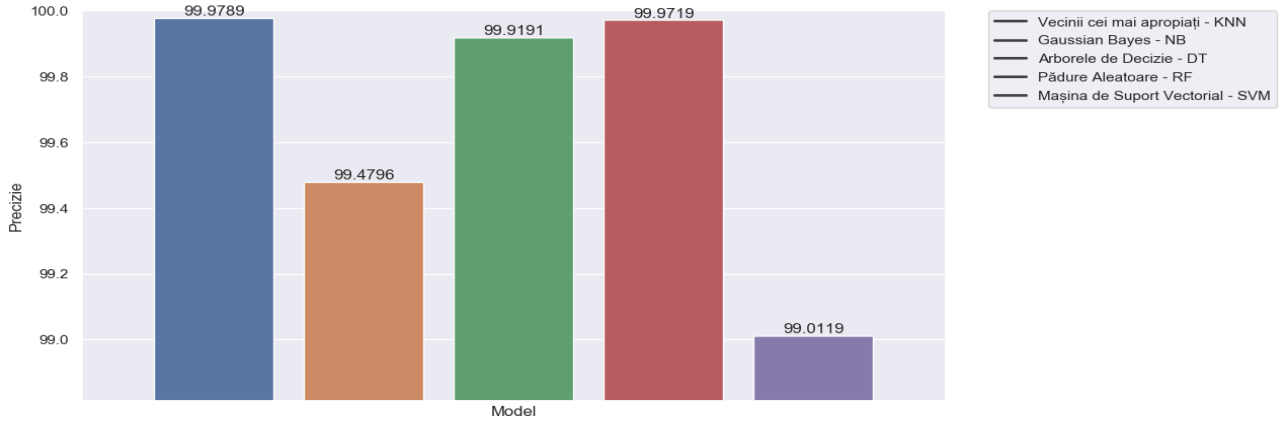


Figura 7 Analiza performanței modelelor evaluate: Rezultatele Evaluării.

	Model	Raport Test	Acuratețe	Precizie	Recuperare	Scor F1	TN	FN	FP	TP
0	Vecinii cei mai apropiați - KNN	0.50	99.98	99.98	99.98	99.98	14329	3	3	14102
1	Gaussian Bayes - NB	0.50	99.48	99.48	99.48	99.48	14245	61	87	14044
2	Arborele de Decizie - DT	0.50	99.92	99.92	99.92	99.92	14319	10	13	14095
3	Pădure Aleatoare - RF	0.50	99.96	99.96	99.96	99.96	14328	7	4	14098
4	Mașina de Suport Vectorial - SVM	0.50	99.01	99.02	99.01	99.01	14113	62	219	14043

Figura 8 Rezultatele testului efectuat folosind setul de date MalMem.

Pentru Figura 36, reprezentările pentru TN, FN, FP și TP sunt ilustrate mai de jos:

- Adevărat Negativ (TN) - cazuri prezise ca benigne, fiind în realitate rău-intenționate;
- Fals Negativ (FN) - cazuri prezise ca benigne, deși sunt rău-intenționate;
- Fals Pozitiv (FP) - cazuri prezise ca rău-intenționate, fiind de fapt benigne;
- Adevărat Pozitiv (TP) - cazuri prezise corect ca rău-intenționate.

Tabelul 2 - Tabel cu analiza comparativă a metodelor de detectare și clasificare a programelor răuvoitoare

Metoda	Acuratețe	Complexitate	Precizie
Metoda propusă	Foarte ridicată	Medie	Foarte ridicată
Carrier et al, 2022	Ridicată	Medie	Ridicată
Dener et al, 2022	Foarte ridicată	Ridicată	Foarte ridicată
Nissima et al, 2019	Ridicată	Medie	Medie

4 SECURITATEA DEFENSIVĂ: DETECȚIA ȘI RĂSPUNSUL AUTOMATIZAT LA AMENINȚĂRI DE SECURITATE CIBERNETICĂ

4.1 AUTOMATIZAREA RĂSPUNSULUI LA AMENINȚĂRILE CIBERNETICE

Scopul acestei secțiuni este dezvoltarea și implementarea unui sistem complet funcțional pentru monitorizarea, detectarea și protecția împotriva secvențelor de cod rău intenționate, utilizând software-uri gratuite (open-source), astfel încât să funcționeze ca un sistem modern, scalabil, gratuit folosit pentru răspunsul la incidente de securitate și securizarea rețelelor interne, dezvoltat pentru sprijinul personalului din cadrul departamentului informatic dintr-o companie/instituție pentru investigațiile de securitate. Sistemul de răspuns la incidente este automatizat pentru a analiza alerte specifice, ajutând specialistul/persoana desemnată să le urmărească și să le remedieze [22].

Rezultatul acestui proiect este un sistem-prototip de tip open-source, complet funcțional și scalabil dezvoltat într-un mediu stabil de cercetare, utilizând module precum SIEM (eng. Security Information and Event Management - Managementul Informațiilor de Securitate și al Evenimentelor), IAM (eng. Identity and Access Management - Managementul Identității și Accesului), inteligența amenințărilor (eng. Threat Intelligence), vânătoarea de amenințări (eng. Threat Hunting), DFIR (eng. Digital Forensics and Incident Response - Răspuns la Incidente și analiză detaliată), managementul vulnerabilităților (eng. Vulnerability Management), monitorizare, SOAR (eng. Security Orchestration, Automation and Response - Orchestarea Securității, Automatizare și Răspuns), modulul de securitate a rețelei (eng. Network Security Module), folosirea sistemelor tip firewall, salvarea datelor (eng. backup).

4.2 COMPARAȚIA SISTEMULUI PROPUS CU SISTEMELE CURENTE DE GESTIONARE A INCIDENTELOR DE SECURITATE

Evaluarea sistemelor curente de gestionare a incidentelor de securitate, abordează o analiză a modalităților prin care organizațiile identifică, răspund și recuperează în urma incidentelor de securitate. Această evaluare este esențială în contextul în care amenințările cibernetice devin din ce în ce mai sofisticate, iar capacitatea de a gestiona eficient aceste incidente poate face diferența între un răspuns rapid și eficace și unul care lasă organizația vulnerabilă la atacuri suplimentare sau la pierderi semnificative.

Evaluarea sistemelor actuale de gestionare a incidentelor evidențiază importanța unei abordări integrate, care să cuprindă proceduri bine stabilite și o cultură organizațională care prioritizează securitatea cibernetică. În Tabelul 3 sunt prezentate soluțiile comerciale de răspuns la incidente în comparație cu sistemul propus:

Tabelul 3 - Sistemele actuale de gestionare a incidentelor de securitate.

Numele sistemului	Automatizarea răspunsurilor la incidente	Integrarea cu alte sisteme	Seturi de proceduri, instrucțiuni	Detectarea atacurilor sofisticate	Managementul vulnerabilităților	Sistem identitate access	Sistem de tip Backup	Modularitate
Sistemul propus (AuraSec)	Da	Da	Da	Da	Da	Da	Da	Da
OpenEDR Xcitium	Nu	Nu	Da	Da	Nu	Nu	Nu	Nu
Bitdefender MDR	Da	Nu	Da	Da	Nu	Nu	Nu	Nu
CrowdStrike Falcon	Da	Da	Da	Da	Nu	Nu	Nu	Nu
Karspersky EDR	Da	Nu	Da	Da	Nu	Nu	Nu	Nu

După cum se poate observa în Tabelul 3, soluția propusă în cadrul cercetării doctorale (denumită și AuraSec) se deosebește în mod semnificativ de celelalte soluții enumerate prin următoarele caracteristici distincte:

- *Modularitate:* Soluția este proiectată într-o manieră modulară, permițând adăugarea, eliminarea sau modificarea componentelor (SIEM, SOAR, Firewall, MDR, etc.) fără a afecta funcționalitatea generală. Această caracteristică oferă flexibilitate și scalabilitate, facilitând adaptarea rapidă la nevoile și cerințele în schimbare ale organizației sau proiectului;
- *Sistem integrat pentru salvarea datelor (backup periodic):* Soluția include un sistem integrat și automatizat pentru backup-ul periodic al datelor, asigurând protecția continuă a informațiilor critice. Acest sistem reduce riscul pierderii datelor în cazul unor incidente neprevăzute, cum ar fi atacurile cibernetice, erorile de sistem sau dezastrele naturale, garantând astfel continuitatea activităților;
- *Sistem de identitate și acces:* Implementarea unui sistem de gestionare a identității și accesului (IAM - Identity and Access Management) este o altă caracteristică distinctivă. Acesta permite controlul strict al accesului utilizatorilor la resursele și informațiile sensibile, bazat pe roluri și permisiuni bine definite;
- *Managementul vulnerabilităților:* Soluția propusă include un sistem integrat de management al vulnerabilităților, care identifică, evaluează și remediază vulnerabilitățile de securitate într-un mod proactiv;
- *Pre-configurarea seturilor de proceduri, instrucțiuni sau acțiuni predefinite pentru răspunsul la incidente:* Soluția include seturi pre-configurate de proceduri, instrucțiuni și acțiuni predefinite pentru gestionarea eficientă a incidentelor de securitate.

4.3 Dezvoltarea și implementarea sistemului pentru răspuns la incidente și detectarea secvențelor răuvoitoare

În epoca actuală, asistăm la o proliferare marcantă a utilizării tehnologiilor informaționale, care pătrunde în toate domeniile activității umane. Prin integrarea tehnologiilor existente și dezvoltarea de componente noi, personalizate, se urmărește realizarea unei soluții autonome capabile să răspundă provocărilor din ce în ce mai complexe din domeniul securității cibernetice, contribuind astfel la îmbunătățirea gradului de securitate pentru toți utilizatorii și entitățile care adoptă această abordare.

Sistemul propus a fost configurat folosind tehnologia Docker, care facilitează virtualizarea și implementarea flexibilă în diverse infrastructuri, fie ele Cloud sau Locale (eng. On-Premise). Cu excepția Cuckoo Sandbox, a cărei integrare folosind Docker, se confruntă cu provocări tehnice majore, fiind considerată aproape imposibilă, toate componentele sistemului au fost optimizate pentru funcționarea într-un mediu securizat [23].

Pentru gestionarea containerelor, a fost adoptată soluția denumită Docker Portainer. Docker Portainer (eng. Docker Portainer) este o interfață grafică ușor de utilizat, care permite administrarea simplă și eficientă a containerelor Docker, oferind vizibilitate și control asupra infrastructurii Docker, fără a necesita cunoștințe avansate de linie de comandă. În Figura 9 sunt evidențiate sistemele utilizate în componența sistemului principal:

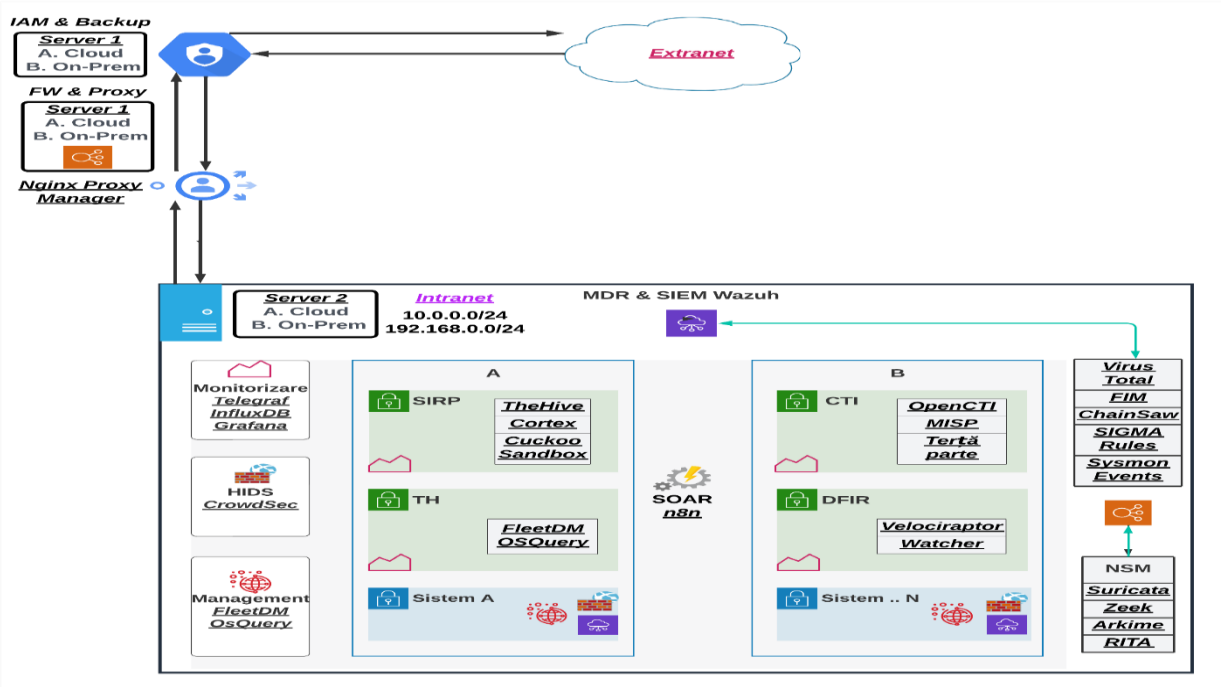


Figura 9 Diagrama sistemului propus pentru răspunsul la incidente, managementul accesului la identitate și salvarea datelor.

În etapa de dezvoltare a sistemului propus au fost implementate modulele și tehnologiile ce se pot observa in Figura 9, pentru gestionarea răspunsului la incidente de securitate și monitorizarea evenimentelor:

4.4 REZULTATE ȘI OBSERVAȚII

Pentru a analiza și testa soluția prezentată, s-au utilizat secvențe de cod rău intenționate, provenite din mediul real, care vizează rețelele și serviciile active. S-a utilizat un mediu virtual ce permite execuția controlată a acestor secvențe nelegitime în scopuri de testare/validare, utilizând servicii comune precum *Domain Name Service (DNS) sau Simple Mail Transfer Protocol (SMTP).* Mostrele de secvențe de cod rău intenționate au fost procurate din surse deschise, inclusiv site-uri de internet specializate în găzduirea acestor mostre nelegitime și pagini personale de GitHub sau institute educaționale ce oferă astfel de mostre în scopuri academice. Autenticitatea și validitatea acestor mostre au fost verificate folosind sistemul conceput în cadrul acestei cercetări. Baze de

date online renumite cum ar fi Malware Bazaar sau Malware Hash Registry, au fost folosite ca referințe în procesul de validare. Înaintea descărcării sau transferului oricăror colecții de date nelegitime în sistem, s-a asigurat implementarea unor măsuri cuprinzătoare de izolare în cadrul mediului. Aceasta a implicat proiectarea unei soluții capabile să detecteze și să analizeze fișierele și resursele de rețea infectate, servind ca un prototip pentru criminalitatea digitală și securitatea sistemelor. Soluția propusă demonstrează abilitatea de a efectua procese esențiale care ajută la analiza fișierelor infectate, oferind în același timp capacități de detecție și de răspuns rapid la incidente. În vederea testării sistemului propus, s-a implementat următorul procedeu-flux pentru analiza secvențelor potențial răuvoitoare:

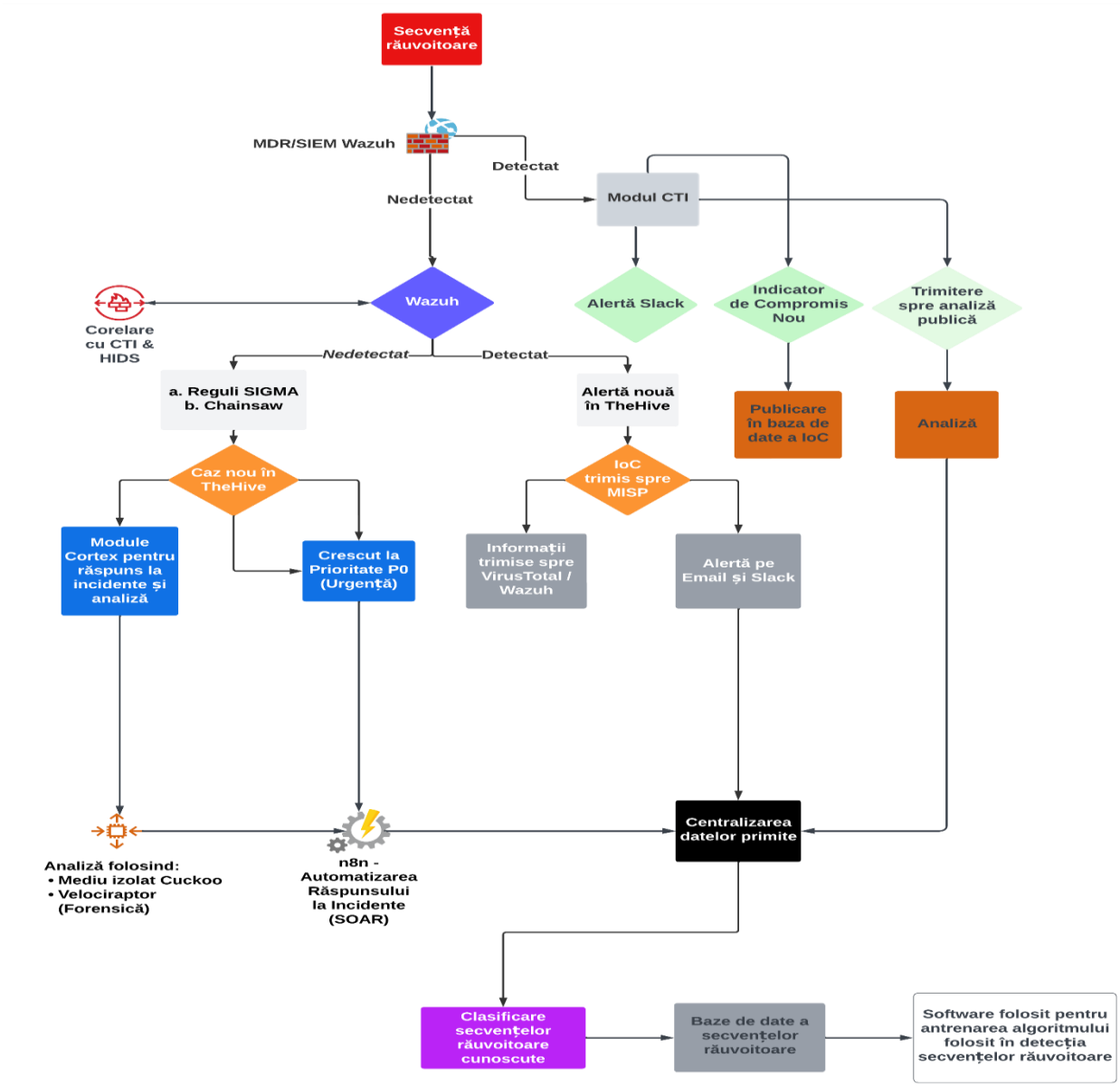


Figura 10 Procesul de detectare a secvențelor răuvoitoare.

Pentru facilitarea testării, s-a configurat o mașină virtuală folosind sistemul de operare: Windows 10. Agenți precum CrowdSec, Wazuh, FleetDM și Velociraptor, proveniți din module open source, au fost instalați pe un sistem Windows 10 izolat (virtualizat); acești agenți

monitorizează activitățile sistemului, detectează și raportează comportamentele anormale, comunicând înapoi către aplicația centrală pentru analiza și corelarea datelor obținute. Prototipul a fost inițiat doar după ce soluția operațională a fost evaluată ca fiind pregătită să gestioneze instalarea activă a mostrelor de secvențe de cod rău intenționate.

Pentru a testa și valida prototipul dezvoltat, au fost implementate *3* scenarii reale în care s-a urmărit confirmarea eficienței sistemului propus în fața amenințărilor cibernetice:

a) Primul caz pentru testarea prototipului studiat este bazat pe tehnica de ocolire a *Interfeței de Scanare Anti-Malware* de la Microsoft (eng. AMSI) utilizând procesul de captare a apelurilor către funcții sau evenimente dintr-un program (eng. Hooking-ul) apelurilor API ale metodelor CLR (eng. Common Language Runtime) este un mediu de execuție pentru programele scrise în limbajele .NET, care gestionează execuția codului, gestionarea memoriei, gestionarea excepțiilor și alte aspecte ale aplicațiilor .NET.

Așa cum se ilustrează în Figura 11, atunci când a fost declanșată funcția „Invoke-Mimikatz", scriptul a fost identificat de Antivirusul Microsoft Defender, indicând capacitatea de a ocoli controalele AMSI. Această observație servește drept dovadă a potențialului de a eluda măsurile de securitate standard bazate pe AMSI oferite de Antivirusul Microsoft Defender.

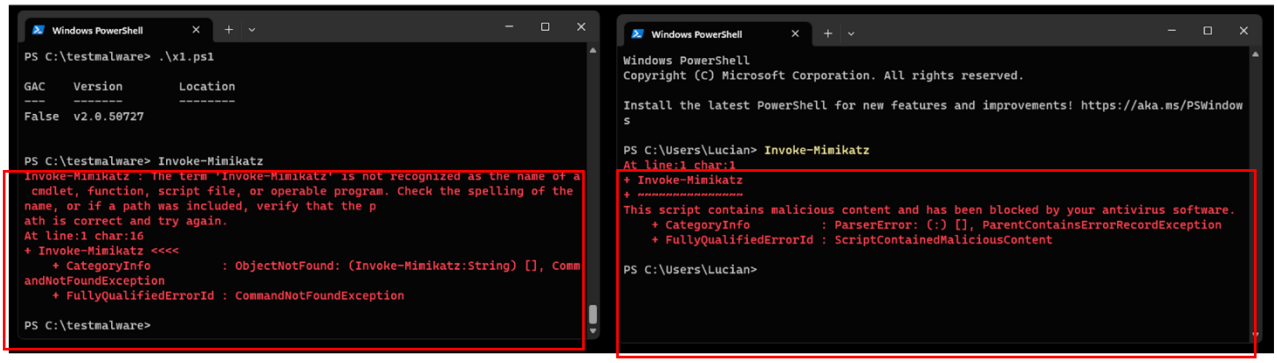


Figura 11 Software-ul folosit pentru ocolirea sistemului antivirus.

Figura 12 prezintă alerta generată de Wazuh, soluția de detectare și răspuns gestionat, precum și de managementul informațiilor și evenimentelor de securitate precum și integrarea sa fără probleme cu platforma de răspuns la incidente, TheHive, utilizând sistemul de orchestrare, automatizare și răspuns în materie de securitate - n8n. La primirea alertei, TheHive inițiază prompt crearea unui caz nou. Această integrare între Wazuh și TheHive facilitează un răspuns eficient la incidente și simplifică gestionarea evenimentelor de securitate într-o manieră optimizată [24].

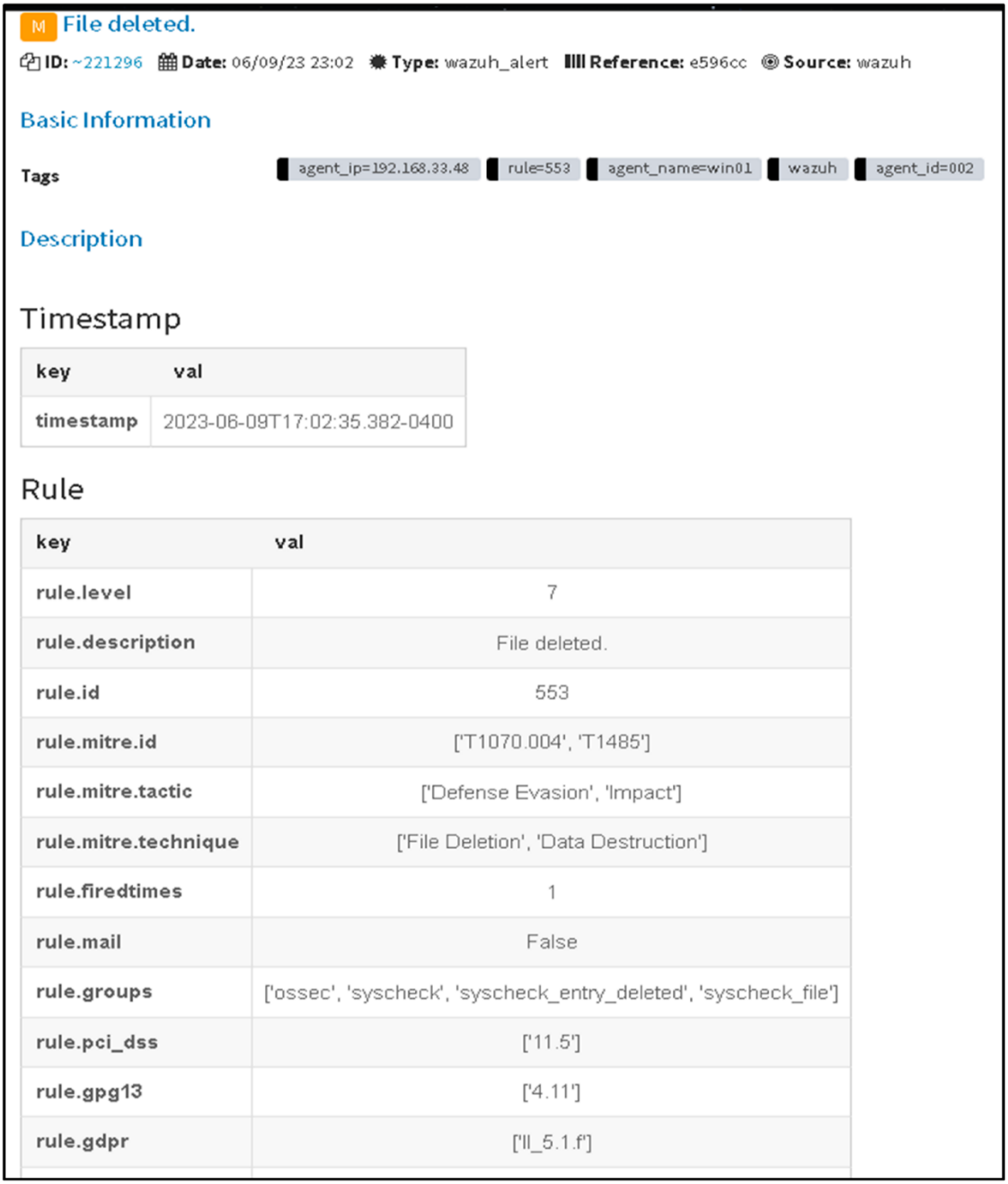


Figura 12 Demonstrarea detectării fișierului suspect.

Așa cum este ilustrat în Figura 13, se remarcă un aspect notabil din fluxul incidentului, prin care Wazuh, platforma de monitorizare a securității, a generat eficient o alertă și ulterior, a transmis-o către platforma Slack cu ajutorul webhook-urilor (eng. webhook - o metodă prin care o aplicație web poate trimite automat informații în altă aplicație web în timp real). O regulă în Wazuh a fost configurată pentru a se conecta cu ajutorul Cuckoo Sandbox. Această regulă va fi declanșată ori de câte ori un fișier este identificat ca fiind rău intenționat de către Wazuh. Până la detectare, regula a folosit informațiile MD5 și SHA256 din hash-urile fișierului și a fost trimisă către Cuckoo Sandbox pentru o scanare și analiză completă.

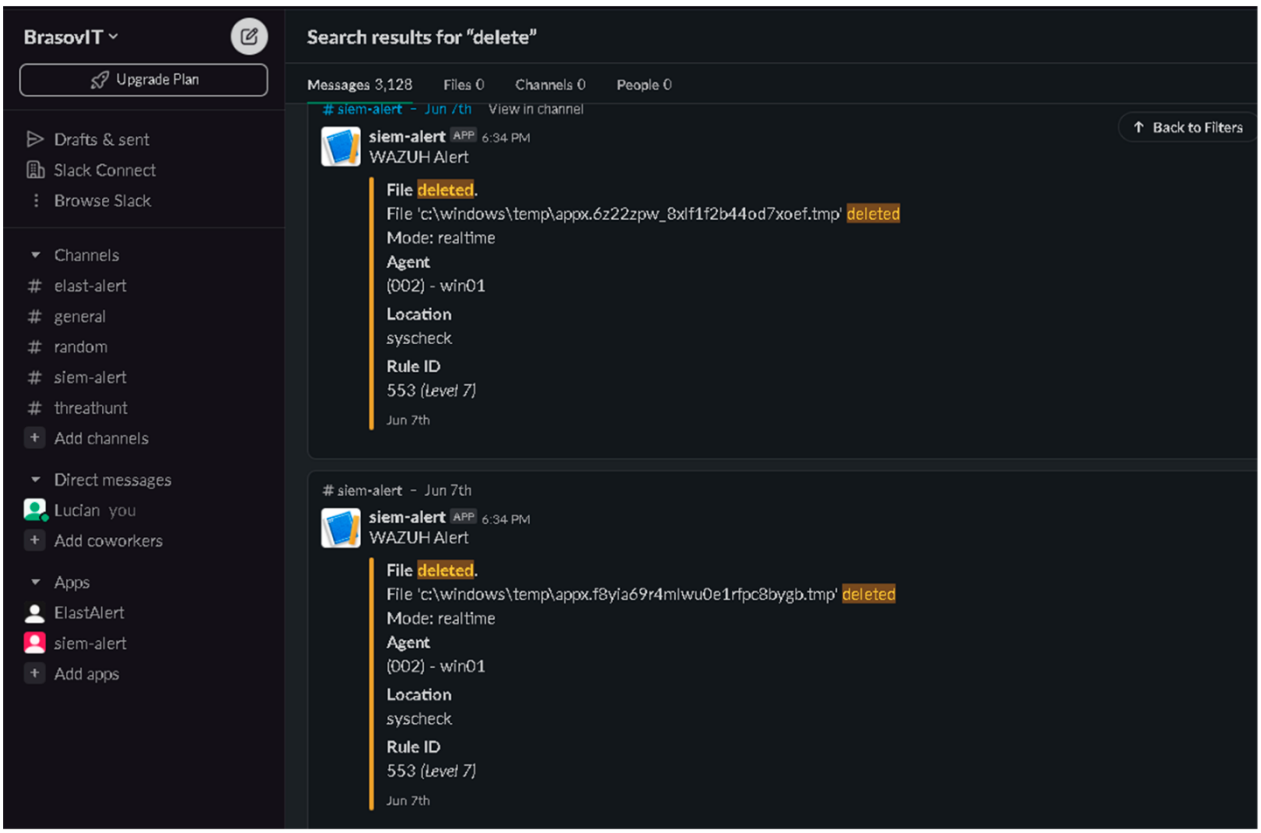


Figura 13 Utilizarea sistemului Slack pentru notificarea administratorilor despre un incident de securitate nou.

b) **Cazul cu numărul 2** propus pentru validarea sistemului/prototipului dezvoltat este reprezentat de utilizarea unui script pentru sustragerea datelor. Acest script utilizează Mimikatz 2.0 (Mimikatz este un instrument de software liber dezvoltat inițial pentru a testa vulnerabilitățile de securitate în sistemele Windows. Este cunoscut pentru capacitatea sa de a extrage parole, chei de autentificare și alte tipuri de credențiale din memoria sistemelor Windows fiind adoptat pe scară largă de actorii de amenințări pentru a facilita atacurile cibernetice, ceea ce îl face un subiect important de studiu în domeniul securității cibernetice) și metoda Invoke-ReflectivePEInjection (tehnică folosită în domeniul securității cibernetice și al testării de penetrare, care permite încărcarea și executarea unui fișier executabil Portable Executable (PE) în memoria unui proces fără a-l scrie pe disc.

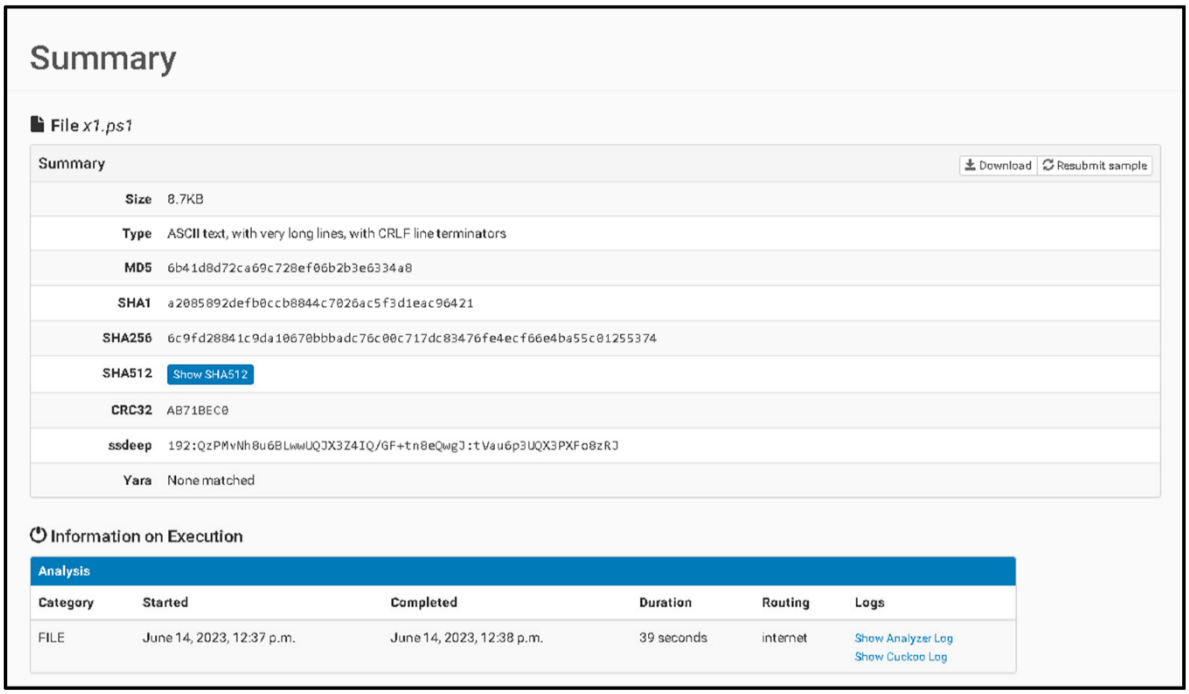


Figura 14 Interacțiunea Wazuh și n8n în analiza secvențelor răuvoitoare folosind Cuckoo Sandbox.

Informațiile furnizate ilustrează informațiile colectate din platforma Cuckoo Sandbox, care prezintă informații legate de o secvență răuvoitoare detectată anterior.

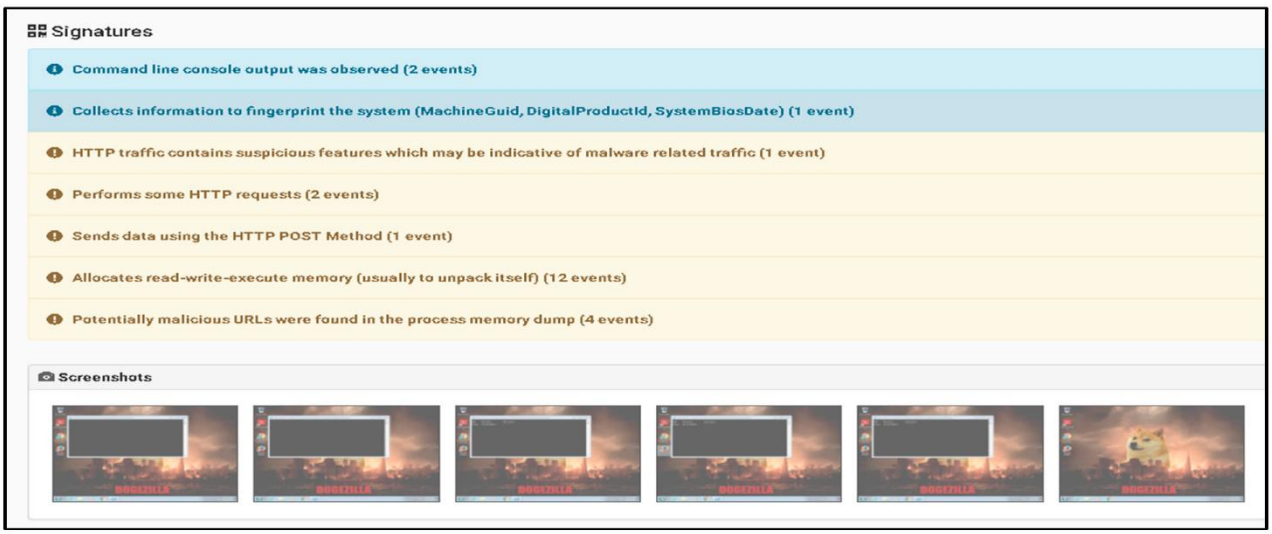


Figura 15 Informații colectate de la Cuckoo Sandbox despre secvența răuvoitoare detectată.

În Figura 16, informațiile prezentate ilustrează scorul atribuit de mediul de testare Cuckoo Sandbox fișierului potențial rău voitor care are un scor ridicat (7.4) din 10, unde 10 reprezintă scorul maxim (fișier răuvoitor 100%). Jurnalul complet din sistemul Wazuh demonstrează că secvența de cod rău intenționată a fost ștearsă din sistem. Utilizarea mai multor tehnici de verificare și răspunsuri active împotriva posibilelor noi amenințări asigură un răspuns rapid la incidente împotriva tuturor amenințărilor emergente.

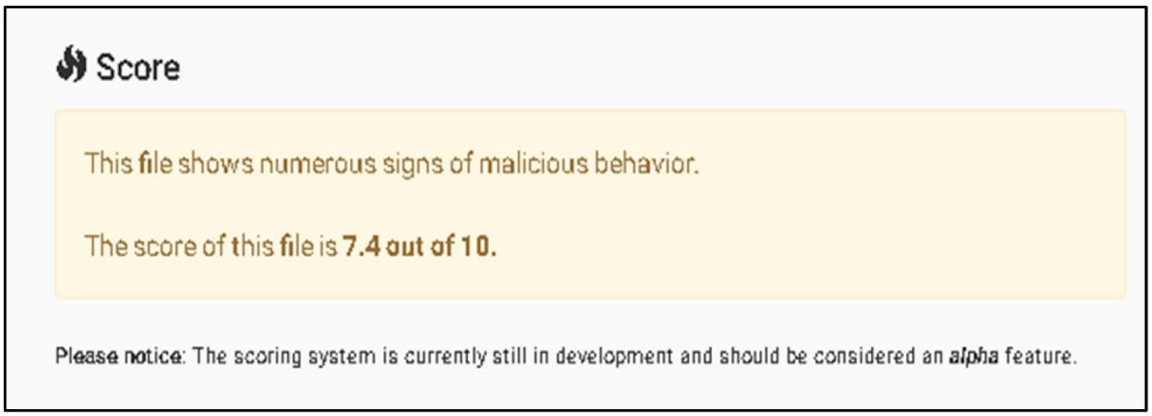


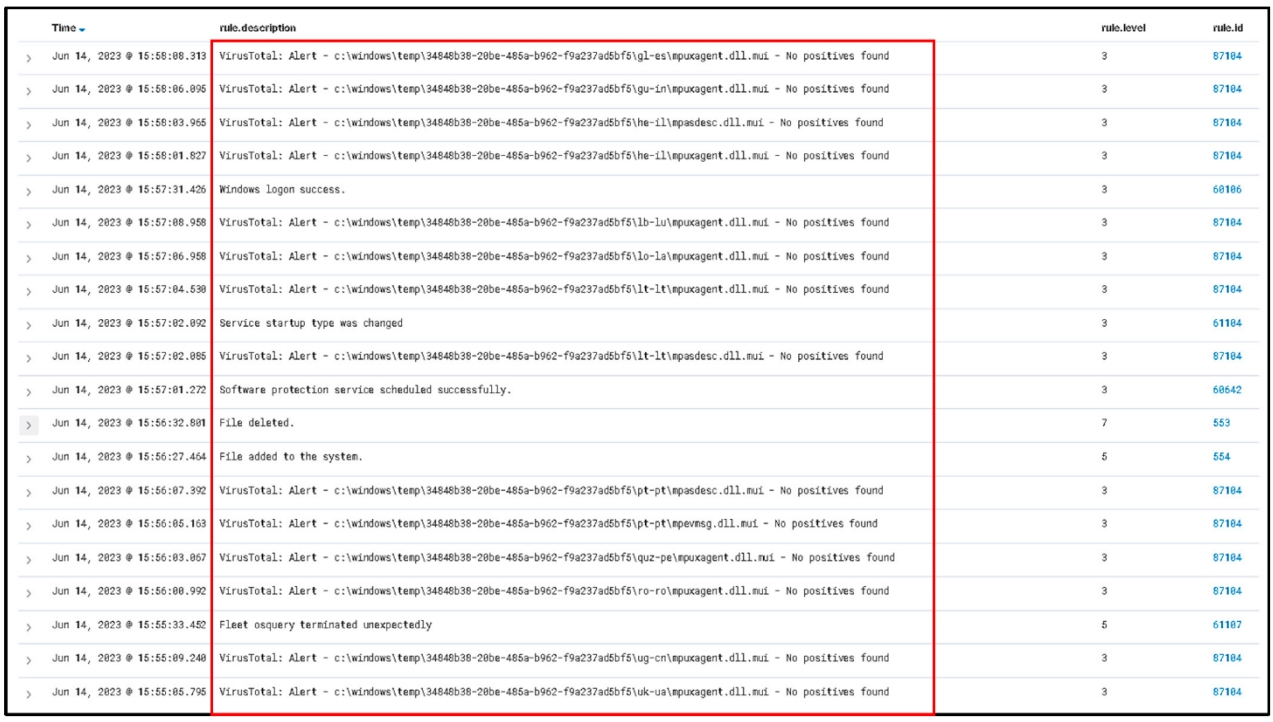
Figura 16 Scorul atribuit Fișierului suspect analizat de sistemul (mediul de test dinamic) Cuckoo Sandbox.

Figura 17 scoate în evidență observația importantă că sistemul Wazuh a îndepărtat cu succes secvență rău intenționată din sistemul de test. Această acțiune reușită demonstrează eficacitatea soluției propuse în abordarea și eliminarea promptă a potențialelor amenințări de securitate. Capacitatea sistemului propus de a detecta și elimina problemele identificate susține în continuare robustețea soluției implementate în atenuarea riscurilor și menținerea unui mediu securizat.

Figura 17 Procedura de neutralizare și eliminare a amenințărilor folosită de sistemul propus.

c) Cazul cu numărul 3 a fost validat utilizând o secvență de cod rău intenționată cunoscută sub denumirea de Qakbot sau Qbot, un troian bancar destinat atacului tuturor sistemelor Windows. Această secvență de cod rău intenționată este proiectată să fure credențiale bancare și alte tipuri de informații sensibile, extinzându-și funcționalitatea pentru a include capacitatea de a livra alte tipuri de secvențe rău intenționate.

Prin combinarea capabilităților, Chainsaw este folosit pentru filtrarea și identificarea preliminară a indicilor de compromis cu analiza aprofundată realizată cu ajutorul Cuckoo Sandbox, după cum se poate observa în Figura 18:



Time	rule.description	rule.level	rule.id
Jun 14, 2023 @ 15:58:08.313	VirusTotal: Alert - c:\windows\temp\34848b38-20be-485a-b962-f9a237ad5bf5\gl-es\mpuxagent.dll.mui - No positives found	3	87104
Jun 14, 2023 @ 15:58:06.095	VirusTotal: Alert - c:\windows\temp\34848b38-20be-485a-b962-f9a237ad5bf5\gu-in\mpuxagent.dll.mui - No positives found	3	87104
Jun 14, 2023 @ 15:58:03.965	VirusTotal: Alert - c:\windows\temp\34848b38-20be-485a-b962-f9a237ad5bf5\he-il\mpasdesc.dll.mui - No positives found	3	87104
Jun 14, 2023 @ 15:58:01.827	VirusTotal: Alert - c:\windows\temp\34848b38-20be-485a-b962-f9a237ad5bf5\he-il\mpuxagent.dll.mui - No positives found	3	87104
Jun 14, 2023 @ 15:57:31.426	Windows logon success.	3	60106
Jun 14, 2023 @ 15:57:08.958	VirusTotal: Alert - c:\windows\temp\34848b38-20be-485a-b962-f9a237ad5bf5\lb-lu\mpuxagent.dll.mui - No positives found	3	87104
Jun 14, 2023 @ 15:57:06.958	VirusTotal: Alert - c:\windows\temp\34848b38-20be-485a-b962-f9a237ad5bf5\lo-la\mpuxagent.dll.mui - No positives found	3	87104
Jun 14, 2023 @ 15:57:04.530	VirusTotal: Alert - c:\windows\temp\34848b38-20be-485a-b962-f9a237ad5bf5\lt-lt\mpuxagent.dll.mui - No positives found	3	87104
Jun 14, 2023 @ 15:57:02.092	Service startup type was changed	3	61104
Jun 14, 2023 @ 15:57:02.085	VirusTotal: Alert - c:\windows\temp\34848b38-20be-485a-b962-f9a237ad5bf5\lt-lt\mpasdesc.dll.mui - No positives found	3	87104
Jun 14, 2023 @ 15:57:01.272	Software protection service scheduled successfully.	3	60642
Jun 14, 2023 @ 15:56:32.801	File deleted.	7	553
Jun 14, 2023 @ 15:56:27.464	File added to the system.	5	554
Jun 14, 2023 @ 15:56:07.392	VirusTotal: Alert - c:\windows\temp\34848b38-20be-485a-b962-f9a237ad5bf5\pt-pt\mpasdesc.dll.mui - No positives found	3	87104
Jun 14, 2023 @ 15:56:05.163	VirusTotal: Alert - c:\windows\temp\34848b38-20be-485a-b962-f9a237ad5bf5\pt-pt\mpevmsg.dll.mui - No positives found	3	87104
Jun 14, 2023 @ 15:56:03.067	VirusTotal: Alert - c:\windows\temp\34848b38-20be-485a-b962-f9a237ad5bf5\quz-pe\mpuxagent.dll.mui - No positives found	3	87104
Jun 14, 2023 @ 15:56:00.992	VirusTotal: Alert - c:\windows\temp\34848b38-20be-485a-b962-f9a237ad5bf5\ro-ro\mpuxagent.dll.mui - No positives found	3	87104
Jun 14, 2023 @ 15:55:33.452	Fleet osquery terminated unexpectedly	5	61107
Jun 14, 2023 @ 15:55:09.240	VirusTotal: Alert - c:\windows\temp\34848b38-20be-485a-b962-f9a237ad5bf5\ug-cn\mpuxagent.dll.mui - No positives found	3	87104
Jun 14, 2023 @ 15:55:05.795	VirusTotal: Alert - c:\windows\temp\34848b38-20be-485a-b962-f9a237ad5bf5\uk-ua\mpuxagent.dll.mui - No positives found	3	87104

Figura 18 Eliminarea secvenței de cod rău intenționată folosind Chainsaw, regulile SIGMA și analiza dinamică.

În contextul analizei competitive efectuate după modelul graficului Quadrant Gartner (Figura 19), explorăm poziționarea diferitelor soluții software de securitate, în raport cu Soluția Propusă. Această abordare identifică punctele forte și oportunitățile de îmbunătățire, oferind o perspectivă clară asupra locului ocupat de prototipul denumit AuraSec în peisajul actual al soluțiilor de securitate.

Prototipul AuraSec este poziționat în apropiere de secțiunea inovatori deoarece indica o puternică orientare spre inovație și adaptabilitate. Poziționarea sa sugerează că oferă funcționalități originale care o disting de concurență, având potențialul de a defini sau de a redefini standardele în domeniul său.

Bitdefender și CrowdStrike (Lideri de Piață) - Aceste soluții sunt plasate aproape de axa Specialiști de Nișă, indicând un standard în piață și recunoașterea valorii lor constante. Ele sunt recunoscute pentru eficacitatea lor în execuție și pentru viziunea strategică, dar și pentru capacitatea de a răspunde eficient la nevoile actuale ale clienților. Plasarea lor sugerează că, deși sunt lideri, încorporează și elemente de specializare care le fac relevante pentru segmente specifice de piață.

Kaspersky (Pretendenți) - se implică o orientare puternică către îmbunătățirea capacității de execuție și a viziunii strategice. Această poziționare ar putea reflecta provocări în a ține pasul cu inovațiile sau nevoia de a își ajusta strategiile pentru a atinge performanțe mai înalte.

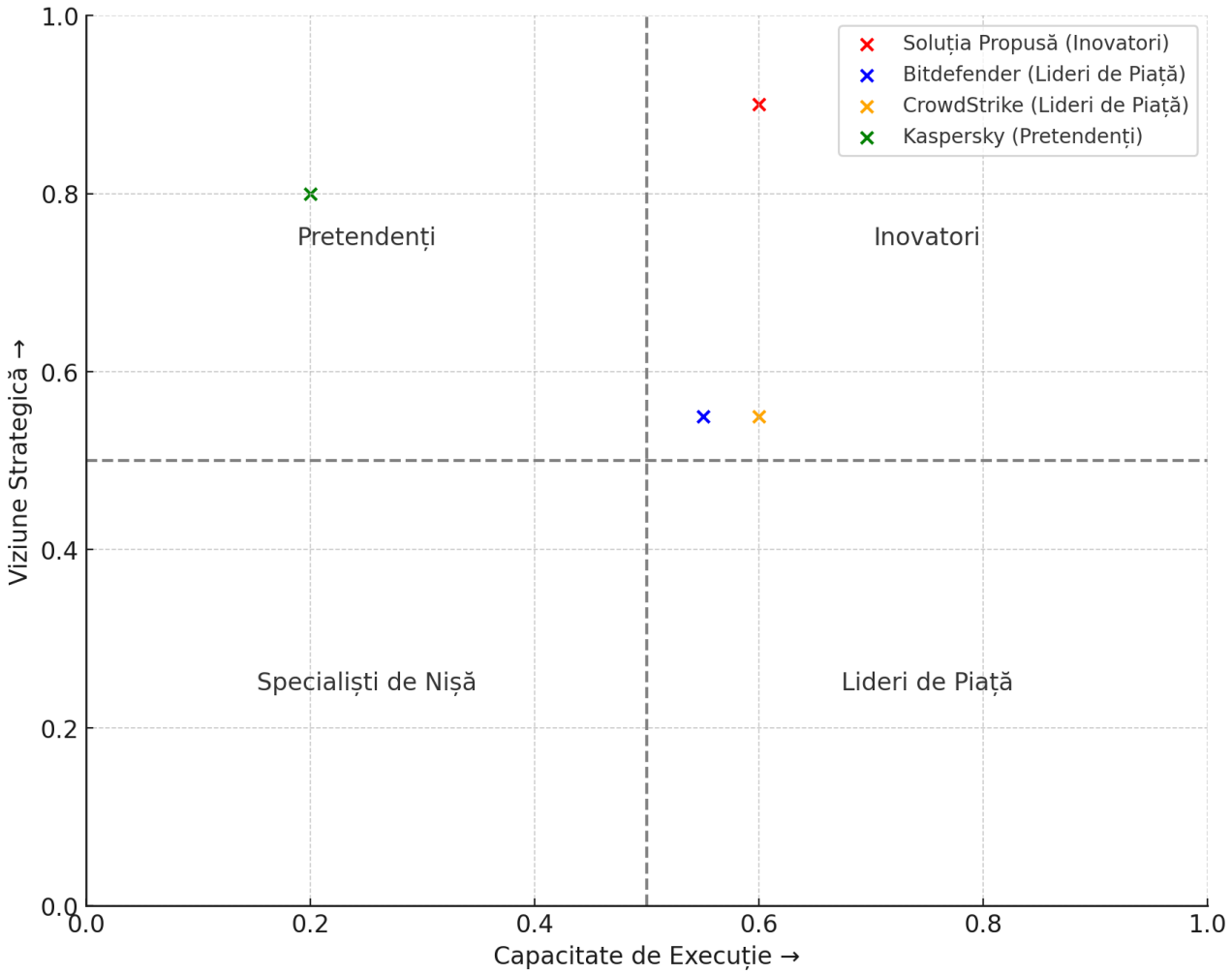


Figura 19 Cadranul generat folosind analiza comparativă a sistemelor software antivirus

De asemenea în Figura 20 se poate observa că soluția propusă demonstrează un timp de reacție impresionant, fiind mai rapidă decât majoritatea soluțiilor testate. Acest aspect important în domeniul securității cibernetice este diferențiator, unde, fiecare secundă contează în detectarea și neutralizarea amenințărilor. Pe lângă performanța remarcabilă în ceea ce privește timpul de răspuns, sistemul se distinge prin capacitatea sa excepțională de a se integra cu un număr mare de alte soluții de securitate. Cu 941 de integrări disponibile, sistemul propus oferă o flexibilitate și scalabilitate, permițându-i să se adapteze și să se integreze eficient în orice mediu de lucru. Aceste caracteristici fac acest prototip să fie eficient în gestionarea incidentelor de securitate și reprezintă o alegere excelentă pentru organizații mici-mijlocii care sunt in căutarea unei soluții versatile și compatibile cu o gamă largă de tehnologii (Docker, Kubernetes, Virtualizare, Cloud, etc.).

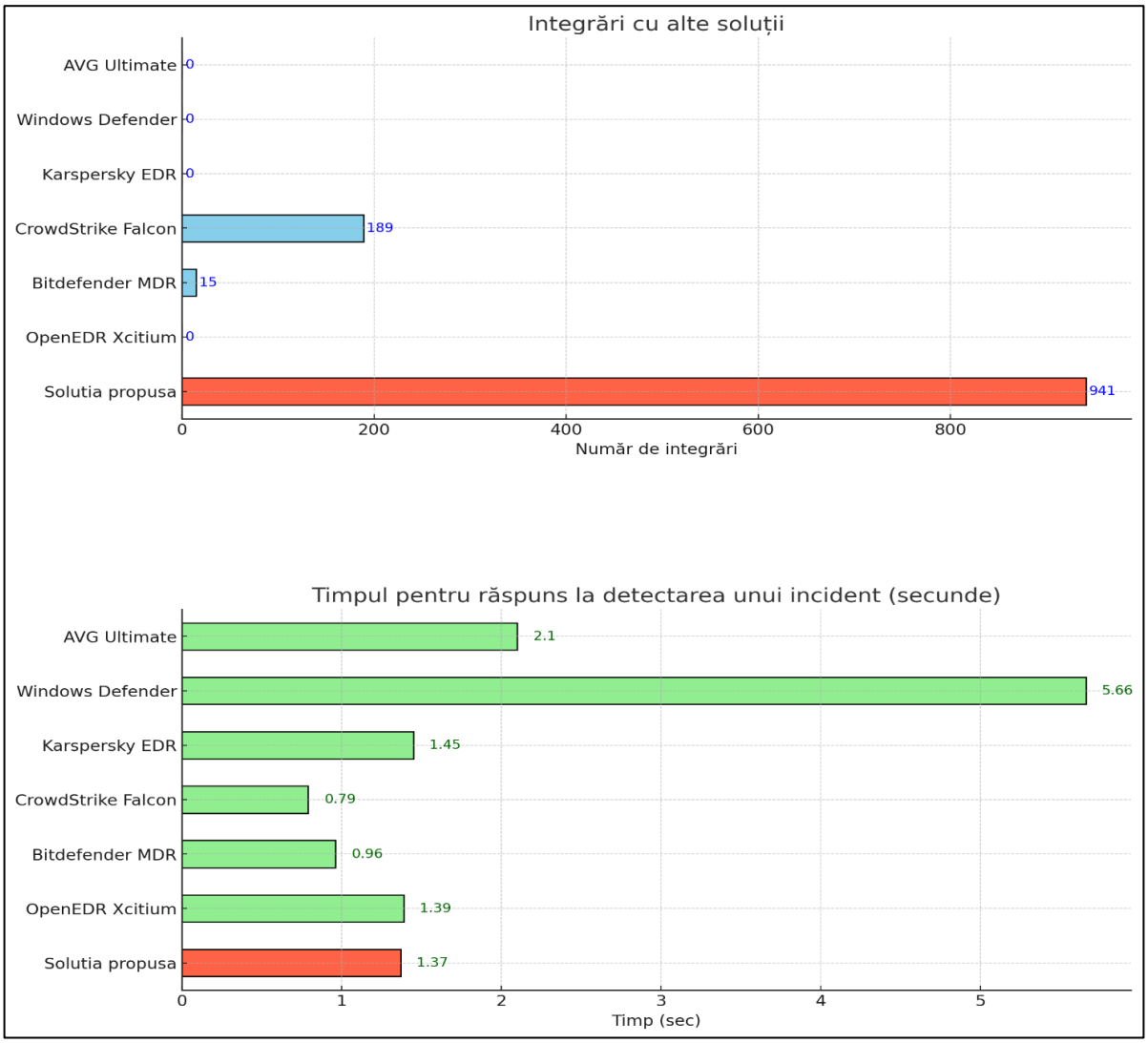


Figura 20 Performanța sistemului propus și timpul de răspuns la incidente de Securitate în comparație cu alte soluții/sisteme prezente pe piață

4.5 CONCLUZII ȘI CONTRIBUȚII ORIGINALE

Pe măsură ce amenințările cibernetice devin mai sofisticate și mai perturbatoare, importanța unei abordări active și bine coordonate în răspunsul la incidente devine importantă. Echipele de răspuns la incidente joacă un rol esențial în protejarea organizațiilor împotriva atacurilor cibernetice și a altor incidente de securitate, prin detectarea rapidă a amenințărilor, limitarea impactului incidentelor și restabilirea operațiunilor normale în cel mai scurt timp posibil. Succesul acestor eforturi depinde de claritatea rolurilor, proceselor eficiente și comunicării eficiente, precum și de utilizarea tehnologiilor avansate pentru analiza datelor de securitate. Pentru a consolida suportul oferit echipelor de securitate în procesul de identificare precisă și eficientă a secvențelor răuvoitoare, acest capitol detaliază dezvoltarea unui sistem avansat, conceput să amplifice capacitatea de detectare, protecție și gestionare a incidentelor. De asemenea, sunt evidențiate contribuțiile semnificative aduse de acest sistem în cadrul domeniului securității informatice.

Printre contribuțiile esențiale ale cercetării prezentate în Capitolul IV, se identifică următoarele:

© Dezvoltarea și implementarea unui sistem/prototip pentru răspunsul automatizat la amenințările cibernetice, utilizând instrumente gratuite (eng. open-source) pentru detectarea secvențelor răuvoitoare. Sistemul demonstrează capacitatea de a identifica, analiza și neutraliza o gamă variată de amenințări cibernetice în timp real, rezultatele fiind documentate și validate în revista de specialitate: Sensors, autori Lucian Florin Ilca, Ogruţan Petre Lucian, Titus Constantin Balan (2023), cu titlul: *„Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response*", https://doi.org/10.3390/s23156757

© Implementarea sistemului a îmbunătățit semnificativ capacitățile de detectare și răspuns la incidente, oferind o soluție eficientă pentru protecția activelor digitale. Originalitatea cercetării este evidențiată prin succesul în identificarea și neutralizarea diferitelor tipuri de secvențe rău intenționate, inclusiv o variantă nouă a secvenței răuvoitoare, Qakbot;

© Dezvoltarea unui sistem de autentificare în doi pași (2FA) și Single Sign-On (SSO) pentru a îmbunătăți securitatea resurselor interne, demonstrând utilitatea acestuia pentru protejarea infrastructurii sistemului propus și posibilitatea de extindere către alte aplicații;

© Dezvoltarea unui sistem pentru detectarea programelor ce conțin vulnerabilități, utilizând limbajul OsQuery și implementarea politicilor de securitate CIS Benchmarks și a interogărilor defensive. Aceasta a facilitat detectarea și mitigarea atacurilor curente, subliniind eficacitatea în protejarea infrastructurii informatice rezultatele fiind documentate și validate în articolul de specialitate ,,Vulnerability Remediation in ICS Infrastructure Based on Source Code Analysis,", autori Ilca Lucian Florin și Titus Constantin Bălan, anul 2020, titlul conferinței: 19th RoEduNet Conference: Networking in Education and Research (RoEduNet), București, România, 2020, pp. 1-6, doi: https://doi.org/10.1109/RoEduNet51892.2020.9324845;

© Folosind un software open-source, s-au dezvoltat seturi detaliate de proceduri și instrucțiuni de automatizare pentru procesul de detectare și notificare a incidentelor de securitate. Utilizând principiile de orchestrare, automatizare și răspuns la incidente (eng. SOAR), sistemul propus facilitează recunoașterea instantanee a amenințărilor cibernetice folosindu-se de celelalte sisteme de protecție și declanșează automat alerte către echipa de răspuns la incidente. Această abordare asigură o intervenție promptă și eficientă, reducând semnificativ timpul de expunere la vulnerabilități și consolidând postura de securitate a organizației;

© Valorificarea avantajelor software-ului cu sursă deschisă, inclusiv transparența, colaborarea, și dezvoltarea condusă de comunitatea academică, pentru a aborda eficient dezvoltarea și continuarea cercetării. Transparența software-ului cu sursă deschisă nu doar îmbunătățește detectarea vulnerabilităților, dar și cultivă încrederea între utilizatori;

© S-a demonstrat că soluțiile cu sursă deschisă sunt adesea mai rentabile și oferă flexibilitate în personalizare și integrare, făcând capacitățile avansate de securitate accesibile unei game largi de organizații, inclusiv celor cu resurse limitate.

Validarea rezultatelor

Rezultatele cercetării au fost diseminate, supuse unui proces de verificare și validate prin publicarea în articolele științifice enumerate mai jos:

- 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

- 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

5 SECURITATEA OFENSIVĂ: PROCEDURI DE TESTARE A SECURITĂȚII SISTEMELOR INFORMATICE

5.1 EVALUAREA RĂSPUNSULUI LA INCIDENTE CU AJUTORUL INGINERIEI SOCIALE

Folosind o metodologie originală și un sistem dezvoltat pentru acest tip de test se facilitează simularea unor atacuri de phishing în condiții controlate, oferind organizațiilor oportunitatea de a evalua cât de bine sunt pregătiți angajații lor să facă față unor asemenea amenințări și eficiența strategiilor de răspuns adoptate. Într-un scenariu real, pentru a demonstra eficiența sistemului propus s-a organizat o campanie de phishing autentică (reală), care a presupus colectarea de date semnificative și a metricilor respective. Rezultatele obținute au fost ulterior analizate în detaliu [25]. Printre obiectivele stabilite, se numără:

- Proiectarea și implementarea unui sistem capabil să integreze diverse instrumente gratuite, facilitând astfel desfășurarea eficientă a campaniilor de phishing și colectarea statisticilor;
- Executarea unei campanii de phishing care să simuleze scenarii avansate de atac. Analiza comparativă a rezultatelor a oferit o perspectivă asupra eficacității diferitelor tipuri de phishing, impactului acestora asupra organizației vizate și nivelului de risc asociat, bazându-se pe ratele de succes ale campaniilor precedente;

În ceea ce privește procedura de livrare a încărcăturii rău intenționate, s-a folosit o platformă gratuită open-source de phishing și testare a securității cibernetice. Acesta permite organizațiilor să creeze și să trimită campanii de phishing pentru a evalua nivelul de conștientizare a securității cibernetice al angajaților lor [26].

Rezultatele cercetării

În cursul campaniei oficiale de phishing, desfășurată între **14 și 17 mai 2021**, s-au înregistrat următoarele metrici avansate de performanță:

- *Numărul total de emailuri expediate:* ***16.185***
- *Emailuri deschise de destinatari:* ***456***
- *Accesări ale linkurilor incluse:* ***314***
- *Trimiteri de date personale de către destinatari:* ***272***

În urma calculului ratei de succes a campaniei, definită ca procentul submisiunilor de date personale în raport cu numărul de email-uri deschise, s-a constatat un indice de performanță de **59,65%.** Această cifră ilustrează gradul de eficacitate al campaniei în determinarea destinatarilor să divulge informații personale, subliniind astfel vulnerabilitățile comportamentale în domeniul securității informaționale. Angajații care au interacționat cu email-ul de phishing, marcându-l ca deschis, au fost incluși în campanii intensive de sensibilizare, cu intenția de a sublinia semnificația vigilenței în fața atacurilor de phishing.

5.2 SECURIZAREA SISTEMELOR PRIN PROCEDURI DE EXERCIȚII COMUNE

Aceste exerciții comune sunt cunoscute sub numele de exercițiu de criză - eng. cyber-crisis sau exercițiul echipei Mov eng. purple-team exercise. Aceste exerciții au rolul de corelare a atacurilor (desfășurate în timp real de către echipa Roșie - echipa atacatorilor) și detectarea secvențelor răuvoitoare cu ajutorul echipei Albastre. Metodele de colaborare propuse sunt testate și comparate într-un mediu controlat. Conceptul echipei Mov în securitatea ofensivă și defensivă se referă la un set de metode, procese sau activități care urmăresc colaborarea între echipele Roșii și Albastre pentru a forma o echipă completă pentru operațiuni de securitate. Se poate folosi o metodologie proprie sau metodologia echipei Mov ATT&CK® (de regulă, se stabilește o metodologie/procedură de către: managerul echipei de operațiuni de securitate, managerul responsabil cu securitatea ofensivă și directorul pentru securitate informatică). Echipamentele informatice depind în mare măsură de securitatea datelor, procesul de transformare a celor mai bune practici într-un mediu securizat, utilizând procese/proceduri necesare.

Rezultatele cercetării

Cazul echipei Mov, prezentat în această secțiune, reprezintă un studiu de caz autentic, desfășurat în cadrul unei companii de dezvoltare software, în contextul unui angajament privat. Rezultatele acestei cercetări au fost diseminate prin publicarea într-o revistă de specialitate relevantă domeniului [27].

Datele relevante au fost obținute prin intermediul unui exercițiu de criză (purple team – exercițiu echipei Mov), desfășurat în cadrul unei companii ce are obiectul de activitate dezvoltarea software, cu un număr de 25 de angajați. În ziua testului, erau prezenți directorul IT, consultantul de securitate care reprezenta echipa Roșie și directorul operațiunilor de securitate care reprezenta echipa Albastră.

Pentru a evalua securitatea companiei, a fost executat un test de tip ofensiv, având în vedere că echipamentul Tenda era considerat punctul slab de intrare. Astfel, echipa Roșie a demonstrat vulnerabilitatea acestui dispozitiv, subliniind importanța actualizării și securizării corespunzătoare a infrastructurii de rețea.

```
┌──(root💀 sld)-[~sld/…/_rev.zip.extracted/_rev.bin.extracted/squashfs-root/etc_ro]
└─# cat passwd
root:$1$nalENqL8$jnRFwb1×5S.ygN.3nwTbG1:0:0:root:/:/bin/sh
admin:6HgsSsJIEOc2U:0:0:Administrator:/:/bin/sh
support:Ead09Ca6IhzZY:0:0:Technical Support:/:/bin/sh
user:tGqcT.qjxbEik:0:0:Normal User:/:/bin/sh
nobody:VBcCXSNG7zBAY:0:0:nobody for ftp:/:/bin/sh

┌──(root💀 sld)-[~sld/…/_rev.zip.extracted/_rev.bin.extracted/squashfs-root/etc_ro]
└─# cat shadow
root:$1$OVhtCyFa$7tISyKW1KGssHAQj1vI3i1:14319::::::
```

Figura 21 ÎEvidențierea informațiilor sensibile din fișierele /etc_ro/shadow și /etc_ro/passwd

În contextul ingineriei inverse, dezasamblarea fișierelor binare reprezintă un pas important în restaurarea codului aplicației software într-o formă vizibilă și inteligibilă. Rezultatul codului

poate fi utilizat în procesele de inginerie inversă pentru a identifica fluxurile logice ale programului sau vulnerabilitățile acestuia într-un mediu operațional.

O altă problemă semnificativă legată de firmware-ul analizat este descoperirea unei vulnerabilități de tip stack overflow în funcția *fromDhcpListClient*. Setând LISTEN=1, programul va ajunge la liniile 30 și 33, ceea ce va duce la această vulnerabilitate de tip stack overflow. Aceasta apare deoarece depășirea stivei suprascrie variabila pointer LISTEN, iar funcția atoi, în încercarea de a converti valoarea, va cauza prăbușirea programului. Acest comportament a fost exploatat pentru a realiza un atac de tip Denial of Service (eng. DoS) la a 2-a iterație a buclei.

```
21  {
22    v1 = atoi(nptr);
23    if ( v1 < i )
24      break;
25    v5[0] = 0;
26    v5[1] = 0;
27    v5[2] = 0;
28    v5[3] = 0;
29    sprintf((char *)v5, "%s%d", "list", i);
30    v10 = sub_2BABC(a1, v5, &unk_EE570);
31    if ( !v10 || !*(_BYTE *)v10 )
32      break;
33    strcpy(dest, (const char *)(v10 + 1));
34    dest[strlen(dest) - 1] = 0;
35    sprintf(s, "dhcps.Staticip%d", i);
36    SetValue(s, dest);
```

Figura 22 Descoperirea funcției problematice pentru a trimtie atacuri împotriva echipamentului.

În concluzie, echipa Roșie a demonstrat capacitatea de a exploata cu succes vulnerabilitățile identificate în firmware-ul routerului cu acces extern la internet. Aceasta a reușit în mod repetat să stabilească conexiuni neautorizate și să insereze cod nelegitim pentru a prelua controlul dispozitivului. Aceste acțiuni au fost posibile prin analiza firmware-ului extras dintr-un dispozitiv similar, analizat într-un mediu de cercetare controlat [28].

Echipa (albastră) însărcinată cu securitatea companiei, în ciuda faptului că sistemul compromis era conectat la infrastructura principală, nu a reușit să identifice și să coreleze informațiile relevante, nici să acceseze jurnalele (log-urile) care ar fi putut semnala atacul. Această situație evidențiază importanța exercițiilor de tip purple team, care combină expertiza echipelor Ofensive (eng. red-team) și Defensive (eng. blue-team), precum și a implementărilor și procedurilor descrise în Capitolul 4. Sistemul propus în Capitolul 4, bazat pe tehnologii gratuite, poate facilita detectarea și răspunsul rapid la potențialele breșe de securitate [29].

Validarea rezultatelor

Rezultatele cercetării au fost diseminate, supuse unui proces de verificare și validate prin publicarea în articolul științific enumerat mai jos:

- 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

5.3 REMEDIEREA VULNERABILITĂȚILOR PRIN ANALIZA CODULUI SURSĂ

Vulnerabilitățile prezente în codul sursă al aplicațiilor pot fi exploatate de către actori rău-intenționați, conducând la compromiterea datelor, pierderi financiare și afectarea reputației organizațiilor. Abordarea proactivă a acestor vulnerabilități, prin intermediul analizei statice a codului sursă, se impune ca o componentă esențială a unui ciclu de dezvoltare a software-ului securizat (SSDLC - Secure Software Development Life Cycle) .

Analiza codului sursă (SCA - Source Code Analysis) se concentrează pe identificarea vulnerabilităților de securitate la nivelul codului scris de dezvoltatori. Obiectivul principal este de a detecta și remedia defectele care ar putea fi exploatate în scopuri nelegitime. Acest proces se poate realiza manual, prin analiza codului sursă, sau automatizat, folosind instrumente de testare statică a securității aplicațiilor (SAST - Static Application Security Testing). Instrumentele SAST, precum SonarQube, Fortify și Checkmarx, cele mai cunoscute și folosite software-uri folosite pentru acest scop [30].

Rezultatele cercetării

Analiza software-ului folosit pentru identificarea diverselor vulnerabilități reprezintă un proces esențial ce trebuie efectuat înainte de implementarea acestuia în orice infrastructură. Printre tehnicile utilizate în acest scop se numără auditul de cod, analiza dinamică a codului sursă, analiza statică a codului sursă, modelarea riscurilor și a amenințărilor [31].

În cadrul auditului de securitate, s-au efectuat teste asupra codului sursă al unui controler PLC utilizat în sistemul de tratare a apei al unei instituții responsabile de administrarea apelor naționale dintr-un stat membru al Uniunii Europene. Acest audit a avut ca scop identificarea și evaluarea potențialelor vulnerabilități de securitate ale controlerului PLC folosit pentru a asigura funcționarea sigură și fără întrerupere a sistemului de tratare a apei.

Sistemul descris reprezintă un sistem automatizat de tratare a apei, utilizat pentru a asigura calitatea apei potabile prin diverse procese de filtrare și purificare. Acest PLC simulează controlul pompelor, supapelor și senzorilor de calitate a apei. Logica de control include activarea diferitelor etape de tratare a apei în funcție de parametrii monitorizați, cum ar fi nivelul de pH și conținutul de clor. Sistemul este compus din senzorul de pH SKU SEN0161 și senzorul de clor SKU SEN0219, utilizând Arduino UNO ca și controller principal. Pentru controlul sarcinilor mari, cum ar fi pompe și supape, se folosește releul de stare solidă Omron G3NA-D210B. Conexiunea la Intranet pentru trimiterea semnalelor și a statisticilor este realizată prin intermediul modulului Arduino

Ethernet Shield 2. În această configurație, principala componentă de interes este controllerul SimpyLC.

SimPyLC funcționează ca un PLC sau un set de PLC-uri și sisteme controlate interconectate. Metodologia urmată în acest proiect se bazează pe utilizarea instrumentelor de analiză a codului sursă (SonarQube, Archery, Owasp Dependecy Check), descărcarea fișierelor din depozitul public al software-ului SimPyPLC și utilizarea metodelor de analiză statică pentru analiza codului sursă. Cu ajutorul metodologiei propuse, s-au identificat 4 noi vulnerabilități și 50 de erori de cod, majoritatea fiind de severitate Medie. Una dintre vulnerabilitățile de severitate medie determinate se referă la generatorul de numere pseudo-aleatorii. Sistemele de control industrial sunt adesea ținta infractorilor cibernetici și a actorilor statali. Din această cauză s-a propus o metodologie pentru validarea securității firmware-ului și a software-ului sistemelor de control industrial. Metodologia propusă pentru analiza codului sursă folosește instrumente dedicate SAST. Utilizarea mai multor instrumente SAST este recomandată pentru a asigura o detecție mai precisă a vulnerabilităților [32]. Cu ajutorul acestei metodologii, dezvoltatorii și administratorii de securitate pot îmbunătăți securitatea software-ului, alegând instrumentele SAST potrivite și implementând măsuri preventive eficiente fiind esențiale în orice proces/pas pentru dezvoltarea unei aplicații [33].

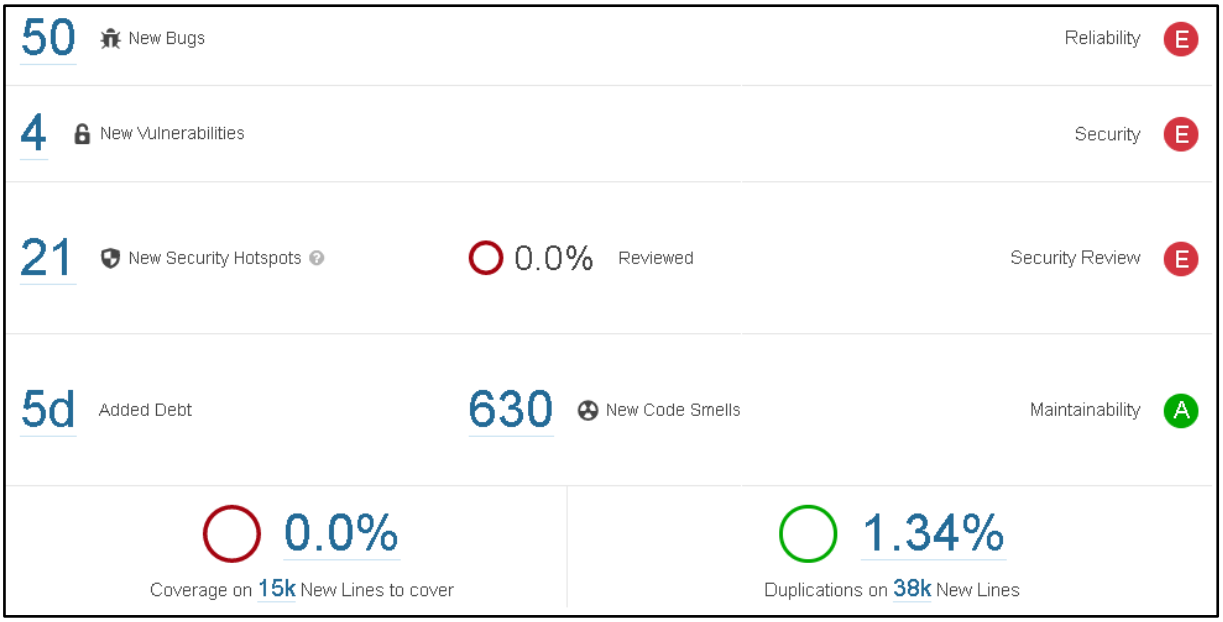


Figura 23 Demonstrarea erorilor și vulnerabilităților detectate prin analiza codului sursă.

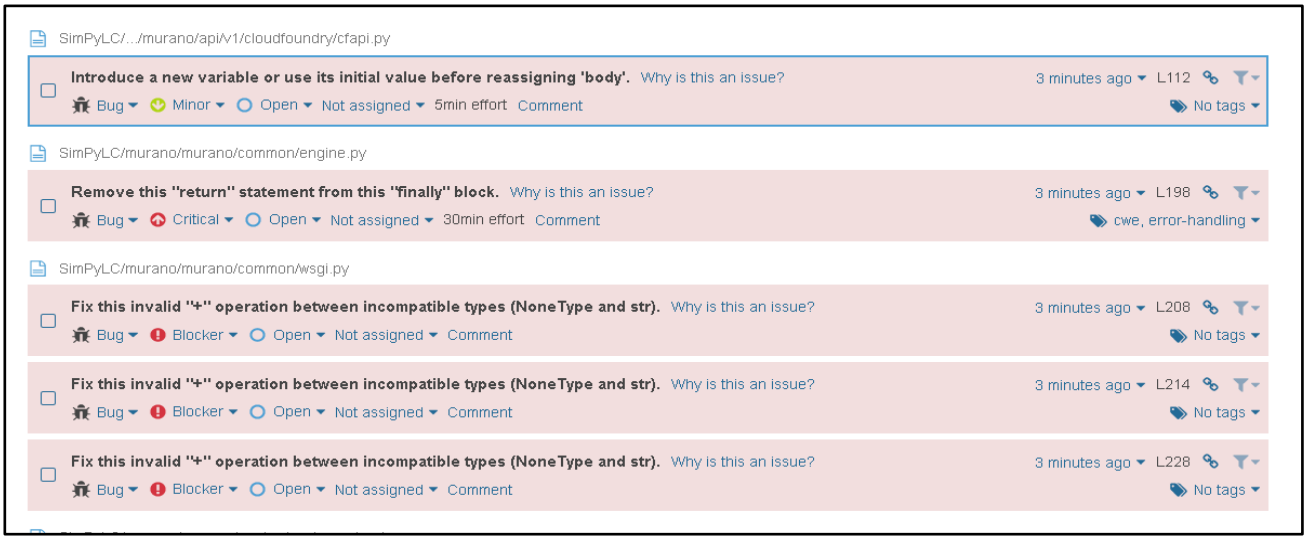


Figura 24 Informații despre tipurile de probleme derterminate și recomandări pentru repararea acestora

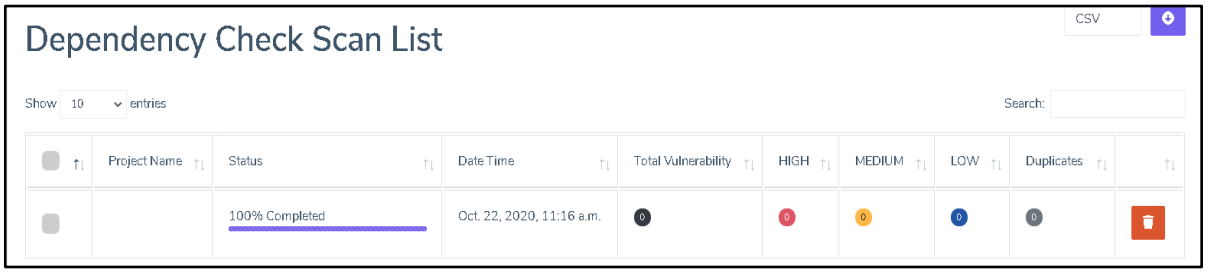


Figura 25 Rezultatul analizei statice folosind OWASP Dependecy Check

Validarea rezultatelor

Rezultatele cercetării au fost diseminate, supuse unui proces de verificare și validate prin publicarea în articolul științific enumerat mai jos:

- 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

Printre contribuțiile esențiale ale cercetării prezentate în Capitolul V, se identifică următoarele:

© Dezvoltarea unui sistem pentru evaluarea răspunsului la incidente, inclusiv o secvență software pentru generarea de nume de domenii omografe și integrarea aplicațiilor într-un sistem PhaaS (eng. Phishing as a Service);

© Dezvoltarea unei proceduri pentru conștientizarea angajaților și a studenților, realizată cu ajutorul unui test de phishing real, din cadrul Universității Transilvania din Brașov, cu scopul de

a îmbunătății procedurile existente pentru creșterea nivelului de conștientizare a amenințărilor cibernetice;

© O altă contribuție semnificativă constă în dezvoltarea unei proceduri pentru securizarea codului sursă al unei aplicații, realizată într-un proiect internațional și detaliată în Subcapitolul: Remedierea vulnerabilităților prin analiza codului sursă.

© O altă contribuție semnificativă constă în dezvoltarea unei proceduri folosită în cadrul unui exercițiu de criză cibernetică (eng. cyber-crisis), având scopul de a îmbunătăți cooperarea între echipele roșii și albastre (echipele de securitate ofensivă și defensivă – parte a echipei Mov), precum și pentru a optimiza procedura de management al incidentelor, răspunsul la incidente, gestionarea vulnerabilităților și remedierea în timp util a breșelor de securitate.

5.4 REZULTATE ȘI OBSERVAȚII

Experimentele de phishing au demonstrat vulnerabilități comportamentale semnificative în fața atacurilor cibernetice. Implementarea sistemului de phishing a contribuit la creșterea nivelului de conștientizare a angajaților și la îmbunătățirea strategiilor de răspuns. De asemenea, eficiența abordării echipei Mov a fost evidentă, colaborarea între echipele roșii și albastre s-a dovedit a fi eficientă în identificarea și remedierea rapidă a riscurilor de securitate (echipamentele afectate au fost dezinstalate).

6 CONCLUZII FINALE. CONTRIBUȚII ORIGINALE. LUCRĂRI PUBLICATE ȘI DIRECȚII VIITOARE DE CERCETARE

6.1 CONCLUZII FINALE

Teza de doctorat explorează o abordare meticuloasă în conceperea unui sistem/prototip avansat destinat răspunsului automatizat la incidentele și breșele de securitate cibernetică, bazându-se pe resurse gratuite, ce pot fi instalate pe orice infrastructură, cu o aplicabilitate specifică în instituțiile de dimensiuni reduse și medii, având până la 250 de angajați, precum și pe implementarea unui sistem de gestionare a securității, identității și accesului și a salvării datelor confidențiale periodic, detaliat în Capitolul 4.

Prin urmare, această lucrare se axează pe elaborarea sistemului menționat, valorificând tehnologiile de inteligență artificială (I.A) și învățare automată (M.L), împreună cu soluțiile software liber accesibile (eng. open-source), pentru a procesa eficient incidentele ce implică secvențe de cod rău intenționate. În cursul elaborării acestei lucrări, s-au consultat sursele bibliografice indicate în secțiunea de referințe. O altă direcție de cercetare propusă în această teză vizează dezvoltarea și implementarea unor proceduri concrete pentru fortificarea posturii de securitate a unei companii. Detaliate în Capitolul 5, aceste proceduri valorifică potențialul securității ofensive, transformând-o într-un instrument strategic esențial pentru identificarea proactivă și remedierea vulnerabilităților înainte ca acestea să fie exploatate de către actori rău intenționați.

Aceste direcții de cercetare subliniază angajamentul lucrării către dezvoltarea unor soluții inovative în domeniul securității cibernetice, adresându-se în mod particular nevoilor instituțiilor de dimensiuni reduse, care se confruntă frecvent cu provocări semnificative în implementarea unor măsuri de securitate eficiente și cost-eficiente.

6.2 CONTRIBUȚII ORIGINALE

© Am dezvoltat și implementat sistem original pentru protecția datelor și managementului identității și accesului (IAM);

© Am implementat o soluție de backup pentru a proteja informațiile stocate, scalabilă și capabilă să salveze atât datele sistemului, cât și pe cele ale utilizatorilor;

© Am creat un sistem avansat de gestionare a incidentelor de securitate și de analiză a codului rău intenționat, integrând diverse software-uri specializate de tip open-source pentru o identificare și contracarare eficientă a incidentelor de securitate;

© Am implementat soluții pentru colectarea, stocarea și analiza jurnalelor de evenimente din diverse surse (sisteme desktop, servere, aplicații, etc.), identificând comportamentele suspecte în timp real;

© Am dezvoltat un sistem pentru evaluarea răspunsului la incidente, incluzând generarea de nume de domenii omografe și integrarea aplicațiilor open-source de phishing într-un sistem denumit PhaaS (Phishing as a Service);

© Gestionarea informațiilor și evenimentelor de securitate a fost optimizată pentru o analiză riguroasă și intervenție rapidă, oferind o perspectivă integrată și măsuri active de protecție împotriva amenințărilor;

© Am corelat evenimentele generate de Sysmon cu identificatorii MITRE ATT&CK pentru a înțelege mai bine tacticile atacatorilor, facilitând detectarea și investigarea activităților suspecte;

© Am implementat și configurat FleetDM și osquery-defense-kit pentru managementul și monitorizarea avansată a sistemelor, detectând librării învechite și posibile probleme de securitate ale sistemelor;

© Am integrat platformele Velociraptor și Watcher pentru îmbunătățirea răspunsului la incidente, extinzând eficacitatea detecției și reacției la amenințări;

© S-a implementat o soluție pentru monitorizarea performanței și stării infrastructurii, facilitând identificarea promptă a problemelor și optimizarea resurselor;

© Am implementat și integrat CrowdSec cu MISP și OpenCTI pentru utilizarea inteligenței colective în identificarea și blocarea atacurilor în timp real, colectând și distribuind date despre amenințări;

© Am contribuit la dezvoltarea modulului pentru securitatea rețelei (eng. network security module), combinând Suricata, Zeek, Arkime și Rita pentru îmbunătățirea monitorizării securității rețelei și detectarea amenințărilor pentru nivelul 2, 3 pe stiva O.S.I (Data Link Layer - Stratul de legătură de date, Network Layer - Stratul de rețea);

© Am dezvoltat o soluție pentru analiza automată a fișierelor atașate la email-uri, utilizând MINI.io, OwnCloud/Nirvashare și Cuckoo Sandbox, pentru a preveni compromiterea comunicațiilor prin email;

© Sistemul propus a îmbunătățit interoperabilitatea și scalarea, gestionând eficient incidentele de securitate și protejând împotriva amenințărilor cibernetice.

© Am dezvoltat o procedură pentru securizarea codului sursă al unei aplicații, exemplificată într-un proiect internațional, detaliată în Subcapitolul: Remedierea vulnerabilităților prin analiza codului sursă.

© Am creat proceduri pentru conștientizarea angajaților și studenților privind amenințările cibernetice cu ajutorul unui test de phishing real;

© Am dezvoltat o procedură pentru un exercițiu de criză cibernetică, îmbunătățind cooperarea între echipele roșii și albastre și optimizând gestionarea incidentelor și vulnerabilităților.

6.3 LUCRĂRI PUBLICATE

Mare parte dintre studiile și experimentele practice realizate pe parcursul studiilor doctorale au fost publicate în jurnale internaționale cu factor de impact sau prezentate în cadrul unor conferințe internaționalele și incluse în volumul conferințelor, ce sunt indexate ISI Web of Science. Astfel, informațiile dezvoltate au fost validate de mai multe grupuri de cercetători, iar conținutul tezei a fost îmbunătățit semnificativ în urma observațiilor primite înainte de publicarea articolelor.

În domeniul tezei s-au realizat următoarele publicații:

A. Lucrări publicate în reviste (jurnale) cu factor de impact indexate ISI WoS:

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. Lucrări publicate în volume de conferințe SpringerLink indexate ISI WoS (sau în curs de indexare) și 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

BIBLIOGRAFIE

[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.