MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică şi Microelectronică
Ingineria Software şi Automatică

Admis la susținere
Şef departament:
Fiodorov Ion, dr., conf. univ.
_____
„____”_____2026

Analiza platformelor de partajare a informațiilor despre amenințări cibernetice și rolul acestora în prevenirea atacurilor cibernetice

Teză de master

Student: _____ **Oprea Loredana, TIA-241M**

Coordonator: _____ **Peca Ludmila, conf. univ., dr.**

Consultant: _____ **Cojocaru Svetlana, asist.univ.**

Chișinău, 2026

REZUMATUL

Autor: Oprea Loredana

Titlul tezei: Analiza platformelor de partajare a informațiilor despre amenințări cibernetice și rolul acestora în prevenirea atacurilor cibernetice

Lucrarea de față examinează, dintr-o perspectivă atât conceptuală, cât și practică, modul în care informațiile de tip cyber threat intelligence pot fi valorificate în sprijinul proceselor operaționale de apărare cibernetică la nivel organizațional. Partea teoretică a lucrării prezintă principalele modele și definiții asociate CTI, ciclul de viață al inteligenței, tipologiile de indicatori de compromitere și standardele utilizate pentru schimbul structurat de informații despre amenințări. În acest cadru este analizată platforma MISP ca soluție open-source dedicată colectării, stocării și partajării datelor CTI, fiind descrise arhitectura sa, mecanismele de distribuție și rolul ecosistemului de module și extensii în consolidarea capacității de analiză.

Componenta practică este centrată pe implementarea și configurarea unei instanțe MISP într-un mediu de laborator, alimentarea acesteia cu date provenite din feed-uri OSINT și utilizarea modulelor de enrichment pentru îmbogățirea indicatorilor cu informații suplimentare de context. Lucrarea detaliază integrarea platformei cu biblioteca PyMISP, prin intermediul căreia sunt automatizate operații esențiale asupra datelor CTI. Pe baza acestor componente este proiectat și realizat un flux de procesare CTI orientat către o echipă națională de răspuns la incidente, care realizează evaluarea indicatorilor și propagă rezultatele sub forma unor alerte sintetice în Microsoft Teams.

Validarea soluției propuse este realizată printr-un studiu de caz ce modelează o campanie de phishing, în cadrul căreia sunt introduși în MISP indicatori reprezentativi. Rezultatele obținute demonstrează că arhitectura propusă contribuie atât la creșterea calității și trasabilității informațiilor CTI, cât și la sporirea gradului lor de utilitate, oferind totodată un punct de plecare pentru dezvoltări ulterioare, precum integrarea cu platforme de monitorizare sau corelarea cu alte surse interne.

Cuvinte cheie: securitate cibernetică, platforme de partajare a informațiilor, platforma MISP, colaborare.

ABSTRACT

Author: Oprea Loredana

Thesis title: An analysis of cyber threat intelligence platforms and their role in preventing cyber attacks

The present thesis examines, from both a conceptual and a practical perspective, how cyber threat intelligence (CTI) can be leveraged to support operational cyber defense processes at the organizational level. The theoretical part of the work presents the main models and definitions associated with CTI, the intelligence lifecycle, the typology of indicators of compromise, and the standards used for the structured exchange of threat information. Within this framework, the MISP platform is analyzed as an open-source solution dedicated to the collection, storage and sharing of CTI data, with focus on its architecture, distribution mechanisms, and the role of its ecosystem of modules and extensions in strengthening analytical capabilities.

The practical component focuses on deploying and configuring a MISP instance in a laboratory environment, populating it with data from OSINT feeds, and using enrichment modules to augment indicators with additional contextual information. The thesis details the integration of the platform with the PyMISP library, through which essential operations on CTI data are automated. Building on these components, a CTI pipeline oriented towards a national incident response team is designed and implemented, performing the evaluation of indicators and disseminating the results as concise alerts in Microsoft Teams.

The proposed solution is validated through a case study that models a phishing campaign, in which representative indicators are introduced into MISP. The results show that the proposed architecture contributes both to improving the quality and traceability of CTI information and to increasing its degree of actionability, while also providing a starting point for future developments such as integration with monitoring platforms or correlation with other internal data sources.

Keywords: cybersecurity, Cyber Threat Intelligence Platforms, MISP Platform, collaboration.

CUPRINS

ABREVIERI ȘI DEFINIȚII

CTI (Cyber Threat Intelligence) – Informații analizate și contextualizate despre amenințări și atacatori, folosite pentru a sprijini deciziile de securitate.

TTPs – Tactici, tehnici și proceduri.

ENISA – Agenția Uniunii Europene pentru Securitate Cibernetică.

IoC – Indicatori de Compromitere.

Intelligence – cunoaștere obținută prin colectarea și analiza sistematică a datelor.

Loguri – înregistrări automate ale evenimentelor din sisteme și rețele.

MISP (Malware Information Sharing Platform) – platformă open-source pentru colectarea, structurarea și partajarea indicatorilor și evenimentelor de securitate între organizații.

SOC (Security Operation Center) – echipă/centru operațional care monitorizează continuu securitatea, detectează incidentele și coordonează răspunsul.

SLA (Service Level Agreement) – acord de nivel de serviciu ce definește clar domeniul de aplicare, indicatorii de performanță și termenele de răspuns la incidente de securitate.

APT (Advanced Persistent Threat) – grup sau campanie avansată, bine finanțată, care urmărește ținte specifice pe termen lung, cu tehnici sofisticate și operațiuni discrete.

SOAR (Security Orchestration, Automation and Response).

TSTEM (Threat Streaming and Extraction Machine) – platformă cognitivă pentru colectarea și extragerea automată de IoC din surse deschise.

CTIMP (Cyber Threat Intelligence Management Platform) – platformă de management al inteligenței despre amenințări, orientată mai ales spre medii industriale

OSSEC Open Source Security (HIDS) and Event Correlation – soluție open-source de tip host-based intrusion detection system

THREATKG (Threat Knowledge Graph) – sistem pentru construire și gestionare de grafuri de cunoștințe despre amenințări.

DYNAMO – proiect european ce combină business continuity management și CTI.

API (Application Programming Interface) – interfață de programare a aplicațiilor.

NIDS (Network Intrusion Detection System) – sistem de detecție a intruziunilor la nivel de rețea.

HIDS (Host-based Intrusion Detection System) – sistem de detecție a intruziunilor la nivel de gazdă.

CISO – Chief Information Security Officer.

IoT – Internet of Things.

TLP – Traffic Light Protocol.

OSINT – Open Source Intelligence.

PoC – Proof of Concept/ Demonstrație de concept.

STIX – Structured Threat Information Expression.

TAXII – Trusted Automated eXchange of Indicator Information.

IMM – Întreprinderi Mici și Mijlocii.

IODEF – Incident Object Description Exchange Format.

VERIS – Vocabulary for Event Recording and Incident Sharing.

ATT&CK – Adversarial Tactics, Techniques & Common Knowledge.

DDoS (Distributed Denial of Service) – atac în care are loc blocarea un serviciu sau a unei rețele prin suprasolicitarea acestuia cu trafic fals, astfel încât serviciul devine indisponibil.

OpenIOC – format pentru definirea indicatorilor de compromis, cu logică de tip condiții AND/OR, folosit mai ales în contextul investigațiilor malware și endpoint.

Malware – software creat cu intenție malițioasă pentru a compromite sisteme sau date.

Framework – set structurat de concepte și bune practici folosit ca schelet pentru a construi sau organiza.

Cloud – model în care resursele IT sunt furnizate prin internet, la cerere, de un furnizor extern.

Machine learning – tehnici prin care un sistem învață automat din date, fără a fi programat explicit.

Ransomware – tip de malware care criptează datele sau blochează sistemele și cere o răscumpărare pentru deblocare.

Phishing și spear-phishing – mesaje în masă înșelătoare pentru a fura date; versiune mult mai țintită și personalizată, către o persoană sau organizație anume.

On-premises – infrastructură IT găzduită și administrată în sediul propriu al organizației, nu la un furnizor cloud.

Multi-tenancy – arhitectură în care aceeași aplicație/instanță servește mai mulți clienți.

Vulnerabilitate zero-day – vulnerabilitate necunoscută public și, de regulă, fără remediere disponibil încă.

AI-powered – care folosește componente de inteligență artificială pentru a îmbunătăți funcționalitatea.

SECOPS (Security Operations) – procese și echipe responsabile de monitorizare, detecție și răspuns la incidente de securitate.

Reasoning – proces de inferență: sistemul trage concluzii noi pe baza unor reguli și a informațiilor existente.

MITRE ATT&CK – bază de cunoștințe publică ce cataloghează tactici, tehnici și proceduri (TTPs) folosite de atacatori, organizate în matrici folosite pentru detecție și threat hunting.

NIST CSF – „Cybersecurity Framework" al NIST, set de funcții și controale (Identify, Protect, Detect, Respond, Recover) folosit ca reper pentru managementul riscului cibernetic.

ISO/IEC – familie de standarde internaționale care definesc cerințe și bune practici pentru managementul securității informațiilor.

GDPR – Regulamentul general privind protecția datelor al UE, stabilește reguli stricte pentru prelucrarea și protejarea datelor cu caracter personal.

HIPAA – lege americană care reglementează confidențialitatea și securitatea datelor medicale și a informațiilor de sănătate protejate.

PCI-DSS – set de standarde de securitate pentru organizațiile care procesează plăți cu cardul, cu cerințe specifice pentru protejarea datelor de card.

Open-source – software sau resurse cu cod sursă, public disponibil, care pot fi utilizate, modificate și distribuite liber, în limitele licenței.

Stakeholderi – părți interesate implicate sau afectate de un sistem/proiect.

Feed – flux de date actualizate.

Kit – set pre configurat de componente folosite pentru atac sau automatizare.

Exploit – cod, tehnică sau secvență de comenzi care valorifică o vulnerabilitate software sau de configurare pentru a obține acces neautorizat sau alte efecte malițioase.

Python – limbaj de programare de nivel înalt, interpretat, foarte folosit în securitate cibernetică și CTI pentru automatizare, analiză de date și integrarea cu API-uri ale platformelor de tip MISP/SIEM.

Enrichment – proces de îmbogățire a indicatorilor cu informații de context suplimentare.

Warning list – liste predefinite de elemente folosite pentru a marca indicatorii, astfel încât să nu fie tratați ca amenințări reale și să se reducă alertele false.

GitHub – platformă online de găzduire a codului și colaborare pentru proiecte software.

INTRODUCERE

Secolul XXI demonstrează că transformarea digitală a societății contemporane a determinat creșterea dependenței organizațiilor de infrastructura informatică, sisteme și servicii interconectate. Cu toate că evoluția tehnologică generează beneficii economice, operaționale și strategice, aceasta conduce simultan către extinderea suprafeței de atac și amplificarea riscurilor asociate securității informaționale. Cu trecerea timpului, peisajul amenințărilor cibernetice devine tot mai complex și caracterizat de atacuri sofisticate, persistente și coordonate, fiind realizate de actori malițioși care utilizează tehnici și tactici avansate de compromitere a sistemelor și exploatare a vulnerabilităților curente.

Ca urmare a nivelului ridicat de complexitate a atacurilor actuale, organizațiile nu mai pot asigura un nivel adecvat de protecție bazându-se doar pe informațiile generate local, de aceea cooperarea interinstituțională și anume prin intermediul schimbului de informații despre amenințările cibernetice devin elemente și instrumente esențiale pentru creșterea capacității de detectare, prevenire și răspuns la incidente de securitate cibernetică.

Schimbul de informații despre amenințări cibernetice este de fapt procesul de partajare a informațiilor de tip threat intelligence și presupune colectarea, analiza și distribuirea datelor despre atacuri, vulnerabilități, tehnici și tactici și indicatori de compromitere. În acest context, platformele open-source destinate schimbului de informații despre amenințări cibernetice au apărut ca soluții tehnologice relevante, oferind mecanisme flexibile, scalabile și accesibile pentru colectarea, structurarea și distribuirea datelor de securitate.

Prezenta lucrare este structurată astfel încât să surprindă, într-o succesiune logică, atât fundamentele teoretice ale domeniului cyber threat intelligence, cât și aplicabilitatea practică a acestuia prin intermediul platformei MISP și al instrumentelor asociate. Lucrarea urmărește trecerea graduală de la cadrul conceptual general către un studiu aplicat, orientat spre automatizarea proceselor CTI și valorificarea operațională a indicatorilor de compromitere. În acest sens, conținutul a fost organizat pe capitole care răspund etapizat obiectivelor propuse, de la definirea conceptelor și analizarea soluțiilor existente, până la configurarea unui mediu de test și validarea unui flux practic de alertare.

Primul capitol este dedicat fundamentării teoretice a domeniului și are rolul de a introduce conceptele esențiale necesare înțelegerii lucrării. În cadrul acestuia sunt prezentate noțiunile de cyber threat intelligence, rolul informațiilor despre amenințări în activitatea de securitate cibernetică, categoriile de indicatori de compromitere și etapele ciclului de viață al inteligenței. Tot aici sunt descrise principalele tipuri de date utilizate în procesele CTI, precum și importanța standardizării și a schimbului structurat de informații între organizații. Acest capitol oferă baza conceptuală pe care se sprijină întreaga lucrare și justifică relevanța practică a temei abordate.

Capitolul al doilea este orientat spre analiza platformelor și tehnologiilor utilizate pentru colectarea, partajarea și gestionarea informațiilor despre amenințări. Accentul este pus pe soluțiile open-source, cu evidențierea platformei MISP ca instrument central al lucrării. Sunt analizate funcționalitățile acesteia, modul de organizare a evenimentelor și atributelor, posibilitățile de integrare cu surse externe și rolul său în susținerea schimbului de date CTI. De asemenea, acest capitol urmărește să evidențieze de ce MISP reprezintă o alegere potrivită pentru implementarea unui scenariu aplicat în contextul unei organizații care dorește să își dezvolte capabilități proprii de threat intelligence.

Capitolul al treilea reprezintă componenta practică și, în același timp, partea finală a lucrării. Acesta descrie implementarea și configurarea unei instanțe MISP într-un mediu de laborator, etapele de alimentare a acesteia cu date din feed-uri OSINT, activarea listelor de filtrare și utilizarea modulelor pentru completarea contextului indicatorilor analizați. În continuare este prezentată integrarea platformei cu biblioteca PyMISP și dezvoltarea unui flux automatizat capabil să interogheze atributele relevante, să ruleze procese de analiză și să transmită alerte sintetice într-un canal Microsoft Teams. În interiorul acestui capitol este inclus și o demonstrare de concept, construită în jurul unui scenariu simulat de phishing.

Lucrarea urmărește atingerea obiectivelor de cercetare: analizarea conceptului de informații despre amenințări cibernetice și a rolului acestuia în securitatea organizațională; identificarea principalelor modele și standarde de schimb de date; examinarea platformelor open-source existente; studierea arhitecturii, funcționalităților și mecanismelor de operare ale platformei MISP; evaluarea beneficiilor operaționale ale utilizării acesteia; precum și identificarea limitărilor și provocărilor asociate implementării.

BIBLIOGRAFIE

[1] S. M. Abu, R. S. Selemat, A. Ariffin şi R. Yusof, „Cyber Threat Intelligence – Issue and Challenges,” *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 10, pp. 371-379, 2018.

[2] S. H. Iqbal, A. Kayes, S. Badsha, H. Alqahtani, P. Watters şi A. Ng, „Cybersecurity data science: an overview from machine learning perspective,” *Journal of Big Data,* vol. 7, 2020.

[3] S. Ainslie, D. Thompson, S. Maynard şi A. Ahmad, „Cyber-threat intelligence for security decision-making: A review and research agenda for practice,” *Computers & Security,* 2023.

[4] P. Santos, R. Abreu, J. C. M. Reis, C. Serôdio şi F. Branco, „A Systematic Review of Cyber Threat Intelligence: The Effectiveness of Technologies, Strategies, and Collaborations in Combating Modern Threats,” *Sensors,* vol. 25, 2025.

[5] R. Jongman, „The CTI Process Hyperloop: A Practical Implementation of the CTI Process Lifecycle,” 14 November 2023. [Interactiv]. Available: https://cloud.google.com/blog/topics/threat-intelligence/cti-process-hyperloop/.

[6] P. John, „Understanding the NIST Threat Intelligence Lifecycle for Enhanced Cybersecurity,” [Interactiv]. Available: https://subrosacyber.com/en/blog/threat-intelligence-lifecycle-nist.

[7] Flashpoint, „Strategic vs Operational vs Tactical Intelligence,” 09 2022. [Interactiv]. Available: https://flashpoint.io/blog/three-types-of-threat-intelligence/.

[8] G. Goldstein, „Level Up Strategic, Tactical, Technical & Operational Threat Intelligence,” June 2023. [Interactiv]. Available: https://cyberint.com/blog/threat-intelligence/strategic-tactical-technical-operational-threat-intelligence/.

[9] I. Shantilawati, J. Zanubiya, F. Fanani, H. Jensen, S. Millah şi N. Lutfiani, „Challenges in Securing Data and Networks from Modern Cyber Threats,” *International Journal of Cyber and IT Service Management (IJCITSM),* vol. 4, nr. 2, pp. 88-96, October 2024.

[10] D. Țurcanu, L. Peca, A. Prisacaru și T. Țurcanu, „CYBER SECURITY PROFESSIONAL DEVELOPMENT WITHIN CYBERCOR,” *Journal of Engineering Science,* vol. XXXII, nr. 2, pp. 87-98, 2025.

[11] M. Chiper, D. Stanescu, T. Becheru şi L. Peca, „Adversarial Attacks for Scripts,” în *Networking in Education and Research (RoEduNet)*, Chişinău, 2025.

[12] L. Peca şi D. Ţurcanu, „REDUCING CYBER RISK THROUGH A HUMAN–CENTRED APPROACH,” *Journal of Engineering Science*, vol. XXXII, nr. 1, pp. 18-31, 2025.

[13] A. Mahida şi A. Tyagi, „CYBER THREAT INTELLIGENCE AND INFORMATION SHARING IN CLOUD ECOSYSTEMS,” *Proceedings on Engineering Sciences*, vol. 7, nr. 1, pp. 43-49, 2025.

[14] M. Dekker şi L. Alevizos, „A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making,” *Security and Privacy*, April 2024.

[15] S. Cojocaru şi L. Peca, „Challenges and solutions on the use of Artificial Intelligence in Internet of Things network security,” în *Electronics, Communications and Computing*, Chişinău, 2024.

[16] C. Abraham, F. Bélange şi S. Daultrey, „Promoting research on cyber threat intelligence,” *Journal of Cybersecurity*, 2025.

[17] B. Dissanayake şi M. Thinyane, „Challenges and Opportunities for Cross-Domain Cyber Threat Intelligence Sharing Towards Whole-of-Society Resilience,” în *European Conference on Cyber Warfare and Security*, 2025.

[18] M. Mahmoud, B. A. Aryee şi K. A. Agyemang, „INVESTIGATING THE ROLE OF AI-POWERED CYBER THREAT INTELLIGENCE SHARING FRAMEWORKS IN ENHANCING NATIONAL SECURITY ACROSS U.S. PUBLIC SECTOR ENTITIES,” *EPRA International Journal of Multidisciplinary Research (IJMR)*, vol. 11, 2025.

[19] A. M. Nainna, M. J. Bass şi L. Speakman, „Factors Amplifying or Inhibiting Cyber Threat Intelligence Sharing,” în *Information Systems*, 2024.

[20] C. R. Viana, M. Lima, B. L. L. de Melo Junior, G. N. Silva şi D. R. Araujo, „Cyber Threat Intelligence Sharing: Challenges and Opportunities”.

[21] S. K. Balakrishnan, „Federated Threat Intelligence Exchange Protocol (F-TIXP): Privacy-Preserving Collaborative Cyber Defense Framework,” pp. 246-252, 2025.

[22] A. de Melo e Silva, J. J. Costa Gondim, R. de Oliveira Albuquerque şi G. García Villalba, „A Methodology to Evaluate Standards and Platforms within Cyber Threat

Intelligence," *future internet*, vol. 12, nr. 6, 2020.

[23] A. Dimitriadis, A. Papoutsis, D. Kavalieros, T. Tsikrika, S. Vrochidis și I. Kompatsiaris, „EVACTI: evaluating the actionability of cyber threat intelligence," *International Journal of Information Security*, 2025.

[24] P. Koloveas, T. Chantzios, S. Alevizopoulou, S. Skiadopoulos și C. Tryfonopoulos, „INTIME: A Machine Learning-Based Framework for Gathering and Leveraging Web Data to Cyber-Threat Intelligence," *Electronics*, vol. 10, nr. 818, 2021.

[25] D. Preuveneers, W. Joosen, J. B. Bernabe și A. Skarmeta, „Distributed Security Framework for Reliable Threat Intelligence Sharing," *Security and Communication Networks*, pp. 1-15, 2020.

[26] J. R. Trocoso-Pastoriza, A. Mermoud, R. Bouyé, F. Marino, J.-P. Bossuat, V. Lenders și J.-P. Hubaux, „Orchestrating Collaborative Cybersecurity: A Secure Framework for Distributed Privacy-Preserving Threat Intelligence Sharing," *Cornell University*, pp. 1-31, 2022.

[27] A. Das, „Automation and Orchestration in Cyber Threat Intelligence (CTI): A Survey," *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, vol. 13, nr. 6, pp. 1964-1970, 2025.

[28] Kela Cyber Team, „What Is a Threat Intelligence Platform and Why Do You Need One?," Kela, 21 July 2025. [Interactiv]. Available: https://www.kelacyber.com/academy/cti/what-is-a-threat-intelligence-platform-and-why-do-you-need-one/. [Accesat 13 03 2026].

[29] I. ȘERBAN, F.-M. CURCĂ și R.-. Ș. ȘANDRU, „Increasing the cyber resilience of SMEs through open-source solutions and international collaboration," *BULLETIN OF "CAROL I" NATIONAL DEFENCE UNIVERSITY*, vol. 13, nr. 4, pp. 266-286, 2024.

[30] J. Manzoor, A. Waleed, A. F. Jamali și A. Masood, „Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs," 2024.

[31] A. A. Kalo, M. Schuba și F. Wiesenfeller, „Open-Source Cyberthreat Intelligence Integration for SMEs," în *In Proceedings of the 2025 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems*, New Yourk, 2025.

[32] K. R. D. Chatziamanetoglou, „Weighted quality criteria for cyber threat intelligence: assessment and prioritisation in the MISP data model," *International Journal of Information*

Security, vol. 24, nr. 160, 2025.

[33] MISP project, „Home: MISP Intelligence Sharing,” MISP Project, [Interactiv]. Available: https://www.misp-project.org/. [Accesat 14 03 2026].

[34] GitHub, „MISP - Threat Intelligence Sharing Platform,” GitHub, Inc., [Interactiv]. Available: https://github.com/MISP/MISP. [Accesat 13 03 2026].

[35] M. Ammi și Y. M. Jama, „Cyber Threat Hunting Case Study using MISP,” *Journal of Internet Services and Information Security (JISIS),* vol. 13, nr. 2, pp. 01-29, 2023.

[36] I. Naseer, „Machine Learning Applications in Cyber Threat Intelligence: A Comprehensive Review,” *ASIAN BULLETIN OF BIG DATA MANAGMENT,* vol. 3, nr. 2, pp. 190-200, 2023.

[37] S. Gillard, D. P. David, A. Mermoud și T. Maillart, „Efficient collective action for tackling time-critical cybersecurity threats,” *Journal of Cybersecurity,* vol. 9, nr. 1, pp. 01-22, 2023.

[38] A. O. Aljahdali, „A cyber threat intelligence model using MISP and machine learning in a SOC environment,” *International Journal of Advanced and Applied Sciences,* vol. 12, nr. 11, pp. 1-11, 2025.

[39] B. Stojkovski, G. Lenzini, V. Koenig și S. Rivas, „What’s in a Cyber Threat Intelligence sharing platform?: A mixed-methods user experience investigation of MISP,” în *Annual Computer Security Applications Conference*, Virtual Event SUA, 2021.

[40] P. Delvecchio, S. Galantucci, A. Iannacon și G. Pirlo, „CARIOCA: prioritizing the use of IoC by threats assessment shared on the MISP platform,” *International Journal of Information Security,* vol. 24, nr. 98, pp. 1-23, 2025.

[41] P. Balasubramanian, S. Nazari, D. K. Kholgh, A. Mahmoodi, J. Seby și P. Kostakos, „A cognitive platform for collecting cyber threat intelligence and real-time detection using cloud computing,” *Decision Analytics Journal,* vol. 14, 2025.

[42] A. Papanikolaou, A. Alevizopoulos, C. Ilioudis, K. Demertzis și K. Rantos, „A Cyber Threat Intelligence Management Platform for Industrial Environments,” *Computer Science > Cryptography and Security,* 2023.

[43] P. Gao, X. Liu, E. Choi, S. Ma, X. Yang și D. Song, „ThreatKG: An AI-Powered System for Automated Open-Source Cyber Threat Intelligence Gathering and Management,” în

Association for Computing Machinery, 2024.

[44] N. Rastogi, S. Dutta, A. Gittens, M. J. Zaki și C. Aggarwal, „A framework for Open source Cyberthreat Intelligence,” în *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Wuhan, China, 2022.

[45] J. Rajamäki și S. McMenamin, „Utilization and Sharing of Cyber Threat Intelligence Produced by Open-Source Intelligence,” în *International Conference on Cyber Warfare and Security*, Epso, 2024.

[46] MITRE ATT&CK, „What is ATT&CK?,” 2015-2025. [Interactiv]. Available: https://attack.mitre.org/resources/. [Accesat 24 03 2026].

[47] R. Amanov, R. Isaev, E. Doszhanov și A. Abdykerimov, „Using the MISP Platform to Collect Incident Data,” *Pre prinst.org*, pp. 1-9, 12 05 2025.

[48] CIRCL Luxembourg, „PyMISP - Python Library to access MISP,” CIRCL LU, 02 10 2024. [Interactiv]. Available: https://www.circl.lu/doc/misp/pymisp/. [Accesat 23 03 2026].

[49] C. Jacquet, „Privacy Aware Sharing of IOCs in MISP,” Université catholique de Louvain, Ottignies-Louvain-la-Neuve, 2017.

[50] L. B. Benjamin, A. E. Adegbola, P. Amajuoyi, M. D. Adegbola și K. B. Adeusi, „Digital transformation in SMEs: Identifying cybersecurity risks and developing ffective mitigation strategies,” *Glogal Journal of Engineering and Technologies Advances*, vol. 19, nr. 2, pp. 134-153, 2024.

[51] A. Bahmanova și N. Lace, „Key factors shaping collaborative cyber resilience in SMEs through open innovation,” *Journal of Open Innovation: Technology, Market, and Complexity,* vol. 12, pp. 01-10, 2026.

[52] L. Peca, S. Cojocaru, M. Dumitrașcu și D. Țurcanu, „Evaluation of cybersecurity training perceptions, adopted practices and strategic directions for capacity building,” *Journal of Engineering Science,* vol. XXXII, nr. 3, pp. 75-90, 2025.

[53] CIRCL Luxembourg, „MISP User Stories,” 02 10 2024. [Interactiv]. Available: https://www.circl.lu/doc/misp/user-stories/. [Accesat 23 03 2026].

[54] MISP Project, „Tools,” [Interactiv]. Available: https://www.misp-project.org/tools/. [Accesat 15 04 2026].

[55] CIRCL Luxembourg, „MISP modules,” 02 10 2024. [Interactiv]. Available:

https://www.circl.lu/doc/misp/modules/. [Accesat 15 04 2026].

[56] CIRCL Luxembourg, „MISP Quick Start,” 02 10 2024. [Interactiv]. Available: https://www.circl.lu/doc/misp/quick-start/. [Accesat 15 04 2026].

[57] Git Hub, „MISP,” [Interactiv]. Available: https://github.com/MISP/MISP/blob/2.5/INSTALL/INSTALL.ubuntu2404.sh. [Accesat 6 04 2026].

[58] cosive, „MISP Feeds: Updated 2025 Guide,” 10 06 2025. [Interactiv]. Available: https://www.cosive.com/misp-feeds. [Accesat 18 04 2026].

[59] Git Hub, „PyMISP - Python Library to access MISP,” 2021. [Interactiv]. Available: https://github.com/MISP/PyMISP. [Accesat 18 04 2026].

[60] A. Dulaunoy, „Building and designing MISP. A practical information-sharing tool for cybersecurity and fraud indicators,” CIRCL Luxembourg, Zurich.

[61] MISP project, „MISP Default Feeds,” [Interactiv]. Available: https://www.misp-project.org/feeds/. [Accesat 20 04 2026].

[62] Recorded Future, „MISP Use Cases,” [Interactiv]. Available: https://support.recordedfuture.com/hc/en-us/articles/360051605794-MISP-Use-Cases. [Accesat 19 04 2026].

[63] CIRCL Luxembourg, „Managing Feeds,” 02 10 2024. [Interactiv]. Available: https://www.circl.lu/doc/misp/managing-feeds/. [Accesat 18 04 2026].

[64] CIRCL Luxembourg, „MISP warninglists,” 02 10 2024. [Interactiv]. Available: https://www.circl.lu/doc/misp/warninglists/. [Accesat 18 04 2026].

[65] A. Dulaunoy, „MISP Taxonomies and Warning-lists,” Luxembourg.

[66] Vanimpe, „Using open source intelligence feeds, OSINT, with MISP,” 23 03 2016. [Interactiv]. Available: https://www.vanimpe.eu/2016/03/23/using-open-source-intelligence-osint-with-misp/. [Accesat 23 04 2026].

[67] GitHub, „MISP modules,” GitHub, 2025. [Interactiv]. Available: https://github.com/MISP/misp-modules. [Accesat 23 04 2026].

[68] CIRCL Luxembourg, „Deep-dive into PyMISP,” [Interactiv]. Available: https://www.foo.be/cours/dess-20182019/pub/14-pymisp.pdf. [Accesat 20 04 2026].