ИНФОРМАТИКА И КОМПЮТЪРНИ НАУКИ
INFORMATICS AND COMPUTER SCIENCES

AUTOMATED THREAT ACTOR PROFILING WITH AI IN CYBER THREAT INTELLIGENCE: A FRAMEWORK FOR REAL-TIME EXTRACTION AND ATTRIBUTION

Vladimir Babanov
South-West University "Neofit Rilski"
https://doi.org/10.70300/EZSK8780

Abstract: *Cyber threat intelligence (CTI) has become essential for a proactive defending against adversaries in cyberspace. However, the majority of valuable information resides in vast volumes of unstructured data and feeds, which renders their analysis an extremely lengthy and error-prone process. This paper aims to present a real-time automated framework that utilizes Natural Language Processing (NLP) and standardized ontologies such as Structured Threat Information Expression (STIX) v2.1 and MITRE ATT&CK to identify indicators of compromise (IoCs), tactics, techniques and procedures (TTPs) from multiple CTI sources and correlate them with a threat actor profile. The approach described in it digests data from open-source threat reports, social media and other sharing platforms. It also uses domain-specific language models and rule-based analyzers to identify entities (e.g. malware, tools, targets), mapping them to STIX objects and linking extracted TTPs to ATT&CK techniques. The framework is tested with a hypothetical ransomware case study, which displays how through extracted indicators, killchain stages and behavioural patterns could be associated with a threat-actor profile. The results demonstrate that the suggested AI-driven pipeline could enormously reduce the manual effort in CTI processing, maintaining high extraction accuracy. The work lays the foundation for implementing automatic CTI profiling of adversaries aiding with proactive defense and attribution efforts.*
Keywords: *Cyber Threat Intelligence; Artificial Intelligence; Threat Actor Profiling; Natural Language Processing; Cybersecurity*

INTRODUCTION

Modern cyberattacks have evolved with increasing sophistication and have been carried out by skilled actors able to operate undetected with unseen adaptability. Relating the criminal activity in cyberspace to certain actors or groups, known as threat attribution or profiling, is vital for effective defense and legal action (Santos et al. 2025). Traditionally, experts conduct this process manually, collecting indicators of compromise (IoCs) and analyzing Tactics, Techniques and Procedures (TTPs) from various sources, visualizing the results and associating them to adversary's profile. This could be an overwhelming effort given the amount of raw data generation online. The necessity for automated tools that process raw information into structured, actionable CTI has never been higher with adversaries already automating significant portion of malicious actions.

Various artificial intelligence (AI) methods have emerged to aid this process, especially machine learning (ML) and natural language processing (NLP). Both are used in correlation of sifting through big amounts of data through NLP and different AI models then cluster and correlate patterns hidden in it (Arazzi et al. 2025). The results are then shaped into the standardized frameworks that Structured Threat Information Expression v.2.1 (STIX v.2.1) and MITRE ATT&CK provide. Combining AI and these standards is the best way to offload the overwhelmed human factor in the constant effort of linking incidents, malware and adversaries. Using such method, security platforms can continuously ingest data, extract key findings and automatically populate threat actors' knowledge graph, turning the process into real-time profiling.

In the current paper, a design of an AI-driven CTI framework for automated threat actor profiling is explored. It consists of NLP techniques to extract names, tools, and techniques from text

sources. With STIX v2.1 encoding this information into sharable knowledge graph and MITRE ATT&CK mapping and normalizing TTPs. A fictional case study is included in the paper to illustrate the assemblance of extracted TTPs into a profile. The main goal is not to detail a working system but to describe a feasible architecture and its upside potential. Grounding in recent research, the paper aims at conceptual clarity rather than technicalities.

METHODOLOGY

The methodology is built upon an in-depth examination of relevant research studies on AI-based CTI, automated construction of knowledge graphs, and identifying and attributing malicious actors. The research establishes both the conceptual and technological base for the proposed model. An empirical evaluation has been included to assess whether open-source CTI documents, social media posts, and structured intelligence databases can be utilized in real-time to automatically extract and correlate IOCs and TTPs. NLP models are used to identify entities and relationships from unstructured text which can then be normalized into STIX v2.1 and MITRE ATT&CK format. The automation framework has been constructed using JavaScript and React for the front-end orchestration and visualization layer and is deployed on Google Cloud to allow for scalable and event-driven processing of threats. The framework's end-to-end pipeline is validated through a hypothetical ransomware case study that demonstrates automatic profiling, ATT&CK mapping, and identification of the threat actor. The methodology incorporates a combination of qualitative methods to analyze the theoretical accuracy of the proposed solution and quantitative methods to evaluate its operational feasibility.

DISCUSSION

Related work

Automatic extraction of CTI and actor profiling have somewhat received academic attention, mainly in systems that translate unstructured reports into structured knowledge. AttacKG is a landmark research study suggesting automatic conversion of CTI text to technique knowledge graphs. Li et al. (2022) evaluated it on over 1,500 real-world reports and achieved F1 scores of 0.79–0.89 in identifying indicators, dependencies, and attack techniques, demonstrating high ability in aggregating CTI into structured threat representations.

Similarly, Satvat, Gjomemo, and Venkatakrishnan's (2021) EXTRACTOR framework infers provenance graphs from narrative incident reports so that downstream threat-hunting systems can comprehend the attack behaviors. This work demonstrates the advantages of extracting behavioral context, as opposed to entities, from text-based CTI.

Subsequently, MultiKG, suggested by Wang et al. (2024), improved the construction of knowledge graph by merging a variety of CTI sources like reports, logs, and static analysis into a unified representation. Utilizing large language models (LLMs) for semantic alignment, they created refined attack graphs, which demonstrated better accuracy and coverage of over 1,000 attack approaches.

In the domain of NLP for CTI, certain works also made noteworthy advancements. The Python library Cybersecurity Named Entity Recognition (CyNER) in conjunction with NLP, advanced by Zhang Y et al. (2025), constructs data extraction system that retrieves non-token-contextual IoCs from CTI texts with higher reliability than traditional sequence-labeling methods. The concept, also known as AttackKG+, allows the constructs of vast threat knowledge graphs by harvesting open-source CTI reports and structuring them via relational modeling, enabling automatic threat intelligence processes.

These papers contribute significantly to the advancement of CTI automation. AttacKG+ and EXTRACTOR aim graph construction from narrative feeds, when MultiKG enhances graph quality through integration of multiple sources. CyNER and ThreatKG, the latter proposed by Gao et al. (2023), increase extraction robustness. They address a pipeline component in isolation, for instance, extraction or graph construction. This paper leverages the contributions by integrating NLP extraction, STIX standardization, ATT&CK mapping, and live graph-based profiling into a real-time pipeline.

Background

CTI refers to processed data gathered from plethora of sources that provides insight into existing or developing cyber threats and is also actionable. CTI prepares the organizations on strengthening cyber defense and system hardening in anticipation of identified malware, malicious domains or IP addresses, social engineering methods, threat actors' behaviour, etc (Rani et al. 2025). To fulfill these expectations, CTI has to possess four key outlines: completeness, accuracy, relevance and timeliness. Without any of these, the provided CTI would not be relevant and could not serve as a basis for further actions. Dissemination and sharing of CTI is facilitated by Threat Intelligence Platforms (TIPs), like IBM X-Force, CISCO Umbrella, Alienvault, etc., and open standards. The exact methods for its sharing are defined by Trusted Automated Exchange of Intelligence Information (TAXII) protocol.

STIX v2.1, developed and approved in 2021 by Organization for the Advancement of Structured Information Standards (OASIS) CTI Technical Committee, established a JSON-based schema for threat information representation, abandoning the XML-files utilized in previous versions. Various types of cyber entities such as threat actors, campaigns, intrusion sets, attack patterns and indicators are defined as STIX Domain Objects (SDOs) which are currently 18 types, separated by fields. Also, STIX v2.1 links objects through relationships. For example, an attack pattern SDO could be linked to threat actor SDO to indicate which actor typically uses the aforementioned pattern. The conducted correlations coalesce into a graph structure that visualizes timeline of a threat displaying who did what, using a definite tool against certain targets (Hu et al. 2024). In addition to SDOs, STIX v.2.1 has two more main object categories- STIX Relationship Objects (SROs) and STIX Cyber-observable objects (SCOs). There are two supporting object types- STIX Meta Objects (SMOs) and STIX Bundle Object (SBO), depicted in Table 1.

Table 1. SDO's categories and types

Category	Description	Example object types
STIX Domain Objects (SDOs)	The core objects that describe the high-level concepts and entities of cyber threat intelligence. They answer the question „what happened?" and are used to build a narrative of an attack. There are **18** SDOs.	threat-actor, malware, campaign, vulnerability, identity, report, indicator, attack-pattern, course-of-action
STIX Cyber-observable Objects (SCOs)	The objects that represent low-level, technical artifacts and data points observed on a system or network. They serve as the „evidence" of an attack and are used to represent concrete data. There are **17** SCOs.	file, ipv4-address, url, domain-name, network-traffic, email-message, process, user-account
STIX Relationship Objects (SROs)	The objects that link other STIX objects together, providing context and showing how different elements relate to each other. They form the edges of the STIX graph model. There are **2** SROs.	relationship, sighting
STIX Meta Objects (SMOs)	Objects that provide metadata and additional context to other STIX objects. They are used to enhance or extend the core objects with extra information. There are **3** SMOs.	language-content, marking-definition, extension-definition
STIX Bundle Objects (SBOs)	A special object that acts as a container to group and transmit any number of other STIX objects together. It is the primary transport mechanism for STIX data. There is **1** SBO.	bundle

In practice, STIX v2.1 bundles CTI in JSON files and TAXII provides the blueprint for exchange between organizations. This process ensures broad interoperability and standardization allowing usage of CTI by a vast majority of tools or analysts.

After the systematization of raw data, the findings could link to tactics and techniques described in MITRE ATT&CK knowledge base for better comprehension of adversarial behaviour and motivation in common language. Security tools compare observed attack traces to MITRE ATT&CK techniques to build scenarios of how an intrusion unfolded. Moreover, a description of an adversary's actions as, for example, „usage of DLL side-loading for persistence maintenance" maps the phrase to ATT&CK technique ID (T1574.001), which normalizes the information. A

major upside of ATT&CK is its continuous update with new techniques which makes it solid and evolving reference (Jiang et al. 2025). It has been proven that combining CTI data with ATT&CK labels and using ML/NLP to extract relevant phrases from raw data, significantly boosts threat analysis.

A major hurdle in leveraging CTI is the textual nature of most of the relevant information. In recent research it has been noted that NLP could be used to crawl and filter CTI data, recognize malware by name, campaign IDs, adversaries' aliases and extract relations and attributions. Processing CTI text trough NLP pipeline could output structured data suitable for knowledge base feed. For example, a tag of the sentence „DarkForest ransomware uses AES encryption" could yield „Indicator: DarkForest, Technique: Data Encryption, Algorithm: AES", which can be inserted into STIX v2.1 objects. Evidently, NLP can transform unstructured CTI into machine-readable statements, significant for automation.

STIX v2.1, MITRE ATT&CK and NLP provide combination, effective for an automated profiling system. The automated framework leverages the aforementioned in the following order: NLP outlines potential threats, indicators and tactics from raw CTI data. These details are mapped into STIX v2.1 object models with nodes and relationships in a threat graph. Then, existing MITRE ATT&CK TTPs are connected to the nodes for context enrichment and finally graph algorithms or rule-based engines infer threat actor profiles.

Proposed framework

The proposed pipeline is comprised of 6 stages that narrow-down an evolving actor profile from raw threat data.

First stage: Data ingestion: Raw CTI data is continuously harvested from a variety of sources which are open-source intelligence (OSINT) feeds, security blogs, social media, GitHub, dark web forums, internal logs, and sharing platforms like MISP and OpenCTI. Each new report alert would be queued for processing and evaluation.

Second stage: NLP Extraction: The digested text data is fed into NLP pipeline. The NLP performs a plethora of activities such as language detection, tokenization, named entity recognition (NER). Pretrained models identify mentions of important CTI entities like malware families, vulnerability names (CVEs), IP addresses, domain names, hashes, campaign names, possible threat actor names or group tags, etc. NLP could be pretrained to scan for certain verbs and phrases suggesting usage of techniques or tactics. For example, from the phrase „DarkForest exploited a zero-day in Apache" the system would extract „Indicator: Apache-CVE-XXXX, Technique: Exploitation of Vulnerability". There are serious indications for high precision in such tasks performed by NLPs (Arazzi et al. 2023).

Third stage: STIX Encoding: Enabled by the previous two stages, the third instantiates each extracted element into STIX v2.1 object or relationship. As mentioned in *Table 1*, common object types include indicator for IoCs like malicious hashes or URLs, malware for specific ransomware or trojans, etc., threat-actor for identified groups or other entities, attack-pattern for abstracted tactics. For example, if NLP identifies new domain *evil.example.com* used in a cyberattack, a STIX indicator object is created. Next, objects are related as an incident or campaign object could relate threat actor „DarkForest Group" to a set of IoCs and a timeline of action. For STIX v2.1 relating multiple sources is natural as repeated IoC consolidate into one indicator object with multiple malware-samples attributes. Adhering to STIX v2.1 is crucial to ensure seamless sharing of the data between TIPs and tools utilization without incompatibilities.

Fourth stage: Mapping to ATT&CK: As threat reports signal for techniques, e.g. persistence via registry run keys, the framework looks up ATT&CK and the extracted behaviour is assigned with the specific ATT&CK technique ID. The profile is enriched with context and an analyst could comprehend which tactics the actor tends to apply. Cross-referencing against known campaigns is also enabled. If a certain combination of techniques is known under a documented advanced persistent threat (APT) in ATT&CK or OSINT repositories, the framework might suggest an attribution. The mapping is implemented through a lookup table or ML classifier recognizing technique keywords.

Fifth stage: Graph Correlation and Profiling: The STIX knowledge graph enriches and grows with time while rule-based engines could infer higher level insights. If a graph query inspects which threat-actor objects are linked to a particular malware and IoCs, the answer might provide a candidate profile. A similarity scoring could also be applied and if a malware demonstrates high overlapping of IoCs with an existing and labeled cluster, the system signals a possible connection. Another correlation to be observed is the behavioural clustering where a malware could be allied with certain infrastructure or detected common TTPs with other actors, indicating possible campaign groups (Gulbay & Demirci 2024).

Sixth stage: Real-Time Updates: The entire framework is designed for streaming operation as new CTI is processed and threat actor graph is updated incrementally. The continuous updating facilitates the near real-time profiling as the manual analysis and profiling is no longer necessary.

The aforementioned framework is conceptual and modular, and all components such as NLP engines, STIX store, graph database, could be chosen from existing tools or developed by more advanced entities. The key point is how AI-driven extraction, structured representation and standard threat models could automate profiling through combination. The following section illustrates the framework in action with a hypothetical example.

Simulation case study: darkforest ransomware

To showcase the framework's operability, the paper takes into consideration a hypothetical ransomware tool called DarkForest used in a campaign. The ransomware infected organizations worldwide in a short timeframe. Analysts stumble upon a scattered reports describing that the malware targets Linux servers and utilizes a version of a well-known encryptor. OSINT forum contains snippets of DarkForest ransom note and references to the leaked source code. All of this raw input would go through the framework's ingestion queue.

Step 1 - NLP Extraction: Reports state that the ransomware was delivered via spearphishing using 4096-bit RSA encryption. The NLP model identifies „actor" DarkForest, „technique", „spearphishing [T1566]" and „crypto details" 4096-bit RSA as an Attack Pattern. On another dark-web forum, an IP address and URL were shared. These became Indicator Objects. In addition, SymBiote rootkit (a fictional tool) was mentioned in the post. This too was tagged as a Malware component by the NLP.

Step 2 - STIX Graph Building: The „DarkForest Group" Threat-Actor has now been created and updates have been made to the Threat-Actor object as new intelligence arrives. Different nodes were assigned to different types of objects. For example, the „Attack Pattern", spearfishing, is connected to the Threat-Actor. Indicators such as phishing domain, payload hash and Malware artifacts are linked to a campaign or intrusion-set referred to as „DarkForest-1". If it is determined that DarkForest's payload has commonalities with a previous malware branch, a connection is established between them. As additional intelligence arrives over time, the graph begins to develop a node cluster around DarkForest with associated IP addresses, domain names, malware signatures and tactics.

Step 3 - ATT&CK Correlation: The framework associates each of the observed behaviors with MITRE's ID as the behavior is mapped to a corresponding tactic identifier. For example, spearphishing is identified as T1566 while rootkit deployment is identified as T1548. All connections are shown visually on the graph. In addition, the system determines that multiple instances of Credential Dumping (T1003) occurred. Previously, a signature of a group called „Epoch-Bear" was found that used the same techniques. This is an indication that DarkForest may be operated by or affiliated with Epoch-Bear.

Step 4 - Inference: With continued inflow of data, the graph illustrates that DarkForest uses ransomware encryption and creates a Command and Control (C2) channel allowing for lateral movement. It appears this profile is identical to a known APT group that specializes in espionage and ransomware. At this point an alert is triggered indicating that DarkForest is likely affiliated with Epoch-Bear due to four common TTPs. For the analysts this is enough to assess the situation as a main lead.

The case study is simplified but it showcases the hypothesis that through AI/NLP and STIX/

ATT&CK, scattered intelligence can be transformed into an actionable CTI. The system in action could refine each step using confidence scores, handling of synonyms for techniques and allow analysts to insert feedback on inferred relations.

RESULTS

Advantages and limitations

The framework proposed in this paper possesses several advantages but also has its limitations. The seamless sharing and comparison of profiles through leveraging of STIX and ATT&CK for standardization of threat data is extremely useful. NLPs and AI additionally speed up the process of analysis that take minutes instead of days. Graph correlations can visualize connections that could be missed by manual processing. Automation of activities like data crawling, extraction and labeling with NLP-based methods enhances further the CTI generation process (Arazzi et al. 2023). Generally, all that would mean faster identification of threat groups and more effective resource allocation by security teams.

The upside potential is clearly visible but the proposed framework has limitations that have to be considered for further study. Automated extraction could produce false outcome based on inaccurate data gathered in bulk or could miss a deeper context as data quality is a permanent issue in CTI. False flags and attributions, deliberate or not, might enter into the profiling process if unchecked. Therefore, the human-in-the-loop remains a safety measure. Explainability is also a concern when it comes to AI suggesting links of an actor to a group without solid evidence, for example a specific shared TTPs.

The context sensitivity is another point which needs attention because a widespread technique like spearfishing may appear in many unrelated campaigns and overgeneralization of the events should be avoided by the framework. A mechanism that stresses more on newer intelligence or requiring multiple sources before confirming a relation is a must. Furthermore, the existing standards mean the framework can profile actors within the known constructs. That means that new threats which use yet unfamiliar methods, may not immediately fit into the existing STIX/ATT&CK categories.

Another limitation is the character of CTI itself. At present, it is more common for nation states and big tech companies to have their own CTI programs tailored for themselves in custom ways. It takes driven entities with clear direction and purpose to maximize on a CTI program because each step of the pipeline demands high degree of technical skills, funding and computational power. This high bar might render the pipeline not suitable for most entities but it does not mean they would not benefit from the end product.

Despite the aforementioned challenges, the integration of AI with CTI is already on the way. Commercial TIPs advertise automatic actor profiling and „lookalike domain“ detection. Academic research also proves the knowledge graphs to be an effective method to aggregate threat data for inference.

CONCLUSION

The paper proposed an automation framework for threat actor profiling that combines AI, particularly NLP, with structured CTI representations, STIX v2.1, and the MITRE ATT&CK model. The exposed approach creates a dynamic knowledge graph of adversary’s behaviour and linked objects, extracted from threat reports after encoding. The concept was showcased by the fictional DarkForest ransomware example proving how scattered intelligence can be unified into coherent actor profile. The results are promising to make threat profiling faster and systematic which would benefits defenders tremendously in attributing campaigns and anticipating attacker moves.

Future research involves prototyping the design utilizing authentic CTI pipelines, such as integrating OpenCTI or MISP, and evaluating it on live data feeds. Advances in LLMs suggest further improvement of CTI extraction with less training. Additionally, enriching the framework with anomaly detection or predictive modules might make possible not only profiling, but also proactive warning of likely new threats. By turning raw data into actionable insights, automating CTI with AI holds a promise to cyber defense.

REFERENCES
ARAZZI, M.; ARIKKAT, D. R.; NICOLAZZO, S.; NOCERA, A.; R. R. K. A.; CONTI, M., 2025. NLP-based techniques for cyber threat intelligence. *Computer Science Review*, 58, 100765. [viewed 9 December 2025]. Available from: https://doi.org/10.1016/j.cosrev.2025.100765
GAO, P.; LIU, X.; CHOI, E.; MA, S.; YANG, X.; SONG, D., 2023. ThreatKG: An AI-powered system for automated open-source cyber threat intelligence gathering and management. *Proceedings of the 1st ACM Workshop on Large AI Systems and Models with Privacy and Safety Analysis*, pp. 1–12. [viewed 9 December 2025]. Available from: https://dl.acm.org/doi/10.1145/3689217.3690613
GULBAY, B.; DEMIRCI, M., 2024. APT-scope: A novel framework to predict advanced persistent threat groups from enriched heterogeneous information networks of cyber threat intelligence. *Engineering Science and Technology, an International Journal*, 57, 101791. [viewed 10 December 2025]. Available from: https://doi.org/10.1016/j.jestch.2024.101791
HU, Y.; ZOU, F.; HAN, J.; SUN, X.; WANG, Y., 2024. *LLM-TIKG:* Threat intelligence knowledge graph construction utilizing large language models. *SSRN Electronic Journal*. [viewed 13 December 2025]. Available from: https://ssrn.com/abstract=4671345 and http://dx.doi.org/10.2139/ssrn.4671345
JIANG, Y.; MENG, Q.; SHANG, F.; OO, N.; MINH, L. T. H.; LIM, H. W.; SIKDAR, B., 2025. *MITRE ATT&CK applications in cybersecurity and the way forward*. *arXiv preprint*, arXiv:2502.10825. [viewed 14 December 2025]. Available from: https://arxiv.org/pdf/2502.10825
LI, Z.; ZENG, J.; CHEN, Y.; LIANG, Z., 2022. AttacKG: Constructing technique knowledge graphs from cyber threat intelligence reports. *European Symposium on Research in Computer Security*. Cham: Springer International Publishing, pp. 589–609. [viewed 14 December 2025]. Available from: https://arxiv.org/pdf/2111.07093
RANI, N.; SAHA, B.; SHUKLA, S. K., 2025. A comprehensive survey of automated advanced persistent threat attribution: Taxonomy, methods, challenges and open research problems. *Journal of Information Security and Applications*, 92, 104076. [viewed 3 January 2026]. Available from: https://doi.org/10.1016/j.jisa.2025.104076
SANTOS, P.; ABREU, R.; REIS, M. J.; SERÔDIO, C.; BRANCO, F., 2025. A systematic review of cyber threat intelligence: The effectiveness of technologies, strategies and collaborations in combating modern threats. *Sensors*, 25(14), 4272. [viewed 3 January 2026]. Available from: https://doi.org/10.3390/s25144272
SATVAT, K.; GJOMEMO, R.; VENKATAKRISHNAN, V. N., 2021. Extractor: Extracting attack behavior from threat reports. *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, pp. 598–615. [viewed 3 January 2026]. Available from: https://arxiv.org/pdf/2104.08618
WANG, J.; ZHU, T.; XIONG, C.; CHEN, Y., 2024. Multikg: Multi-source threat intelligence aggregation for high-quality knowledge graph representation of attack techniques. *arXiv preprint*, arXiv:2411.08359. [viewed 3 January 2026]. Available from: https://arxiv.org/pdf/2411.08359
ZHANG, Y.; DU, T.; MA, Y.; WANG, X.; XIE, Y.; YANG, G.; CHANG, E. C., 2025. AttacKG+: Boosting attack graph construction with large language models. *Computers & Security*, 150, 104220. [viewed 4 January 2026]. Available from: https://doi.org/10.1016/j.cose.2024.104220

АВТОМАТИЗИРАНО ПРОФИЛИРАНЕ НА ЗЛОНАМЕРЕНИ АКТЬОРИ ЧРЕЗ ИЗКУСТВЕН ИНТЕЛЕКТ И КИБЕРРАЗУЗНАВАНЕ: РАМКА ЗА ИЗВЛИЧАНЕ И СЪОТНАСЯНЕ В РЕАЛНО ВРЕМЕ

Резюме: *Киберразузнаването (CTI) се превърна във важен елемент от проактивната защита срещу заплахи в киберпространството. Въпреки това голямата част от важната информация е скрита в обширни масиви от неструктурирани данни и потоци, което прави анализа им изключително времеемък и податлив на грешки. В тази статия е разгледана автоматизирана система, работеща в реално време и ползваща обработка на естествен език (NLP) и стандартизирани онтологии, като например Structured Threat Information Expression (STIX) версия 2. 1 и MITRE ATT&CK, за откриване на индикатори за компрометиране (IoC), тактики, техники и процедури (TTP) от различни източници на CTI, които същевременно се сравняват с профили на злонамерени актьори. Предложената стратегия анализира информация от публични доклади, социални мрежи и различни платформи за споделяне. Рамката е тествана с хипотетичен случай на ransomware, който демонстрира как извлечени индикатори и поведенчески модели могат да бъдат свързани със спецификите на злонамерен актьор. Резултатите показват, че рамката, движена от изкуствен интелект, има потенциала да редуцира значително ръчния труд при обработката на CTI, като същевременно запазва висока точност. Работата поставя основите за внедряване на автоматизирано CTI профилиране на противници, което ще подпомогне проактивната защита и усилията за съотнасяне.*

Ключови думи: *киберразузнаване; изкуствен интелект; профилиране; обработка на естествен език; киберсигурност*

гл. ас. д-р Владимир Бабанов
ORCID 0000-0001-8596-6493, SCOPUS ID: 60021493300
Югозападен университет „Неофит Рилски“
Благоевград, България
E-mail: v.babanov@law.swu.bg