International Journal for
Electronic Crime Investigation

ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

DOI: https://doi.org/10.54692/ijeci.2026.1001/265

Research Article

Vol. 10 issue 1 Jan-Jul 2025

A Threat Intelligence Approach to APTs via MISP and MITRE

Muhammad Saeed Liaqat[1], Gohar Mumtaz[1]

[1]Faculty of Computer Science and Information Technology, Superior University, Lahore, 54000, Pakistan

Corresponding Author: saeedliaqat0786@gmail.com

Received: April 02,2025, **Accepted:** April 8,2025; **Published:** April 8,2025

ABSTRACT

Advanced Persistent Threats (APTs) can be characterized as one of the most sophisticated and dangerous forms of cyberattacks in the modern world. Such cyberattacks might remain undetected by an established defense system and cause enormous harm to the critical infrastructure. It implies that the indicators of malign activity should not be observed in isolation, but rather the broader global perspective of the activity, including techniques, methods, and objectives, should also be provided. Nevertheless, the current system of mapping Indicators of Compromise (IoCs) to adversary practices defined in the MITRE ATT&CK framework, as facilitated by the Malware Information Sharing Platform (MISP), is largely manual, time-consuming, and error-prone, resulting in a high reaction time and insufficient remediation. The coverage of this exigency in the proposed study incorporates an automated framework that integrates MISP and MITRE ATT&CK to form a threat detection pipeline based on intelligence. The proposed framework connects the IoCs to the associated Tactics, Techniques, and Procedures (TTPs), provides contextual data, and also significantly reduces the time required to recognize and fully analyze APT campaigns. Such automation can be evaluated with the help of scenario-based testing and case studies that demonstrate a considerable reduction in analysis time, growth in mapping accuracy, and situational awareness. Tags being tracked in the Automation Army claim that an organization can no longer use reactive handling but can utilize situational awareness and participate in proactive hunting. The given article overcomes one of the most urgent problems of the contemporary security of cyberspace, establishing a pattern of normatively faster, smarter, and more dynamic protection. The implementation of paradigm shifts transforms the entire process of recognition, analysis, and response to APT attacks, making them easier to establish.

Keywords: MISP, MITRE ATT&CK, Cyber Threat Intelligence, Advanced Persistent Threats, Automated IoC–TTP Correlation, Threat Detection and Response.

1. INTRODUCTION

The traditional defense mechanisms are primarily responsive in nature, thus unable to anticipate threats or prevent their occurrence. On the contrary, APT campaigns require a fundamentally different defense strategy—one that prioritizes constant monitoring, exhaustive behavioral analysis, superior situational awareness, and proactive, preventive defense mechanisms [1]. This need has led to the emergent reliance on threat intelligence within modern security operations. This approach enables organizations to gain a more profound insight into adversary intent, tactics, methods, and progression throughout the attack lifecycle. Such intelligence-based awareness enhances timely decision-making, supports swift identification, and empowers security teams to act more effectively before significant damage takes place [2], [3].

MITRE ATT&CK and Malware Information Sharing Platform (MISP) are the two flag bearers within the threat intelligence community. The MITRE ATT&CK architecture provides a broad knowledge base of adversary tactics and techniques, offering a structured taxonomy of the TTPs exploited by attackers during the course of the cyber kill chain [4]. This tool enables defenders to create models of a technical stack used by the attacker, depending on the manner in which they seek information. MISP, in turn, is an open-source threat sharing system that accumulates IoCs including malicious IP addresses, domains, hashes, and phishing artifacts. In this manner, expediting collaborative threat intelligence sharing among organizations improves situational awareness [5].

Despite the fact that both platforms work well in their respective domains, they are frequently used in isolation and independently, which has serious limitations. MISP primarily efforts on gathering, structuring, and disseminating IoCs across organizations and tools, but it frequently lacks extensive contextual or behavioral data on threat actors and campaign intent. On the other hand, the MITRE ATT&CK framework offers a broad behavioral taxonomy of adversary tactics and techniques that aids defenders in comprehending the behavior of an attacker at a strategic level. However, it typically needs external data to populate and contextualize its models [6]. Without incorporating these capabilities, security teams face challenges to correlate low-level indicators with high-level adversary behavior, which limits their ability to produce actionable and well-timed intelligence for improved detection and response [7]. Security teams are presented with several challenges:

- **Fragmented Analysis:** refers to the one in which the IoCs are not related to the behavioral context and hence it cannot be applied [8], [10].
- **Delayed Detection:** Manual comparison of MISP to MITRE ATT&CK is a process by hand that is time-consuming and error-prone. This lack of automation leads to delays in threat recognition and increases the likelihood of inconsistencies, thereby undermining the timeliness and trustworthiness of defensive responses [10].
- **Weaker Actionability:** Threat intelligence lacking automatic correlations is less actionable and difficult to operationalize, delaying its effective usage in real-time security processes [9].
- These inconsistencies point to the fact that a great amount of work needs to be done to find a holistic solution that takes the best of both platforms, in which MISP provides an extensive collection of IoCs, while the MITRE ATT&CK framework provides refined behavioral intelligence.

The proposed work contributes to filling this gap by introducing an automated integration with the MISP and MITRE ATT&CK architectures. The automatic retrieval of the IoCs extracted from MISP with corresponding TTPs in the MITRE

ATT&CK framework, the approach improves contextualization of threat intelligence, thereby allowing more efficient detection, analysis, and response to APTs. This automated mapping alone is economical to reduce the manual load of the analysts, but it is also faster to connect the low-level indicators to high-level adversary behaviors. This will assist organizations to identify threats faster, more accurately, and hence respond to them in a more informed and deliberate manner.

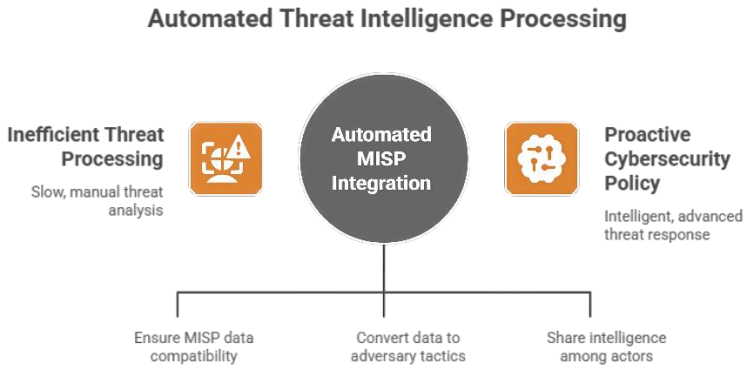

Figure 1: Automated Threat Intelligence Processing

2. RELATED WORK

Advanced Persistent Threats (APTs) have emerged as a major concern in the cybersecurity landscape, predominantly as digital infrastructures become more and more complex. In contrast to conventional cyberattacks, APTs will probably be unnoticed, highly targeted, multiphase, and structured, either by the state machine or by a group of highly advanced cybercriminals [11], [12]. These threats are further differentiated by their survival over long periods, employing zero-day vulnerabilities and customized vectors of attacks to particular targets [13]. Consequently, the perimeter-based security methods have become ineffective in mitigating such threats, particularly in the context of the increasing complexity of attacks and rapid digital transformation [14].

Threat intelligence (TI) has emerged as a proactive cybersecurity defense paradigm to mitigate sophisticated and persistent threats. It includes the systematic collection, examination, and sharing of information about threat actors, including their intentions, strategies, tactics, and operational methods to improve organizational awareness and reaction capabilities [15]. Despite its potential, the efficacy of TI is often restricted by scattered data sources, low automation, and a lack of reliable analytical models [16]. To address such challenges, the combination of low-level technical indicators with higher-level behavioral context is essential. Contemporary TI models are increasingly supported by this strategy.

2.1 Threat Intelligence Standards and Frameworks

TI exchange-oriented standards, such as Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXII), have greatly enhanced cross-organizational connections by aiding the structured and automated distribution of threat intelligence [17]. These standards facilitate the machine-readable exchange of attack patterns, IoCs, and actor profiles, thus

enhancing interoperability of security platforms. Nevertheless, their primary emphasis continues on information sharing rather than on modeling and contextualizing adversarial behavior [18]. The MITRE ATT&CK framework attempts to address this gap; it ensures a complete knowledge base of adversary tactics, techniques, and procedures (TTPs) related to real-world incidents [19]. MITRE ATT&CK supports incident response, threat hunting, and detection engineering by allowing the analyst to determine the development of attackers within different stages of intrusion [20]. However, MITRE ATT&CK does not provide threat information; it needs to be incorporated with other sources to distribute actionable intelligence [21].

2.2 Integrating MISP with MITRE ATT&CK for Enhanced APT Detection

The combination of MISP and MITRE ATT&CK produces a powerful strategy for optimizing the detection of APTs. The IoC-based intelligence of MISP beats the ATT&CK in the behavioral analysis as it allows automatic mapping between indicators and TTPs in raw forms [24]. This integration enables faster detection, enhanced prioritisation of threats, and more appropriate response strategies [25].

2.3 Identified Gaps and Future Research Prospects in MISP and MITRE ATT&CK Integration

Although there are important improvements, there are still various problems that remain with regard to integrating MISP and ATT&CK. Numerous methods are non-scalable and wrestle with big and highly heterogeneous data [23]. The manual forms of processing are still common and it prompts delays and chances of errors [24]. Additionally, the problems of data quality, trust, and privacy do not support the sharing of intelligence created by the cross-organizational [25].

Table 1 presents a comparative analysis of the available research dedicated to MISP, MITRE ATT&CK, and their combination (Area). Some of the challenges identified in the analysis include the lack of automation, uneven data quality, incomplete threat intelligence, and poor contextual correlation (Identified Gap / Challenge). Such restrictions hinder the existing threat intelligence practice by increasing detection latency and falseness, which leads to reduced efficiency in response actions (Impact on Current Practice). Even though automation has been identified as a critical success factor in enhancing precision and response efficiency [22] through standardization of data definition, correlation, and matching, several organizations find it challenging to achieve the process successfully [23].

The literature data show that the combination of MISP and MITRE ATT&CK has a significant positive affected impact on detecting and mitigating APTs. MISP works well in assisting the organization and disseminating the IoCs, and ATT&CK offers the environment of behavioral patterns that is required to comprehend the functioning. The most important pioneers include automation, scalability and real-time data processing requirement development. The context of these gaps, which are to be addressed, will see organizations assume a proactive position in the efforts towards responding to cybercrime rather than a reactive position, which will help in increasing the resilience in the face of the changes in cyber threat responses.

Table 1: Gap identification and research prospects for integrating MISP and MITRE ATT&CK

Area	Identified Gap / Challenge	Impact on Current Practice	Research Prospect / Future Direction
Scalability & Heterogeneous Data	Many existing approaches are non-scalable and struggle with large, diverse, heterogeneous threat data.	Limited ability to process high-volume IoCs and complex APT campaigns in real time.	Design composite, scalable architectures; use distributed processing, graph databases, and streaming pipelines.
Reliance on Manual Processing	Manual correlation and analysis remain common for MISP–ATT&CK mapping.	Delays, higher analyst workload, and increased risk of human error.	Develop fully automated IoC–TTP correlation engines with explainable logic to reduce manual overhead.
Data Quality, Trust & Privacy	Issues of data quality, trustworthiness, and privacy hinder cross-organizational sharing.	Incomplete, inconsistent, or withheld intelligence limits collective defense.	Frameworks for data validation, reputation scoring, anonymization, and privacy-preserving sharing across entities.
Limited Use of Advanced Analytics	Under-utilization of graph analytics, adaptive ML, and advanced correlation techniques.	Missed relationships between campaigns, actors, and TTP chains.	Integrate graph-based TI models, adaptive/online ML, and correlation across temporal and relational threat contexts.
Real-time Processing Constraints	Lack of robust real-time ingestion and correlation between MISP and ATT&CK.	Reactive posture; delayed detection and mitigation of APT activities.	Develop real-time TI pipelines and event-driven architectures for continuous MISP–ATT&CK alignment.
Emerging Technologies & APT Evolution	Limited understanding of how quantum computing, post-quantum crypto, and new tech affect APT behavior.	Potential future blind spots in detection strategies and threat models.	Study the impact of emerging technologies on attacker capabilities; extend ATT&CK-style models and MISP schemas accordingly.
Proactive vs Reactive Posture	Organizations still largely respond reactively despite available TI frameworks.	Slower adaptation to evolving threats; reduced resilience.	Use integrated MISP–ATT&CK automation to enable predictive, proactive defense models and continuous readiness.

3. METHODOLOGY

In this research work, a conceptual research methodology will be employed to outline the automated threat intelligence system that will combine the Malware Information Sharing Platform (MISP) with the MITRE ATT&CK framework. The goal of this methodology can be to describe the way automation can improve the linkage between Indicators of Compromise (IoCs) and adversary Tactics, Techniques, and Procedures (TTPs) related to Advanced Persistent Threats (APTs).

It should be noted here that there is no system implementation or empirical analysis in this research work; only the definition of a structured model has been targeted in this research.

.

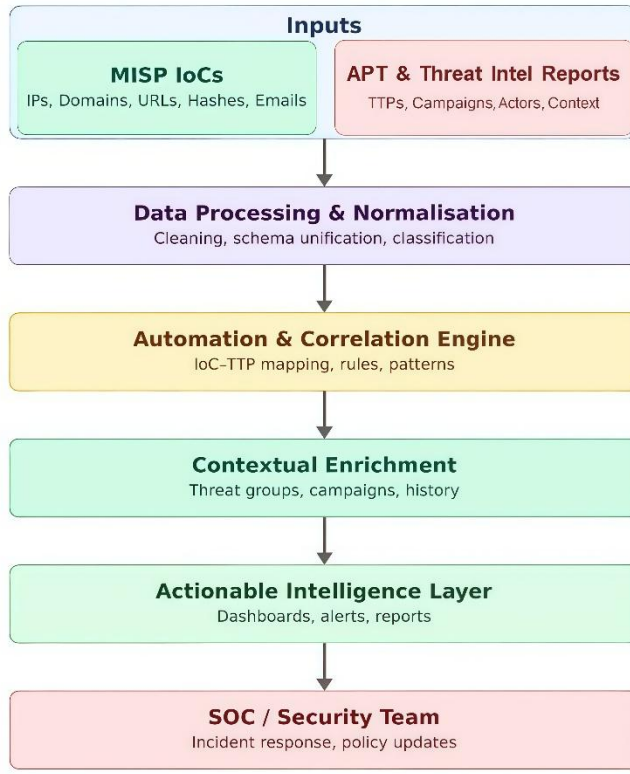

Figure 2: Conceptual architecture of the proposed MISP-based automated threat-intelligence framework.

The proposed methodology follow a conceptual design to alleviate dependence on manual analysis of threat intelligence. Under current security processes, analysts have to manually relate IoCs extracted from MISP to corresponding ATT&CK techniques, which is time-consuming with a potential for inconsistency. Conceptually, this work seeks to conceptualize the efficiency of automation of this exercise to quicken decision-making by security teams.

3.1 Research Approach and Aim

The proposed methodology follow a conceptual design to alleviate dependence on manual analysis of threat intelligence. Under current security processes, analysts have to manually relate IoCs extracted from MISP to corresponding ATT&CK techniques, which is time-consuming with a potential for inconsistency. Conceptually, this work seeks to conceptualize the efficiency of automation of this exercise to quicken decision-making by security teams.

This connection is of vital importance as currently, modern usage presupposes an overwhelming dependency on human analysts as the ones who carry out manual correlation. This dependency does not only cut down on the response time, but also increases the chance of inaccuracies or omissions. Through automation, the study aims to explain how security users can expressly improve the rate at which threats are interpreted, improve decision-making, and reduce reliance on human interventions.

3.2 Data Collection

To comprehensively evaluate the effectiveness of different classification algorithms for spam detection, we trained and tested multiple models on the preprocessed dataset. Each model was selected to represent different learning approaches, allowing us to compare their strengths and limitations for this task.

The quality and the heterogeneity of the data used determines the effectiveness of any threat-intelligence process. This study, therefore, recommends the following two main sources of data to be used:

- **Information provided by the Malware Information Sharing Platform (MISP):** MISP is supported by many cybersecurity units because of the possibilities to share and obtain information about potential threats. The data includes IoCs (indicators of compromise), including suspicious IP address, domain names, file hash and URL, as well as email address. These IoCs prove irreplaceable because they provide technical evidence of bad activity done on a network or outside of one.
- **Information gathered through publicly released Advanced Persistent Threat (APT) and threat-intelligence reports:** This is a good source of information and it is typically compiled in the form of a report by a cybersecurity agency, research team, or government and provides an in-depth account of an attacker. They often contain details about the behaviour of attackers, the campaign goals, and the correlative to the MITRE ATT&CK model. Show in Table 2.

Table 1: Model Performance for Different Test Sizes

Source	Type of Data	Example Fields	Role in Framework
MISP Platform	Technical IoCs	IP, domain, URL, hash, email, malware family	Core raw indicators for automated correlation
Public APT / Threat-Intel Reports	Contextual & behavioural intelligence	TTPs, campaigns, threat actors, timelines	Provides context and behavioural mapping

The two data sources (the technical data provided by MISP and the contextual information that is provided by reports) incorporated in the proposed methodology would guarantee that both low-level technical data and high-level behavioral intelligence are at the behest of the analysts.

3.3 Random Forest

After collection, threat data needs to be preprocessed to remove inconsistencies and enable it to be ready for automation processing. The preprocessed stage comprises data cleansing to eliminate duplicate data, data synchronization to convert data into a standardized form, extraction of data from unstructured threat reports, as well as classification of IoCs into distinct types, including network-based or host-based IoCs.

This steps involves several sub-processes:

- **Data Cleaning:** Only sufficient amount of data is saved to analysis by removing duplicate or irrelevant data.
- **Standardization:** IoC data are all represented in a uniform structure, e.g. JSON or CSV to make them processable by automation.
- **Keyword and Metadata Extraction:** Unstructured reports are extracted to identify useful keywords and attacker identities, timestamps and campaign allusions.
- **Classification:** IoCs are grouped into types: network, host-based, or behavioral which simplifies mapping to the correct TTPs.

This preprocessing ensures that the data are correct, conforming and ready to be used in the later automation phase. The preprocessing pipeline (Figure 3) consists of four key steps, detailed in Table 2.

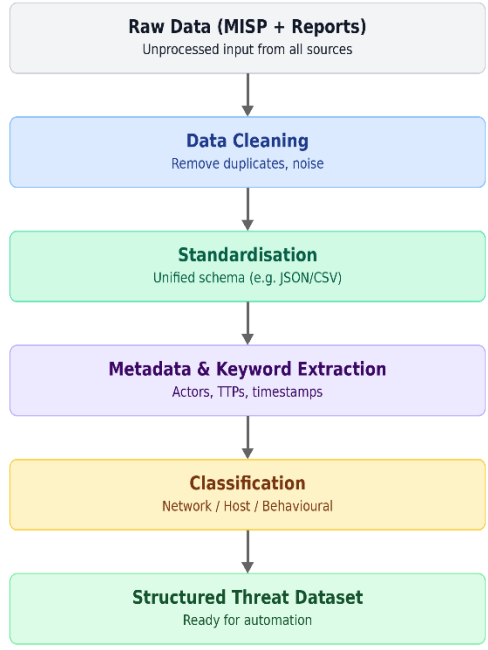

Figure 3: Data processing and normalization pipeline

3.4 Automation and Correlation Process

At the core of this approach is an automated correlation process to map IoCs in MISP to certain MITRE ATT&CK techniques based upon predetermined rules. Each IoC is connected to appropriate TTPs with additional contextual information like known actors/attackers of specific campaign patterns. This automated process of map-making helps lessen the workload of humans in the process, as well as making the interpretation of threats more consistent. The correlation process consists of three main tasks:

- **IoC Extraction:** The system is automatically used to extract the IoCs on the MISP platform which has the potential to extract thousands of data points based on varying sources.
- **TTP Mapping:** When we have IoCs, applying some predefined logic, rule sets, pattern-matching methods is performed to match each IoC to its possible corresponding TTP- such as a malicious URL can be paired with a phishing technique or a command-and-control technique.
- **Contextual Linking:** The system makes the data that is mapped complementary by providing other context, linking the IoC and the TTP with information: known attacker groups, names of a campaign, or other past attack patterns, which helps to develop a full understanding of the motives and implementation of the incidence.

The methodology significantly decreases the time between the threat analysis and can provide more information about attacker behavior, through this automated mapping and enrichment.

Table 3: Example IoC–TTP Mapping

IoC Type	Example IoC	Mapped TTP ID	TTP Name	Possible Context (Example)
Domain	`login-secure-example.com`	T1566.002	Phishing: Spearphishing Link	Credential theft campaign
IP	`185.10.10.10`	T1071	Application Layer Protocol (C2)	C2 infrastructure for APT activity
Hash	`ab3f...`	T1204	User Execution	Malicious attachment execution
URL	`hxxp://malicious-example`	T1105	Ingress Tool Transfer	Payload download

3.5 Multi-Layer Perceptron

The framework finally presents actionable intelligence in the form of conceptual dashboards, alerts, and structured reports once the correlation is complete. These outputs will support security analysts by highlighting attack stages, adversary behaviors, and recommended response actions, thus allowing more informed and timely decisions on defense. The generated intelligence uses:

- Identifying the means that are likely applied by the opponents.
- The stage of the attack lifecycle (i.e.

initial access, execution, persistence).

- The mapping of associations between IoCs, attacker patterns and APT campaigns in the known.
- Countermeasures/ response actions of defense.

This is categorised and valuable intelligence which can be employed to assist organisations in prioritizing the incidents to form strong making defensive positions and distribute resources where they can be used to maximum advantage.

Once IoCs are mapped and enriched, the system generates actionable intelligence in the form of dashboards, alerts, and structured reports. Figure 4 conceptually depicts such a dashboard.

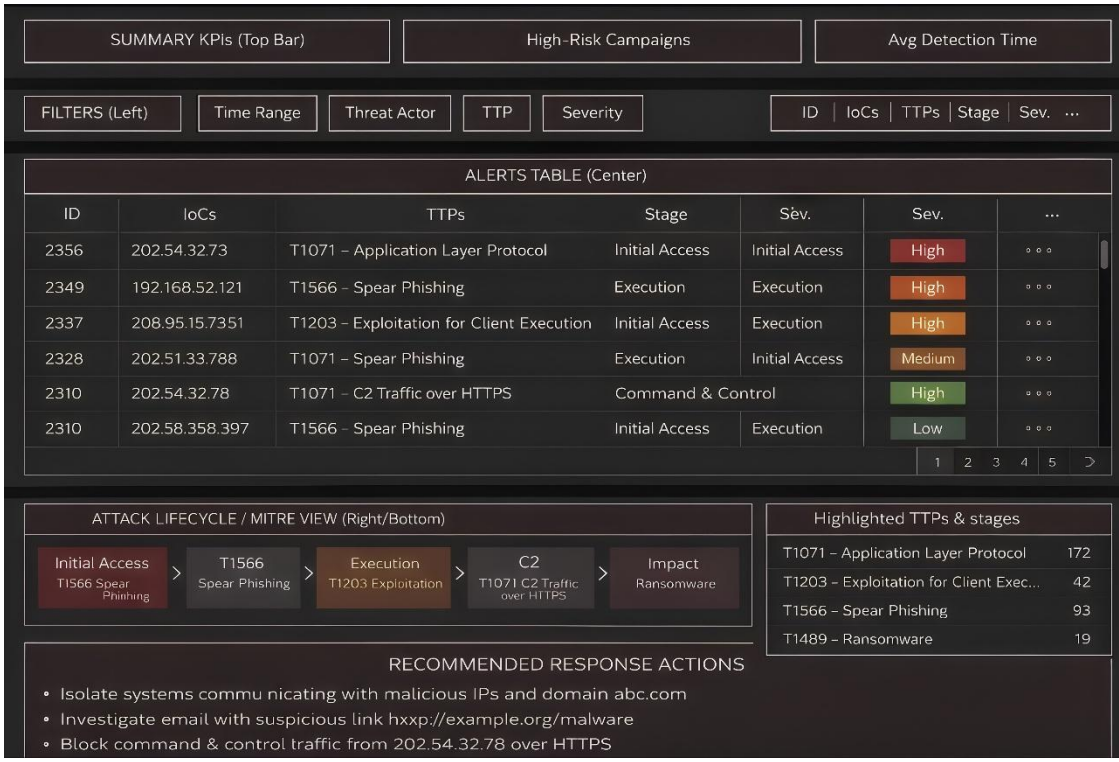

Figure 4: Conceptual threat-intelligence dashboard layout

Table 4: Example Actionable Intelligence Outputs

Alert ID	Key IoCs	Associated TTPs	Attack Stage	Recommended Response
A-001	IP, domain, URL	T1566, T1071	Initial Access, C2	Block IoCs, reset creds, check email logs
A-002	File hash, process artefacts	T1059, T1105	Execution	Quarantine host, run EDR/AV scan
A-003	Multiple C2 IPs, proxies	T1071, T1090	C2 / Persistence	Block ranges, monitor outbound connections

3.6. Applications of the Methodology to Achieve Results

In adopting the above methodology, organizations would expect to perform some important modifications in their cybersecurity procedures:

- **Quickening Detection:** TTPs incorporating automation, it is time-consuming to locate the IoCs with TTPs and thus, saves on time needed to be able to detect the threat.
- **Greater Accuracy:** There is the benefit that automated logic will reduce the human error and make the threat analysis more accurate.
- **Greater Threat Visibility:** The combination of both granular technical data and high-level behavioural intelligence yields the provision of the area of threat in a larger scale.
- **Better Decision-Making:** The security teams will be able to develop better strategic and tactical response with increased and more accurate intelligence.

These discoveries are directly related to the findings that were established in this paper, which, in its turn, are the reduced degree of manual labor, shorter time of detection, greater accuracy, and situation awareness.

3.7. Issues of Ethics and Practice

The methodology supposes the application of the ethical concerns. The information utilized in the present study is publicly available or anonymized and the proposed system is not intended to serve other purposes than defensive purposes. The general objective is to improve the level of cybersecurity, privacy, strengthen the law compliance process, and ethical standards.

Table 5: Methodology Components and Expected Benefits

Ethical Principle	Practical Measure
Data Minimisation	Only process required IoCs and relevant intel
Anonymisation	Remove / mask sensitive or personal identifiers
Legal Compliance	Align with organisational, national, and data laws
Defensive Use Only	Restrict framework usage to protection and monitoring

4. RESULTS

The results in this section are conceptual and obtained from the proposed automated threat-intelligence framework and not from any empirical or experimental measurements. These results highlight how the integration of MISP with the MITRE ATT&CK framework for IoC–TTP correlation would create an impact, based on established threat intelligence best practices and literature. The figures and tables included in this section serve as illustrative representations of the framework's anticipated benefits for security analysts and incident-response teams.

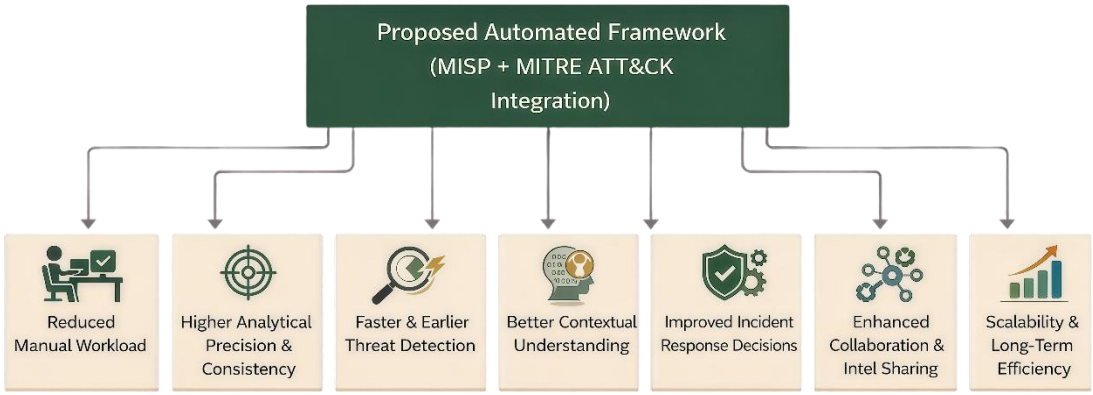

Figure 5: Overall Impact of the Proposed Framework

4.1. It Drastically Cut the Recurrent Hand Work.

One of the main outcomes of the specified solution is the fact that the number of manual work that will be required to process the threat information will decrease significantly. The analysts customarily take a very long time manually parsing Indicators of Compromise (IoCs) that have been retrieved using MISP, and then attempt to align it with the corresponding Tactics, Techniques, and Procedures (TTPs) defined as part of the MITRE ATT&CK framework. Besides being a time-consuming process, this procedure is also associated with inconsistency and inclination to mistakes. With the incorporated automated methodology, the duration that is used on the manual correlation is greatly reduced. The automation engine automatically collects and processes as well as links the IoCs with appropriate TTP without human intervention at every point. Therefore, activities, which would have taken several hours or even days to accomplish them, could now take a significantly shorter amount of time to be accomplished, i.e. in some cases it took minutes. By easing manual workload, this will allow cybersecurity personnel to focus on tasks of a more complex nature, including polishing on and coming up with offense measures in advance or researching high-priority incidents.

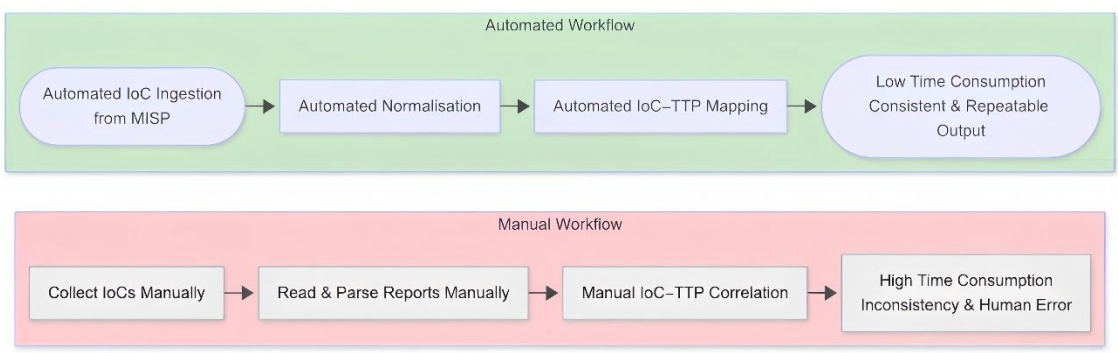

Figure 6: Reduction in Manual Effort (Manual vs Automated)

4.2. Better Analytical Precision and Consistency of the Threat.

The other interesting implication of the proposed methodology is that the accuracy and consistency of the process of correlation of threat information will improve significantly. The human analysis can be easily affected by bias, exhaustion, or lack of the context information, which may render inaccurate or partial results. Automation on the contrary uses the same set of set rules and logic of correlation over and over again resulting in the same and reproducible results. The computerized mapping of IoCs to TTPs ensure that the analysis of every indicator will be carried out against the objective criteria and will result in a minimum amount of erroneous associations. After this practice, more reliable threat intelligence which can be relied on by security teams can be acquired. Moreover, the standardized correlation procedure makes sure the analogy comes up with similar conclusion among the disparate analysts/ organizations using the same methodology, a must-have in the collaboration and intelligence sharing.

4.3. Faster Detection and Earlier Threat Detection.

One of the most important factors of cybersecurity is speed which the given methodology provides at a faster pace compared to conventional methods. Since EIoCs are automatically connected with attacker activities, this concept grants security team's instant insight into the strategies used by attackers. This will accelerate detection and identification of attack threats at earlier stages of an attack. The promptness of detection enables the organizations to react before an attacker achieves his or her goals and thus the organization reduces the impact of an attack. As an example, the loss of data can be eliminated significantly by detecting a phishing campaign at the delivery level instead of at the data exfiltration level. The increased speed of detection can be seen as one of the brightest examples of the efficacy of the offered system.

4.4. Better Contextual Understanding of Threats

The main difficulty in the standard threat analysis is the lack of situational knowledge: that is, regarding the aim of an attacker, the choice of techniques, and an orientation to follow. The suggested methodology is able to tackle this problem, by providing behavioral and strategic context to raw IoC data based on the MITRE ATT&CK framework.

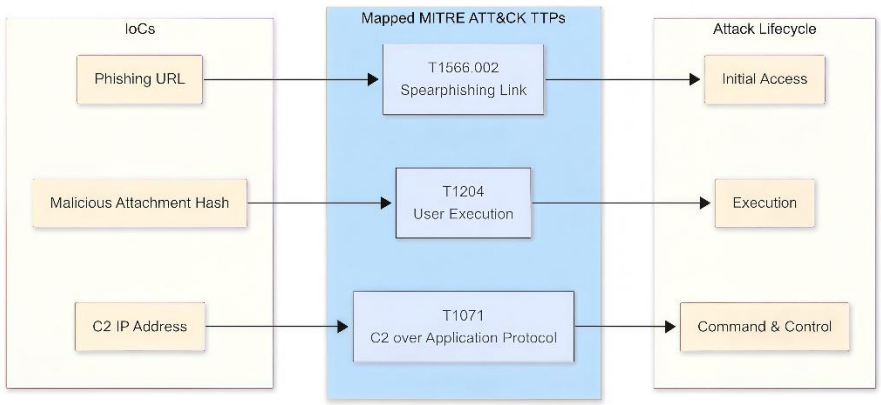

Figure 7: Contextual View of an Attack (IoCs → TTPs → Kill Chain)

After the IoCs are connected to one of the TTPs, the analyst would be able to see the bigger picture of an attack. They can know which step in the attack life cycle approach is underway, how the indicators that they are looking at are coming together as part of the larger strategy of the attacker, and what the next potential course of that attacker would be. This increased intelligence gives the organization a more realistic and viable view of the threat environment and as such it is able to prioritize protection and allocation of resources with greater efficacies.

4.5. Improved Response to Decisions and Incident Response

The methodology improves the reaction to the incident in the decision-making process since it is able to give much more accurate, timely and context-specific intelligence. Security teams are no longer driven to work with incomplete and manually correlated information. Instead they receive a clear report on the kind of threat, techniques used and make direct contact with the probable targets of the enemy. With such information, organizations can come up with faster decisions as well as depend on response strategies. They can make decisions to identify the most appropriate counteractions, priorities to key incidences and long-term defense plan arrangements. This results in a reduced response time, less impact and more aggressive stand in cyberspace.

4.6. Better Interagency Relations and Intelligence Clarifications

The other major outcome of such a methodology is that it will foster better cooperation and exchange of intelligence. As the mapping of the IoCs to TTPs is an automated process, even non-similar organizations or security groups that adhere to the strategy can easy share the results. The application of standard structures and generalized intelligence simplifies the exchange of the data and simplifies the comparison of the results of the researches and enables people to cooperate and detect and eliminate all the existing threats. The multi-layered approach reinforces the overall cybersecurity structure and increases overall defensive capabilities. Having improved intelligence sharing among the organizations, the organizations will be able to install mass campaigns earlier and come up with strategies of countering it.

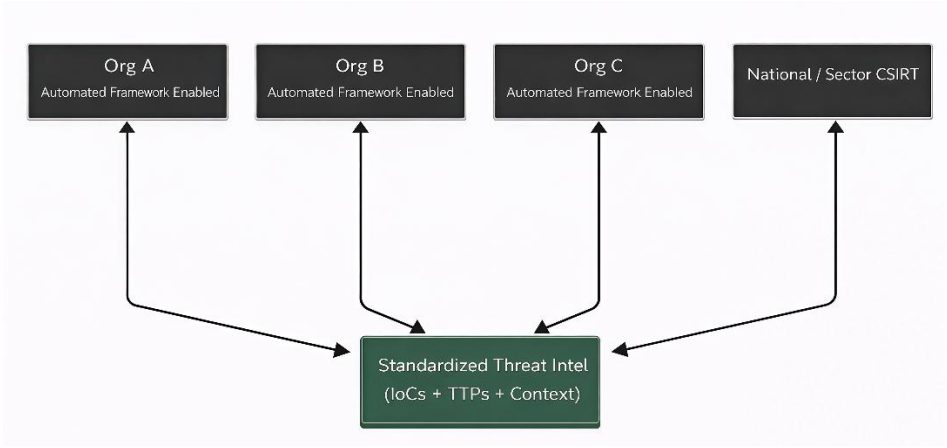

Figure 8: Enhanced Collaboration & Intelligence Sharing

4.7. Scalability and Long-Term Benefits.

The solution proposed can also be scaled to a great extent, and they can enable control over more and more threat data sets as companies increase their digital resources. The process of automation can be left to continue processing and analysing new IoCs that are being collected and assembled without much extra work being applied to it. This attribute of the scale has made sure that the system cannot be rendered irrelevant because the threat environment is also changing and getting more complex. Overall, these conceptual results highlight the potential of the proposed framework to support more efficient is consistent, and content -aware threat-Intelligence operations.

5. CONCLUSION

This research aimed to fix a major dilemma in the modern cyberspace security the high dependency on manually procedures to match a threat intelligence gathered through MISP with the bot techniques and methods defined within a MITRE ATT&CK system. Through the conceptual approach, the investigation also improved an automated process that has a significant impact on improving the velocity, accuracy and effectiveness of Advanced Persistent Threat (APT) detecting and analysis. The concept of automating this workflow conceptually demonstrates how the manner in which organization collect, analyze respond to threat intelligence can evolve in a more structured and efficient way.

Among the implications of the study, one should mention the empirical validation of the fact that automation can significantly reduce the manual workload traditionally handled by security personnel. Dynamic loading of Indicators of Compromise (IoCs), defined systematically and linked to relevant Tactic, Technique, and Procedure (TTPs) and contextual enhancement eliminate the substantial component of the time-consuming nature of the threat intelligence processing. This is the acceleration that will help organizations to swiftly detect any threats and be in a position to counter the threats before they cause such severe harm.

Moreover, automated mapping is standardized and consistent and this is an aspect that enhances the reliability of threat intelligence hence it is easier and more vibrant to distribute it to groups and organizations.

The other positive aspect with regards to the level of contribution the study has provided has been the emphasis on the contextual knowledge. Unlike the unified approach to the attackers of the Internet, the method takes the IoCs as a continuation of larger patterns of attacker behavior. In its turn, organizations become familiar with the macro image of an incidence, its evolution, the possible objectives of the opponent, and the possible future behavior of the opponent. These insights are valuable for supporting proactive defense efforts and informed cybersecurity planning and thus they alter the direction on which cybersecurity is operated to responsive response rather than proactive efforts. The main contributions of this work are threefold:

1. The design of a structured conceptual workflow for automated IoC-TTP mapping.
2. Improved contextual understanding of APT campaigns for security analysts.
3. Enhanced decision support for faster and more informed incident response.

6. FUTURE WORK

Although this work provides a strong conceptual basis for automated correlation between IoCs and TTPs, there are certain paths yet to be explored by future work. First and foremost, there is the implementation and testing of the proposed model by means of a testable prototype system developed within real-world security scenarios, thus allowing for the determination of certain real-world metrics, such as the accuracy

of detections, speed, and false positives.

Another future work is incorporating machine learning and AI algorithms into the correlation process. Use of adaptive learning approaches, in addition to Natural Language Processing (NLP) algorithms, would be useful in enhancing automated intelligence extraction from unstructured threat intelligence sources and enabling improved accuracy in IoC mapping against ATT&CK frameworks.

The future work may also target the integration of the proposed model with SIEM & SOAR systems to facilitate intelligence sharing in a real-time environment. In addition to this, integrating the model with future domains such as IoT & ICS would also add to its applicability in overcoming APT threats in an efficient manner.

7. REFERENCES

[1] C. Gilbert, M. Gilbert, and M. Jnr, "Detection and response strategies for advanced persistent threats (APTs)," *International Journal of Scientific Research and Modern Technology*, 2025, doi: 10.38124/ijsrmt.v4i4.367.

[2] P. Santos, R. Abreu, M. Reis, C. Serôdio, and F. Branco, "A systematic review of cyber threat intelligence: The effectiveness of technologies, strategies, and collaborations in combating modern threats," *Sensors*, vol. 25, 2025, doi: 10.3390/s25144272.

[3] M. Alazab, R. Khurma, M. García-Arenas, V. Jatana, A. Baydoun, and R. Damaševičius, "Enhanced threat intelligence framework for advanced cybersecurity resilience," *Egyptian Informatics Journal*, 2024, doi: 10.1016/j.eij.2024.100521.

[4] MITRE Corporation, "MITRE ATT&CK®: A knowledge base of adversary tactics and techniques," MITRE.

[5] C. Wagner *et al*., "MISP: The design and implementation of a collaborative threat intelligence sharing platform," in *Proc. ACM CCS Workshop*.

[6] B. Al-Sada, A. Sadighian, and G. Oligeri, "MITRE ATT&CK: State of the art and way forward," *ACM Computing Surveys*, vol. 57, pp. 1–37, 2023, doi: 10.1145/3687300.

[7] Y. Jiang *et al*., "MITRE ATT&CK applications in cybersecurity and the way forward," *arXiv preprint* arXiv:2502.10825, 2025.

[8] M. Husák *et al*., "Survey of attack projection, prediction, and forecasting in cyber security," 2019.

[9] S. Mittal *et al*., "Cyber threat intelligence: State of the art and research directions," *ACM Computing Surveys*, 2019.

[10] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," 2018.

[11] Y. Chen and J. Lee, "Advanced persistent threats: Evolving trends and mitigation," *IEEE Security & Privacy*, vol. 19, no. 4, pp. 22–31, 2021.

[12] FireEye, "The rise of APT groups and their operational strategies," *FireEye Threat Intelligence Report*, 2020.

[13] E. Hutchins, M. Cloppert, and R. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns," *Lockheed Martin Cyber Kill Chain Whitepaper*, 2011.

[14] L. Rossi, A. Bianchi, and M. Conti, "Post-cloud APT evolution and detection challenges," *ACM Transactions on Cybersecurity*, vol. 33, no. 2, pp. 55–69, 2024.

[15] J. Park and H. Kim, "Proactive threat intelligence strategies for modern cybersecurity," *Journal of Information Security*, vol. 45, no. 2, pp. 98–112, 2025.

[16] S. Barnum, "Standardizing cyber threat intelligence information with STIX," *MITRE*

Technical Report, 2014.

[17] OASIS, "STIX/TAXII specifications: Threat intelligence sharing standards," *OASIS Consortium Report*, 2023.

[18] MITRE, "ATT&CK framework: Adversarial tactics, techniques, and common knowledge," *MITRE ATT&CK Documentation*, 2022.

[19] F. Skopik, G. Settanni, and R. Fiedler, "Collaborative threat intelligence and automated response," *Computers & Security*, vol. 60, pp. 154–170, 2022.

[20] A. Smith and R. Brown, "Collaborative threat intelligence: Opportunities and challenges," *Computers & Security*, vol. 96, p. 101890, 2020.

[21] CIRCL, "MISP: Malware information sharing platform and threat sharing," *CIRCL Documentation*, 2023.

[22] P. Gupta, V. Mehra, and A. Shah, "Threat intelligence enrichment using MISP APIs," *International Journal of Cyber Threat Analysis*, vol. 12, no. 3, pp. 250–266, 2022.

[23] T. Khan, L. Abbas, and F. Rahman, "Automation in MISP for large-scale threat data correlation," *IEEE Transactions on Information Forensics and Security*, vol. 19, no. 1, pp. 67–81, 2024.

[24] G. Wang, M. Li, and S. Zhou, "Scalability and privacy challenges in cross-organizational threat intelligence sharing," *IEEE Access*, vol. 13, pp. 11576–11589, 2025.

[25] A. Dsouza and F. Khan, "Automated mapping of threat indicators to ATT&CK techniques," *IEEE Access*, vol. 12, pp. 5560–5573, 2024.