

Threat Intelligence Quality Assessment Model Based on ATT&CK Framework for Multiple Application Scenarios

Guangxiang Dai^{1,2}, Peng Wang^{2(✉)}, and Pengyi Wu²

¹ School of Cyberspace Security, University of Chinese Academy of Sciences

² Institute of Information Engineering, Chinese Academy of Sciences
wangpeng3@iie.ac.cn

Abstract. With the increasing severity of cyber threats, cyber threat intelligence (CTI) has become a crucial tool for enhancing cyber security protection. Maximizing the potential value of threat intelligence requires properly and efficiently sharing. However, the sharing process often faces challenges such as quality assessment. To tackle the problem of quantification in quality assessment and remedy the gaps of current methods, this paper proposes a threat intelligence quality assessment model based on ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework for multiple application scenarios. We introduce assessment metrics from event perspective, take TTPs (Tactics, Techniques, and Procedures) and other elements into account, and incorporate specific application scenarios to objectively evaluate threat intelligence so as to provide practical guidance for security practitioners and filter out intelligence with practical value. Finally, we demonstrate the effectiveness, practicality, and high coverage in terms of event-relevant metrics of the model through experimental assessment.

Keywords: Threat Intelligence, Quality Assessment, Intelligence Sharing, Security Application Scenario.

1 Introduction

As cyber threats become more pervasive and persistent, the cost of cyber attacks is gradually decreasing due to diverse entry points, advanced intrusion methods and systematic attack tools, and threat intelligence solutions featuring “one point of discovery, global sharing and collaborative linkage” are becoming the mainstream response. However, the fragmentation of intelligence gathering and analysis in the security field not only increases information silos, but also restricts the active flow of intelligence between organizations, which is not conducive to the formation of a healthy and efficient threat intelligence ecosystem. The utilization of threat intelligence sharing and exchange technologies allows for the timely acquisition of threat intelligence generated in other networks, thus maximizing its value. This, in turn, enhances the threat detection and emergency response capabilities of all participating entities, ultimately mitigating

the asymmetry between offensive and defensive confrontations. According to the National Cybersecurity Strategy published by the U.S. White House in March of 2023[1], the federal government aims to enhance the speed and scope of sharing cyber threat intelligence. This will enable proactive alerting of cyber protectors and timely notification of potential victims, concerning potential attacks or threats targeted at organizations.

Though CTI holds a crucial role for security organizations in cyber risk discovery and analysis, in the process of threat intelligence sharing, the quality of each intelligence varies, which can result in issues such as “free-riding”. In the “SANS 2023 CTI Survey” report, it highlights the distribution and feedback of threat intelligence as a crucial step in maximizing the potential of intelligence. However, this process is hindered by challenge such as fake intelligence[2]. Aiming at the problem of false intelligence, Gao et al.[3] constructed a trust assessment framework for threat intelligence based on graph mining, which extracts intelligence features from multi-dimensions of source, content, time, and feedback, and provides automatic and interpretable trust assessment for large-scale heterogeneous threat intelligence. The fact is, however, that credible intelligence still has a high or low quality which needs to be further quantified. The utilization of low-quality threat intelligence, such as redundant or outdated information, could affect the efficiency and accuracy of security organizations’ decision-making. Hence, it is imperative to implement filtration mechanisms in the intelligence sharing process to exclude low-quality intelligence.

Current quality assessment methods of threat intelligence predominantly target structured intelligence, specifically the underlying Indicators of Compromise (IOCs), which typically relate to short-lived intelligence such as the domain name utilized by a specific phishing website in a single attack event and numerous researchers conduct quantitative assessments by considering various metrics like accuracy and timeliness[4-8]. However, in the case of Advanced Persistent Threat (APT) attacks, a narrow concentration solely on low-level IOCs metrics related to the attack techniques is insufficient for obtaining comprehensive contextual information about the attack[9]. To address this limitation, cybersecurity experts have introduced the concept of Tactics, Techniques, and Procedures (TTPs)[10]. TTPs belong to long-term intelligence, requiring expert experience to analyze the logic between IOCs and single attack events. Within the well-known “Threat Intelligence Pyramid of Pain”[11], TTPs hold the highest value, which detail the attacker’s steps, the interconnections between these steps, the techniques employed, and the associated IOCs, and are often hidden in unstructured intelligence. However, existing quality assessment methods for unstructured threat intelligence lack focus on assessing the TTPs within them[12-15]. In addition, upon examining threat intelligence quality assessment methods, it is evident that current methods fail to consider the different requirements of intelligence consumers in various application scenarios.

Facing the unstructured credible threat intelligence data, this paper proposes a threat intelligence quality assessment model based on ATT&CK framework for multiple application scenarios, aiming to tackle the challenges encountered in current practices of threat intelligence sharing and bridge the limitations of existing quality assessment methods. The primary contributions of this paper include:

- With the aim of analyzing the attack methods embodied in the intelligence at a finer granularity, our assessment is dedicated to extracting TTP-related high level information from unstructured CTI text and quantifying the metrics in conjunction with the ATT&CK framework, thus guiding security practitioners to more effectively utilize CTI to understand adversary tactics and objectives and prevent future attacks.
- Our scheme establishes a metric system based on the elements in attack event and combines with the general application principles while considering specific intelligence application scenarios, so as to filter out intelligence with practical value.
- It has been experimentally validated that, our approach could effectively filter out high-quality intelligence for specific application scenarios, such as attack attribution analysis.

The following sections of this paper are organized as follows: Section 2 gives a concise overview of related work; Section 3 introduces the proposed threat intelligence quality assessment model based on ATT&CK framework for multiple application scenarios; Section 4 introduces a CTI sharing scenario incorporating with the proposed model; Section 5 conducts an experimental analysis; and lastly, Section 6 summarizes the entire work and explores future research directions.

2 Related Work

2.1 Quality Assessment of IOC Intelligence

IOC intelligence, as a structured intelligence, primarily focuses on the features associated with tools used by attackers and network infrastructure information, including file hash, ip, domain name, program run paths and registry entries, etc. Security Operations Centers (SOCs) frequently utilize this intelligence to detect and counter emerging cyber threats. Additionally, IOC intelligence proves valuable for threat hunting teams in tracking Advanced Persistent Threats (APTs) and other covert adversaries. The quality of IOC intelligence could be effectively assessed by considering metrics such as completeness, accuracy, relevance and timeliness.

Shi Huiyang et al.[4] proposed a threat intelligence assessment method based on blockchain and neural network, which utilizes the data provided by intelligence vendors and sharing platforms, transforms them into STIX format after preprocessing, and applies hierarchical analysis to filter out secondary metrics. Subsequently, the validity and operability of the assessment model are verified using a neural network algorithm. Hu Yuxi et al.[5] proposed a threat intelligence source quality assessment model based on hierarchical analysis, which considers both intelligence sources and intelligence data, establishes a hierarchical structure, determines the weights of the metrics, and quantitatively calculates the assessment. Experimental results demonstrate that this model effectively differentiates between intelligence sources of varying qualities and facilitates dynamic monitoring and selection of the best sources. Schlette D et al.[6] proposed a method to measure and visualize the quality of threat intelligence in STIX format. This method defines multiple dimensions associated with the quality of threat intelligence and establishes metrics for evaluating each dimension. Furthermore, it exhibits good

extensibility to other data formats. By expanding the interactive visualization of existing threat intelligence analysis tools, it enhances transparency in the quality assessment process for security analysts. Griffioen H et al.[7] developed a taxonomy for assessing the quality of CTI feeds. The taxonomy evaluates the timeliness, sensitivity, originality, and impact of CTI feeds, as well as their utility and risk to organizations, by analyzing network traffic data and regional transmission data. Zhang Xiaohui et al.[8] proposed a reputation-based threat intelligence sharing model that utilizes federated blockchain technology. The model aims to enhance security, trustworthiness, and address the issue of false intelligence during the sharing process. It incorporates a Proof of Reputation (POR) consensus algorithm to ensure validity and security requirements are met. Finally, they designed three test scenarios implemented in a simulation environment for a comprehensive evaluation, and the results demonstrate that the proposed sharing model successfully fulfills the necessary criteria for efficient threat intelligence data exchange in terms of speed, scalability, and security.

2.2 Quality Assessment of Unstructured Intelligence

As previously noted, TTPs focus on the attacker’s modes of action and attack patterns, and offer more comprehensive contextual information than IOCs, and are therefore more conducive to grasp the attacker’s tactics and logic of action, thus assisting organizations in predicting and mitigating forthcoming attacks. Nonetheless, such intelligence is often hidden in unstructured text, posing challenges in evaluating its quality.

Mitra S et al.[12] proposed a method for filtering false threat intelligence using the Threat Intelligence Knowledge Graph (TIKG), which incorporates both the content of threat intelligence and the source information to calculate the confidence level of the intelligence. Purohit S et al.[13] proposed a threat intelligence sharing and defense system called “DefenseChain”. This system establishes a credibility-based evaluation model that measures the value of intelligence by considering the “quality of detection” and “quality of mitigation”. Tundis A et al.[14] proposed an automated method for assessing the quality and predicting the relevance of open-source cyber threat intelligence sources. Based on metadata and word embedding models, the method predicts the relevance scores of intelligence sources on Twitter by training regression models, which improves the processing efficiency and accuracy of threat intelligence. Zhang Shuqin et al.[15] proposed the Cyber Threat Intelligence Automated Assessment Model (TIAM) as a method for the automatic evaluation of CTI. This model, in conjunction with the ATT&CK matrix, enables the assessment of sparsely available threat intelligence from multiple dimensions, aiding in promptly addressing cyber threats by automating the evaluation process.

Table 1. Comparison of Methods Related to Quality Assessment.

Related Work	Methodology	Type of Intelligence
[4]	Metric Quantification, Hierarchical Analysis	Unspecified

[5]	Neural Networks, Hierarchical Analysis, Reputation Computing	STIX-based
[6]	Quantification of Metrics	Unspecified
[7]	Quantification of Metrics	IOC
[8]	Reputation Computing, Bayesian	STIX-based
[12]	Knowledge Graph, NLP	Unstructured Text
[13]	Quantification of Metrics	Unstructured Text, IOC
[14]	Quantification of Metrics, Regression Analysis	Unstructured Text (Twitter)
[15]	Quantification of Metrics	Unstructured Text

Analysis of **Table 1** reveals that current methods for assessing threat intelligence quality primarily focus on establishing a metric system and conducting quantitative analysis. These methods overlook the assessment of high-value TTP information within intelligence and fail to sufficiently link quality assessment to practical application scenarios, leading to problems related to practicality and coverage.

2.3 ATT&CK Framework

The ATT&CK framework, developed by MITRE enterprise, serves as a comprehensive database of observed malicious activities in the real world, including TTPs. It provides a detailed description of the threat landscape related to specific business operations and offers a malicious activity chain from initial access to the ultimate target. Consequently, it guides security personnel in predicting subsequent attack actions[16]. In recent years, there has been a great amount of work surrounding the ATT&CK framework, focusing on two main aspects. On the one hand, efforts have been made to extract ATT&CK knowledge from unstructured texts[17-20]. On the other hand, there are efforts towards analyzing the extracted ATT&CK knowledge and offering guidance for security decision making[21-23].

In our method, we assess threat intelligence from an event perspective and introduce assessment metrics associated with TTPs that can provide practical guidance to security practitioners. Currently, the extraction and analysis of ATT&CK framework within the academic community have reached a relatively mature stage, enabling the framework's utilization in assessment of TTPs.

3 Threat Intelligence Quality Assessment Model Based on ATT&CK Framework for Multiple Application Scenarios

The “2023 Threat Intelligence and APT Activity Analysis Report” by Threatbook summarizes the trends concerning phishing and ransomware attacks[24], noting:

- Attackers commonly register a large number of new domains to deploy phishing pages and mainly use relatively cheap first-level domains in order to reduce the cost. In addition, in recent years, phishing attacks have shown a trend of “templatization”.

- From 2019 to 2023, the average ransom price of ransomware continues to rise, which indicates that attackers are conducting targeted attacks on high-value targets and technology is constantly advancing.
- There has been a trend of repeated ransoms targeting the same victims. It is possible for different ransom organizations to carry out second attacks on the same victim after an initial attack.

The above trends have indicated that, in cyber attack events with high complexity and persistence, there are elements that are easily changeable, such as attack methods, and elements that present resistance to change, such as attack targets and attack motives, where the former reflects the diversity and complexity and the latter reflects the strong organization and purposefulness of cyber attacks.

Before conducting the assessment, it is necessary to standardize the representation of threat intelligence. An ontology is a formal description of important concepts shared in a specific domain, mitigating conceptual and terminological ambiguities[25]. Therefore, an event-based threat intelligence ontology will be introduced[26], which on the one hand enables the expression of the various event elements in the intelligence by means of the semantic properties of events, and on the other hand facilitates intelligence sharing after quality assessment.

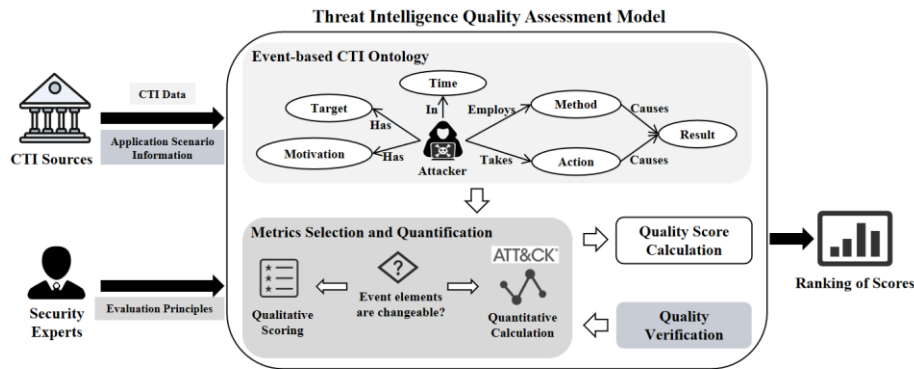


Fig. 1. Overall architecture of Threat Intelligence Assessment Model. Collect threat intelligence from various CTI sources; convert and fuse data through threat intelligence ontology; establish the system of metrics and conduct quantitative analysis in line with general principles while combining the application scenario information; and calculate the quality score of threat intelligence.

Regarding the evaluation of data quality, Joseph M. Juran, author of Juran’s Quality Handbook[27], defines that “Data are of high quality if they are fit for their intended uses in operations, decision making and planning.” In other words, intelligence that fails to meet its intended purpose in practical application is not deemed high-quality. Therefore, we consider to propose a series of general principles to guide the quality assessment of threat intelligence from the perspective of practical application.

Building upon the analysis above, this paper proposes a quality assessment model designed to provide practical guidance for security practitioners and filter out intelligence with practical value, which considers assessment metrics from event perspective,

takes TTPs and other elements into account, incorporates the ATT&CK framework and combines with practical application principles and specific application scenarios. The overall architecture of the model is shown in **Fig. 1**.

3.1 Event-based Threat Intelligence Ontology

To enhance the dynamic semantic expression and reasoning ability of threat intelligence, we leverage the improved skeleton method to construct the event-based threat intelligence domain ontology, in which the formal concept analysis(FCA) method is used to elevate the automation level of ontology construction[26].

Then, we convert the unstructured CTI text into event-based threat intelligence, encompassing essential event elements such as time, attacker, target, action, motive, attack method and result. The detailed description of each element can be found in **Table 2**, where the first four elements are necessary, while the remaining three are optional (participants can choose whether to provide them or not). For further explanation on the ontology construction and definition of entities, attributes and relationships, we recommend consulting our previous work[26].

Table 2. Event-based Threat Intelligence Information.

Essential Elements	Explanation	Examples	Necessity
Time	Time of occurrence	2023/6/29 10:01:23	Necessary
Attacker	Attacker IP (pool) or identity information	10.11.10.12 or APT 29	Necessary (partial)
Target	Target IP (pool) or identity information	10.11.10.12 or Winter Olympics official website	Necessary (partial)
Action	Types of attacks	Access, scanning, vulnerability exploitation	Necessary
Motivation	Motivation for the attack	Intelligence acquisition, covert control, attack paralysis	Optional
Method	Methods employed by the attacker	MITRE ATT&CK ID	Optional
Result	Extent of harm caused by the attack	No effect, minor, serious, particularly serious	Optional

3.2 Assessment Principles from the Event Perspective

After ontology mapping, we introduce several general principles for assessing the quality of intelligence based on the practical security operation scenarios, aiming to objectively assess the value of intelligence.

- The time of intelligence disclosure should align closely with the time of the attack.
- The background of the attacker should be as strong as possible.
- The attack target should be of utmost importance.
- Unusual attack actions should be disclosed whenever possible.

- The motive of the attack should be significant.
- The attack chain in the attack method should be as comprehensive as possible.
- The attack chain in the attack method should be as coherent as possible.
- The impact of the attack should be maximized.

Concerning the second principle, the scale of the attack group is used to measure the attacker's background. For the fourth principle, we believe that the rarer the attack action, the higher its intelligence value. Both principle 6 and 7 pertain to the attack method, and we posit that a attack chain that more complete and coherent is highly beneficial for security analysts to understand the overall attack strategy and develop corresponding countermeasures.

3.3 Metrics Selection and Quantification

Subsequently, we establish assessment metrics for the information in ontology-based intelligence, in line with the proposed general principles. Taking into account the changeability of the event elements and the uniqueness of each metric, we employ both qualitative scoring and quantitative calculation methods to quantify the defined metrics, as detailed in **Table 3** and **Table 4**.

The formulas (1) and (2) for the metrics in **Table 4** along with their corresponding variables are defined below. Specifically, *techniques* refers to all techniques associated with the intelligence-related attack chain. ω_t represents the weight value of the tactics corresponding to the t-th technique and here we refer to the similarity results in [28] which embodies the principle 4, while n_t represents the total number of techniques corresponding to the tactics of the t-th technique. Similarly, *tactics* signifies all tactics linked to the intelligence-related attack chain. *technique(t)* denotes the number of techniques associated with the t-th tactic, and *len(t, t + 1)* indicates the length of the transition between two tactics.

$$Attack_chain = \sum_{t=1}^{techniques} \frac{\omega_t}{n_t} \quad (1)$$

$$Attack_chain_coh = \omega_0 + \sum_{t=1}^{tactics-1} \frac{technique(t)}{len(t, t+1)} \quad (2)$$

For the ‘‘Attack Impact’’ metric in **Table 3**, we quantify it from two perspectives: the type of attack event and the implementation of the attack. The latter includes ‘‘*actual,’’ ‘‘*generic,’’ and ‘‘*other,’’ which respectively denotes events that have actually occurred, events that are undetermined whether they have occurred, and events that have failed to occur. The scores of these three categories are multiplied by the scores of the corresponding attack event types, and the resulting values serve as the final score for this metric.

Table 3. Assessment Metrics and Corresponding Scores.

Metrics	Related Event Information	Number of Attributes	Attributes	Score
Disclosure Time	Time	3	Within a week	3
			Within a month	2
			Within a year	1
Type of Attacker	Attacker	2	Organization	2
			Person	1
			Organization	3
Asset Owner Associated with the Victim	Target	6	Device	2
			Person	1
			Software	1
			System	1
			Website	1
			Malware spreading	3
Attack Motive	Motivation	8	Unauthorized access	3
			Gathering data	2
			Further attack	1
			Publish data	1
			Selling	1
			Monetary	1
			Other	
			Patch Vulnerability	3
Attack Impact	Result	5	Discover Vulnerability	3
			Ransom	2
			Databreach	1
			Phishing	1
			*Actual	0.5
			*Generic	0.5
*Other				

Table 4. Assessment Metrics and Corresponding Quantization Formula.

Metrics	Related Event Information	Attributes
Techniques - Attack Chain	Action and Method	Formula (1)
Techniques - Attack Chain Coherence		Formula (2)

We aim for the captured chain of attacks in threat intelligence to be complete and coherent, enabling organizations to utilize CTI effectively in understanding adversary tactics and objectives, preventing future attacks, and expediting remedial measures.

In addition, even though we rely on the ATT&CK framework in the selection of metrics, utilizing formal conceptual analysis in ontology construction[26] allows us to extract implicit information from CTI text, and such information will then feedback to security experts who propose the general assessment principles. Thus, in cases where threat intelligence reveals attack methods not covered by the ATT&CK framework, experts can introduce new principles based on the refined ontology to achieve efficient and objective assessments.

3.4 Quality Verification

Consumers of threat intelligence will encounter varied requirements, resulting in CTI teams producing intelligence with diverse content focuses. For instance, in the attack portrait analysis scenario, analysts need to review numerous security reports about threat actors to understand attack trends, characteristics, and potential actions. While for the incident response scenarios, since the actions of incident response are rapid, the team has no time to read a large number of reports about threat actors, and instead requires detailed IOC and techniques information about tactics, i.e., how the adversary commonly delivers the payload and establishes persistence, etc.

Therefore, merely satisfying the general principle is insufficient to assess the quality of intelligence objectively and fairly. In this regard, threat intelligence sources should not only provide intelligence data but also offer the primary application scenarios for the intelligence, which derived from consumers. We introduce a quality verification module that defines additional assessment metrics according to specific application scenarios, enabling the identification of intelligence with practical value. Several typical application scenarios have been summarized, as shown in **Table 5**.

Table 5. Typical Application Scenarios for Cyber Threat Intelligence.

Application Scenario	Related Event Information	Main Types of Intelligence
Attack Portrait Analysis	All the Event Information	Unstructured Text
Attack Attribution Analysis	Attacker, Action and Method	Unstructured Text and TTPs
Attack Chain Analysis	Action and Method	IOC and TTPs
Incident Response	Action and Method	IOC
Attack intention analysis	Attacker, Target and Motivation	Unstructured Text
Impact Analysis	Target, Result	Unstructured Text

3.5 Calculation of Quality Score

In this section, we calculate the quality score for specific threat intelligence by utilizing the Technique for Order Preference by Similarity to an Ideal Solution (TOPSIS) method [29]. The TOPSIS method follows the principle of sorting by measuring the distance between the assessment object and the optimal and worst solutions. To ensure a more

objective assessment of intelligence quality, we integrate the entropy weight method (EWM)[30], which assigns weights to the assessment metrics based on their degree of variation, thus mitigating deviations caused by human factors.

4 Threat Intelligence Sharing based on Quality Assessment Model

In this section, we briefly describe how the proposed assessment model can be applied to CTI sharing and provide descriptions of its various components and their interactions in the sharing scenario. The overall process of CTI sharing is illustrated in **Fig. 2**.

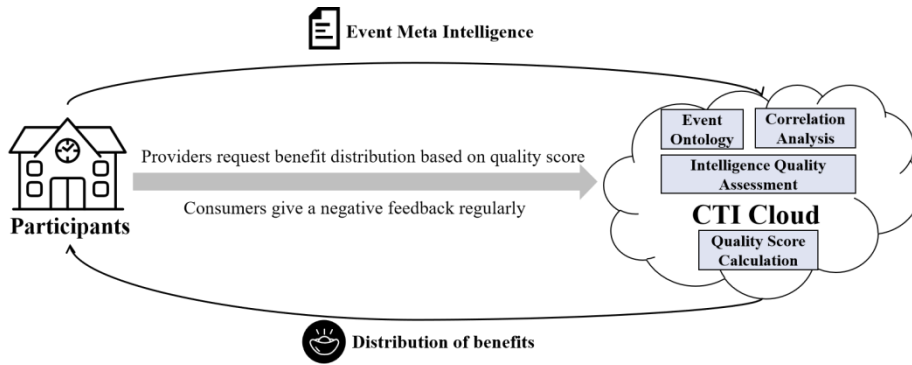


Fig. 2. Overall Process of Threat Intelligence Sharing.

The components of the sharing process are explained as follows:

- **Participant:** The engaging authority in intelligence sharing, including intelligence consumers and providers.
- **CTI Cloud:** The authority responsible for quality assessment, correlation analysis and benefit distribution.
- **Event Meta Intelligence:** Threat intelligence containing essential event elements, as previously depicted in **Table 2**.
- **Event Ontology:** An event-based threat intelligence ontology model utilized for standardizing shared intelligence format and facilitating correlation analysis and calculation of quality score.

The subsequent section describes the interactions among these components within the framework to facilitate CTI sharing.

- Participants share only event meta intelligence, excluding sensitive intelligence (e.g., vendor product vulnerability information) and private data (e.g., organization and identity information) to overcome trust barriers.
- A national authority serves as the CTI Cloud, aggregating and pre-processing raw intelligence from each participant to generate unified intelligence.

- The CTI Cloud conducts correlation analysis based on diverse intelligence application scenarios and establishes metrics to assess the quality of each unified intelligence, which then serves as a basis for filtering out low-quality intelligence.
- To encourage more participants to provide high-quality intelligence, the distribution of benefits is essential. The primary criterion for distribution is the quality score and the benefit may take various forms, such as licensing, certification, or access to subscription services offering high value intelligence.
- The CTI Cloud implements a negative feedback mechanism from intelligence consumers regularly to facilitate dynamically adjustments of quality score.

5 Experimental Analysis

5.1 Intelligence Acquisition and Processing

Our model assesses the quality of publicly available annotated intelligence data presented in [31], which comprises 973 cyber security news published between 2017 and 2018. We employ the method described in [26] to extract attack methods and align techniques and tactics with the ATT&CK framework. Regarding other event information, we map the structured text annotations to the defined ontology structure. The mapping relations are illustrated in **Table 6**, where we merge the “realis” and “event type” indexes to denote the event information of “result”.

Table 6. Mapping Relations Between Defined Ontology and Annotated Data.

Metrics	Related Event Information	Index of Annotated Data
Disclosure Time	Time	Time
Type of Attacker	Attacker	Attacker
Type of Asset Associated with the Victim	Target	Victim
Attack Motive	Motivation	Purpose
Attack Impact	Result	Realis and Event type

5.2 Intelligence Quality Verification

As an illustrative case, we utilize attack attribution analysis to further assess the aforementioned news data. We introduce additional assessment metrics and propose a quantification method for attribution information to represent the usable value of intelligence in the attribution analysis of APT organizations. The specific steps are outlined below:

- Following the “teaching model” presented by Travis Smith [32], where he organized the ATT&CK Matrix by difficulty of exploitation, as shown in **Fig. 3**, we crawl the

group data from MITRE official website and construct assessment matrices corresponding to all APT organizations by ATT&CK navigator [33].

- Calculate the importance score for each APT organization based on the exploitation difficulty, as defined in formulas (3).
- Identify the ATT&CK IDs from the intelligence data, obtain the APT organization that are most similar to the attack behaviors embodied in this intelligence, and quantify the attribution information metric by combining the similarity and the importance of APT organization. The relevant definitions are given in formulas (4).

$$APT_imp = \sum_i \sum_j Matrix_apt \tag{3}$$

$$Attack_attri = \frac{\sum_i \sum_j (Matrix_cti \cap Matrix_apt)}{\sum_i \sum_j (Matrix_cti \cup Matrix_apt)} \times APT_imp \tag{4}$$

Among the equations above, *Matrix_apt* denotes the assessment matrix constructed based on the navigator corresponding to an APT organization provided on the MITRE official website, while *Matrix_cti* denotes the assessment matrix constructed after extracting the TTPs from the threat intelligence.



Fig. 3. ATT&CK Navigator Organized with Difficulty of Exploitation. Blue- not really exploitable; green- the easiest techniques to exploit; yellow- need some sort of tool; orange- requires some level of infrastructure to setup; red- the most advanced techniques which require an in-depth understanding of the OS or custom DLL/EXE files for exploitation; purple- high level techniques which include sub-techniques of varying levels; and white - not labeled due to version of ATT&CK matrix.

5.3 Calculation of Quality Score

Subsequently, we employ the TOPSIS evaluation method, incorporating entropy weight calculation, to calculate the quality score of threat intelligence. The weight values of each metric, derived through the entropy weight method, are presented in **Table 7**. To verify the potential impact of data dimension on metric weights, we normalize the scoring results, conduct comparative analysis, and find no significant changes.

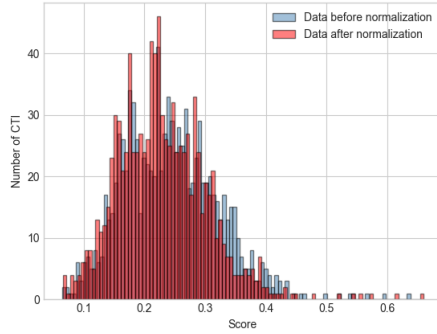


Fig. 4. Quality Scores with Metric of Attack Attribution Analysis.

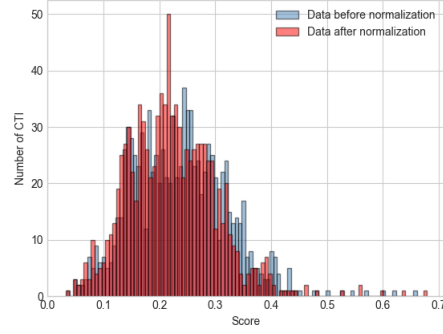


Fig. 5. Quality Scores without Metric of Attack Attribution Analysis.

Table 7. Weight of Each Metric Calculated by Entropy Weight Method.

Metrics	Weight	Weight After Normalization
Disclosure Time	0.26397972	0.24509534
Type of Attacker	0.14825647	0.13765061
Asset Owner Associated with the Victim	0.08764677	0.08137676
Attack Motive	0.13684413	0.12705468
Attack Impact	0.08119971	0.10302874
Techniques - Attack Chain	0.07866813	0.08515788
Techniques - Attack Chain Coherence	0.11796986	0.14131257
Attack Attribution	0.08543521	0.07932341

Finally, we assign scores to each threat intelligence and conduct a comparison analysis for the selection of attack attribution metrics, and the scores are illustrated in **Fig. 4** and **Fig. 5**. Upon scrutinizing the experimental results, it is apparent that the scores calculated by our proposed method, are generally low. The majority of scores are below 0.4, with all scores normalized within a range of 0 to 1. We attribute this outcome to three primary factors. Firstly, there exists a limitation in the accuracy of the information extraction process regarding TTPs. Secondly, the chosen data, cyber security news, primarily consists of short texts that may lack comprehensive event information. Lastly,

world in 2017[34], and this intelligence holds significant values for security practitioners in conducting attack attribution analysis. Consequently, the score ranking of this intelligence improved to 382 after introducing assessment metrics relevant to attack attribution, which shows the capability of our proposed method to filter out intelligence with practical utility in specific application scenarios.

Coverage. Lastly, we conduct a comparative analysis of proposed model with other relevant methods for threat intelligence assessment regarding metric coverage, as presented in **Table 8**. The main components in the Information Security Technology Cybersecurity Threat Information Format Specification[35] serve as the evaluation criteria for measuring metrics coverage, so as to facilitate quality assessment during intelligence sharing. The results demonstrate that the proposed model exhibits extensive metric coverage.

Table 8. Comparison with Coverage of Metrics.

Evaluation Criteria	Our Proposed Model	[12]	[4]	[5]	[7]	[9]	[15]	[14]
Type of Threat	✓	✓	×	×	✓	×	×	×
Time	✓	✓	✓	✓	✓	✓	✓	✓
Impacted Assets	✓	×	×	×	×	×	×	×
Motivation of Threat	✓	×	×	×	×	×	×	×
Impact Assessment	✓	×	×	×	✓	✓	×	×
Credibility	×	✓	×	✓	✓	×	×	✓
Observable Data	✓	×	✓	✓	×	✓	✓	✓
Attack Stage	✓	×	×	×	×	×	✓	×
Attack Method	✓	×	×	×	×	✓	✓	✓
Information Source	×	✓	✓	✓	✓	✓	×	✓
Vulnerability	×	✓	×	×	×	✓	✓	×

6 Conclusion and Future Work

This paper proposes a threat intelligence quality assessment model based on ATT&CK framework for multiple application scenario to tackle challenge concerning quality assessment during CTI sharing. Firstly, we utilize an event-based threat intelligence ontology to convert unstructured threat intelligence into structured data, facilitating the representation, storage, and extraction of relevant event details. Additionally, we propose a set of principles aligned with practical application scenarios and establish assessment metrics from event perspective based on these principles. Subsequently we employ both qualitative scoring and quantitative calculation methods to quantify the defined metrics. Notably, we introduce quality verification module that defines additional assessment metrics according to the specific application scenarios. Finally, we adopt the TOPSIS comprehensive evaluation method in conjunction with entropy

weight method to calculate the quality score of threat intelligence, utilizing it as a reference for assessing intelligence quality.

Our future research will involve adopting dynamic weights for metrics related to attack chain, as the significance of distinct stages within the attack chain continually shifts based on the objectives of real-world attacks. Furthermore, given the advancing landscape of AI-related attacks[36], we intend to explore the possibility of integrating the ATLAS framework[37] as a complement to the ATT&CK framework. Lastly, we will investigate more efficient information extraction methods and choose more complex data, such as APT reports.

Acknowledgments. This work was supported by the National Natural Science Foundation of China (NSFC) (Grant 62376265).

Disclosure of Interests. The authors have no competing interests.

References

1. National cybersecurity strategy (2023), <https://www.whitehouse.gov/oncd/national-cybersecurity-strategy>
2. Brown R, N.K.: Sans 2023 cti survey: Keeping up with a changing threat landscape, white paper of sans (2023), <https://www.sans.org/white-papers/2023-cti-survey-keeping-up-changing-threat-landscape>
3. Gao, Y., Li, X., Li, J., Gao, Y., Guo, N.: Graph mining-based trust evaluation mechanism with multidimensional features for large-scale heterogeneous threat intelligence. In: 2018 IEEE International Conference on Big Data (Big Data). pp. 1272–1277. IEEE (2018)
4. Huiyang, S., Peng, L., He, W.: Threat intelligence evaluation based on blockchain and a neural network. *Journal of Tianjin University (Science and Technology)* 55(5), 527–534 (2022)
5. Hu, y., Jia, y.: A threat intelligence source quality evaluation model based on analytic hierarchy process. *Information Technology* (06), 131–138 (2022)
6. Schlette, D., Böhm, F., Caselli, M., Pernul, G.: Measuring and visualizing cyber threat intelligence quality. *International Journal of Information Security* 20, 21–38 (2021)
7. Griffioen, H., Booij, T., Doerr, C.: Quality evaluation of cyber threat intelligence feeds. In: Applied Cryptography and Network Security: 18th International Conference, ACNS 2020, Rome, Italy, October 19–22, 2020, Proceedings, Part II 18. pp. 277–296. Springer (2020)
8. Zhang, X., Miao, X., Xue, M., et al.: A reputation-based approach using consortium blockchain for cyber threat intelligence sharing. *Journal of Security and Communication Networks* 2022 (2022)
9. Alam, M.T., Bhusal, D., Park, Y., Rastogi, N.: Looking beyond iocs: Automatically extracting attack patterns from external cti. In: Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses. pp. 92–108 (2023)
10. MITRE: Att&ck official website (2024), <https://attack.mitre.org/matrices/enterprise>
11. DavidJBianco: Enterprise detection response: The pyramid of pain (2024), <https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>
12. Mitra, S., Piplai, A., Mittal, S., Joshi, A.: Combating fake cyber threat intelligence using provenance in cybersecurity knowledge graphs. In: 2021 IEEE International Conference on Big Data (Big Data). pp. 3316–3323. IEEE (2021)

13. Purohit, S., Neupane, R., Bhamidipati, N.R., Vakkavanthula, V., Wang, S., Rockey, M., Calyam, P.: Cyber threat intelligence sharing for co-operative defense in multi-domain entities. *IEEE Transactions on Dependable and Secure Computing* (2022)
14. Tundis, A., Ruppert, S., Mühlhäuser, M.: A feature-driven method for automating the assessment of osint cyber threat sources. *Journal of Computers & Security* 113, 102576 (2022)
15. Zhang, S., Chen, P., Bai, G., Wang, S., Zhang, M., Li, S., Zhao, C., et al.: An automatic assessment method of cyber threat intelligence combined with att&ck matrix. *Journal of Wireless Communications and Mobile Computing* 2022 (2022)
16. Al-Sada, B., Sadighian, A., Oligeri, G.: Mitre att&ck: State of the art and way forward. *arXiv preprint arXiv:2308.14016* (2023)
17. Tsai, C.E., Yang, C.L., Chen, C.K.: Cti ant: Hunting for chinese threat intelligence. In: 2020 IEEE International Conference on Big Data (Big Data). pp. 1847–1852. IEEE (2020)
18. Satvat, K., Gjomemo, R., Venkatakrishnan, V.: Extractor: Extracting attack behavior from threat reports. In: 2021 IEEE European Symposium on Security and Privacy (EuroS&P). pp. 598–615. IEEE (2021)
19. Liu, C., Wang, J., Chen, X.: Threat intelligence att&ck extraction based on the attention transformer hierarchical recurrent neural network. *Journal of Applied Soft Computing* 122, 108826 (2022)
20. Orbinato, V., Barbaraci, M., Natella, R., Cotroneo, D.: Automatic mapping of unstructured cyber threat intelligence: An experimental study:(practical experience report). In: 2022 IEEE 33rd International Symposium on Software Reliability Engineering (ISSRE). pp. 181–192. IEEE (2022)
21. Al-Shaer, R., Spring, J.M., Christou, E.: Learning the associations of mitre att&ck adversarial techniques. In: 2020 IEEE Conference on Communications and Network Security (CNS). pp. 1–9. IEEE (2020)
22. Rahman, M.R., Williams, L.: Investigating co-occurrences of mitre att&ck techniques. *arXiv preprint arXiv:2211.06495* (2022)
23. Nisioti, A., Loukas, G., Laszka, A., Panaousis, E.: Data-driven decision support for optimizing cyber forensic investigations. *IEEE Transactions on Information Forensics and Security* 16, 2397–2412 (2021)
24. Threatbook: 2023 threat intelligence and apt activity analysis report (2023), <https://archive.threatbook.cn/threatbook/2023-ThreatBook-CTI-APT-Analysis-Report.pdf>
25. Chen, J., Fan, H.: Ontological threat intelligence sharing in cyberspace security. *Journal of Communications Technology And Electronics* 51(01), 171–177 (2018)
26. Wang, P., Dai, G., Zhai, L.: Event-based threat intelligence ontology model. In: International Conference on Science of Cyber Security. pp. 261–282. Springer (2023)
27. Juran, J.M.: *Juran’s quality handbook* (1999)
28. Shin, Y., Kim, K., Lee, J.J., Lee, K.: Art: automated reclassification for threat actors based on att&ck matrix similarity. In: 2021 world automation congress (WAC). pp. 15–20. IEEE (2021)
29. Hwang, C.L., Yoon, K., Hwang, C.L., Yoon, K.: Methods for multiple attribute decision making. *Multiple attribute decision making: methods and applications a state-of-the-art survey* pp. 58–191 (1981)
30. Li, X., Wang, K., Liu, L., Xin, J., Yang, H., Gao, C.: Application of the entropy weight and topsis method in safety evaluation of coal mines. *Procedia engineering* 26, 2085–2091 (2011)
31. Satyapanich, T., Ferraro, F., Finin, T.: Casie: Extracting cybersecurity event information from text. In: Proceedings of the AAAI conference on artificial intelligence. vol. 34, pp. 8749–8757 (2020)

32. Travis Smith, T.: Mitre att&ckcon 2018: att&ck as a teacher (2018), <https://www.slideshare.net/attackcon2018/mitre-attckcon-2018-attck-as-a-teacher-travis-smith-tripwire>
33. MITRE: The att&ck navigator (2024), <https://mitre-attack.github.io/attack-navigator>
34. Wikipedia: Wannacry-wikipedia (2024), <https://zh.wikipedia.org/wiki/WannaCry>
35. Cai, l., Ye, r., Yang, j.e.a.: Information security technology—cyber security threat information format (2018)
36. Gartner: The top cybersecurity trends for 2024 (2024), <https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024>
37. MITRE: Atlas official website (2024), <https://atlas.mitre.org/matrices/ATLAS>