Studies	Research Objectives	Output Formats	Identify Entity	Identify Relation	Context of Relation	Methods
AttacKG [33]	Extract attack behavior graph & identify attack techniques	Attack Behavior Graphs	V	V		Entity Recognition, Graph Alignment
TTPDrill [34]	Learn attack pattern (TTPs)	STIX Objects	V		V	Ontology TF-IDF, Dependency Parser
LADDER [35]	Extract attack patterns	Knowledge Graph Triplet	V	V	△	BERT, TuckER
EXTRATOR [36]	Extract attack behaviors	Attack Behavior Graphs	V	V	△	ER, Semantic Role Labeling
Our Research	Extract attack activities	OP_{en} pair	V	V	V	Dependency Parser, BERT embedding

表格二: Threat Report Processing

表格描述: Comparison of automatic threat report extraction and processing researches. The triangle symbol represents that only predefined context words or relationship type can be assigned.

\cite{li_2022_attackg, husari_2017_ttpdrill, alam_2022_looking, satvat_2021_extractor}

#可以用白色的 ref{} 來產生論文的引用編號，再把引用編號寫死在表格上。

Studies	Research Objectives	Data Source		Label System Objects	Graph Representation	Approach
		Audit Logs	Syscall Traces			
HOLMES [25]	Technique Classification	V			V	Event Rules
TPG [26]	Technique Classification	V		V	V	Rules by Symantic EDR
Log2Vec [40]	Anomaly Detection	V			V	Graph Rules, Cluster Detection
Tiresias [41]	Event Forecast	V				RNNs
SetConv [42]	Tactic Classification		V	V		OAML, CNNs
Our Research	Display & Query Malware Execution Steps		V	V	V	Execution Causal Relationship

表格三: Log Processing and Provenance Graph Construction

表格描述: Comparison of log processing researches. Most of the studies convert and merge log data as a provenance graph-like data-structure. \cite{milajerdi_2019_holmes, hassan_2020_tactical, liu_2019_log2vec, shen_2018_tiresias, akbar_2021_identifying}

Studies	Research Objectives	Target on Platform	Target on Document	Require Expert
[5]	Construct contextual CTI Ontology	V		V
[6]	Propose Data Quality methodologies	V		
[7]	Evaluate Quality of CTI services	V		V
[8]	Evaluate Quality of CTI feeds	V		△
[32]	Evaluate Trustworthiness of CTI sources	V		
Our Research	Evaluate Quality of CTI documents		V	

表格一: Cyber Threat Intelligence Evaluation

表格描述: Comparison of CTI evaluation researches. The triangle symbol represents that there is a requirement of establishing lists of unroutable and active IPs by experts.

將這五篇論文寫成 related work 章節。

Several studies have examined the effectiveness of threat intelligence platforms or feeds [x,x,x,…] by 自定義的 quality metrics. 這些 quality metrics 往往十分仰賴 STIX 格式，藉由 STIX object 中的屬性來計算分數。因此無法運用在 CTI report 的評估上。可惜的是，目前並沒有專門對 CTI report 資訊價值的評估文獻。

Mavroeidis et. al [5] 的目的是評估情資的 taxonomies (如 CVE, NVD, ATT&CK), sharing standards (如 STIX, MAEC, OpenIOC), 和 ontologies (如 OVM, UCO)，作者欲研究如何建立上下文相關且明確的 CTI ontology。由於這是一篇 survey 論文，作者沒有一一對各論文提出解決方案，而是以 Detection Maturity Level Model 和 Cyber Threat Intelligence Model 作為衡量工具。在 DISCUSSION 章節我們能推論出 (1) 目前的 ontologies 彼此間並不 connected or unified (2) 若 taxonomies and existing ontologies 有更標準化的連結便能消除 ambiguity。

Schlette et. al [6] 的目的是提出一個 relevant quality dimensions and metrics 來評估 CTI artifacts on the platform。當組織對一起事件發布一連串的情資報告時，會產生 inaccurate (軟體版本誤植), outdated (惡意程式已變種), or duplicated information of threat intelligence 等情形。於是作者提出了 data quality (DQ) methodologies，涵蓋了三種層面: (1) Report Level，如 reports 的數量。(2) Object Level，如 STIX-object 的 Representational Consistency，及發佈者和資料集的 reputation。(3) Attribute Level，如 Concise representation (表示資料的 expressiveness 和冗餘性), Timeliness (被創造和被修改的時間), Objectivity (使用機器學習方法判斷 STIX object 得內容客觀或不客觀), 等。

Li et. al [7] propose a comprehensive evaluation method of threat intelligence services in user perspective. The goal is to help users choose appropriate threat intelligence vendors and services. The proposed method evaluates threat intelligence services in several dimensions, including categories, functions, properties, testing methods, and items.

Li et. al [8] 的目的是提供 CTI feeds 的全面分析，比較不同的來源並判斷 CTI feeds 對特定目的的適用性。他們提出了 6 個 threat intelligence metrics: Volume, Differential Contribution, Exclusive Contribution, Latency, Coverage and Accuracy.

Schaberreiter et. al [9] propose a methodology for quantitatively evaluating the trustworthiness of CTI sources. The proposed approach allows for an evaluation of sources to be carried out automatically without the need for interference by human experts, which leads to several benefits from an operational perspective. 作者定義了 10 種 parameter (如 Maintenance, False Positives, Verifiability 等)，透過各個 source 的相互比較來計算分數，並使用不同的權重來計算 CTI source 的信賴程度。

四篇評估 CTI platform/feeds 的論文分別是:

- [5] Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence
- [6] Measuring and visualizing cyber threat intelligence quality
- [7] A quality evaluation method of cyber threat intelligence in user perspective
- [8] Reading the tea leaves: A comparative analysis of threat intelligence
- [9] A Quantitative Evaluation of Trust in the Quality of Cyber Threat Intelligence Sources

老師好，我是晟維，
我從引用論文[7][8]的文獻中挑出了論文[9]，在 3、40 篇文獻中，他們的主題幾乎是 Improve blacklist、CTI 爬蟲蒐集研究或是 report extraction，只有論文[9]較契合 CTI 品質評估的主題，被引用數也高。但他也是對於 CTI sources 的信賴程度評估，而非針對 reports。

論文[5] 的目的是評估情資的分類法(taxonomies, 如 CVE, NVD, ATT&CK), 標準(sharing standards, 如 STIX, MAEC, OpenIOC), 和本體(ontologies, 如 OVM, UCO)，作者欲研究如何建立上下文相關且明確的 CTI ontology。

面臨的問題包括: (1)CTI ontology 較少關注 strategic, operational, and tactical 的層面. (2)concepts 的定義模糊使 ontology 難以整合和被採用. (3)現行的 taxonomies 多使用短文章(prose)來描述類別，這破壞了可查詢性和執行推理的能力。

由於這是一篇 survey 論文，作者沒有一一對各論文提出解決方案，而是以 Detection Maturity Level Model 和 Cyber Threat Intelligence Model 作為衡量工具。在 DISCUSSION 章節，作者說明以上問題的原因，我們能推論出 (1) 目前的 ontologies 彼此間並不 connected or unified (2) 若 taxonomies and existing ontologies 有更標準化的連結便能消除 ambiguity。

論文[6] 的目的是提出一個 relevant quality dimensions and metrics 來評估 CTI artifacts on the platform。在 Motivational example 章節中作者表示，當組織對一起事件發布一連串的情資報告時，會產生 inaccurate (軟體版本誤植), outdated (惡意程式已變種), or duplicated information of threat intelligence 等情形。

於是作者提出了 data quality (DQ) methodologies，涵蓋了三種層面: (1) Report Level，如 reports 的數量，(2) Object Level，如 STIX-object 的 Representational Consistency，及發佈者

和資料集的 reputation。(3) Attribute Level，如 Concise representation (表示資料的 expressiveness 和冗餘性), Timeliness (被創造和被修改的時間), Objectivity (使用機器學習方法判斷 STIX object 得內容客觀或不客觀), Relevancy (對於消費者的實用性，如 STIX object 被 refer 的次數，是否有 CVE 的欄位), Syntactic accuracy (格式是否遵守 data schema)。

(發現讀錯篇了!! A Quality Evaluation Method of Cyber Threat Intelligence in User Perspective 才是對的)

論文[7] 的目的是衡量 CTI feeds 的品質。本研究採用的 data sources 為 24 種 Open Source Intelligence Feeds (如表 1)，並額外使用 NetFlows (透過 ISP 的資料判斷一個 IP 是否有在傳輸資料) 和 zone transfers (紀錄 domain 和 IP) 來評估以下指標: timeliness, accuracy, completeness and relevance。

在評估 CTI feeds 時的困難和限制有: (1) Information Overload 資訊量太多了，一天能產生出 250 million indicators [12]。(2) Short Lifespan of Threat Intelligence，隨著時間遞移情資的有效性會減少，因此需要衡量 CTI 的相關性和即時性。(3) Incompleteness of Blocklists，研究[9]顯示 blocklists 的情資不齊全，找不到 Ground truth 來做基準，因此研究常使用 empirical evaluation 來驗證他們不是沒用的，因此這些論文沒有提出指標 [7, 10, 11]。也有論文設計 test suit 來測試 blacklist [8]。

作者提出 4 個 dimensions 來衡量 CTI feeds:

- Timeliness: the “speed” at which the feed provides information about new threats and the frequency of updates. The authors use NetFlow data and zone transfers to benchmark the timeliness of the feeds.
- Sensitivity: the “relevance” and “specificity“ of the information provided by the feed. The authors assess the sensitivity of the feeds by analyzing the number of false positives and false negatives.
- Originality: the “uniqueness” and novelty of the information provided by the feed. The authors assess the originality of the feeds by analyzing the overlap between different feeds.
- Impact: the “effectiveness” of the feed in mitigating attacks and reducing harm. The authors analyze the impact of the feeds by evaluating the adoption of the indicators listed on the feeds and estimating their ability to "save" clients and networks from future harm.

論文[8] 的目的是提供 CTI feeds 的全面分析，比較不同的來源並判斷 CTI feeds 對特定目的的適用性。他們提出了 6 個 threat intelligence metrics: Volume, Differential Contribution, Exclusive Contribution, Latency, Coverage and Accuracy.

- Volume: The total number of indicators appearing in a feed over the measurement interval (通常是 daily). It helps determine the quantity of information.
- Differential Contribution: 在同段時間內，feed A 中的 indicators 沒有出現在 feed B 中的比例。DiffA,B = 1 indicates that the two feeds have no elements in common。
- Exclusive contribution: 在同段時間內，feed A 中的 indicators 出現在 feed B 中的比例。UniqA,B = 0 means that every element of feed A appears in some other feeds。
- Latency: 表示一個 indicator 首次出現時間 (t)，與在其他 feed 中出現時間 (t’) 的間隔。
- Accuracy: 表示 feed 中的 indicator 正確的比例。類似 IR 領域中的 precision 指標。
- Coverage: the proportion of the intended indicators contained in a feed. 類似 IR 領域中的 recall 指標。

CTI feeds 包括了公開的或私人的和付費的平台，誠如我論文第二頁所描述。Those CTI platforms including well-known public blacklists and reputation feeds such as AlienVault (9), Badips (10), Abuse.ch (11) and Packetmail (12), enterprise closed community platform such as Meta ThreatExchange (13), and paid feed aggregator (PA) such as ThreatBook (14) and IBM XForce (15).

有幾項 limitation 論文並沒有考慮和處理。分別是: (1) 儘管本論文使用多種的 feeds 但還有十分昂貴或有版權的資料，沒有辦法納入資料來源。(2) 企業用戶對情資的使用途徑可能不同。(3) Lack of ground truth: 就像其他同樣做 measurement 的 work，很難為 certain category of threat 找到一個明確的 reference point。本研究使用的是 Internet telescope and VirusTotal 的資料來模擬 ground truth。

---

[9] A Quantitative Evaluation of Trust in the Quality of Cyber Threat Intelligence Sources

The main goal of paper [9] is to propose a methodology for quantitatively evaluating the trustworthiness of CTI sources. The proposed approach allows for an evaluation of sources to be carried out automatically without the need for interference by human experts, which leads to several benefits from an operational perspective. 作者定義了 10 種 parameter (分數)，透過各個 source 的相互比較來計算分數(如下表)，並使用這 10 個分數不同的權重，來計算一個 CTI source 的信賴程度。

對於 CTI sources，作者只有提供定義，沒有列出使用了哪些平台作為實驗，文末只有一個簡單 case study (可能是因為頁數限制)。CTI sources 的定義: entities that provide information about potential cyber threats or attacks，比如提供 suspicious domain names, hashes for malicious executables 或 IPs 的網站。接下來，我會介紹幾個與我們研究較相關的指標，但經過研讀我發現論文[9]十分仰賴 STIX 格式，可能指標的名稱取名得專業，但實質上是取 STIX 的某些欄位做運算。

False Positives 並不是與標準答案比較，因為無法得知 Ground Truth。作者的做法是查詢 STIX 的 revoke (撤銷)欄位是否為 True，通常一筆 indicator 被撤銷代表有新的證據/改動出現，因此作者發現 FP 高的 source 反而代表較高的品質。

$$p_3 = 1 - \left(\frac{F_{s_x}}{\sum_{i=1}^{n} F_{s_i}}\right)$$

Verifiability 一個 source 的資料是否有標記外部來源。作者透過 STIX 的 external_references 來檢驗平台的資訊是否可被驗證。

$$p_4 = \left\| \frac{\left\|\frac{1}{z}\sum_{i=1}^{z} r_i\right\|}{\text{avg}(p_4 s_1, \ldots, p_4 s_n)} \right\|$$

Intelligence 是除基本資訊外，CTI source 提供的附加價值。計算方法是看某種 type object 具有多少的 relationship，由 STIX 的 related-to or derived-from 欄位可計算得知。

$$p_5 = \left\| \frac{\left\|\frac{1}{z}\sum_{i=1}^{z} l_i\right\|}{\text{avg}(p_5 s_1, \ldots, p_5 s_n)} \right\|$$

Similarity 是比較 source 的 information 與其他來源的相似程度。

$$p_8 = \frac{1}{z}\sum_{i=1}^{z}(y_i)$$

Completeness 就像是 coverage 指標。計算了一個 source 的資訊在所有 source 中的佔比。

$$p_{10} = \frac{|B| - |A|}{|B|}$$

我也另外整理了各論文如何定義 CTI 和 CTI report，如下表。通常在做 report extraction 的論文會將 CTI 與 CTI report 混用(如 Extractor、Ladder)。我的想法是在論文中同時定義 CTI 與 CTI report，而 CTI report 屬於被包含的小集合。

且結構化的 CTI 是給機器自動化的交換/使用。非結構化的 report 是給人類受眾閱讀的，而每一篇 report 也有它撰文的目的以傳達內容。

類別	出處	定義
CTI	[6] Measuring	CTI is to provide meaningful knowledge about cyber security threats.
	[7] Quality Evaluation	a highly perishable good, since as soon as it is discovered and distributed to clients, adversaries will also know that one of their tools or assets has been discovered. 一種易腐爛的商品，因為一旦它被發現並分發給客戶，駭客也會知道他們的工具或資產被發現。
	[8] Tea Leaves	By far the most common form of such data are so-called indicators of compromise: simple observable behaviors that signal that a host or network may be compromised.
	Ladder	Called cyber threat intelligence (CTI), this information is disseminated through paid subscriptions or shared freely on blogs, bulletins, news, and reports (open-access CTI).
	我的論文	CTI is an essential asset for security analysts in enterprises to prevent currently raging malware or conduct internal threat-hunting activities. (可以是任何形式的資料，主要指結構化的 IoC，目的是讓機器自動化的交換/使用情資)
CTI reports	AttacKG	a well-written report will precisely describe attack behaviors through enumerating attack-relevant entities (e.g., CVE-2017-11882) and their dependencies (e.g., stager connecting to C&C server).
	Extractor	Cyber Threat Intelligence (CTI), as commonly reported in technical reports, whitepapers, blogs, and newsgroups, is a valuable source of information about cyber-attacks.
	Ladder	CTI sources that describe malware and APT attacks,

		thereby improving threat detection at scale.
	我的論文	Malware CTI documents provide knowledge of the activities, harm, and whereabouts of malware in natural language and record the spatiotemporal background of the incident, allowing readers to reconstruct the victim's situation. (屬於 CTI 的一種，非結構化的文本報告提供了活動、危害、足跡、時空背景等多方面的資訊，目的是讓人類閱讀，不需要身歷其境也能理解當下的事件)