Heliyon 7 (2021) e05969

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Review article

A review of threat modelling approaches for APT-style attacks

Matt Tatam, Bharanidharan Shanmugam *, Sami Azam, Krishnan Kannoorpatti

College of Engineering, IT and Environment, Charles Darwin University, NT, 0810, Australia

ARTICLE INFO

Keywords:
Advanced persistent threats
Threat modelling
Cyber threat model
Intelligence

ABSTRACT

Threats are potential events, intentional or not, that compromise the confidentiality, integrity, and/or availability of information systems. Defending against threats and attacks requires actionable threat intelligence. Using this intelligence to minimise risk, requires a systematic methodology or framework that recognises every possible threat scenario. This can be done with Threat Modelling (TM), which assists with identifying, understanding and providing visibility of threats affecting an organisation. The focus of this study is to determine TM limitations, strengths, and any perceivable gaps. It has also focused on identifying any possible enhancements that may improve TM performance and efficiency when modelling sophisticated attacks such as Advanced Persistent Threats (APT).

1. Introduction

To adequately protect an organisation, a defender requires visibility over its assets, associated vulnerabilities and the threats to them. Vulnerabilities are weaknesses that can be exploited via the intersection of three elements: a system susceptibility or flaw, an attacker access to the flaw, and attacker capability to exploit the flaw [1]. NIST defines a threat as "The potential for a threat source to exploit (intentional) or trigger (accidental) a specific vulnerability" [2].

Threat Modelling (TM) is a process during which specific potential security vulnerabilities and their associated risks are identified, so that they can be addressed in a targeted manner [3]. It is a mechanism to evaluate controls, system security and a key task for developing secure applications. TM creates and formalises a process that identifies threats and analyses the vulnerabilities of an individual or combination of Information and communications technology (ICT) asset's [4]. By modelling threats, our aim is to be proactive in identifying, classifying and describing them, to enable the visibility of an attack or a campaign of attacks.

This study uses a literature review approach designed to identify the knowledge that currently exists in modelling threats. The contributions of this study are to provide a critical review, to determine which framework or a combination of frameworks can be used for successful TM. It will also discuss possible enhancements with a view to the future direction of threat modelling Advanced Persistent Threats (APT).

1.1. Research motivation

Identifying attackers within a network or on a host, requires having visibility of suspicious events or actions, that can be identified through indicators. An indicator of Compromise (IoC) is an action known to be caused by or under the influence of an adversary [5]. Identifying these indicators are a primary function of a Security Information and Event Management (SIEM). A SIEM correlates events, alerts and other lower levels of IoC from multiple disparate sources. To accomplish this, the complex relationships between the collated data and actual intrusions needs to be explicitly defined.

An APT is a heavily resourced attack group that remains undetected for an extensive period, after initially compromising a computer host or network. To detect an APT, these SIEM rules need to be aware of the correlations of all levels of IoC. This can be done by combining identifying low-level IoC's to derive a high-level picture of an individual or group of related attack patterns. It should also be noted that other events not representing an IoC can also provide contextual information that can be essential in the identification of an APT campaign [6]. To identify an active persistent attack scenario current event data, and the aggregation of behaviour and events over time is required. This approach means that high-level IoC's, such as, an attackers Tactics (goals), Techniques (actions) and Procedures (TTP) need to be researched [5, 7, 8].

TTPs are “descriptive” in nature and are for characterising the how and what of an adversary's behaviour [9]. Lower level indicators are “detective” in nature and are for specifying conditions or states that may exist to indicate the presence of a TTP along with relevant contextual

* Corresponding author.
E-mail address: bharanidharan.shanmugam@cdu.edu.au (B. Shanmugam).

https://doi.org/10.1016/j.heliyon.2021.e05969
Received 16 September 2020; Received in revised form 5 November 2020; Accepted 8 January 2021

information. Lower level indicators are not used to characterise the particulars of any given adversary's behaviour, only how to detect it (Figure 1).

There are several methods that can assist with identifying these high-level IoC's [8, 11, 12]. This is the motivation for this research, that is, we will identify the knowledge and approaches that currently exist, in modelling APT threats.

Threat modelling is centred around four main approaches. These include an asset-centric, system -centric, threat-centric and a data-centric approach (Figure 2).

This motivation has led to the following research questions.

1) What are the current knowledge gaps or limitations in modelling APT style attacks?
2) What additional processes and approaches can be employed to increase the effectiveness and performance of modelling APT style attacks?

1.2. Research methodology

The papers our study has evaluated were selected based on our research questions. We have investigated these selected papers (Table 1) using a list of search terms and then have critically analysed the documented approaches and methods. We identify if the study has been effective, the robustness and impact of the proposed solution, and to address the limitations and strengths the model may have. Only the papers showing significant impact were selected as those considered for further research.

To identify available studies on Threat Modelling (TM), a systematic query was conducted using 3 leading English language scientific databases. To provide additional visibility we also used a library search engine provided by the researcher's university [13], whose search repository consists of 253 databases. The initial search results provided this study with 70 results with an overlap of 9 papers.

To facilitate non-biased results, we used the generic keyword “threat model”. This result set was then refined further by applying filters (Table 2) resulting in 101 papers identified for further study. A final 49 were used.

The primary publications selected by this research closely discuss approaches to modelling APT's. The associated articles that have been reviewed are tabled and ordered chronologically (Table 9).

To analyse our result set, a local database was developed to store the publications their related entities and metadata in a structured, normalised and relational format. This result set was also used to identify advantages and limitations specific to the modelling approaches discussed. To demonstrate consistency among observational ratings provided by multiple reviewers, research designs require the assessment of inter-rater reliability (IRR) [14]. This will be discussed at length in the inter-rater reliability section.

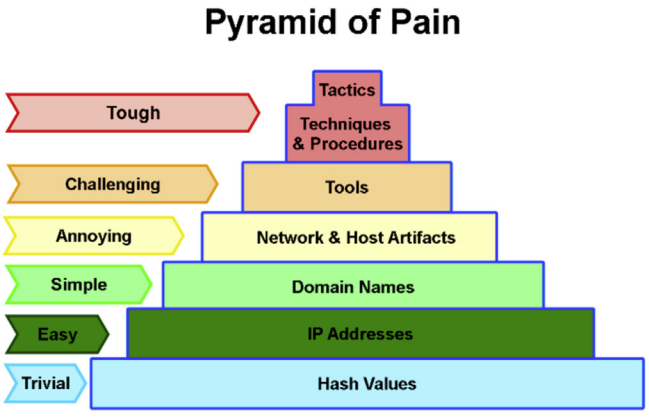

Figure 1. The pyramid of pain [10].

A common theme in the reviewed papers were the 4 aspects to Cyber Threat Intelligence (CTI) (Figure 3) [15], Centric based TM (Figures 2, 4, and 5) [16, 17], and types of TM (Figures 6, 7, and 8) [16, 18, 19]. An axis and quadrant style representation encouraged by ENISA [15] was used for our study's original figures, including a the recreation of their representation of the CTI program (Figure 3). Mind maps in this quadrant inspired format, were used to graphically display TM attribute groupings (Figures 2, 3, and 8). These supporting data entities also documented and linked additional attributes, such as, the software tools used, features and related datasets to TM.

1.3. Structure of the paper

This review paper has been structured to ensure the background and motivation of our study are addressed first to give context to our research. The rest of the paper is organised as follows: Section 2 details the vulnerabilities, threats and attacks. Section 3 will discuss threat intelligence. Section 6 identifies tools and standards that assist in enhancing relevant Threat Modelling techniques (Section 4) and Taxonomies (Section 5).

To better understand current trends Tables 7 and 8 identify threat model advantages and limitations and Section 7 details the insights that have been gained as the result of the critical review. Section 8 highlights the possible future direction of the research followed by the conclusion.

1.4. Interrater reliability

Interrater reliability refers to the extent to which two or more individuals agree. That is, IRR measures the extent to which one person will interpret the data in the same way and assign it the same metadata over time [20, 21, 100]. Our research design required the assessment of IRR to demonstrate consistency among our reviewers in the extraction of TM strengths and limitations. To ensure transparency, validity a subjective view of extracting current strengths and limitations in modelling APT style attacks, we will discuss the IRR data and our analysis used by three reviewers (Tables 3 and 4).

For consistency and to identify any discrepancies in how the reviewer's evaluation of the TM may have differed, our study used an IRR training agreement test tool. The main author (Reviewer A) initially identified TM related excerpts (145) from the identified papers that explicitly identified strengths and/or limitations of a specific TM. These initial TM strengths (35) and limitations (27) were collated and used to create our IRR codes (Table 5 - Iteration 1). This provided our study with the ability for consistent reviewer agreements (IRR codes) based on supporting evidence (excerpts). A then allocated these IRR codes to the 145 excerpts. IRR Training tests were then created to test the if the reviewers agreed upon the assignment of codes to their relevant TM excerpts.

These IRR tests were conducted after the research papers were identified (Iteration 1) and throughout our study. Tables 3 and 4 identify at each iteration the reviewer (A, B, C) who took an agreement test. That is, to determine consistency in associating TM strengths and weaknesses an agreement test (Table 5) was used after each iteration to identify and resolve any reviewer disagreements [21].

There were three iterations required to assign strength codes to the 11 TM (Table 3 – iteration 1). The first iteration used only reviewer A and was an initial discovery of all relevant strengths (Table 5 – iteration 1) identified in excerpts from the 49 primary papers. As our research question is to identify limitations a second reviewer was used in the first iteration for the agreement on limitation codes (Tables 4 and 5 -Iteration 1).

The second iteration required all reviewers to evaluate and agree in the list and their associated excerpts. In doing so, both strengths and limitations were reduced, from 35 to 26 and from 27 to 20 respectively

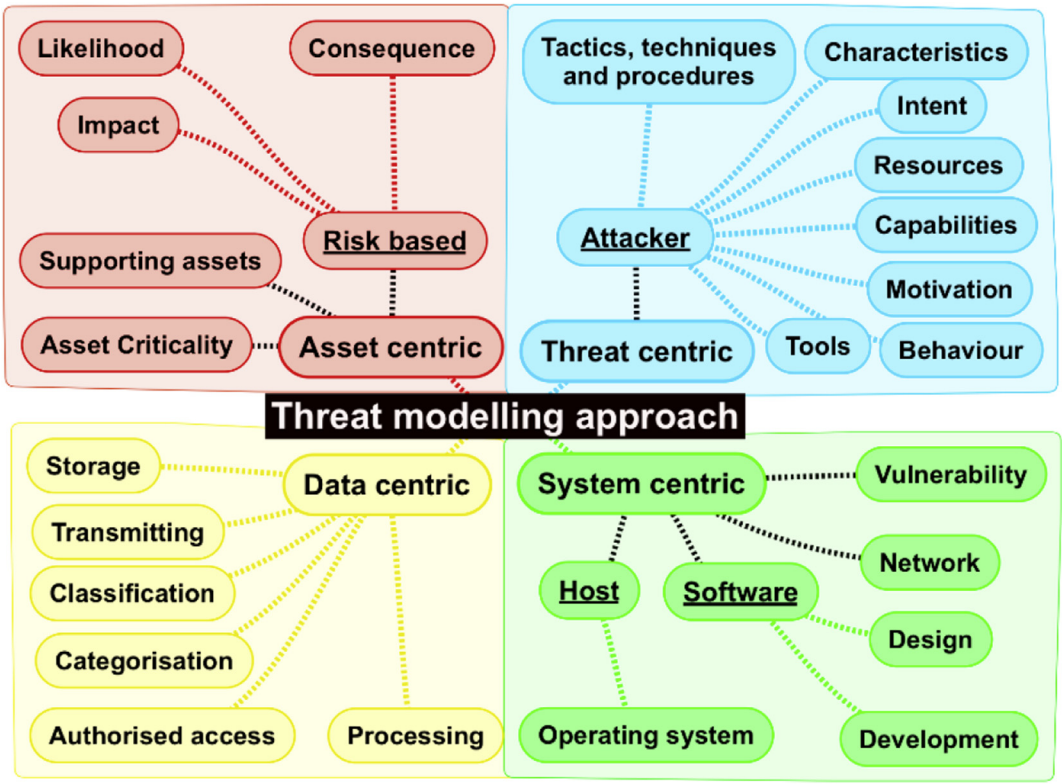

Figure 2. Threat modelling approaches.

Table 1. Research papers identified.

Source	CDU Library	IEEE-Explore	Science Direct	Misc.	Total
Results	70	22	14		
Filtered	9	0	0		
Duplicates	9	10	9		
Primary	44	13	12	4	49
Secondary	17	9	2	13	40
Additional				12	12
					101

(Table 5 – iteration 1–2). This was due to the removal of some and others were combined, such as, Extensible/Flexible and Pre/Post compromise. Once consensus on these codes was agreed upon in iteration 2, multiple tests assign codes to TM related excerpts were used to.

The final iteration was to measure the extent to which reviewers had interpreted the excerpts in the same way, that is, to assign it the same metadata/code in tests over the last two iterations.

The ability to finalise excerpts that explicitly identified a strength or limitation allowed a perfect agreement (1.0) to be reached with all three reviewers over the two final iterations.

2. Vulnerabilities, attacks and threats

To compromise a system an attacker would need to discover a target and identify an exploitable vulnerability. The challenge is to identify the priorities, when reducing vulnerabilities and their associated threats. There are several sources [22, 23, 24, 25] that provide quantifiable metrics, attributes and scoring on known vulnerabilities and exploits. These vulnerability metrics or scores combined with a process to identify relevant threats can guide defenders in targeting and prioritising solutions. A number of studies has identified that the analysis of vulnerability/threat combination remains a manual process [16, 26, 27, 28].

Solving the problem of linking attackers to vulnerabilities can be dated back to 1998 was evident in a number of research projects [29, 30, 31, 32].

There are several repositories that exists to assist in identifying and determining if a vulnerability is relevant to a setting or misconfiguration. The following are the major initiatives [33] that can assist defenders in identifying weakness in their infrastructure and environment:

1. Common Platform Enumeration (CPE) is a structured naming scheme for information technology systems, software, and packages. It is a standard that describes and identifies classes of hardware devices, operating systems, and host applications. This standard naming can

Table 2. Research search criteria.

Search String	"Threat Model" "Threat Modelling" "Threat Intelligence" "APT" Cyber
Inclusion filter	Journals, Early Access Articles, Articles Dissertations, Text Resources, Years: 2017–2020, Added results outside CDU Library
Exclusion filter	Sharing

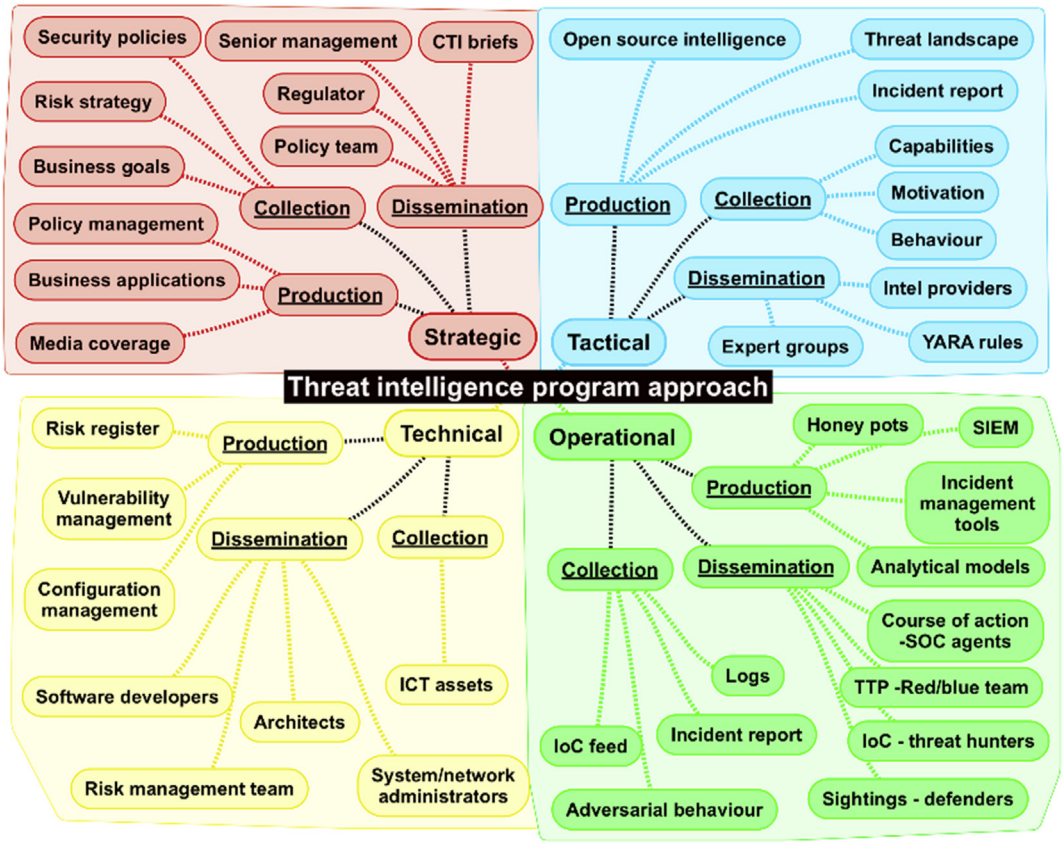

Figure 3. Cyber Threat Intelligence approaches [15].

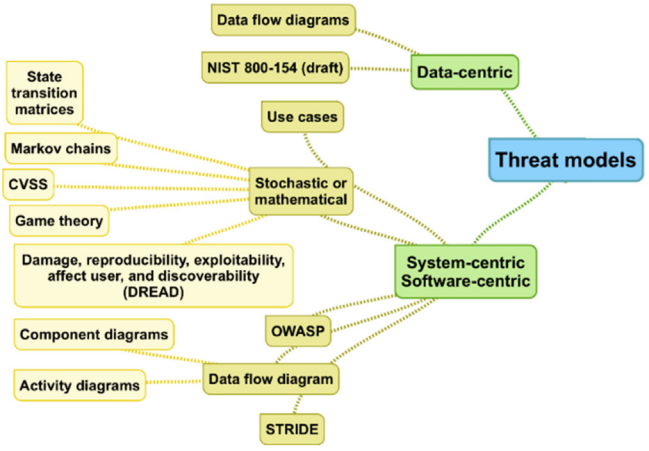

Figure 4. Reviewed papers data and system-centric.

then be used to identify associated vulnerabilities in the configuration of the asset or in the asset itself.

2. The Common Vulnerability and Exposure (CVE) identifies vulnerability and exposure information; however, it does not necessarily identify any of the weaknesses in the libraries from third parties, that are included in the final product. The Common Weakness Enumeration (CWE) assists with this shortcoming. It identifies the causes of vulnerabilities that exist within code are catalogued. CWE is integrated into the scoring of CVE. Common Vulnerability Scoring System (CVSS) was developed separately, but specifically, to provide severity scoring to identified CVEs.
3. Inventory Vulnerability Analysis (IVA) is a system developed by Luis Alberto Benthin Sanguino [34]. It was designed to automate the process of finding possible vulnerabilities in software products. It receives as input a list of software products and employs both the CPE dictionary and the CVE feeds. It creates a list of CPE candidates that match a software product and searches for CVEs that possibly match the assigned CPE.

Based on our review, there is no single research/model that has proposed a complete solution that uses CVE information to correlate the common characteristics of attackers, exploits and vulnerabilities for attack prediction. There is also a lack of literature that attributes the actors' tactics using the mapping of CVE and CPEs.

CVSS scores vulnerabilities by combining and quantifying a vulnerability, through documented standards. Two common uses of CVSS are prioritisation of remediation activities and in calculating the severity of vulnerabilities. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities [22]. Researchers [19, 35] have used CVSS data in their studies, however, the limitation of this scoring system is that it does not take into consideration the environmental context, asset value, likelihood and impact if the vulnerability was exploited.

To be relevant to a defender, a threat requires access to an asset that has a weakness. Threats can be grouped into malicious, non-malicious, internal and external. The potential risk of being compromised, is viewed as the association between a threat, a vulnerability and an asset [36]. Threats can be further broken down into threat agents and threat events.

A Threat Agent is an entity that initiates an attack, so it may be technology, processes, human, natural events, environmental factors, or a combination of any of these. Attacking is the actual activity or event in which the Threat Agent attempts to compromise an Asset. An attacker profile defines a group of attackers with similar goals and capabilities. By classifying attackers, their characteristics and aligning them with

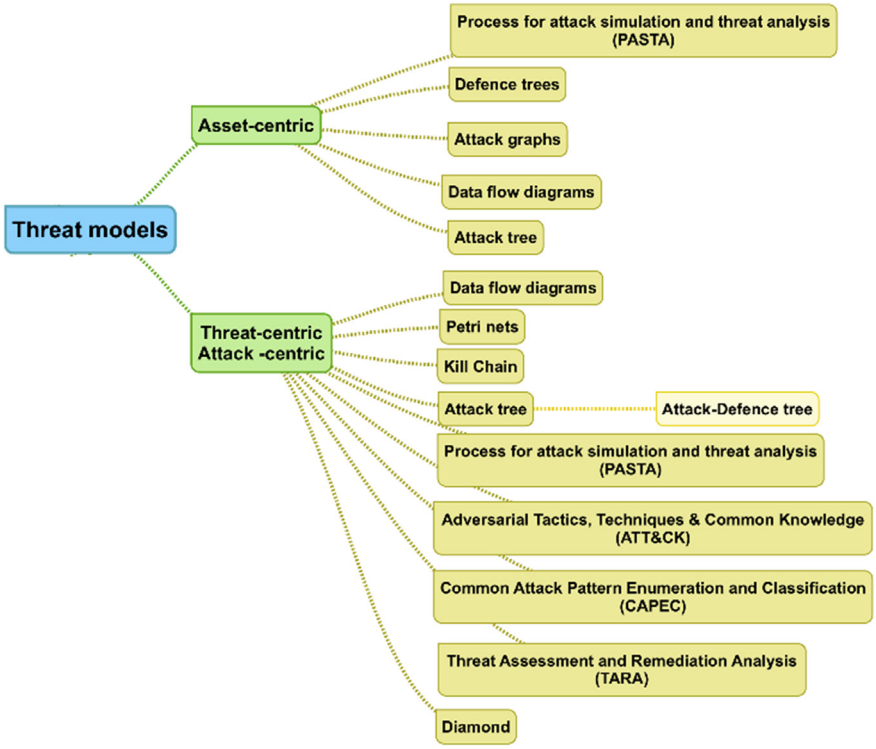

Figure 5. Reviewed papers asset and threat-centric.

associated vulnerabilities, an analyst can start to learn how an asset can be compromised [37, 38]. To defend against attackers, a better understanding of the nature of current vulnerabilities as well as existing and future cyber threats is needed to make an informed decision [39].

2.1. Advanced persistent threat (APT)

Advanced Persistent Threats (APTs) are surreptitious attacks that are employed by knowledgeable and resourceful adversaries whose intent is to compromise the Confidentiality, Integrity and Availability (CIA) of an information and/or critical infrastructure. An APT's attack is well planned and consists of multiple phases, that are designed to reach and persist in the target system without detection. APT's choose their tools based on the environment and steps required, to achieve their goal [40, 41].

The capability of APT's has evolved over time as these groups continue to expand on their current targets and therefore implementing enhanced or new TTP's [99]. These groups can develop fit for purpose malware and data exfiltration methods. APT Threat Modelling is an extension of general threat modelling. It recognises that attacks or campaigns are usually conducted through a series of phases. The development of the cyber Kill-chain [42] and MITRE's ATT&CK [43] framework has been developed from years of APT observations and related threat intelligence.

3. Cyber threat intelligence

Cyber Threat Intelligence (CTI) focuses on the identification, collection, processing and analysis of threat intelligence about existing and

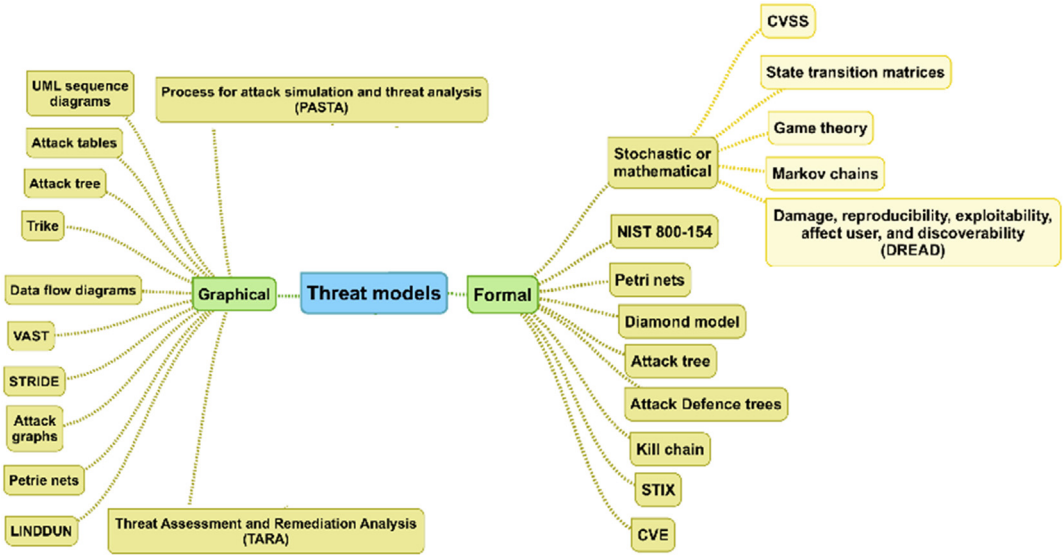

Figure 6. Reviewed papers Formal/Graphical TM.

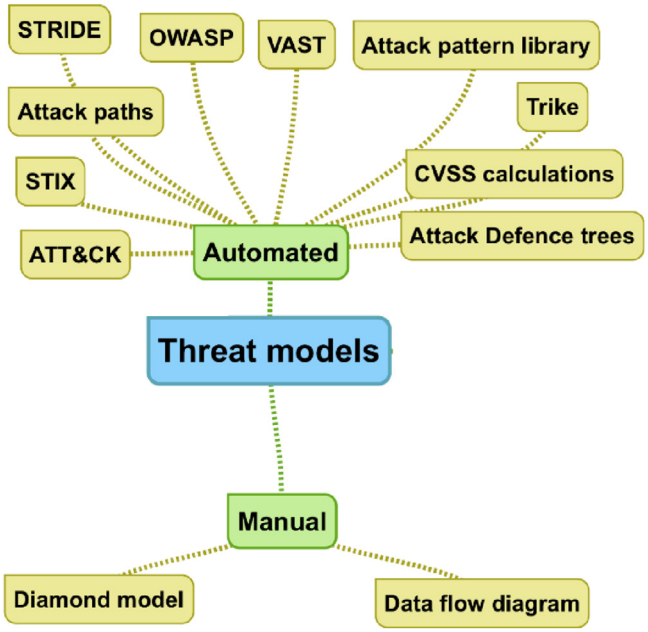

Figure 7. Reviewed papers automated or manual TM.

potential attacks. Based on our research, we have identified and focused on four areas of Cyber Threat Intelligence namely Strategic, Tactical, Operational and Technical (Figure 3). These functions determine the sources of data required for actionable intelligence.

The sources for threat modelling are primarily from the tactical and operational quadrants, however, the technical and strategic areas add value to some models by providing relevance and context.

Strategic CTI is is high-level information, relevant to senior executives that aligns security objectives to business goals [98]. Operational CTI is relevant to penetration testers, defenders and incident response personnel. Technical CTI informs technical staff who monitors and configure systems and controls. Tactical CTI is often referred to as Tactics, Techniques and Procedures (TTPs) produced from internal sources or obtained externally [15, 44]. CTI traditionally analyses attacks after they have already happened, resulting in reactive advice. Therefore, to be relevant the Cyber Threat Intelligence Cycle needs to be a continuous iterative process. At all stages there requires feedback and review to validate and assure that it produces actionable intelligence [45, 46].

Operational teams and researchers have been seeking to develop proactive CTI by better understanding current threats. Samtani et al. [47] explains that potential threats can be identified directly from malicious intruder communities. They identified a framework that contributes to the understanding and implementation of proactive identification of cyber threats [47]. The framework identifies many openly available, malicious assets (unstructured data and artefacts) in the dark web such as crypters, keyloggers, SQL Injections, and password crackers. A limitation of this research is that forums only provide data from attacks that have already occurred. Therefore, a similar comprehensive opensource or internal dataset on historical attacks, can deliver the same intelligence.

To be effective, CTI requires reputable sources of data that can be provided by vendors, opensource repositories, as well as internally sourced datasets. To support the security community, ENISA (European Network and Information Security Agency) has released a reliable cybersecurity search engine named Open-CSAM. This tool aims to continuously monitor CTI sources, highlighting trending cybersecurity threat content, using artificial intelligence (AI) [15].

CTI can be collected in structured and unstructured format. However, to be useable almost all data collected needs to be transformed in some understandable form, whether it be a manual (human) or automatic (computer) process [48]. Structured data, such as STIX (Structured Threat Information eXpression), from reputable sources, follow standards and are easy to automatically ingest [49]. Unstructured data such as reports, web sites or community forums can present a challenge to consume and require some sort of manual analysis. Structuring data and indicating their relationships is where a threat taxonomy fits within the CTI lifecycle. A threat intelligence capable organisation can use threat taxonomies to provide probability estimates for threat activities [28].

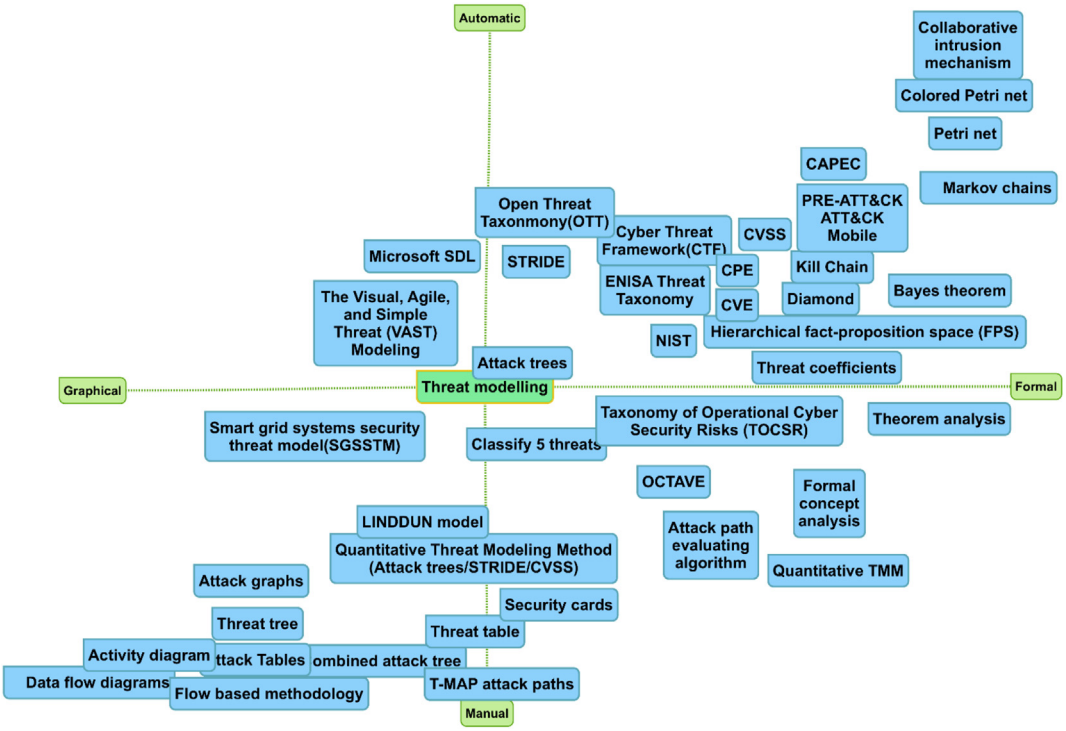

Figure 8. Quadrants identifying Automated/Manual and Formal/Graphical Threat Models.

Table 3. Assigning strengths to Threat models.

Strength	Iteration 1			Iteration 2			Iteration 3		
	1 Reviewer (A)			3 Reviewers (A, B, C)			3 Reviewers (A, B, C)		
Threat Models	A	B	C	A	B	C	A	B	C
DFD	✓			✓	✓	✓	✓	✓	✓
STRIDE	✓			✓	✓	✓	✓	✓	✓
Attack Trees	✓			✓	✓	✓	✓	✓	✓
Stochastic	✓			✓	✓	✓	✓	✓	✓
Kill chain	✓			✓	✓	✓	✓	✓	✓
PRE-ATT&CK	✓			✓	✓	✓	✓	✓	✓
ATT&CK	✓			✓	✓	✓	✓	✓	✓
CAPEC	✓			✓	✓	✓	✓	✓	✓
TARA	✓			✓	✓	✓	✓	✓	✓
Diamond	✓			✓	✓	✓	✓	✓	✓
NIST 800-154	✓			✓	✓	✓	✓	✓	✓

Table 4. Assigning limitations to Threat models.

Limitation	Iteration 1			Iteration 2			Iteration 3		
	2 Reviewers (A, B, C)			3 Reviewers (A, B, C)			3 Reviewers (A, B, C)		
Threat Models	A	B	C	A	B	C	A	B	C
DFD	✓	✓		✓	✓	✓	✓	✓	✓
STRIDE	✓	✓		✓	✓	✓	✓	✓	✓
Attack Trees	✓	✓		✓	✓	✓	✓	✓	✓
Stochastic	✓	✓		✓	✓	✓	✓	✓	✓
Kill chain	✓	✓		✓	✓	✓	✓	✓	✓
PRE-ATT&CK	✓	✓		✓	✓	✓	✓	✓	✓
ATT&CK	✓	✓		✓	✓	✓	✓	✓	✓
CAPEC	✓	✓		✓	✓	✓	✓	✓	✓
TARA	✓	✓		✓	✓	✓	✓	✓	✓
Diamond	✓	✓		✓	✓	✓	✓	✓	✓
NIST 800-154	✓	✓		✓	✓	✓	✓	✓	✓

Table 5. Post iteration Code Agreement matrix.

	Iteration 1			Iteration 2			Iteration 3		
	Reviewers (A, B)			Reviewers (A, B, C)			Reviewers (A, B, C)		
Code	A	B	C	A	B	C	A	B	C
Strength	35	0	-	21	21	21	26	26	26
Limitation	27	22	-	19	19	19	19	19	19
Agreement	1.0	0.8	-	1.0	1.0	1.0	1.0	1.0	1.0

A graphical representation of applying CTI to detect and respond initiatives was introduced by David Bianco. This "Pyramid of Pain" (Figure 1) shows the hierarchical relationship between indicator types used to detect an attackers actions and "how much pain it would cause them when you are able to deny those indicators to them" [10]. The higher up the pyramid, the longer these indicators will exist. That is, it focusses more on the higher-level Indicator of Compromise's (IOC) which are less dynamic and provide actionable intelligence. At all levels, these IOC's can be correlated by a SIEM that will alert incident responders for investigation and remediation if deemed necessary. Once Tactics, Techniques and Procedures (TTP) are identified and controlled, the attacker will need to adapt new attack patterns to continue to be a threat. Noor U.

et al. utilised this pyramid and believes that the low-level IOCs can only useful for a limited time period, as the attacker can vary their indicators by using alternate service providers, IP addresses, attack servers and domain names etc. [50].

The most common standard for effective information sharing is STIX. STIX 2.0 defines a set of Cyber Observable Objects for characterising host-based, network, and related entities. Each of these objects correspond to a single or group of data attributes that are commonly represented in CTI and digital forensics. STIX's has 12 Domain Objects that provide additional context to the enclosed data. They are Attack Pattern, Campaign, Course of Action, Identity, Indicator, Intrusion, Malware, Observed Data, Report, Threat Actor, Tool and Vulnerability [46, 49]. This structured data specifically references the Kill chain phases (Attack Pattern, Indicator, Malware, Tool), CAPEC(Attack Pattern) and can be used by Markov chains, to predict attack paths [39, 42, 51].

Cyber-Physical Systems (CPS) are systems that integrate physical, computational, and networking components. In a study by Martins, et al. [16], it was identified that there is limited tools available assist with methodically analysing CPS threats. The scarcity of these tools is due to the diverse features of a CPS. That is, CPS's can be consist of various hardware and/or software components that make it difficult for one tool to model threats. Martins, et al. proposed a Generic Modelling Environment from a previous research paper [52] that supported their CPS threat analysis model.

Malware Information Sharing Platform (MISP) is an open source Threat Intelligence Platform and Standards for Threat Information Sharing. The MISP threat sharing platform is a free and open source software that assists in sharing threat intelligence including IoC's. It is a threat intelligence platform for gathering, storing and sharing of the IoC's of targeted attacks. These are sourced from vulnerability repositories, CTI, financial fraud, criminal activities and terrorism related information [53].

4. Threat modelling

A risk model is a quantitative representation identifying the likelihood and impact a threat will have on an asset. As such, Threat Modelling (TM) is a component of a Risk Modelling. TM is an iterative process that defines and profiles an asset, identifies, prioritises and monitors security threats and evaluates their associated controls. It formalises the process to analyse the security vulnerabilities and risks of a host, an application and/or network service [4, 54].

The aim of TM is to be proactive in identifying, classifying and describing threats, that provide visibility of an attacker or a campaign of attacks. This promotes the evolution of resilience, by anticipating, withstanding and recovering from a security incident. There are 4 recognised approaches to modelling threats (Figure 2). The first, is an approach that focuses on individual account, system and/or data that has a value to the attacker. It is the target the attacker requires to compromise to complete their objective, and it is the asset that requires protection [55].

The second, a system or software-centric threat modelling, begins with an architectural design model of a system and its software. It focuses on all identifying all components and their possible related attack vectors. The third is a draft publication published by NIST. This publication examines data-centric system threat modelling, which is threat modelling that is focused on protecting particular types of data within systems [17].

The threat-centric or attacker-centric is the last approach and it efforts concentrate on evaluating the attackers target, and attempts to identify the possible vectors needed for to fulfill their objective [42, 56, 57]. This study is focused on a identifying the best model and approaches that can reduce the risk of APT's.

Most existing approaches for threat modelling that use CTI (Figure 3), can be generally divided into two core approaches, Graphical and Formal. Formal modelling is a method based on mathematical (stochastic) models [16]. Whilst graphical modelling uses attack trees, attack graphs, Data Flow Diagrams (DFDs), or tables [27].

The 10 most relevant threat model approaches identified in the research reviewed, will be discussed. Data Flow Diagrams represent a graphical model, Attack Trees are both graphical and formal, whilst the remaining approaches (ATT&CK, Kill Chain, STRIDE, TARA, CAPEC, Diamond and NIST 800-154) are formal models.

4.1. Data flow diagrams

A Data Flow Diagram (DFD) is a graphical representation of a system, that shows all the inputs, logical internal processes and outputs. Threat Modelling (TM) with DFD's focusses on external entities, trust boundaries, the data store as well as, the processing and flow of the data through the system.

Making a DFD can be a time-consuming task, and it is not to be used in isolation, it can be strongly advocated that it is only one phase of the threat modelling process [58, 59].

DFD's can be used within other threat modelling approaches. Studies from Eng et al. [55] and Cheung [60] incorporated DFD's with a complementing modelling technique called STRIDE (Spoofing, Tampering, Repudiation, Denial of Service and Elevation of Privilege). They both identified that DFD elements (Table 6) can be used in conjunction with the threat types of STRIDE (Spoofing, Tampering, Repudiation, Denial of Service and Elevation of Privilege).

4.2. STRIDE (Spoofing, tampering, repudiation, Denial of Service and Elevation of Privilege)

STRIDE (Spoofing, Tampering, Repudiation, Denial of Service and Elevation of Privilege) is a system/software-based taxonomy for identifying threats based on their explicit type. It was first introduced to developers at Microsoft in 1999 and was used to assist developers in identifying threats relevant to their software products. The root cause can be categorised as security flaw in design, a security bug in coding, or an issue due to insecure configuration [61].

STRIDE helps address threats to confidentiality, integrity, availability, authentication, authorisation, and nonrepudiation [18]. However, it does not identify specific attack vectors or actions, it primarily categorises general types of threats, therefore, to be thorough, additional vectors from known attack libraries need to be also investigated and considered [54, 62, 63, 64]. A STRIDE Category can have multiple threats and alternatively a threat can have multiple STRIDE categories.

To effectively apply Machine Learning (ML) to threat models requires some level of automation and portability. Shevchenko et al. identifies the

Table 6. Threat types for the four elements of a DFD.

DFD Element Type	S	T	R	I	D	E
External Entity	✓		✓			
Data Flow		✓		✓	✓	
Data Store		✓	✓	✓	✓	
Process	✓	✓	✓	✓	✓	✓

use of both STRIDE and CVSS are able to be automated [19], however, because of its narrow software focus it requires additional support to identify all possible threats.

4.3. Attack trees

Attack Trees are conceptual diagrams that use a branching, hierarchical data structure. They map threats and their possible attack vectors required, to achieve their goal or state. Bruce Schneier introduce this concept to model threats against computer systems. It breaks down all the known attacks to a system, and then attaches a risk and cost values to each attack vector [31].

Attack trees formally identify and define the variety of attacks a system can be subjected to. The common steps in the attack tree approach is to define the overall goal and decompose it into sub goals. It represents all possible attacks in a hierarchical tree structure, with the root node signifying the goal of the attack and the leaf nodes depicting the many permutations of paths that may be followed to fulfill the objective [16].

The leaf nodes are potential sub-goals and/or states that an attacker requires to achieve before the next level of compromise. The sub-goals can be either OR or AND sub goals. That is, an AND sub goal requires both sub goals to be achieved, whereas an OR requires only one to be achieved to continue the attacker's path [65]. Attack Trees are both graphical and formal, that is, apart from the graphical nature of an attack tree, you can also assign values to the various leaf nodes. Using these values can assist in predicting whether an attack may happen. That is, if an attack costs the perpetrator more than the benefit, that attack will most likely not occur [66]. One common limitation of Attack Trees is that they are static in nature and the ability to scale is resource intensive [16, 32, 39, 62, 65, 66].

Defence trees extends the attack tree approach by incorporating various defensive measures against the attack vector. This model was further extended by the University of Luxembourg by formally introducing an attack-defence tree [37]. An attack-defence tree (ADTree) considers the actions taken by an attacker to achieve their objective, as well as, associating additional defence actions and/or controls that may be used to mitigate one or many, attack paths [16].

4.4. Stochastic or mathematical models

Stochastic (Stochastic or Mathematical) model-based threat modelling approaches commonly convert attack actions and associated attributes to Markov chains, and analyses them through the use of state transition matrices. That is, the next state of the system depends entirely on the current state. This aspect allows Markov Chains the ability identify chains of attack vectors that require preceding and current system states to be met before an attack can continue on its current path [39].

The use of game theory has also been used to assist in modelling APT's. game-theoretic foundation by establishing a multi-stage Bayesian game framework to capture incomplete information of deceptive APTs and their multistage multi-phase movement. Another stochastic approach was used to conduct behavioural analysis of an attacker once a system had been compromised. Martins, et al. [16] discusses an "integrated security and dependability evaluation approach" using a formal game theory approach to model the intruders behaviour. It believes a formal stochastic based model that incorporates behaviour, will provide a better solution when compared to the attack tree alternative [67].

4.5. Kill chain

The European Network and Information Security Agency (ENISA) identified the two main trends of adopting the philosophy and methods of Military Intelligence and introducing Artificial Intelligence into technologies for counteraction of cyber-attacks. The first was the qualitative transition to new cyber defence tools involving use of artificial intelligence methods to analyse information exchanged, network flows, sources of threats, and to plan effective impact measures, including proactive ones [15].

The second direction was the use in Cyber Defence of the techniques and methods of traditional military science and military intelligence, that is, Kill chains. The term kill chain, was originally used as a military concept related to the structure of the attack. The idea is to effectively prevent or counteract the opponent in the various phases of the attack lifecycle [42, 68, 69].

The intrusion kill chain is defined as reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives (AOO) [42]. The intelligence-driven computer network defence (CND) model in Hutchins et al. study used Lockheed's kill chain model to describe the phases of intrusions and then maps the adversary kill chain indicators to defending courses of action [70]. This approach has specific defence techniques that leverage knowledge about adversaries to create an intelligence feedback loop, decreasing the likelihood of a successful compromise. The model is designed to mitigate both vulnerabilities and threat components of a risk.

To attribute cyber threats effectively, it is necessary to identify them based on their attack patterns different phases of the kill chain. These are tactics, techniques, procedures and the tools used (software). Tactics are the goals or states an attacker tries to achieve to complete their mission. A technique is how a specific behaviour or activity achieves that goal or state. A tactic can have many techniques and a technique can have many tactics (Figure 9). Procedures and software identify the tools or steps used to complete a series of actions conducted in a certain order or manner. To achieve one of these steps an APT's can use many tactics. In turn, these tactics are accomplished by using one or many techniques and/or software tools.

The researchers Hutchins et al. [70] and Noor U. et al. [50, 71] confirm that the TTP's of the attacker remains consistent over a period of time. This allows greater confidence in the predictability of the lower level indicators of attack. It also identifies the individual attack patterns that can be linked to a broader intrusion set (see Figure 9) and promotes the iterative nature of intelligence gathering. The continuous risk-based model also confirms that environment needs to be re-assessed to determine if additional threat data affects the likelihood of an asset or its supporting asset being compromise.

An evolution of the kill chain is Lockheed Martin Intelligence Driven Defense® model (LMIDDM). It gathers intelligence from the adversary during the threat life cycle and uses it to minimise the impact of an attack. Methodology and maturity using SOC services, Situational awareness, knowledge management, analysis, mitigation and measurement [70]. The Cyber Kill Chain® framework is component of LMIDDM. There have been only 2 articles reviewed associated with Lockheed Martin [42, 70]. However, this does not reflect the significant contribution from Lockheed Martin to the modelling approach we will take in our study.

In each phase of their kill chain model Noor et al provides examples of the existence of the adversary's attack patterns in the form of TTPs, which in turn can be linked to their attack and detection mechanisms [50]. However, Kill chains on their own are not effective at mapping these actions to their associated vulnerabilities, which limits identifying relevant controls and detection mechanisms [63].

4.6. Adversarial Tactics, techniques & Common Knowledge (ATT&CK)

There are several frameworks that describe and categorise adversarial behaviours based on real-world observations of their tactics and techniques. In 2013 to better understand cyber threats, the MITRE corporation developed the Adversarial Tactics Techniques & common Knowledge (ATT&CK) Framework [56]. Pre October 2020, MITRE had ATT&CK matrices associated with Enterprise assets (Linux/MacOS/Windows) [72], Mobile devices [73], and an initial PRE-ATT&CK [74] pattern. PRE-ATT&CK was a framework which aligns with the first three phases of the kill chain, that is, reconnaissance, weaponization, and

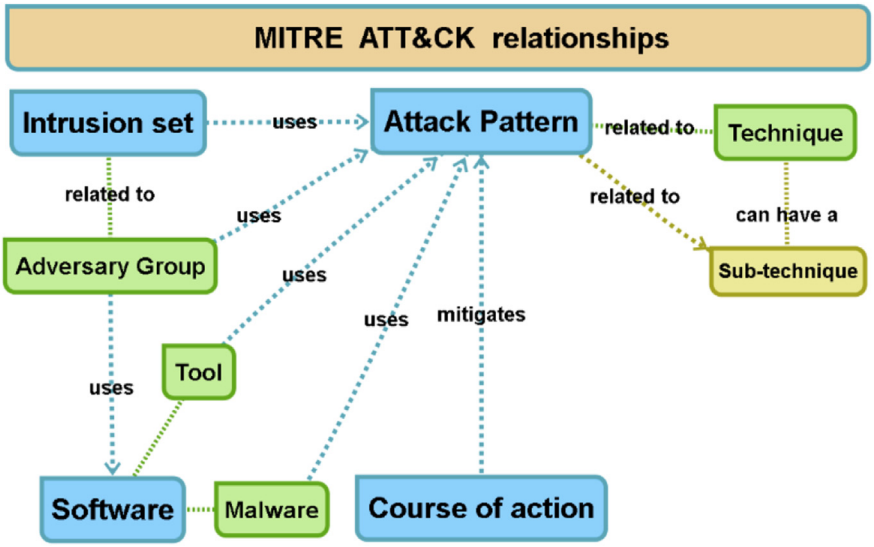

Figure 9. ATT&CK Model relationships [63].

delivery. Version 8 of the ATT&CK Enterprise framework now incorporates PRE_ATT&CK and now aligns closer to all phases of the kill chain including the post access phases of exploitation, installation, C2, and AOO [72].

Tactics represent the highest level of abstraction within the ATT&CK model. They are the tactical goals an adversary has during an operation. The techniques within the ATT&CK model describe the actions that adversaries may take to achieve their tactical objectives [5]. ATT&CK builds on the Cyber Kill Chain, by focusing on the Techniques, Tactics, Software and indicators associated with specific adversaries (Figure 9). An important distinction between a technique in ATT&CK and an IOC is that many of the ATT&CK techniques are legitimate system functions that can be used for malicious purposes [5], which makes it harder for defenders to detect. MITRE has also mapped Software attacks from publicly reported technique use and accounts for the capability of the software adversary to use a technique [75].

The ATT&CK framework uses a quantitative data model that addresses the gaps that exist between strategic & operational, and operational & tactical intelligence. That is, at a strategic level, the executive leadership use actionable intelligence to prioritise and maximise their resources whilst minimising risk. At the operational level, this framework assists in threat analysis, vulnerability management and relevant security awareness based on the current threat landscape [15].

Xiong, Zhu et al. believes an overly complicated multiphase model can be used only to better understand APTs, not to detect them [41]. The study discusses three main problems using existing research conducted by Milajerdi et al [40], to support their claim. The first identifies that "detecting hundreds of techniques is hard to implement and can cause high detection overhead", however, Milajerdi et al identifies this challenge and provides a directed provenance and high-level scenario graph as the solution [40]. Our review also found a minor discrepancy in Xiong, Zhu et al. study as it was limited to only 11 tactics of the MITRE ATT&CK framework, ATT&CKv7 consisted of twelve tactics Initial Access, Execution, Persistence, Privilege Escalation, Defence Evasion, Credential Access, Discovery, Lateral Movement, Collection, C2, Exfiltration and Impact [41, 72], ATT&CKv8 includes the two additional phases of Reconnaissance and Resource Development merged from PRE-ATT&CK.

Our study agrees with Xiong, Lagerström et al. [27] who's second issue of identifying vulnerabilities, require prior knowledge, and it is hard to detect unknown attacks. However, their approach would still be able to detect known attacks, in a real-time detection system. Another challenge was that it was unnecessary to detect all phases and presenting some common and redundant phases would increase false alarms. Milajerdi et al. addressed this technical challenge by identifying benign patterns and heuristics that assigned weights to the nodes and paths in the graph that enabled a ranking system [40].

Noor et al, developed a novel framework that uses TTPs derived from both unstructured and structured cyber threat intelligence as a means for investigating data breaches. It suggested the attackers' TTPs remain the same and they are "re-used over and over again with little innovation" [71]. The fundamental principle of the proposed framework is the TTP Threat Detection (TTD) semantic network. This approach uses the ability to map the higher-level tactics and techniques to the lower-level threat artefacts of an attacker or group of attackers.

The methodology and the results presented in this study highlighted that security incidents can be mapped to TTPs, that are further mapped to their associated artefacts, in a way that an ML algorithm could automatically forecast or predict connections with a large degree of certainty. This approach can also assist even if a dataset contains only partial or incomplete information. In the case of an unforeseen threat, the system provides the security analyst details of the most probable attack pattern that uses the threat artefacts and recommends effective detection and control measures. The supporting CTI and detection mechanisms are able to be dynamically updated, as new data becomes available or a new version of MITRE's ATT&CK taxonomy is released [71].

A second study also by Noor et al. [50] researched a Machine Learning (ML) based cyber threat attribution framework using high-level IoC's. The authors present a framework that investigates cyber threat incidents and attributes them to an adversary using TTP's extracted from structured and unstructured CTI sources. The framework is based primarily on mapping these low-level threat artefacts to an attacker's high-level indicators such as tactics, techniques, procedures, tools and malware. The researchers tested 5 Machine Learning classification approaches to attribute an adversary based on the TTPs identified in CTI being mapped to feature labels derived from MITRE's ATT&CK taxonomy.

Noor et al. admit that their study is far from being conclusive as the framework is dependent on the integrity of the threat data it uses [50]. That is, for effective attribution, the reputation of CTI sources needs to be objectively weighted to ensure the ML algorithm is provided with relevant CTI data specific to the environmental context and MITRE's ATT&CK taxonomy.

4.7. Common Attack Pattern Enumeration and Classification (CAPEC)

The Common Attack Pattern Enumeration and Classification (CAPEC) is a standard vulnerability database. CAPEC is a list of the most common methods attackers use to exploit vulnerabilities identified in Common Weakness Enumerations (CWE). That is, CAPEC is focused on application security, and describes the common attributes and techniques employed by attackers to exploit known vulnerabilities. CAPEC analyses and classifies cyber-attacks into a list of attack patterns which may occur pre or post exploitation. It also identifies the steps in common cyber-attacks and documents their mitigation steps. There are three levels (Meta, Standard, and Detailed) within the CAPEC Model [51, 57].

An attack pattern describes the common attributes and approaches employed by adversaries to exploit known weaknesses in cyber-enabled capabilities. Attack patterns define the challenges that an adversary may face and how they go about solving it.

The first is meta attack patterns, which intentionally lack details of specific technology or implementation. The second is standard attack patterns which are more procedural and specific. The third pattern is the detailed attack pattern. This pattern is very specific as it provides in-depth detail including any other associated or supporting detailed attack pattern. The STIX Attack Pattern Domain Object contains references to the CAPEC taxonomy. STIX relationships also help identify what vulnerabilities it targets, and which tools and malware use it [49].

4.8. Threat Assessment & Remediation Analysis (TARA)

Threat Assessment & Remediation Analysis (TARA) is also an initiative by MITRE. It identifies, assesses cyber threats and well as their counter measures. TARA includes a threat matrix of an adversaries TTP's, called the Cyber Threat Susceptibility Analysis (CTSA). To complete the TARA process CTSA is then used in combination with Cyber Risk Remediation Analysis (CRRA) [76].

CSTA consists of defining the assets in scope, identify related TTP's, remove unlikely TTP's, apply a ranking system and construct a threat matrix that defines the score, target assets, and adversary type. Although it was only discussed in three studies, its usage of TTP type categorised to assets is relevant to this review. Its uses of taxonomies such as such as MITRE CAPEC, ATT&CK, CVE and CWE to create a TTP catalogue appropriate to its assets is a technique that not many TM employ. An additional benefit is its scoring system. It uses 12 factors with a standard range of values from 1 to 5 that covers Proximity, Locality, Recovery Time, Restoration Costs, Impact on Confidentiality, Integrity, and Availability, Prior Use, Required Skills, Required Resources, Stealth, and Attributions [54, 62, 64].

4.9. Diamond

The Diamond threat model (Figure 10) is a formal method for applying scientific principles to intrusion analysis, it is a model that maps the relationships and characteristics of adversary's capability to a target's infrastructure. It is used to track attack groups with the assumption that and attacker will change its targets and its TTPs over time. It gets its name from the diamond shape used to graphically identify the four different elements of any intrusion activity (Figure 10) adversary, infrastructure, capability and victim [47, 77].

The diamond approach is similar to the Kill Chain and ATT&CK models in that it is based an attacker requiring to take steps toward an intended goal by using capability (TTP) over infrastructure against a target. That is, it can correlate specific events and their links to each other called activity threads. It then uses the in the Kill Chain to link relationships between these activity threads. It is a method that applies formal principles to intrusion analysis. It can also be extended to include features such as phase, result, direction, methodology and resources. It provides a testable and repeatable method that identifies activity and correlates an attack using quantifiable measures. This approach although not popular is relevant to this study as it provides an effective formal method to modelling APT's [28, 44, 63, 77, 79, 80].

4.10. NIST special publication 800-154

The National Institute of Standards and Technology has a draft guide (800-154) for threat modelling system that is centred around data. It is intended to be an introduction to data-centric system threat modelling. It discusses a qualitative approach to threat modelling using four steps [17].

The first is the identification and characterising process. It includes only specific data on a specific host or a small group of closely related hosts and devices. Storage, transmission, and processing related to the security objectives that allow authorized people and processes to access the data.

The second stage identifies the potential attack vectors of an adversary based on risk assessments (likelihood and impact). The third phase addresses the security controls for mitigating specific attack actions and patterns. Feasible risk mitigation controls are identified. In the final phase, the threat model is analysed, to determine all the attack vectors and controls across all the unacceptable risks [54]. This method is a relatively novel approach and was included in this review to provide visibility and coverage of a data-centric approach.

To visualise the modelling and taxonomies that our research discovered, we used a mind mapping exercise (Figures 2, 3, 4, 5, 6, and 7). Figure 4 includes the more technical orientated approaches (data, system/software) [17], and Figure 5 focuses on business and risk related approaches (assets, threats) [16]. In additional to this we classified the TM into quadrants based on a Graphical/Formal and a Manual/Automated axis (Figure 8).

5. Threat model advantages and limitations

This section will discuss the capability across all TM approaches and will compare the advantages and limitations of each of the models mentioned. To identify and agree upon the advantages (Table 7) and limitations (Table 8) associated with the 11 threat models we used an IRR approach.

Most studies acknowledged that most threat modelling work remains to be conducted manually [16, 28, 29, 35, 39, 46]. This was strongly articulated in the conclusion of Xiong & Lagerström [27], whom presented a systematic Literature review of threat modelling based on research using four leading scientific databases. This study identified and assessed 54 articles that related to existing and new contributions to the threat modelling process. These articles were analysed in terms of the

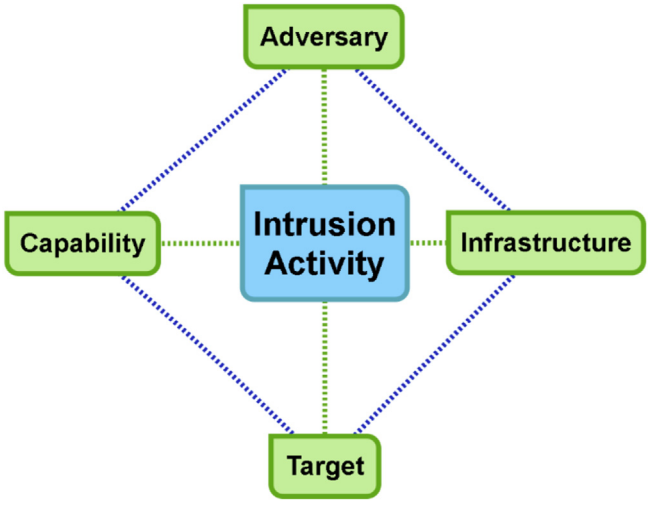

Figure 10. The diamond model [77, 78]

Table 7. Threat Model strengths.

Advantages (✓)	DFD	STRIDE	Attack Trees	Stochastic	Kill Chain	PRE-ATT&CK	ATT&CK	CAPEC	TARA	Diamond	NIST 800-154
Accessible in MISP						✓	✓				
Adversary Capability [51, 54, 72, 74]					✓	✓	✓	✓		✓	
Available from Threat feeds [39, 82]					✓	✓	✓	✓			
Usage with STIX [39, 82]		✓		✓	✓	✓	✓	✓			
Can automate TM process		✓		✓				✓			
Can be combined with other threat models	✓	✓	✓			✓	✓		✓		
Maps exploits against vulnerable systems & environment to attack vectors								✓	✓	✓	
Identifies data at risk – storage, processing & in-transit [17, 83]					✓						✓
Easy to use [19]	✓	✓	✓								
Extensible/Flexible [17, 54]		✓	✓	✓		✓	✓	✓	✓	✓	✓
Good documentation [19]	✓	✓	✓		✓	✓	✓	✓			
High Maturity [19, 60, 70, 79]	✓	✓	✓		✓	✓	✓	✓			
Identifies gaps [19, 70, 79]		✓			✓	✓	✓		✓		✓
Identifies phases/elements/patterns in Attacks (composite threats) [15, 75]				✓	✓	✓	✓	✓		✓	
Link individual intrusions to campaign (APT)					✓	✓	✓			✓	
Map defensive controls or countermeasures		✓			✓	✓	✓		✓		✓
Prioritises Threats [17]									✓		✓
Software design, analysis, testing and support [75]		✓					✓	✓			
Standards based or well structured		✓			✓	✓	✓	✓			
Taxonomy for Pre & Post compromises		✓			✓	✓	✓	✓		✓	
Models the time-agnostic nature of TTP (APT)										✓	
Used for Attack simulations or Penetration testing				✓		✓	✓	✓			
Used for Investigations						✓	✓				
Used for Threat Hunting/Detections				✓	✓	✓	✓	✓		✓	
Uses one or many threat catalogues	✓		✓	✓					✓		
Validate/assesses capability of defensive controls						✓	✓				✓

models' approach, the type of attack and how their contribution was validated (empirically or theoretically).

There are four TM methods that can be combined with another model or models. Attack Trees and DFD can be used within other frameworks to enhance the modelling capability. Additionally, STRIDE and TARA can also be used by other models such as ATT&CK and Kill-chain to augment the identification of TTP's and their associated controls or remediation actions.

For a maturing organisation, the ability to be able to quickly adopt a TM approach allows them to be able to Identify, Protect, Detect, Respond and Recover [22]. Our study has identified Lockheed Martin's Kill-chain, STRIDE and MITRE's approaches as structured and well documented. MITRE's stands out in this aspect as it has invested a large amount of resources developing and documenting their structured PRE-ATT&CK, ATT&CK, CAPEC approaches [51, 72, 73, 74].

The models that were effective in threat hunting and detecting intrusions, did however, have some limitations. Our study found a common limitation with ATT&CK, CAPEC, Diamond and Kill Chain. These models can identify the phases and elements in attacks and composite threats, however, they did have challenges when mapping attacks TTP's to the organisations environment (data, configurations, vulnerabilities) and the many permutations of the associated events and actions [19, 29, 79].

Martins, et al. [16] also concluded that there aren't any publicly available tools (or techniques) that automatically perform a systematic analysis of security threats in Cyber Physical Systems, that is, threat modelling remains a manual process. Some of the approaches identified that can be limited by labour intensive and time-consuming aspects are DFD's, STRIDE, CAPEC, Diamond and TARA [19, 60, 65, 81].

An efficient TM is one that can evolve with the organisations maturity and is easily scalable. Alternatively, having a TM that requires constant updating and maintenance, becomes very labour intensive and time consuming. We also found that to effectively apply Machine Learning to threat models requires some level of automation and portability. Our study identified several threat models that use automation at different stages in their approach.

TM approaches that are more formal have the potential attributes required to automated threat modelling. When applying automation to TM a taxonomy is an advantageous factor. Taxonomies were common in

Table 8. Threat model limitations.

Limitations (✗)	DFD	STRIDE	Attack Trees	Stochastic	Kill Chain	PRE-ATT&CK	ATT&CK	CAPEC	TARA	Diamond	NIST 800-154
Challenging map attacks (TTP's) to environment (data, configurations, vulnerabilities) [79]		✗			✗	✗	✗				
Challenging to determine malicious vs non-malicious techniques [63]					✗	✗	✗				
Challenging to map attacks to defences against an attack (Controls) [19]			✗								
Challenging to map/detect all the many permutations of event, actions and execution		✗			✗	✗	✗				
Has trouble scaling to large environments	✗	✗		✗				✗	✗	✗	
High rate of false negatives [19]		✗									
Identifies high level details not specific attack details		✗	✗								
Labor intensive or time consuming to develop and maintain [19, 60, 65, 81]	✗	✗		✗				✗	✗	✗	
Limited in modelling insider threats					✗						
Limited scoring analysis [17]				✗							✗
Limited to software/application threat modelling		✗						✗			
Manual	✗			✗							
Not all phases are used in a compromise					✗						
Not an exhaustive enumeration of attack vectors against software						✗	✗				
Not effective at how sequences of actions relate to adversary objectives		✗			✗			✗			
Not Extensible/Not Flexible?			✗								
Requires constant updating/Maintenance			✗					✗	✗	✗	
Requires expertise and environmental (contextual/vulnerability chaining) knowledge	✗		✗								
Requires high level of maturity of processes [17]											✗

the mature TM frameworks, such as, PRE-ATT&CK, ATT&CK, CAPEC, Diamond, Kill Chain and STRIDE [42, 51, 72, 74]. However, a challenge to these taxonomies was the time needed to map the many permutations of TTP's to a specific environment [19, 79]. Additionally these approaches were not effective in determining how sequences of actions were related to an adversary objectives [29] and were also unable to effectively determine malicious vs non-malicious techniques [63].

6. Taxonomy

To effectively model an attack, a Taxonomy is required that associate attackers and threats to vulnerabilities, assets, controls and detection methods. A Taxonomy is the practice of classifying objects into groups based on similarities or differences of their attributes. It structures data to produce information and can improve communicating a threat model.

Clear definitions of threats are broken down to clarify any ambiguity due to barriers that may exist between professionals specialising in different fields. Supported by this common language is a taxonomy based on the entire threat landscape enabling the analysis and assessment at various granularities [28].

In 2017 the Office of Director of National Intelligence (ODNI) provided a vocabulary for the Cyber Threat Framework (CTF) has been likened to a threat taxonomy [54]. The CTF is a threat-centric framework, consisting of four stages of adversary attacks. They are Preparation, Engagement, Presence, and Effect/Consequence. The CTF was designed to improve communication between across many departments within the United States governments intelligence community.

Another publicly available taxonomy is the Open Threat Taxonomy (OTT). It has four threat components, an agent, a target, an action and a consequence. The objective is to rate and catalogue threats into the following four threat categories, Physical, Resources, Personnel and Technical [28, 91].

The European Network and Information Security Agency (ENISA) has designed the ENISA Threat Taxonomy (ETT). It is used as an analysis mechanism for collecting and sorting threat information. purpose for its taxonomy is to also provide a vocabulary for threat terms. The ETT group's 75 threat actions, their related objectives and consequences, into eight high-level threat categories. These high-level threats comprise of disasters, outages, failures & malfunction, physical attack, unintentional damage, malicious damage, legal and interception of communications [15].

National Institute of Standards and Technology (NIST) categorises all threat events into Adversarial and non-adversarial. They also identify a threat scenario as a series of threat events [22, 25].

Taxonomy of Operational Cyber Security Risks (TOCSR) is another comprehensive threat taxonomy from Carnegie Mellon University. This taxonomy has 4 high levels, Actions of people, Systems and technology failures, Failed internal processes and External events [28].

As discussed, MITRE has a publicly available taxonomy called the Adversarial Tactics, Techniques and Common Knowledge (ATT&CK). ATT&CK v8 comprises of 14 high level TTPs, malware and software tools used by Cyber Threat Actors in their attacks. MITRE provides ATT&CK in the Structured Threat Information Expression (STIX) 2.0 JSON format via GitHub. ATT&CK classifications include the following, Initial Access, Execution, Persistence, Privilege Escalation, Defence Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command & Control, Exfiltration and Impact [72].

An additional MITRE Taxonomy is the Common Attack Pattern Enumeration and Classification (CAPEC). It was created to assist in the building of secure software is a taxonomy that identifies attack patterns, schemas and classification taxonomy [51, 57]. MITRE also has developed the Cyber Analytics Repository (CAR) which is a knowledge base of analytics on the MITRE ATT&CK adversary model. CAR defines a analytic data model that describes the function, domain (host, network, process, external), associated ATT&CK Techniques and Tactics, implementation (pseudocode) and the unit test for triggering the analytic [92].

Most taxonomies provide tactical, operational and technical information for cyber resilience, there is very little taxonomies that assists in strategic guidance. Ferdinand believes that organisations still lack the metrics required to make informed decisions in cyber security and [93] proposes two taxonomies to solve this challenge. A cyber threat taxonomy and a cyber-attack taxonomy. These two taxonomies can provide a maturity assessment that enable managers and executives to make informed business decisions on resource and procurement decisions.

7. An analytical dissection of the studies

This section will illuminate key insights derived from critically analysing 49 (Table 9) threat modelling papers.

7.1. Analysis of reviewed papers

Within the 49 papers reviewed 125 collective threat models were discussed. Most studies reviewed were inclined to discuss 4 models per paper, and these tended to include a mean of only 2.7 of the threat models discussed in our study. 11 out of 49 research papers studied 3 of our 11 models this supports the fact that there are many approaches that exist that model threats.

The extensive amount of research and resources the MITRE corporation invests in threat modelling was evident in the studies researched. 51 of the 125 models discussed were PRE-ATT&CK, ATT&CK, TARA and CAPEC. Additionally, both the ATT&CK and Cyber Kill chain were the most common researched methods, with 32% of papers discussing this approach.

Not all papers were able to cover the many TM approaches acknowledged through our research. The origins of the studies were a mixture of academic institutes, government bodies, as well, as the private sector. This identifies that TM are continuingly being researched in both a theoretical and practical environment. Two of the main research reviews in our study (Bodeau et al.) were prepared by the Homeland Security Systems Engineering and Development Institute (HSSEDI) [54, 62]. The research conducted by Bodeau et al. covered 8 of the 11 threat models reviewed in our study. Bodeau also included 15 additional threat modelling approaches not discussed in our study. It does not address the Diamond approach or Data flow diagrams as a standalone model. The study concludes that there is no widely accepted model that currently addresses all possible scopes. The study points to the need for a threat

Table 9. Threat Modelling studies.

DFD	STRIDE	Attack Trees	Stochastic	Kill Chain	PRE-ATT&CK	ATT&CK	CAPEC	TARA	Diamond	NIST 800-154
[16, 19, 27, 29, 33, 37, 55, 60, 61]	[18, 19, 27, 37, 50, 54, 55, 60, 61, 62, 63, 64, 65, 71, 81]	[16, 18, 19, 27, 29, 31, 32, 37, 54, 55, 60, 61, 62, 64, 65, 66, 81, 84, 85, 86]	[16, 17, 39, 45, 67, 68, 81, 84, 85], [87]	[9, 15, 17, 27, 28, 39, 40, 41, 42, 44, 45, 49, 50, 54, 62, 63, 68, 70, 71, 79, 82, 83, 84, 88, 89]	[28, 33, 50, 51, 54, 56, 57, 61, 63, 71, 74, 81, 89, 90]	[5, 9, 15, 26, 28, 33, 40, 41, 44, 50, 51, 54, 56, 57, 61, 62, 63, 71, 72, 75, 79, 81, 82, 88, 89, 90]	[9, 28, 33, 40, 49, 50, 51, 54, 56, 57, 61, 62, 63, 71, 81, 82, 89, 90]	[17, 54, 62, 64]	[28, 63, 77, 80, 82, 84]	[17, 54, 62]

modelling framework which can be used at multiple scales and tailored to different purposes.

7.2. Findings

7.2.1. Finding I: actionable intelligence

In a dynamic threat landscape, modelling the behaviour of a threat actors using TTP's is a limited approach. In a study [41] Xiong, Zhu et al. concluded that a multiphase model can be used only to better understand APTs, not to detect them. There was no research that could effectively map TTP's to data, configurations, and other controls. Using attacker TTP's in identification and detection mechanisms is a challenge, as legitimate behaviours can be identified as malicious.

Noor et al's research attempted to solve this attribution, however, several questions regarding the collection and integrity of the CTI data need to be addressed, as data can be fabricated or outdated, causing incorrect attribution. This research did not address the question of how effective attribution can be achieved if an Indicator of Compromise (IoC) can be mimicked or impersonated by another attacker. Adding to this challenge is that there are also few datasets available for the evaluation of multi-step attack detection systems [50].

Abubakara et al. [94] reviewed the advances made in the cyber security benchmark datasets for the evaluation of machine learning and data mining-based intrusion detection systems. The review indicated that previous datasets, on which researchers relied heavily, have lost their relevance because of the significant changes in computer technology. The lack of actionable intelligence matching the requirements of CTI consumers is also confirmed in other studies [50, 71]. There is a need to be able to impartially and dynamically provide a quantitative means to rank the reputation of CTI sources.

7.2.2. Finding II: data processing and usage

The amount of data collected and used is tending to be larger as storage has become increasing cheaper over the period of studies researched. The ability to analyse large amounts of disparate datasets has given the ability to conduct behaviour analysis [95]. However, the ability to gain access to these historical and real-time datasets have limited some studies.

An example of using limited data is a study [33] of a system that applied causal reasoning to predict enterprise-related external cyber threats. The model tried to match the CPE/nation-state actor mappings to a rule. If a match existed, the model predicted when an attack exploiting the vulnerabilities would occur (metadata/details including the CVEs/-tactics, industry, volume of discussions, probability, type and target). The breadth and depth of data is limited in this research as the types of insider attacks were limited to an email, destination IP or the existence of Malware.

Another example of limited data was explicitly stated by Al-Shaer et al. in their study. Al-Shaer identified that collecting a larger dataset of real-life attacks was needed in order to increase the quantity and quality of attack chaining technique associations [75].

The ability to not only store large amounts of data, but to process it has given rise to more studies involving Machine Learning (ML). Prediction of numeric values and classifying objects based on their attributes or behaviour, requires training a machine with sets of data. Ognawala et al. [35] presented a data mining and machine learning based technique for correlating features of vulnerable components discovered by compositional analysis to predict CVSS3 base-score values. The research provided a high-level overview of the implemented methods, including data collection, compositional analysis, initial feature extraction, and interactive feedback from an analyst to assist learning. This research concluded that the random-forest classifier was the most efficient machine learning approach, and how the use of feedback from analysts assisted with refining the feature selections used. The researchers only consider a very limited dataset buffer-overflows, which limited their study.

7.2.3. Finding III: use case usage

Various scenarios or use cases were identified in 16 research papers. They include potential and realised behavioural (user, attacker and system) threats that identify and explore security vulnerabilities. Our review identified that to determine how thorough, adaptable and customisable an approach is, multiple use cases should be applied to each threat model. Additionally, multiple threat models should also be applied to a single use case. Farooq et al. [89] used ATT&CK Technique use cases to evaluate Machine learning (ML) approaches (Table 10).

APT use cases were used to evaluate the differences, strengths and limitation between the ML approaches. To the best of our knowledge, there was no study that compared many use cases to many TM to identify which were applicable to either.

7.2.4. Finding IV: combined models

A combination of threat models can leverage of each other's strengths to minimise weaknesses. Most papers re-enforced the view that combining models specific to security requirements is the best approach. Data flow diagrams was the most popular model used when reviewing or proposing a combination of TM's. Bland et al. [81] investigates the potential of extensions to existing cyber-attack modelling methods. It proposes using CAPEC as input and having attack patterns modelled as an extension of Petri nets. This extension then applies a reinforcement machine learning (ML) algorithm for predictive analysis.

Campbell et al. [90] and Bodeau [54] approach were to combine the categories established by CAPEC with MITRE's ATT&CK threat information. Campbell et al. [90] then evaluates two ML approaches (Support

Table 10. Machine learning applied to ATT&CK Techniques.

ATT&CK Technique	Use Case	Evaluated Algorithms	Most Effective Algorithm
Initial Access	Message Classification	Random Forest Classifier	Random Forest Classifier
Executions	Anomalous Process Executions	- One-Class SVM (OCSVM) Classifier - Gaussian Kernel - Linear Kernel - Polynomial Kernel - Radial Kernel	OCSVM Classifier Linear Kernel
Discovery	Predicting User's Processes	- Linear Regression - Decision Tree Regression - Random Forest Regression	Linear Regression
Ex-Filtration	Data Rate Analytic	- K-Means Clustering - Density-Based Spatial Clustering (DBSCAN) - Balanced Iterative Reducing and Clustering using Hierarchical (BIRCH)	K-Means Clustering
Exploitation	Parent Child Process' Analytic	- Logistic Regression - Decision Trees - Naive Bayes - Decision Tree classifiers	Logistic Regression

Vector Machine and Neural Network) to classifying an open source dataset, to these combined categories. This study has identified several ML and threat modelling approaches that could be considered in future research.

In another study a unified version of the Lockheed Martin's kill chain was developed that extended the original cyber kill chain [88]. It achieved this by combining and extending the kill chain with MITRE's ATT&CK framework. This "unified kill chain" identifies 18 attack phases that can be present in the process of compromising a target. It involved an ordered arrangement of activities that could possibly occur either outside and/or within a defended network. As a result, the unified kill chain addressed the limitations of the original kill chain and the uncertainty of the nature of time in relation to MITRE's ATT&CK TTP's and their associated permutations.

7.2.5. Finding V: different audience levels of models

Threats, vulnerabilities and associated controls stored in an accessible and understandable format, can extend the limited capability of security knowledge resources within an organisation. It can reduce the language barriers between professionals with a wide range of business and technical knowledge. Our review has found that there is a need for threat models to be targeted and specific audience levels. A taxonomy-based model is essential in empowering various levels of business to have a clear understanding of relevant threats. This was identified in Bodeau 's study and we agree with this type of approach. It complements the strategic, Tactical, operational and technical aspects of threat intelligence. We have identified three potential models that could solve this need. The first is a contextual threat model that identifies specific threats specific to the current individual systems technical environment, to enable internal local risk assessment, gap analysis, treatment, detection, response and recovery aspects [54].

Once an organisation's maturity increases, the second generic threat model can add value. This model details generic techniques and attack patterns, that provides threat modelling for operational and tactical purposes. This includes multiple system interactions within the IT infrastructure.

The final approach is a high-level TM that identifies generic threats, goals capabilities and behaviour from a strategic point of view. This approach identifies enterprise risk and a sector specific threat landscape and further extends Bodeau's approach [54].

7.2.6. Finding VI: APT modelling

Modelling APT's were discussed in 23 research papers that were reviewed. The approaches discussed to model an APT multi-step attack included attack trees, NIST 800-154, CAPEC, MITRE's TARA, and Cyber Kill Chain. One study believes that APT's receive no benefits by going back to previous stages, as they have a specific target at the final stage [85]. This can be challenged that if one avenue of attack is thwarted by a control then resorting to a previous phase to circumvent this obstacle is in their best interest. Being aware of different permutations to a target is required to enable a defender to successfully defend. Navarro recommends conducting studies on the links between the steps that exist in multi-step attacks, so that this can be accounted for [29].

ATT&CKv8 provides a list of adversary groups (Intrusion-set), 64 software tools and over 458 malware families used within its structure. The initial release of ATT&CKv8 identified 108 different adversaries, having nearly 250 combined alias'. The intrusion set provides references and descriptions of known APT groups that have been collated by MITRE from various CTI providers and security communities [43]. For a threat modelling system to be suited to an APT, our study found that it needs to identify and document TTP's, targets (data etc.) by using actionable intelligence relevant to the target environment.

There was one significant paper that proposed a "unified model" (ATT&CK/Killchain) that could analyse, compare and defend against end-to-end cyber-attacks by advanced persistent threats (APTs) [88]. This approach may be further researched to identify the feasibility to automate the model extend it with machine learning.

7.2.7. Finding VII: threat model automation using a taxonomy

The ability to correlate threats to events is a rapidly evolving science. The ability to ingest threat intelligence automatically is assisted by standards such as STIX. The process of collating disparate sources of data has also been assisted by SIEMs.

Our review has found that with the current tools available, threat modelling requires some manual process. Martins, et al. concluded that no publicly available tools (or techniques) exist that automatically perform a systematic analysis of security threats in Cyber Physical Systems [16]. However, our research also identified that automation can be implemented at different stages of the TM process. TM approaches that are more formal have the potential attributes required to automated threat modelling (Figure 8). We found that to semi-automate TM, a system needs to have the ability to gather actionable intelligence, correlate this data with a taxonomy (TTP's) and apply it to the context of an organisation's environment.

Shevchenko et al. [19] identifies both STRIDE and CVSS as being able to be automated. However, other studies identify that STRIDE does not provide specific details of attack vectors or patterns, it only categorises general types of attack actions that may need to be investigated further [54, 63].

Our study also found novel ways to simulate attacks and determine controls using automation. Bland et al. identifies a system that simulates an attack. It achieves this by semi-automatically converting the vulnerabilities stored in a CAPEC repository, into Attack Trees, that is, one per vulnerability [81]. This study also discusses a tool that retrieves attack patterns from the CAPEC based on its relevance to STRIDE. Salter [30] produced a methodology for enumerating the vulnerabilities of a system, to determine countermeasures or controls for mitigation and remediation. The project classified adversaries in terms of their capabilities and the targets accessibility. It correlated the attacker's characteristics (resources and objectives) with the assets vulnerability characteristics to determine if an actual threat existed. Although this project was novel approach, it not been considered due to its age.

Modelling current and future APT attacks requires the ability to identify and correlate attack techniques that may follow a chain of linked paths or events. Al-Shaer et al. proposes an approach that identifies the attack TTP interdependencies and relationships, using hierarchical clustering [75]. Our study identified that Markov Chains can then use the fine and coarse grain associations to forecast likely attack path permutations. A Markov Chain moves through a series of transitions between adjacent states where the next state of the system depends entirely on the current state. Based on this approach and the cyber threat descriptions within STIX, researchers have identified an effective approach to generate possible cyber threat trajectories that follow attack paths [39].

A similar approach to predict attacks within a risk management system is also proposed by Polatidis [96]. It also builds attack graphs using all identified attack paths. It uses attack graph analysis combined with a recommendation system to predict possible future attack steps. A future enhancement proposed in their study, was to evaluate the use of Machine Learning classification algorithms such as Naïve Bayes and random forests.

7.2.8. FINDING VIII: machine learning

Our study found several Machine Learning (ML) techniques being applied to categorise and predict threats [50, 71, 75, 89, 97]. We also found that to effectively apply Machine Learning to threat models requires some level of automation and portability. Noor et al. have had two papers reviewed that use Machine Learning and TTP's. Both present a machine learning framework based on an attackers Tactics, Techniques and Procedures (TTP). The first paper [71] presents a ML framework that determines threat occurrences by determining a probable relationship

between threats and TTPs. The second paper [50] presents an additional ML framework that attributes cyber threats to an entity using TTP's.

Farooq et al. [89] has also analysed, modelled and evaluated 11 different machine learning approaches against 4, ATT&CK Technique use cases (Table 10) lists the Evaluated algorithms and the most effective algorithm identified. A combination of threat model could be investigated and evaluated in the study to leverage of each other's strengths and minimise their weaknesses.

8. Future work and APT threat modelling research directions

Possible future research may be to identify the most effective approach to contextualise current and new attack vectors by using machine learning in a cyclical process to understand the threat, its intent, capability, doctrine, and patterns of operation.

Our study found that some level of automation and portability is required to effectively apply Machine Learning to threat models. An approach could use a Quadrant style approach to map TM quadrants (Figure 8) to ML quadrants. To be able to manage risk and predict relevant threats a system requires data on assets, their vulnerabilities and how accessible they are to threats. It also requires visibility of the threat actor's tactics, techniques and procedures, as well as their motivation, intent, knowledge, tools and resources available to them.

To predict possible future threats requires an effective process that consumes historical and current data, on threats, attack vectors and vulnerabilities, combined with the current data on organisations assets. A potential researched system could attempt to predict unknown threats by using an effective machine learning model. This would require a cyclical automated process to predict the threat, its intent, capability, doctrine and vector.

Future work may be to research and review the most effective approach to extract data from structured threat repositories. This framework may then be able to identify the supporting assets and their relevant threats, vulnerabilities and potential exploits. It could also be able to analyse the data and model collectively and identify existing known/unknown threats, and the resulting likelihood of a compromise.

To effectively implement this proposed framework, future research would need to compare machine learning algorithms and identify the best combined Machine Learning Algorithms for all tasks of the proposed framework. The risks identified from vulnerabilities, threat intelligence and models, could then be part of a feedback loop, providing itself with training data. The iterative system could possibly analyse and put into context asset/threat/vulnerability data and attempt to make point-in-time predictions on known, unknown and emerging threats. Keeping in mind that new threats, vulnerabilities, applying controls or changes in likelihood or consequences would need to be constantly reviewed.

The approaches that are more formal and automated (Figure 8) have the attributes required to construct a taxonomy of Threat Entities (ToTE). This ToTE could then be used to train a ML approach that can model current threats, categorise and predict future threats. Future tasks could be to identify novel threat model approach using a taxonomy that ensures a comprehensive coverage and mapping of data and feature sets that will be available to train the ML algorithms [101].

9. Conclusion

This literature review has identified the broad and disparate threat model methodology and approaches in the research community. They all provide different strengths and limitations as they have been tailored for individual purposes. The approaches are specific to each level of an organisation, its associated project and requirements. At the software development and operations level system-centric and data-centric are more relevant. We found that attacker and asset-centric approaches can be used to model both technical and non-technical threats and that they are able to provide explicit information that can be used for assessing risk.

We identified that the complexity of current systems requires a hybrid approach to threat modelling. Understanding the attackers, their motivation and skillsets will identify threat relevance. Visibility of these threats to all stakeholders, assists in identifying all threat vectors at all stages and levels.

There is no threat modelling approach that can be used across all permutations of vulnerabilities, asset, threats, system and data. The strengths and limitations we have identified can be used to determine a TM approach, specific to the audience, maturity level and current technical environment. Our review has found that there is a need for threat models to be targeted and specific audience levels. To complete our study the following features can assist in determining which approach should be taken.

1. Use correlated and actionable threat intelligence from multiple internal and external sources.
2. Identify organisational specific threat agents, their motives and capability.
3. Identify critical assets and controls.
4. Find all relevant threats whose likelihood and business impact level are above the organisation's risk appetite.
5. Include as many stakeholders as possible from all areas and levels of an organization.
6. Identify boundaries of environments within the scope of the system.
7. Identify Authentication and authorisation aspects.
8. Choose a consistent approach and methodology that best fits requirements, maturity level, audience and environment.

This review has discussed findings from reviewing 49 current studies and has provided insights into threat models and their strengths and limitations. A consensus of the papers review identified that the current threat modelling approaches remains a manual process, with automation assisting at different stages. There was no individual approach that could model threats based on strategic, tactical, operational and technical intelligence, specific to an organisation's environment.

There is a need to combine existing frameworks, to enable an organisation to have the required visibility to ensure adequate risk management. Having reviewed all these studies, we have identified three potential hybrid approaches that could solve the identified limitations. They are:

1) Contextual threat model based on the technology suite of the organisation
2) Operational and tactical model, based on generic techniques and attack patterns
3) Based on the organisations risk threshold, a strategic threat Model, that models' generic threats, goals, capabilities and behaviour, and assesses it against the current sector specific threat landscape.

Studies were also identified that used machine learning as a viable approach to address TM deficiencies. There were several automated approach's that were able to gather actionable intelligence and correlate it with a taxonomy (TTP's etc.) in an automated setting. However, it did not have ability to apply the model within the context of an organisation's environment. Machine learning is one future direction to developing an automated, effective and efficient TM approach. However, the data and features required to train an effective ML approach needs to be actionable threat intelligence in the context of current technical environment.

Declarations

Author contribution statement

All authors listed have significantly contributed to the development and the writing of this article.

Funding statement

This work was supported by the Australian Government Research Training Program Scholarship and Charles Darwin University has also funded the Article Publication Charges by Open Access Support for Increased Citations (OASIC) scheme.

Data availability statement

No data was used for the research described in the article.

Declaration of interests statement

The authors declare no conflict of interest.

Additional information

No additional information is available for this paper.

References

[1] J. Hughes, Quantitative Metrics and Risk Assessment: the Three Tenets Model of Cybersecurity, Technology Innovation Management Review, 2013.
[2] NIST, Glossary: threat [Online]. Available: https://csrc.nist.gov/glossary/term/threat [Accessed 1 2020].
[3] K. Pendergrass, Toward environmentally sustainable digital preservation, Am. Archivist 82 (2019) 165–206.
[4] R. Dahbul, Enhancing honeypot deception capability through network service fingerprinting, IOP Conf. Series: J. Phys. Conf. Series 801 (2017), 012057.
[5] B. Strom, Finding Cyber Threats with ATT&CK™-Based Analytics, June 2017 [Online]. Available: https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyber-threats%20with%20att%26ck-based-analytics.pdf [Accessed 11 Oct 2020].
[6] A. Aleroud, Contextual Information Fusion for Intrusion Detection: a Survey and Taxonomy, 17 Feb 2017 [Online]. Available: https://link.springer.com/article/10.1007/s10115-017-1027-3 [Accessed 2020].
[7] F. Honkus, A Need for Tactics, Techniques, and Procedures (TTP), 2015 [Online]. Available: http://sites.nationalacademies.org/cs/groups/depssite/documents/webpage/deps_169626.pdf [Accessed 2020].
[8] M.A.H. Shahi, Tactics, Techniques and Procedures (TTPs) to Augment Cyber Threat Intelligence (CTI): A Comprehensive Study, 2018. Culminating Projects in Information Assurance, no. 54.
[9] P. Delgado, Developing an Adaptive Threat Hunting Solution: the Elasticsearch Stack, University of Houston, Houston, 2018.
[10] D. Bianco, Pyramid of Pain, Mar 2013 [Online]. Available: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html.
[11] Microsoft Defender ATP Research Team, From Unstructured Data to Actionable Intelligence: Using Machine Learning for Threat Intelligence, 8 Aug 2019 [Online]. Available: https://www.microsoft.com/security/blog/2019/08/08/from-unstructured-data-to-actionable-intelligence-using-machine-learning-for-threat-intelligence/ [Accessed 2020].
[12] L. Gundert, A practical guide to identifying TTPs with threat intelligence [Online]. Available: https://go.recordedfuture.com/hubfs/white-papers/identifying-ttps.pdf [Accessed 2020].
[13] Charles Darwin University, Search - A-Z Databases, 2019 [Online]. Available: http://libguides.cdu.edu.au/az.php.
[14] K.A. Hallgren, Computing inter-rater reliability for observational data: an overview and tutorial, Tutorials in quantitative methods for psychology 8 (1) (2012) 23–34.
[15] ENISA, European Union Agency for Network and Information Security - Threat Landscape Report 2018, European Union Agency for Network and Information Security (ENISA), 2019.
[16] G. Martins, S. Bhatia, X. Koutsoukos, K. Stouffer, C. Tang, R. Candell, Technical report: towards a systematic threat modeling approach for cyber-physical systems, in: Proc 2015 Resil Week RSW, 2015.
[17] M. Souppaya, Draft NIST Special Publication 800-154 - Guide to Data-Centric System Threat Modeling, 14 Mar 2016 [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-154/draft [Accessed 2020].
[18] D. Xu, Automated security test generation with formal threat models, IEEE Trans. Dependable Secure Comput. 9 (4) (2012) 526–540.
[19] N. Shevchenko, Threat Modeling for Cyber-Physical System-Of-Systems: Methods Evaluation, Carnegie Mellon University, 2018.
[20] J. Belur, Interrater Reliability in Systematic Review Methodology: Exploring Variation in Coder Decision-Making, 24 Sept 2018 [Online]. Available: [Accessed 21 Oct 2020].
[21] ScienceDirect, Interrater reliability, ScienceDirect, [Online]. Available: https://www.sciencedirect.com/topics/nursing-and-health-professions/interrater-reliability. (Accessed 21 October 2020).
[22] NIST, National Vulnerability Database (NVD), May 2020 [Online]. Available: https://nvd.nist.gov/.
[23] Exploit Database, May 2020 [Online]. Available: www.exploit-db.com/.
[24] Rapid7, Vulnerability & Exploit Database, May 2020 [Online]. Available: www.rapid7.com/db/.
[25] NIST, National Vulneability Database - Vulnerability Metrics, July 2019 [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss.
[26] K. Heckman, Active cyber defense with denial and deception: a cyber-wargame experiment, Comput. Secur. 37 (2012) 72–77.
[27] W. Xiong, R. Lagerström, "Threat modeling – a systematic literature review, Comput. Secur. 84 (2019) 53–69.
[28] S. Launius, Evaluation of Comprehensive Taxonomies for Information Technology Threats, SANS Institute Information Security Reading Room, 2018.
[29] J. Navarro, A systematic survey on multi-step attack, Comput. Secur. 76 (2018) 214–249.
[30] C. Salter, Toward a secure system engineering methodology, in: New Security Paradigms Workshop, 1998, pp. 2–10.
[31] B. Schneier, Attack Trees - Dr. Dobb's Journal, December 1999, Dec 1999 [Online]. Available: https://www.schneier.com/academic/archives/1999/12/attack_trees.html.
[32] S. Haque, An evolutionary approach of attack graph to attack tree conversion, Int. J. Comput. Network Inf. Secur. 11 (2017) 1–16.
[33] M. Almukaynizi, E. MArin, E. Nunes, P. Shakarian, G.I. Simari, D. Kapoor, T. Siedlecki, DARKMENTION_A Deployed System to Predict Enterprise-Targeted External Cyberattacks, 30 Oct 2018, pp. 1–6, eprint arXiv:1810.12492.
[34] L.A.B. Sanguino, Software Vulnerability Analysis Using CPE and CVE, 15 May 2017 [Online]. Available: https://www.groundai.com/project/software-vulnerability-analysis-using-cpe-and-cve.
[35] S. Ognawala, Automatically Assessing Vulnerabilities Discovered by Compositional Analysis, Sep 2018 [Online]. Available: https://www.researchgate.net/publication/326586522_Automatically_Assessing_Vulnerabilities_Discovered_by_Compositional_Analysis.
[36] M. Jouini, Classifications of security threats in information systems, Procedia Comput. Sci. (32) (2014) 489–496.
[37] B. Felter, C. Harpes, G. Schaff, M. Martins, B. Kordy, R. Trujillo, D. Ionita, TREsPASS - Currently Established Risk-Assessment Methods - Technology-Supported Risk Estimation by Predictive Assessment of Socio-Technical Security, EU Consortium, 2014.
[38] J. Meszaros, A. Buchalcevova, Introducing OSSF: a framework for online service cybersecurity risk management, Comput. Secur. 65 (2017) 300–313.
[39] R. Gore, Markov chain modeling of cyber threats, J. Defense Model. Simulat. Appl. Methodol. Technol. 14 (3) (2017) 233–243.
[40] S. Milajerdi, HOLMES: real-time APT detection through correlation of suspicious information flows, in: IEEE Symposium on Security and Privacy, 2019, pp. 1137–1152.
[41] C. Xiong, CONAN: A practical real-time APT detection system with high accuracy and efficiency, IEEE Trans. Dependable Secure Comput. (2020).
[42] Lockheed Martin, Gaining the advantage: Applying Cyber Kill Chain® Methodology to Network Defense, 2015 [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf.
[43] MITRE.org, MITRE.org, MITRE.org, 2020 [Online]. Available: https://MITRE.org.
[44] C. Pace, The Threat Intelligence Handbook, CyberEdge Group, LLC, Annapolis,MD, 2018.
[45] R. Trifonov, Artificial neural network intelligent method for prediction, in: Mathematical Methods and Computational Techniques in Science and Engineering, 2017.
[46] T. Osako, Proactive Defense model based on Cyber threat analysis, FUJITSU Sci. Tech. J. 52 (3) (Jul 2016) 72–77.
[47] S. Samtani, R. Chinn, H. Chen, J.F. Nunamaker, Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence, J. Manag. Inf. Syst. 34 (2017) 1023–1053.
[48] T.N. Brooks, Survey of Automated Vulnerability Detection and Exploit Generation Techniques in Cyber Reasoning Systems, Computer Science Department, Seidenberg School of Computer Science and Information Systems, Pace University, New York, 2017.
[49] OASIS, Introduction to STIX, Aug 2019 [Online]. Available: https://oasis-open.github.io/cti-documentation/stix/intro.
[50] U. Noor, A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise, Future Generat. Comput. Syst. 96 (2019) 227–242.
[51] MITRE, CAPEC - Common Attack Pattern Enumeration and Classification, MITRE.org, 2017. Version 2.11.
[52] A. Ledeczi, The generic modeling environment, in: IEEE International Symposium on Intelligence Signal Processing, 2001.
[53] MISP Community, Malware Information Sharing Platform and Threat Sharing, Aug 2019 [Online]. Available: https://www.misp-project.org.
[54] D. Bodeau, Cyber Threat Modeling: Survey, Assessment, and Representative Framework, The Homeland Security Systems Engineering and Development Institute (HSSEDI), 2018.
[55] D. Eng, Integrated Threat Modelling, UNIVERSITY OF OSLO, Oslo, 2017.
[56] MITRE.org, ATT&CK Matrix, 2019 [Online]. Available: https://attack.mitre.org/matrices/enterprise/.
[57] MITRE, CAPEC VIEW: Mechanisms of Attack, 30 Sept 2019 [Online]. Available: https://capec.mitre.org/data/definitions/1000.html.
[58] L. Sion, Solution-aware data flow diagrams for security threat modeling, in: Symposium on Applied Computing, Pau, France, 2018.

[59] A. Shostack, Threat Modeling: Designing for Security, John Wiley & Sons, Inc., 2014.
[60] C.Y. Cheung, Threat Modeling Techniques - Program: MSc Systems Engineering, Policy Analysis and Management, Delft University of Technology, the Netherlands, 2016.
[61] OWASP, Testing Guide 4.0 - Open Web Application Security Project, OWASP, 2015.
[62] D. Bodeau, System-of-System Threat Model, The Homeland Security Systems Engineering and Development Institute (HSSEDI), McLean VA 22102, 2018.
[63] B.E. Strom, A. Applebaum, P.D. Miller, K.C. Nickels, A.G. Pennington, C.B. Thomas, MITRE ATT&CK™: Design and Philosophy, July 2018 [Online]. Available: https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf.
[64] M. Kamal, ICS Layered Threat Modeling, 1 Jan 2019 [Online]. Available: https://www.sans.org/reading-room/whitepapers/ICS/paper/38770.
[65] S. Krishnan, A Hybrid Approach to Threat Modelling, 2017.
[66] V. Saini, V. Paruchuri, Q. Duan, Threat Modeling using attack trees, J. Comput. Sci. Coll. 23 (4) (2008) 124–131.
[67] AMLC Team at UniMelb, Data61, Swinburne Univ., T. Abraham, O. de Vel, P. Montague, Adversarial Machine Learning for Cyber-Security: NGTF Project Scoping Study, Cyber and Electronic Warfare Division, Edinburgh, South Australia, 2018.
[68] R. Trifonov, Artificial intelligence methods for cyber threats intelligence, Int. J. Comput. 2 (2017) 129–135.
[69] Microsoft Corporation, Microsoft Advanced Threat Analytics, Jan 2018 [Online]. Available: https://www.microsoft.com/en-us/cloud-platform/advanced-threat-analytics.
[70] E. Hutchins, Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, 2019 [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.
[71] U. Noor, A machine learning framework for investigating data breaches based on semantic analysis of adversary's attack patterns in threat intelligence repositories, Future Generat. Comput. Syst. 95 (2019) 467–487.
[72] MITRE Corporation, MITRE ATT&CK Enterprise Framework, 2020 [Online]. Available: https://attack.mitre.org/docs/attack_matrix_poster_2020.pdf.
[73] MITRE Corporation, Mobile Matrices, 24 Oct 2019 [Online]. Available: https://attack.mitre.org/matrices/mobile/.
[74] MITRE Corporation, PRE-ATT&CK Matrix, 18 Apr 2018 [Online]. Available: https://attack.mitre.org/matrices/pre/.
[75] R. Al-Shaer, Learning the Associations of MITRE ATT&CK Adversarial Techniques, 12 May 2020 [Online]. Available: https://arxiv.org/abs/2005.01654. (Accessed 19 October 2020).
[76] J.E. Wynn, Presentation-threat assessment & remediation analysis (TARA) methodology overview, Oct 2013 [Online]. Available: https://www.mitre.org/publications/technical-papers/presentation-threat-assessment-remediation-analysis-tara-methodology.
[77] C. Carreon, Recorded Future, 25 July 2018 [Online]. Available: https://www.recordedfuture.com/diamond-model-intrusion-analysis/.
[78] Applying Threat Intelligence to the Diamond Model of Intrusion Analysis, 25 Jul 2018 [Online]. Available: https://www.recordedfuture.com/diamond-model-intrusion-analysis/. (Accessed 15 January 2021).
[79] A. Piazza, ATT&CKing Threat Management: A Structured Methodology for Cyber Threat, SANS Institute, 2019.
[80] S. Caltagirone, Diamond Model of Intrusion Analysis, in Huntpedia, Vienna, VA, 2017, pp. 24–27.
[81] J.A. Bland, Machine Learning of Cyber Attack and Defense Strategies, ProQuest LLC, Ann Arbor, MI, 2019.
[82] W. Tounsi, What is Cyber Threat Intelligence and how is it evolving?, in: Cyber-Vigilance and Digital Trust Wiley-ISTE, 2019.
[83] D. Kiwia, A cyber kill chain based taxonomy of banking Trojans for evolutionarycomputational intelligence, J. Comput. Sci. 27 (2018) 394–409.
[84] B. Stojanovi, APT datasets and attack modeling for automated detection methods: a review, Comput. Secur. 92 (2020) 101734. Elsevier Ltd.
[85] L. Huang, Adaptive strategic cyber defense for advanced persistent threats in critical infrastructure networks, Perform. Eval. Rev. 46 (2) (2018) 52–56.
[86] Y. Mishina, A method of threat analysis for cyber-physical system using vulnerability databases, IEEE 978-1-5386-3443-1 (2018).
[87] L. Huang, Q. Zhu, Adaptive Strategic Cyber Defense for Advanced Persistent Threats in Critical Infrastructure Networks, Sept 2018 [Online]. Available: https://dl.acm.org/citation.cfm?id=3305239.
[88] P. Pols, The Unified Kill Chain, 7 Dec 2017 [Online]. Available: https://www.csacademy.nl/images/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf.
[89] H.M. Farooq, N.M. Otaibi, Optimal machine learning algorithms for cyber threat detection, in: UKSim-AMSS 20th International Conference on Modelling & Simulation, 2018.
[90] R.K. Campbell, Cyber Incident Anomaly Detection Using Multivariate Analysis and Machine Learning, ProQuest LLC, Ann Arbor, MI, 2018.
[91] J. Tarala, Open Threat Taxonomy v1.1, Oct 2015 [Online]. Available: http://www.auditscripts.com/resources/open_threat_taxonomy_v1.1a.pdf [Accessed 2020].
[92] MITRE Corporation, MITRE Cyber Analytics Repository, MITRE Corporation, 2020 [Online]. Available: https://car.mitre.org/. (Accessed 11 October 2020).
[93] J. Ferdinand, The Cyber Security Ecosystem: Defining a Taxonomy of Existing, Emerging and Future Cyber Threats, 2 Oct 2017 [Online]. Available: https://ssrn.com/abstract=3047753.
[94] A.I. Abubakara, A review of the advances in cyber security benchmark datasets for evaluating data-driven based intrusion detection systems, in: The 2015 International Conference on Soft Computing and Software Engineering, 2015.
[95] D. Westcott, K. Bandla, APT Notes, Apr 2020 [Online]. Available: https://github.com/aptnotes.
[96] N. Polatidis, From Product Recommendation to Cyber-Attack Prediction: Generating Attack Graphs and Predicting Future Attacks, 22 May 2018 [Online]. Available: https://link.springer.com/content/pdf/10.1007/s12530-018-9234-z.pdf.
[97] D. Liu, Understanding and detecting newly emerging, 2018 [Online]. Available: https://www.semanticscholar.org/paper/Understanding-and-detecting-newly-emerging-attack-Liu/f19bd9ced6f791cc9f5a73abe0dcf39cb4484c2f.
[98] The Open Group - O-ISM3, Information Security Management Using O-ISM3, The Open Group, 2019 [Online]. Available: https://www.ism3.com/node/42 [Accessed July 2019].
[99] T. Madsen, Sun Tzu's 'The Art of War' for Cybersecurity," Infosecurity-Magazine, 2017 May 2017 [Online]. Available: https://www.infosecurity-magazine.com/opinions/sun-tzus-art-of-war-cybersecurity/ [Accessed July 2019].
[100] A. Shoufan, On inter-Rater reliability of information security experts, J. Inf. Secur. Appl. 37 (2017) 101–111.
[101] W. Kool, ATTENTION, learn to solve routing problems!, ICLR (2019).